MALICIOUS

Classifications: Spyware | Downloader | Injector | Exploit

Threat Names: RedLine | RedLine.A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Word Document**
File Name	**Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc**
ID	#10708709
MD5	9edc82805ecc2d30f07d99973883c3c6
SHA1	877fae637a454593a1b66bfede20356803833266
SHA256	927e8668d7e5b22d0d278cb66ecbb15a51420f2fc5299aaa324d43a7d04719a2
File Size	16.04 KB
Report Created	2024-06-24 16:43 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | ms_office

OVERVIEW

VMRay Threat Identifiers (37 rules, 152 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	RedLine configuration was extracted	1	Spyware
	• A configuration for RedLine was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
	• YARA detected "RedLine_SOAPCommunication" from ruleset "Malware" in web response data from "hxxp://185[.]38[.]142[.]10:7474". • YARA detected "RedLine_A" from ruleset "Malware" in memory dump data from (process #6) notorious53209.exe. • YARA detected "RedLine_A" from ruleset "Malware" in memory dump data from (process #7) regsvcs.exe.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, collects hardware information, queries network configuration and collects operating system information which indicates system fingerprinting.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #7) regsvcs.exe takes screenshots and potentially exfiltrates data.			
4/5	Obfuscation	Reads from memory of another process	75	-

- (Process #6) notorious53209.exe reads from (process #7) regsvcs.exe.
- (Process #9) wmiprvse.exe reads from dwm.exe.
- (Process #9) wmiprvse.exe reads from taskhost.exe.
- (Process #9) wmiprvse.exe reads from explorer.exe.
- (Process #9) wmiprvse.exe reads from iexplore.exe.
- (Process #9) wmiprvse.exe reads from daughter-kill.exe.
- (Process #9) wmiprvse.exe reads from look.exe.
- (Process #9) wmiprvse.exe reads from notsense.exe.
- (Process #9) wmiprvse.exe reads from class_seek_finish.exe.
- (Process #9) wmiprvse.exe reads from american here interview.exe.
- (Process #9) wmiprvse.exe reads from nearly.exe.
- (Process #9) wmiprvse.exe reads from activity_top_a.exe.
- (Process #9) wmiprvse.exe reads from institution.exe.
- (Process #9) wmiprvse.exe reads from attack.exe.
- (Process #9) wmiprvse.exe reads from studentreceivesee.exe.
- (Process #9) wmiprvse.exe reads from armlose.exe.
- (Process #9) wmiprvse.exe reads from body late.exe.
- (Process #9) wmiprvse.exe reads from get.exe.
- (Process #9) wmiprvse.exe reads from however tax.exe.
- (Process #9) wmiprvse.exe reads from physical shoulder.exe.
- (Process #9) wmiprvse.exe reads from material.exe.
- (Process #9) wmiprvse.exe reads from little.exe.
- (Process #9) wmiprvse.exe reads from of_almost_create.exe.
- (Process #9) wmiprvse.exe reads from perthey.exe.
- (Process #9) wmiprvse.exe reads from ccv_server.exe.
- (Process #9) wmiprvse.exe reads from creditservice.exe.
- (Process #9) wmiprvse.exe reads from alftp.exe.
- (Process #9) wmiprvse.exe reads from afr38.exe.
- (Process #9) wmiprvse.exe reads from centralcreditcard.exe.
- (Process #9) wmiprvse.exe reads from edcsvr.exe.
- (Process #9) wmiprvse.exe reads from fpos.exe.
- (Process #9) wmiprvse.exe reads from isspos.exe.
- (Process #9) wmiprvse.exe reads from mxslipstream.exe.
- (Process #9) wmiprvse.exe reads from omnipos.exe.
- (Process #9) wmiprvse.exe reads from spcwin.exe.
- (Process #9) wmiprvse.exe reads from spgagentservice.exe.
- (Process #9) wmiprvse.exe reads from utg2.exe.
- (Process #9) wmiprvse.exe reads from my probably class.exe.
- (Process #9) wmiprvse.exe reads from check_management.exe.
- (Process #9) wmiprvse.exe reads from legalvotefinancial.exe.
- (Process #9) wmiprvse.exe reads from catch_west.exe.
- (Process #9) wmiprvse.exe reads from 3dftp.exe.
- (Process #9) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #9) wmiprvse.exe reads from barca.exe.
- (Process #9) wmiprvse.exe reads from bitkinex.exe.
- (Process #9) wmiprvse.exe reads from coreftp.exe.
- (Process #9) wmiprvse.exe reads from far.exe.
- (Process #9) wmiprvse.exe reads from filezilla.exe.
- (Process #9) wmiprvse.exe reads from flashfxp.exe.
- (Process #9) wmiprvse.exe reads from fling.exe.
- (Process #9) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #9) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #9) wmiprvse.exe reads from icq.exe.
- (Process #9) wmiprvse.exe reads from leechftp.exe.
- (Process #9) wmiprvse.exe reads from ncftp.exe.
- (Process #9) wmiprvse.exe reads from notepad.exe.
- (Process #9) wmiprvse.exe reads from operamail.exe.
- (Process #9) wmiprvse.exe reads from outlook.exe.
- (Process #9) wmiprvse.exe reads from pidgin.exe.
- (Process #9) wmiprvse.exe reads from scriptftp.exe.

Score	Category	Operation	Count	Classification
4/5	Discovery	Collects hardware properties	3	-
	• (Process #7) regsvcs.exe queries hardware properties via WMI: SELECT * FROM Win32_VideoController. • (Process #7) regsvcs.exe queries hardware properties via WMI: SELECT * FROM Win32_DiskDrive. • (Process #7) regsvcs.exe queries hardware properties via WMI: SELECT * FROM Win32_Processor.			
4/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #7) regsvcs.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntivirusProduct".			
4/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #7) regsvcs.exe tries to detect anti-spyware software via WMI query: "SELECT * FROM AntiSpyWareProduct".			
4/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #7) regsvcs.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
4/5	Discovery	Queries OS version via WMI	1	-
	• (Process #7) regsvcs.exe queries OS version via WMI query: SELECT * FROM Win32_OperatingSystem.			
4/5	Exploit	Exploits a vulnerability in MS Office	1	Exploit
	• Exploits equation editor vulnerability CVE-2017-11882 or CVE-2018-0802 in MS Office.			
4/5	Network Connection	Performs DNS request	1	-
	• (Process #7) regsvcs.exe resolves hostname "api.ip.sb" to IP "172.67.75.172".			
4/5	Network Connection	Connects to remote host	2	-
	• (Process #7) regsvcs.exe opens an outgoing TCP connection to host "172.67.75.172:443". • (Process #7) regsvcs.exe opens an outgoing TCP connection to host "185.38.142.10:7474".			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #4) eqnedt32.exe downloads Windows executable via http from hxxps://universalmovies[.]top/ExtExport2.exe.			
4/5	Network Connection	Downloads file	1	Downloader
	• Downloads file via http from hxxps://universalmovies[.]top/notorious.doc.			
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #7) regsvcs.exe connects to hxxp://185[.]38[.]142[.]10:7474.			
4/5	Network Connection	Attempts to connect through HTTPS	2	-
	• (Process #4) eqnedt32.exe connects to hxxps://universalmovies[.]top/ExtExport2.exe. • (Process #7) regsvcs.exe connects to hxxps://api[.]ip[.]sb/geoip.			
4/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #7) regsvcs.exe tries to connect to TCP port 7474 at 185.38.142.10.			
4/5	Heuristics	Document contains a phishing URL	1	-
	• Document "C:\Users\kEecfMwgj\Desktop\Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc" contains a phishing URL hxxps://universalmovies[.]top/notorious.doc.			

Score	Category	Operation	Count	Classification
4/5	Execution	Document tries to create process	2	-
	• Document creates (process #9) wmiprvse.exe. • Document creates (process #6) notorious53209.exe.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #6) notorious53209.exe modifies memory of (process #7) regsvcs.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #6) notorious53209.exe alters context of (process #7) regsvcs.exe.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• Embedded file "C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe" is a known malicious file. • Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Malicious host or URL detected via reputation	4	-
	• Contacted URL "hxxps://universalmovies[.]top/notorious.doc" is a known malicious URL and was reported as "Phishing and Malware". • (Process #4) eqnedt32.exe contacted known malicious URL hxxps://universalmovies[.]top/ExtExport2.exe and was reported as "Phishing and Malware". • Contacted URL "hxxps://universalmovies[.]top" is a known malicious URL and was reported as "Phishing and Malware". • Resolved domain "universalmovies.top" is a known malicious domain and was reported as "Phishing and Malware".			
4/5	Network Connection	URL does not use standard port	1	-
	• HTTP URL hxxp://185[.]38[.]142[.]10:7474 does not use port 80.			
3/5	Privilege Escalation	Enables process privileges	2	-
	• (Process #7) regsvcs.exe enables process privilege "SeDebugPrivilege". • (Process #9) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
3/5	Discovery	Enumerates running processes	1	-
	• (Process #7) regsvcs.exe enumerates running processes via WMI query SELECT * FROM Win32_Process Where SessionId='1'.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #7) regsvcs.exe takes a screenshot using BitBlt API.			
3/5	Defense Evasion	Template Injection	1	-
	• c:\users\keecfmwgj\desktop\invoice lgmsch0040924 paid - eft remittance advice and receipt.doc loads a remote template from "https://universalmovies.top/notorious.doc".			
3/5	Anti Analysis	Makes direct system call to possibly evade hooking based monitoring	5	-
	• (Process #6) notorious53209.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #6) notorious53209.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #6) notorious53209.exe makes a direct system call to "NtResumeThread". • (Process #6) notorious53209.exe makes a direct system call to "NtCreateSection". • (Process #6) notorious53209.exe makes a direct system call to "NtMapViewOfSection".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #6) notorious53209.exe tries to detect a debugger via API "IsDebuggerPresent".			
2/5	Discovery	Reads network adapter information	1	-

Score	Category	Operation	Count	Classification
	• (Process #7) regsvcs.exe reads the network adapters' addresses by API.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #7) regsvcs.exe searches for sensitive data of FTP application "Total Commander" by file.			
2/5	Discovery	Searches for cryptocurrency wallet locations	2	-
	• (Process #7) regsvcs.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #7) regsvcs.exe searches for the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
2/5	Discovery	Searches for sensitive browser data	23	-
	• (Process #7) regsvcs.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Chromium" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Opera" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Maple Studio" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "7Star" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Chedot" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Kometa" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Elements Browser" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Uran" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Torch" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "CocCoc" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Mozilla Firefox" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "k-Meleon" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Comodo IceDragon" by file. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Cyberfox" by file.		
2/5	Discovery	Searches for sensitive mail data	2	-
	• (Process #7) regsvcs.exe searches for sensitive data of mail application "Windows Mail" by file. • (Process #7) regsvcs.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #7) regsvcs.exe tries to gather information about application "Steam" by registry. • (Process #7) regsvcs.exe tries to gather information about application "FileZilla" by file.			

Malware Configuration: RedLine

Metadata	Key	Extracted Value
Version	Value	1
Mission ID	Value	wordfile
Socket	Address Port Network Protocol C2 Listen	185.38.142.10 7474 tcp ✔ ✖

Mitre ATT&CK Matrix

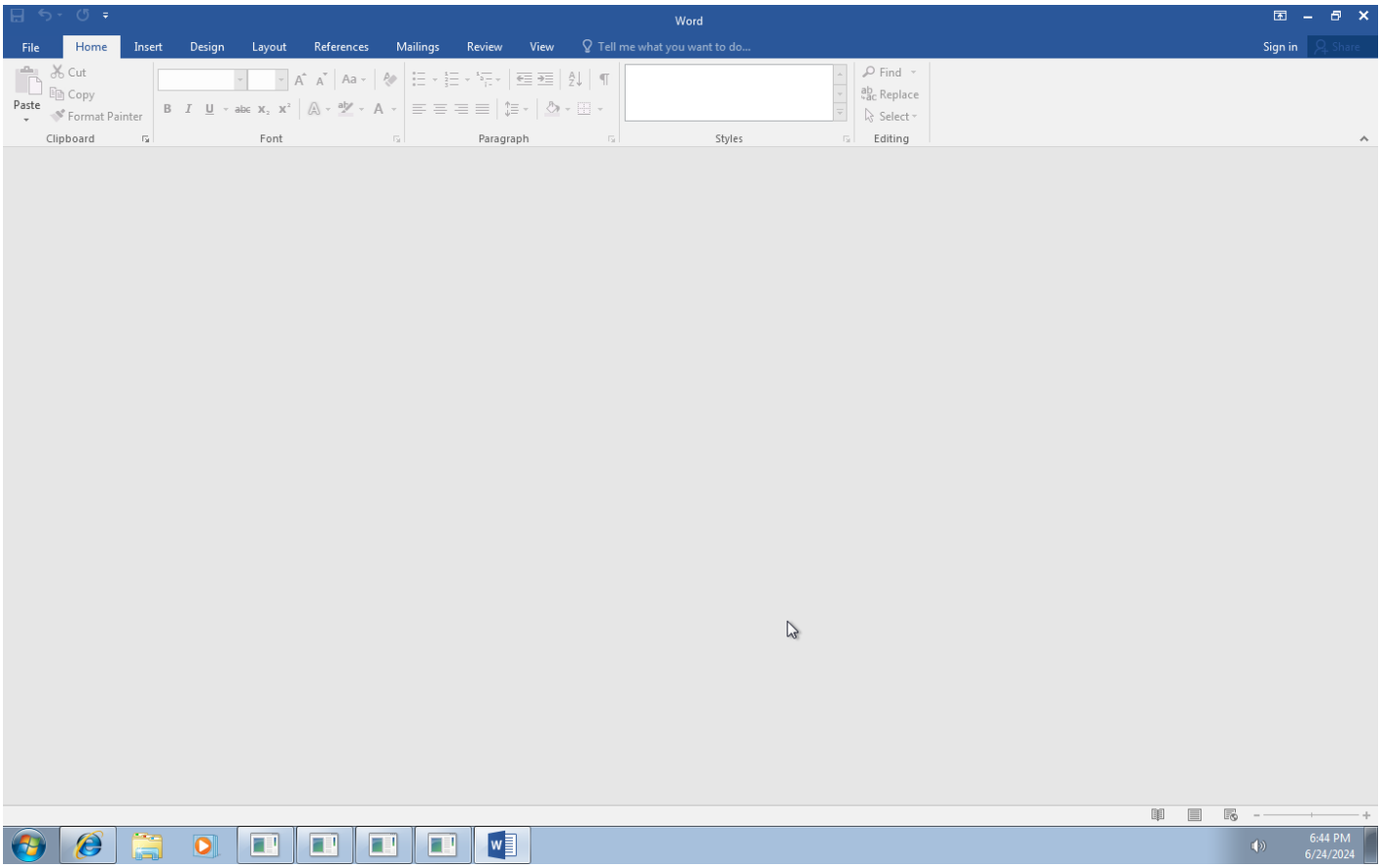
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
#T1193 Spearphishing Attachment	#T1047 Windows Management Instrumentation			#T1221 Template Injection	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
#T1566.001 Spearphishing Attachment	#T1203 Exploitation for Client Execution			#T1221 Template Injection	#T1056 Input Capture	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
	#T1047 Windows Management Instrumentation				#T1552.001 Credentials In Files	#T1082 System Information Discovery		#T1113 Screen Capture	#T1032 Standard Cryptographic Protocol		
	#T1203 Exploitation for Client Execution				#T1056 Input Capture	#T1063 Security Software Discovery		#T1056 Input Capture	#T1065 Uncommonly Used Port		
						#T1012 Query Registry		#T1119 Automated Collection	#T1071.001 Web Protocols		
						#T1016 System Network Configuration Discovery		#T1005 Data from Local System	#T1105 Ingress Tool Transfer		
						#T1083 File and Directory Discovery		#T1113 Screen Capture	#T1573.002 Asymmetric Cryptography		
						#T1082 System Information Discovery		#T1056 Input Capture	#T1571 Non-Standard Port		
						#T1518.001 Security Software Discovery					
						#T1012 Query Registry					

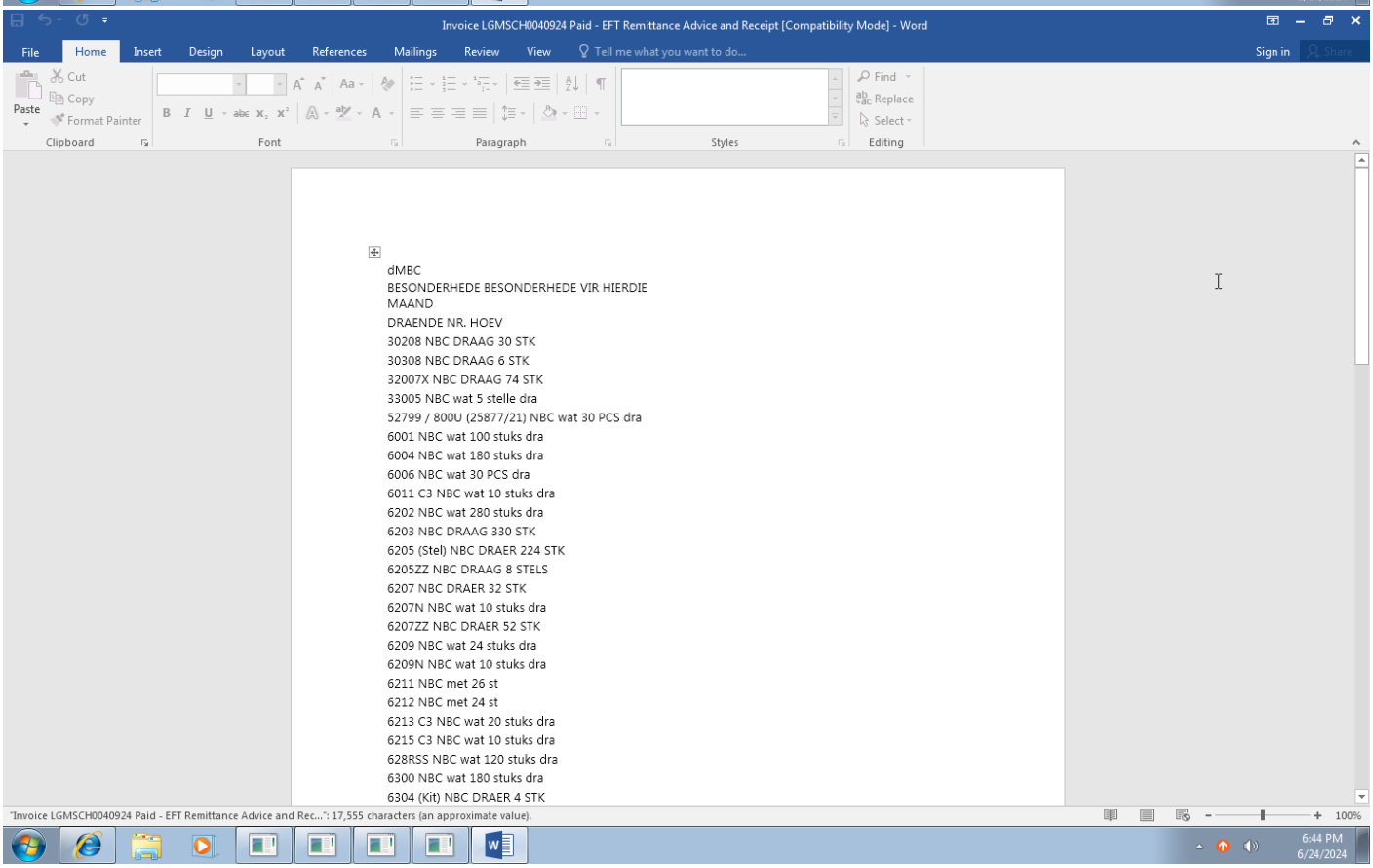
Sample Information

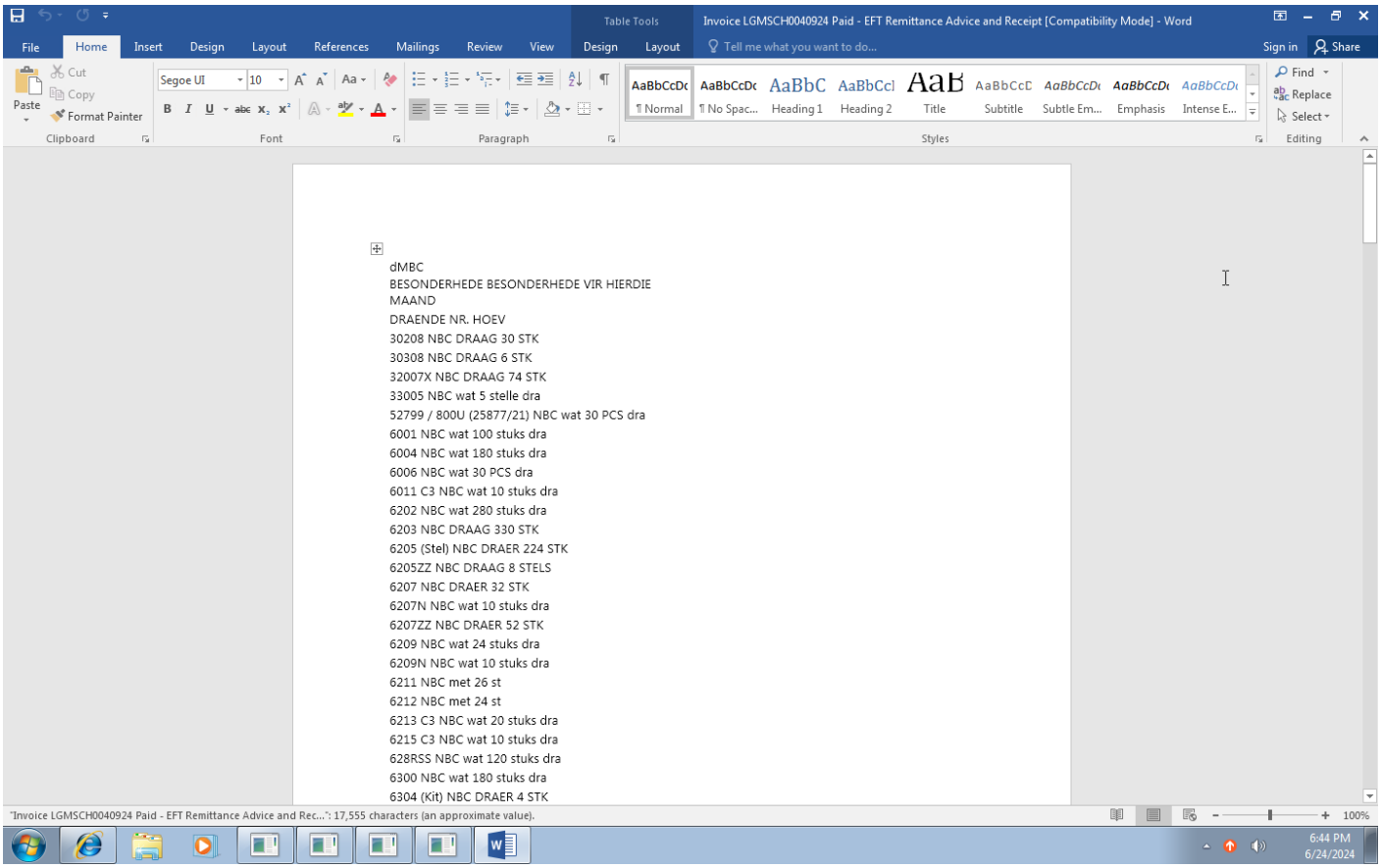
ID	#10708709
MD5	9edc82805ecc2d30f07d99973883c3c6
SHA1	877fae637a454593a1b66bfede20356803833266
SHA256	927e8668d7e5b22d0d278cb66ecbb15a51420f2fc5299aaa324d43a7d04719a2
SSDeep	384:tyXxo8qWds8PL8wi4OEwH8TIbE91r2fR3JYovij7XCnp:tcxIq5P3DOqnYJZ1vO7XCp
File Name	Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc
File Size	16.04 KB
Sample Type	Word Document
Has Macros	✔

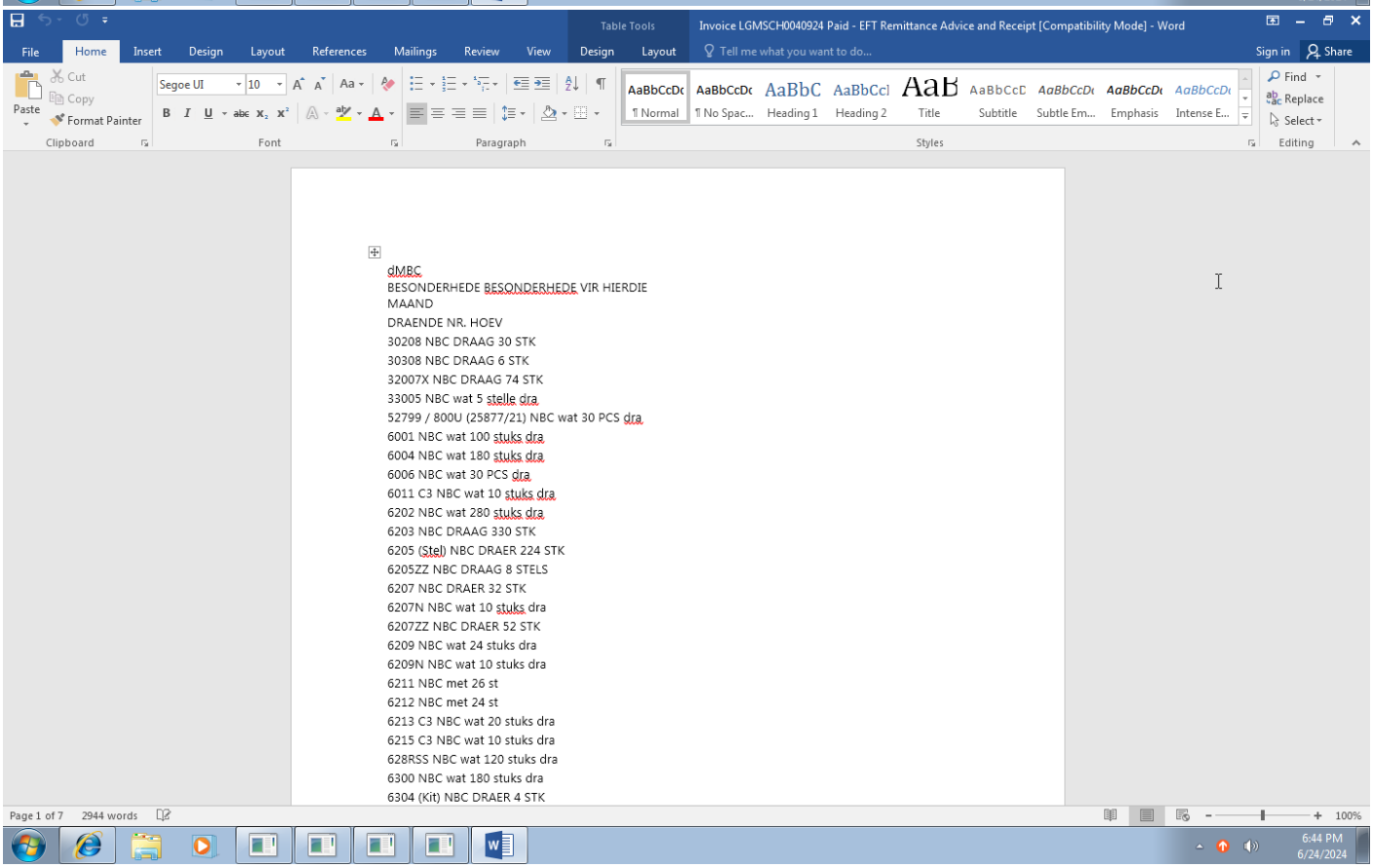
Analysis Information

Creation Time	2024-06-24 16:43 (UTC)
Analysis Duration	00:04:02
Termination Reason	Timeout
Number of Monitored Processes	8
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3


Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
6:44 PM
6/24/2024


Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt [Compatibility Mode] - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
dMBC
BESONDERHEDE BESONDERHEDE VIR HIERDIE MAAND
DRAENDE NR. HOEV
30208 NBC DRAAG 30 STK
30308 NBC DRAAG 6 STK
32007X NBC DRAAG 74 STK
33005 NBC wat 5 stelle dra
52799 / 800U (25877/21) NBC wat 30 PCS dra
6001 NBC wat 100 stuks dra
6004 NBC wat 180 stuks dra
6006 NBC wat 30 PCS dra
6011 C3 NBC wat 10 stuks dra
6202 NBC wat 280 stuks dra
6203 NBC DRAAG 330 STK
6205 (Stel) NBC DRAER 224 STK
6205ZZ NBC DRAAG 8 STELS
6207 NBC DRAER 32 STK
6207N NBC wat 10 stuks dra
6207ZZ NBC DRAER 52 STK
6209 NBC wat 24 stuks dra
6209N NBC wat 10 stuks dra
6211 NBC met 26 st
6212 NBC met 24 st
6213 C3 NBC wat 20 stuks dra
6215 C3 NBC wat 10 stuks dra
628RSS NBC wat 120 stuks dra
6300 NBC wat 180 stuks dra
6304 (Kit) NBC DRAER 4 STK
"Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Rec...": 17,555 characters (an approximate value).
100%
6:44 PM
6/24/2024





Screenshots truncated

NETWORK

General

1055.40 KB total sent

1327.44 KB total received

3 ports 7474, 443, 53

4 contacted IP addresses

0 URLs extracted

8 files downloaded

4 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

5 URLs contacted, 3 servers

5 sessions, 3152.65 KB sent, 2020.77 KB received

HTTP Requests

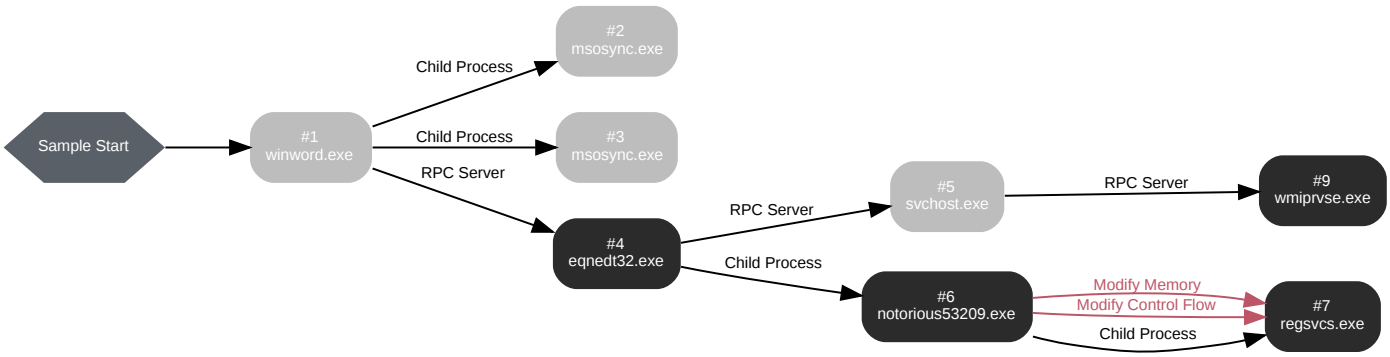
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://185[.]38[.]142[.]10:7474	-	-	-	0 bytes	MALICIOUS
GET	hxxps://universalmovies[.]top/notorious.doc	-	-	-	0 bytes	MALICIOUS
OPTIONS	hxxps://universalmovies[.]top	-	-	-	0 bytes	MALICIOUS
GET	hxxps://universalmovies[.]top/ExtExport2.exe	-	-	-	0 bytes	MALICIOUS
GET	hxxps://api[.]ip[.]sb/geoip	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	universalmovies[.]top	NO_ERROR	104.21.74.191, 172.67.162.95	-	MALICIOUS
A	api[.]ip[.]sb, api[.]ip[.]sb[.]cdn[.]cloudflare[.]net	NO_ERROR	172.67.75.172, 104.26.12.31, 104.26.13.31	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net	CLEAN

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
File Name	c:\program files\microsoft office\office16\winword.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 55411, Reason: Analysis Target
Unmonitor End Time	End Time: 260832, Reason: Terminated
Monitor duration	205.42s
Return Code	0
PID	3724
Parent PID	-
Bitness	64 Bit

Process #2: msosync.exe

ID	2
File Name	c:\program files\microsoft office\office16\msosync.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63501, Reason: Child Process
Unmonitor End Time	End Time: 67603, Reason: Terminated
Monitor duration	4.10s
Return Code	0
PID	3928
Parent PID	3724
Bitness	64 Bit

Process #3: msosync.exe

ID	3
File Name	c:\program files\microsoft office\office16\msosync.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63538, Reason: Child Process
Unmonitor End Time	End Time: 298029, Reason: Terminated by timeout
Monitor duration	234.49s
Return Code	Unknown
PID	3936
Parent PID	3724
Bitness	64 Bit

Process #4: eqnedt32.exe

ID	4
File Name	c:\program files\common files\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 70578, Reason: RPC Server
Unmonitor End Time	End Time: 77097, Reason: Terminated
Monitor duration	6.52s
Return Code	0
PID	2928
Parent PID	3724
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe	629.00 KB	b5e250a95073b5dfe33f66c13cc89da0fc8d3af226e5efb06bb8fcfd9a4cd6ec	✖

Host Behavior

Type	Count
Module	6
File	1
Process	1

Network Behavior

Type	Count
HTTPS	1

Process #5: svchost.exe

ID	5
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 73803, Reason: RPC Server
Unmonitor End Time	End Time: 298029, Reason: Terminated by timeout
Monitor duration	224.23s
Return Code	Unknown
PID	876
Parent PID	2928
Bitness	64 Bit

Process #6: notorious53209.exe

ID	6
File Name	c:\users\keecfmwgj\appdata\roaming\notorious53209.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 75303, Reason: Child Process
Unmonitor End Time	End Time: 112031, Reason: Terminated
Monitor duration	36.73s
Return Code	0
PID	2980
Parent PID	2928
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\Keily	95.50 KB	97d29f1e5e3bb5c8c1eb956c0135a820825973869c1b098705490010e0216fa8	✖
C:\Users\KEECFM~1\AppData\Local\Temp\lophophorine	28.08 KB	33ce9852b482618cce0e5c282fd710e02400cb310cee839537db9c2585167adb	✖
C:\Users\KEECFM~1\AppData\Local\Temp\aut6BD1.tmp	75.62 KB	8fad249f983dbf5caaef3d72a53210f4a1b2be6d81b2eb3a59cf7151bf5666c1	✖
C:\Users\KEECFM~1\AppData\Local\Temp\aut6E04.tmp	9.61 KB	d36e5c68763ed63f3068f5330f4d80488a0294c05663c30ade57e017ea50f842	✖

Host Behavior

Type	Count
Module	384
System	56
File	79
Environment	1
Registry	3
-	1
Window	2
Process	1
-	3
-	2

Process #7: regsvcs.exe

ID	7
File Name	c:\windows\microsoft.net\framework\v4.0.30319\regsvcs.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 106043, Reason: Child Process
Unmonitor End Time	End Time: 298029, Reason: Terminated by timeout
Monitor duration	191.99s
Return Code	Unknown
PID	2868
Parent PID	2980
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\keecfmwgj\appdata\roaming\notorious53209.exe	0xba8	0x400000(4194304)	0x1e000	✔	1
Modify Memory	#6: c:\users\keecfmwgj\appdata\roaming\notorious53209.exe	0xba8	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#6: c:\users\keecfmwgj\appdata\roaming\notorious53209.exe	0xba8 / 0xb38	0x77a701c4(2007433668)	-	✔	1

Dropped Files (10)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A4C.tmp	69.34 KB	bea0ab0557fa4f611aa981f06928b86b5a1239235d69b254b7c0fdd82a95a57d	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp998B.tmp	162 bytes	5ee74b175686b662f4e3e7c6576f1c14f0af55849520e28b1297ac884d8feaae	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993B.tmp	20.19 KB	eb4d94a4b1dda069e1a106840ba590e1295ef596fc36bea370a577c5a1744eb5	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99EB.tmp	83.99 KB	38c62a9fa1c8bfc041ded191e6a97d3df52573b8ed0eb100979320b928df10ac	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A2A.tmp	91.98 KB	7206d6259658c04b684edf9625fe4a7c5a16c69935f92f824820b76efc85b887	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp98DC.tmp	8.17 KB	5c9c660dfeee77d28765bf62e36c8f22b3b560f434f8c020f57d9d657b2688f9	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A3B.tmp	18.38 KB	87aa935c79ecee24e7a368083b674f5f6439fd577b830a83459020513109b095	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993A.tmp	16.04 KB	927e8668d7e5b22d0d278cb66ecbb15a51420f2fc5299aaa324d43a7d04719a2	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99DA.tmp	6.89 KB	1a75db162d5af2e75c9fa889ed3af9a2b347a62df5fcc7d111ae4c37fed98b3e	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp997B.tmp	18.29 KB	33b5894094c57e730222d4553045b817846a90a85fae7d32c91785e7d8bed089	✖

Host Behavior

Type	Count
Module	73
Registry	273

Type	Count
File	293
-	12
User	3
System	212
Environment	8
-	2
Keyboard	3
COM	191
-	12
Window	1

Network Behavior

Type	Count
HTTP	3
HTTPS	1
DNS	1
TCP	2

Process #9: wmiprvse.exe

ID	9
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 235122, Reason: RPC Server
Unmonitor End Time	End Time: 298029, Reason: Terminated by timeout
Monitor duration	62.91s
Return Code	Unknown
PID	3380
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
User	2
System	225
Process	649
-	1050
Registry	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
927e8668d7e5b22d0d278cb66ecbb15a51420f2fc5299aaa324d43a7d04719a2	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993A.tmp, C:\Users\kEecfMwgj\Desktop\Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc	Dropped File	16.04 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Access, Create, Delete, Read, Write	MALICIOUS
b5e250a95073b5dfe33f66c13cc89da0fc8d3af226e5efb06bb8fcfd9a4cd6ec	C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe, c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c\extexport2[1].exe	Downloaded File	629.00 KB	application/vnd.microsoft.portable-executable	Access, Create	MALICIOUS
75a7c0cb892f4af439e1590182d5afed2467e5143c5a01da1051e111d5f4b5a8	-	Blob	5.20 KB	-	-	MALICIOUS
518ed3cd2af45e79cdba8d8d440666661a22106aa2b194ce2fdf18eda32f3081	-	Memory Dump	96.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a740ec491f9cd353e283dfcf7c21e1b97562ef3c859b2f562ba3ffa6013a18db	-	Memory Dump	120.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
59fb57baf1ed70984221ca94cd509b46a1242a99092ec0c05585c2b58c74ccf5	-	Downloaded File	137 bytes	text/plain	-	CLEAN
86df651850a7cf084bff38e62aca1a54d165735533e3b182a0224e3a80f5c9c9	-	Downloaded File	212 bytes	text/plain	-	CLEAN
c7effe833dabd5a007460d8fcd17f5b36284c933be0f9d40a8a65fb68d102dcd	-	Downloaded File	144 bytes	text/plain	-	CLEAN
54dec80fc8344b4123d4fe9981b1338e947822e758b62eda47b8ec39a582fbfb	-	Downloaded File	4.63 KB	text/plain	-	CLEAN
262d95391c07f588b9c11c58cfa50001b9580cfd8adc021e5914f5f22cd62c3a	-	Downloaded File	614.51 KB	text/plain	-	CLEAN
bf89362748b9e66c11aaa49ddf83b1665fe038d04225b36de4f26cffc11a0f3d	-	Downloaded File	604.43 KB	text/rtf	-	CLEAN
43580270910ee9931690af4be61798afb0081c5d3e8026220d6054284a435902	-	Downloaded File	338 bytes	application/json	-	CLEAN
b5fabd4fcbcdda3d96752c9703daca8118bcc6392838d464cb1f510c858d020d	-	Extracted File	10.22 KB	image/png	-	CLEAN
8fad249f983dbf5caaef3d72a53210f4a1b2be6d81b2eb3a59cf7151bf5666c1	C:\Users\KEECFM~1\AppData\Local\Temp\aut6BD1.tmp	Dropped File	75.62 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
97d29f1e5e3bb5c8c1eb956c0135a820825973869c1b098705490010e0216fa8	C:\Users\KEECFM~1\AppData\Local\Temp\Keily	Dropped File	95.50 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d36e5c68763ed63f3068f5330f4d80488a0294c05663c30ade57e017ea50f842	C:\Users\KEECFM~1\AppData\Local\Temp\aut6E04.tmp	Dropped File	9.61 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
33ce9852b482618cce0e5c282fd710e02400cb310cee839537db9c2585167adb	C:\Users\KEECFM~1\AppData\Local\Temp\lophophorine	Dropped File	28.08 KB	text/plain	Access, Create, Read, Write	CLEAN
5c9c660dfeee77d28765bf62e36c8f22b3b560f434f8c020f57d9d657b2688f9	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp98DC.tmp	Dropped File	8.17 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
eb4d94a4b1dda069e1a106840ba590e1295ef596fc36bea370a577c5a1744eb5	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993B.tmp	Dropped File	20.19 KB	application/CDFV2	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
33b5894094c57e730222d4553045b817846a90a85fae7d32c91785e7d8bed089	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp997B.tmp	Dropped File	18.29 KB	application/CDFV2	Access, Create, Delete, Read, Write	CLEAN
5ee74b175686b662f4e3e7c6576f1c14f0af55849520e28b1297ac884d8feaae	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp998B.tmp	Dropped File	162 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
1a75db162d5af2e75c9fa889ed3af9a2b347a62df5fcc7d111ae4c37fed98b3e	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99DA.tmp	Dropped File	6.89 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
38c62a9fa1c8bfc041ded191e6a97d3df52573b8ed0eb100979320b928df10ac	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99EB.tmp	Dropped File	83.99 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
7206d6259658c04b684edf9625fe4a7c5a16c69935f92f824820b76efc85b887	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A2A.tmp	Dropped File	91.98 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
87aa935c79ecee24e7a368083b674f5f6439fd577b830a83459020513109b095	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A3B.tmp	Dropped File	18.38 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
bea0ab0557fa4f611aa981f06928b86b5a1239235d69b254b7c0fdd82a95a57d	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A4C.tmp	Dropped File	69.34 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\Invoice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc	Accessed File, Sample File	Access	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993A.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c\extexport2[1].exe	Downloaded File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\aut6BD1.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\Keily	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\aut6E04.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\lophophorine	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
c:\users\keecfmwgj\appdata\local\temp\cab564e.tmp	Downloaded File, Extracted File	-	CLEAN
c:\users\keecfmwgj\appdata\local\temp\tar565f.tmp	Dropped File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp98DC.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp993B.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp997B.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp998B.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99DA.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp99EB.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A2A.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A3B.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9A4C.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\ntdll.dll	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe.Config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\~$voice LGMSCH0040924 Paid - EFT Remittance Advice and Receipt.doc	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YaAddon	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://universalmovies[.]top/notorious.doc	Contacted, Extracted	172.67.162.95, 104.21.74.191	-	GET, HEAD	MALICIOUS
hxxp://185[.]38[.]142[.]10:7474	Contacted, Extracted	185.38.142.10	Portugal	POST	MALICIOUS
hxxps://universalmovies[.]top/ExtExport2.exe	Contacted, Extracted	172.67.162.95, 104.21.74.191	-	GET	MALICIOUS
hxxps://universalmovies[.]top	Contacted, Extracted	172.67.162.95, 104.21.74.191	-	OPTIONS	MALICIOUS
hxxps://api[.]ip[.]sb/geoip	Contacted, Extracted	104.26.13.31, 172.67.75.172, 104.26.12.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
universalmovies[.]top	172.67.162.95, 104.21.74.191	-	HTTPS, DNS, TCP	MALICIOUS
api[.]ip[.]sb	104.26.13.31, 172.67.75.172, 104.26.12.31	-	HTTPS, DNS, TCP	CLEAN
api[.]ip[.]sb[.]cdn[.]cloudflare[.]net	104.26.13.31, 172.67.75.172, 104.26.12.31	-	HTTPS, DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.38.142.10	-	Portugal	HTTP, TCP	MALICIOUS
172.67.75.172	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net, api[.]ip[.]sb	-	HTTPS, DNS, TCP	MALICIOUS
104.21.74.191	universalmovies[.]top	-	HTTPS, DNS, TCP	CLEAN
172.67.162.95	universalmovies[.]top	-	DNS	CLEAN
104.26.12.31	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net, api[.]ip[.]sb	-	DNS	CLEAN
104.26.13.31	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net, api[.]ip[.]sb	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Control Panel\Mouse	access	notorious53209.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons	access, read	notorious53209.exe	CLEAN
HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt	access	notorious53209.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	access, read	regsvcs.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	access, read	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	access, read	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	regsvcs.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
notorious53209.exe	"C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe"	MALICIOUS

Process Name	Commandline	Verdict
eqnedt32.exe	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	SUSPICIOUS
regsvcs.exe	"C:\Users\kEecfMwgj\AppData\Roaming\notorious53209.exe"	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
winword.exe	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN
msosync.exe	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"	CLEAN
msosync.exe	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	RedLine_A	RedLine Stealer, RedLine.A variant	Memory Dump	-	Spyware	5/5
Malware	RedLine_A	RedLine Stealer, RedLine.A variant	Memory Dump	-	Spyware	5/5
Malware	RedLine_SOAPCommunication	RedLine Stealer SOAP response	-	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	windows 7 (64bit SP1 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.3.1
Dynamic Engine Version	2024.3.1 / 06/10/2024 04:30
Static Engine Version	2024.3.1.0 / 2024-06-10 03:00:36
AV Exceptions Version	2024.3.1.2 / 2024-06-08 13:32:38
Link Detonation Heuristics Version	2024.3.1.3 / 2024-06-10 20:59:54
Smart Memory Dumping Rules Version	2024.3.1.2 / 2024-06-08 13:32:38
Config Extractors Version	2024.3.1.3 / 2024-06-10 20:59:54
Signature Trust Store Version	2024.3.1.2 / 2024-06-08 13:32:38
VMRay Threat Identifiers Version	2024.3.1.7 / 2024-06-20 14:30:49
YARA Built-in Ruleset Version	2024.3.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows