MALICIOUS

Classifications: Exploit | Spyware | Downloader | Injector

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

Verdict Reason: -

Sample Type	**Word Document**
File Name	**bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09.doc**
ID	#10720423
MD5	15c09feba4b5e3928f38c6637295e7b8
SHA1	0c2dec1dde335d2ea464145a5f5960d2800aaef5
SHA256	bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09
File Size	16.04 KB
Report Created	2024-06-26 13:39 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | ms_office

OVERVIEW

VMRay Threat Identifiers (37 rules, 151 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_A" from ruleset "Malware" in memory dump data from (process #7) regsvcs.exe. • YARA detected "RedLine_A" from ruleset "Malware" in memory dump data from (process #6) notorious69281.exe. • YARA detected "RedLine_SOAPCommunication" from ruleset "Malware" in web response data from "hxxp://185[.]38[.]142[.]10:7474".			
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	73	-

- (Process #6) notorious69281.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 campaign mention.exe.
- (Process #9) wmiprvse.exe reads from money_shot.exe.
- (Process #9) wmiprvse.exe reads from staff various.exe.
- (Process #9) wmiprvse.exe reads from behind.exe.
- (Process #9) wmiprvse.exe reads from kind.exe.
- (Process #9) wmiprvse.exe reads from sufferexecutivehead.exe.
- (Process #9) wmiprvse.exe reads from dreamteacher.exe.
- (Process #9) wmiprvse.exe reads from change grow.exe.
- (Process #9) wmiprvse.exe reads from outside-husband-clearly.exe.
- (Process #9) wmiprvse.exe reads from presentdirectionsupport.exe.
- (Process #9) wmiprvse.exe reads from beyond-science.exe.
- (Process #9) wmiprvse.exe reads from ago-dream-serious.exe.
- (Process #9) wmiprvse.exe reads from avoid.exe.
- (Process #9) wmiprvse.exe reads from fact.exe.
- (Process #9) wmiprvse.exe reads from soon.exe.
- (Process #9) wmiprvse.exe reads from enough-seat-attorney.exe.
- (Process #9) wmiprvse.exe reads from partner reflect task.exe.
- (Process #9) wmiprvse.exe reads from spgagentservice.exe.
- (Process #9) wmiprvse.exe reads from flashfxp.exe.
- (Process #9) wmiprvse.exe reads from bitkinex.exe.
- (Process #9) wmiprvse.exe reads from utg2.exe.
- (Process #9) wmiprvse.exe reads from spcwin.exe.
- (Process #9) wmiprvse.exe reads from omnipos.exe.
- (Process #9) wmiprvse.exe reads from mxslipstream.exe.
- (Process #9) wmiprvse.exe reads from isspos.exe.
- (Process #9) wmiprvse.exe reads from fpos.exe.
- (Process #9) wmiprvse.exe reads from edcsvr.exe.
- (Process #9) wmiprvse.exe reads from creditservice.exe.
- (Process #9) wmiprvse.exe reads from centralcreditcard.exe.
- (Process #9) wmiprvse.exe reads from ccv_server.exe.
- (Process #9) wmiprvse.exe reads from aldelo.exe.
- (Process #9) wmiprvse.exe reads from afr38.exe.
- (Process #9) wmiprvse.exe reads from accupos.exe.
- (Process #9) wmiprvse.exe reads from active-charge.exe.
- (Process #9) wmiprvse.exe reads from yahoomessenger.exe.
- (Process #9) wmiprvse.exe reads from winscp.exe.
- (Process #9) wmiprvse.exe reads from whatsapp.exe.
- (Process #9) wmiprvse.exe reads from webdrive.exe.
- (Process #9) wmiprvse.exe reads from trillian.exe.
- (Process #9) wmiprvse.exe reads from thunderbird.exe.
- (Process #9) wmiprvse.exe reads from smartftp.exe.
- (Process #9) wmiprvse.exe reads from skype.exe.
- (Process #9) wmiprvse.exe reads from scriptftp.exe.
- (Process #9) wmiprvse.exe reads from pidgin.exe.
- (Process #9) wmiprvse.exe reads from outlook.exe.
- (Process #9) wmiprvse.exe reads from operamail.exe.
- (Process #9) wmiprvse.exe reads from notepad.exe.
- (Process #9) wmiprvse.exe reads from ncftp.exe.
- (Process #9) wmiprvse.exe reads from leechftp.exe.
- (Process #9) wmiprvse.exe reads from icq.exe.
- (Process #9) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #9) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #9) wmiprvse.exe reads from fling.exe.
- (Process #9) wmiprvse.exe reads from filezilla.exe.
- (Process #9) wmiprvse.exe reads from far.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_Processor. • (Process #7) regsvcs.exe queries hardware properties via WMI: SELECT * FROM Win32_DiskDrive.			
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	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	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 "104.26.13.31".			
4/5	Network Connection	Connects to remote host	2	-
	• (Process #7) regsvcs.exe opens an outgoing TCP connection to host "104.26.13.31:443". • (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://covid19help[.]top/wordpad.exe.			
4/5	Network Connection	Downloads file	1	Downloader
	• Downloads file via http from hxxps://covid19help[.]top/notori.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://covid19help[.]top/wordpad.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\bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09.doc" contains a phishing URL hxxps://covid19help[.]top/notori.doc.			

Score	Category	Operation	Count	Classification
4/5	Execution	Document tries to create process	2	-
	• Document creates (process #6) notorious69281.exe. • Document creates (process #9) wmiprvse.exe.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #6) notorious69281.exe modifies memory of (process #7) regsvcs.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #6) notorious69281.exe alters context of (process #7) regsvcs.exe.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• Reputation analysis labels embedded file "C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.exe" as Mal/Generic-S. • The sample itself is a known malicious file.			
4/5	Reputation	Malicious host or URL detected via reputation	6	-
	• Contacted URL "hxxps://covid19help[.]top/notori.doc" is a known malicious URL and was reported as "Spam, Phishing and Malware". • Reputation analysis labels the URL "hxxp://185[.]38[.]142[.]10:7474" which was contacted by (process #7) regsvcs.exe as Mal/HTMLGen-A. • (Process #4) eqnedt32.exe contacted known malicious URL hxxps://covid19help[.]top/wordpad.exe and was reported as "Spam, Phishing and Malware". • Contacted URL "hxxps://covid19help[.]top" is a known malicious URL and was reported as "Spam, Phishing and Malware". • Resolved domain "covid19help.top" is a known malicious domain and was reported as "Spam, Phishing and Malware". • Reputation analysis labels the contacted IP address 185.38.142.10 as Mal/HTMLGen-A.			
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	Data Collection	Takes screenshot	1	-
	• (Process #7) regsvcs.exe takes a screenshot using BitBlt API.			
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	Obfuscation	Obfuscates control flow	1	-
	• Modifies exception handler (e.g., the instruction pointer is modified within an exception handler filter).			
3/5	Anti Analysis	Makes direct system call to possibly evade hooking based monitoring	4	-
	• (Process #6) notorious69281.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #6) notorious69281.exe makes a direct system call to "NtMapViewOfSection". • (Process #6) notorious69281.exe makes a direct system call to "NtCreateSection". • (Process #6) notorious69281.exe makes a direct system call to "NtResumeThread".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #6) notorious69281.exe tries to detect a debugger via API "IsDebuggerPresent".			

Score	Category	Operation	Count	Classification
2/5	Discovery	Reads network adapter information	1	-
	• (Process #7) regsvcs.exe reads the network adapters' addresses by API.			
2/5	Discovery	Searches for sensitive browser data	23	-
	• (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. • (Process #7) regsvcs.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.		
2/5	Discovery	Searches for sensitive mail data	2	-
	• (Process #7) regsvcs.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #7) regsvcs.exe searches for sensitive data of mail application "Windows Mail" 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	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.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #7) regsvcs.exe searches for sensitive data of FTP application "Total Commander" 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

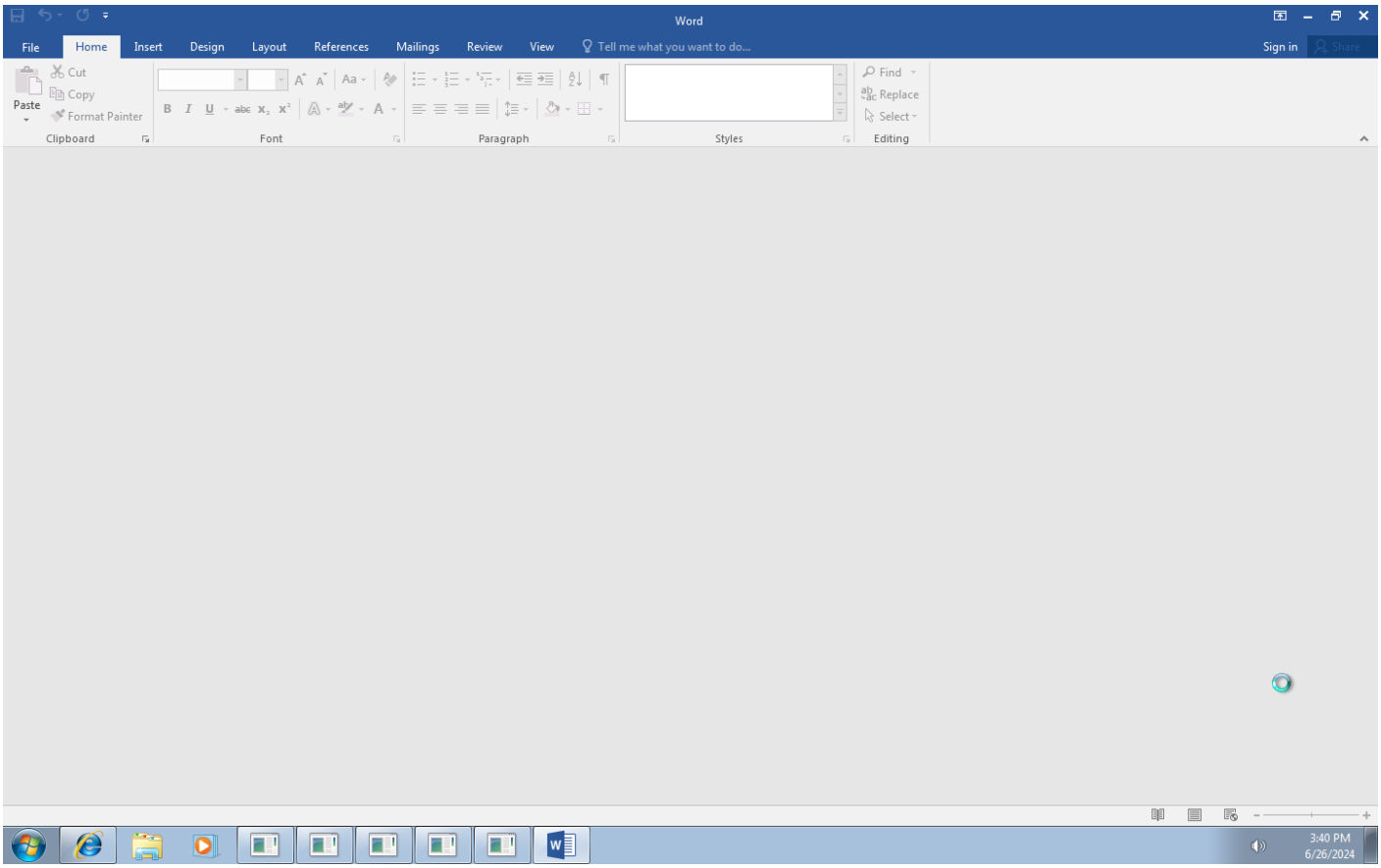
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
#T1193 Spearphishing Attachment	#T1047 Windows Management Instrumentation			#T1045 Software Packing	#T1081 Credentials in Files	#T1016 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			#T1027 Obfuscated Files or Information	#T1056 Input Capture	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
	#T1047 Windows Management Instrumentation			#T1027.002 Software Packing	#T1552.001 Credentials In Files	#T1082 System Information Discovery		#T1113 Screen Capture	#T1032 Standard Cryptographic Protocol		
	#T1203 Exploitation for Client Execution				#T1056 Input Capture	#T1012 Query Registry		#T1056 Input Capture	#T1065 Uncommonly Used Port		
						#T1063 Security Software Discovery		#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		
						#T1012 Query Registry					
						#T1518.001 Security Software Discovery					

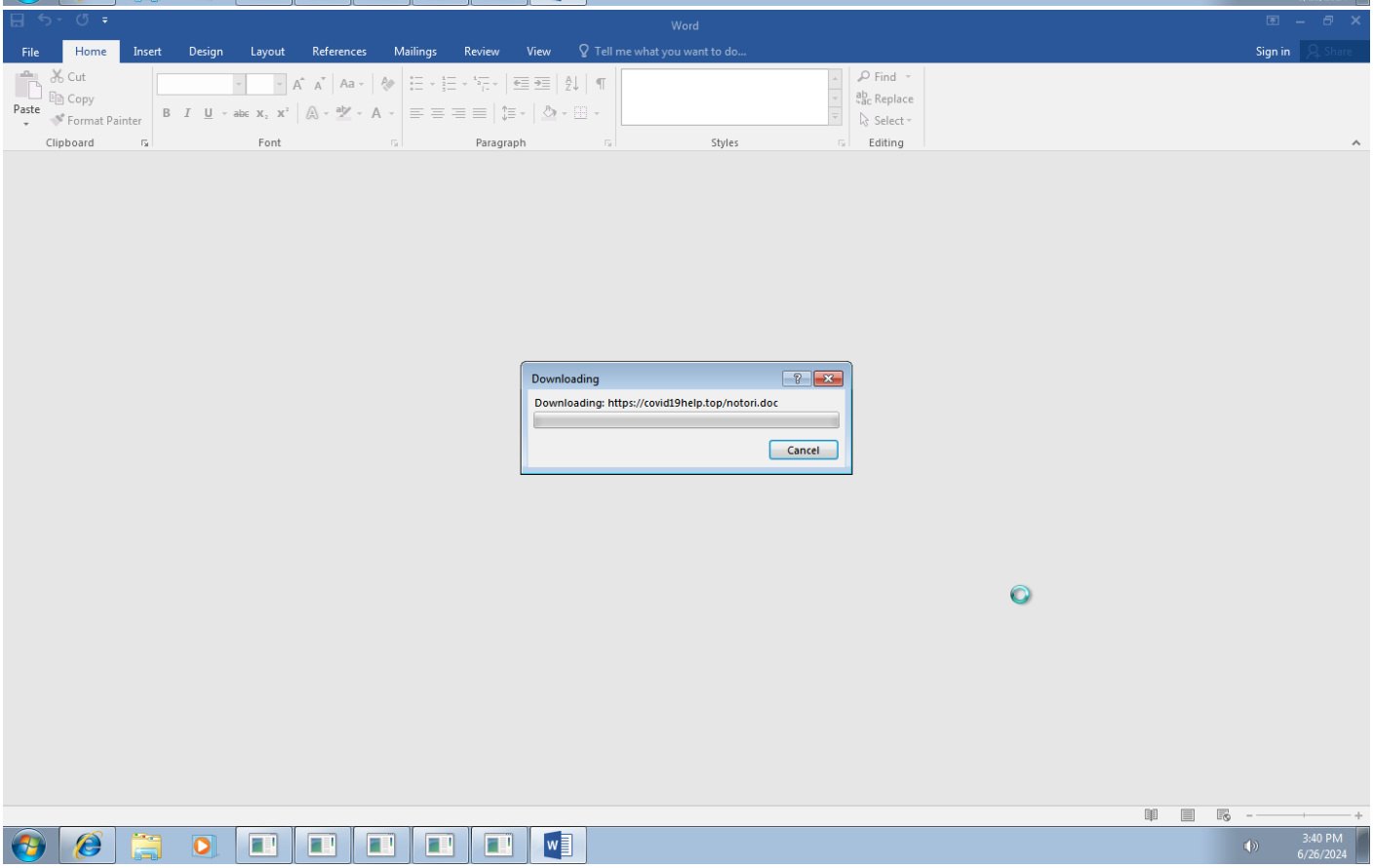
Sample Information

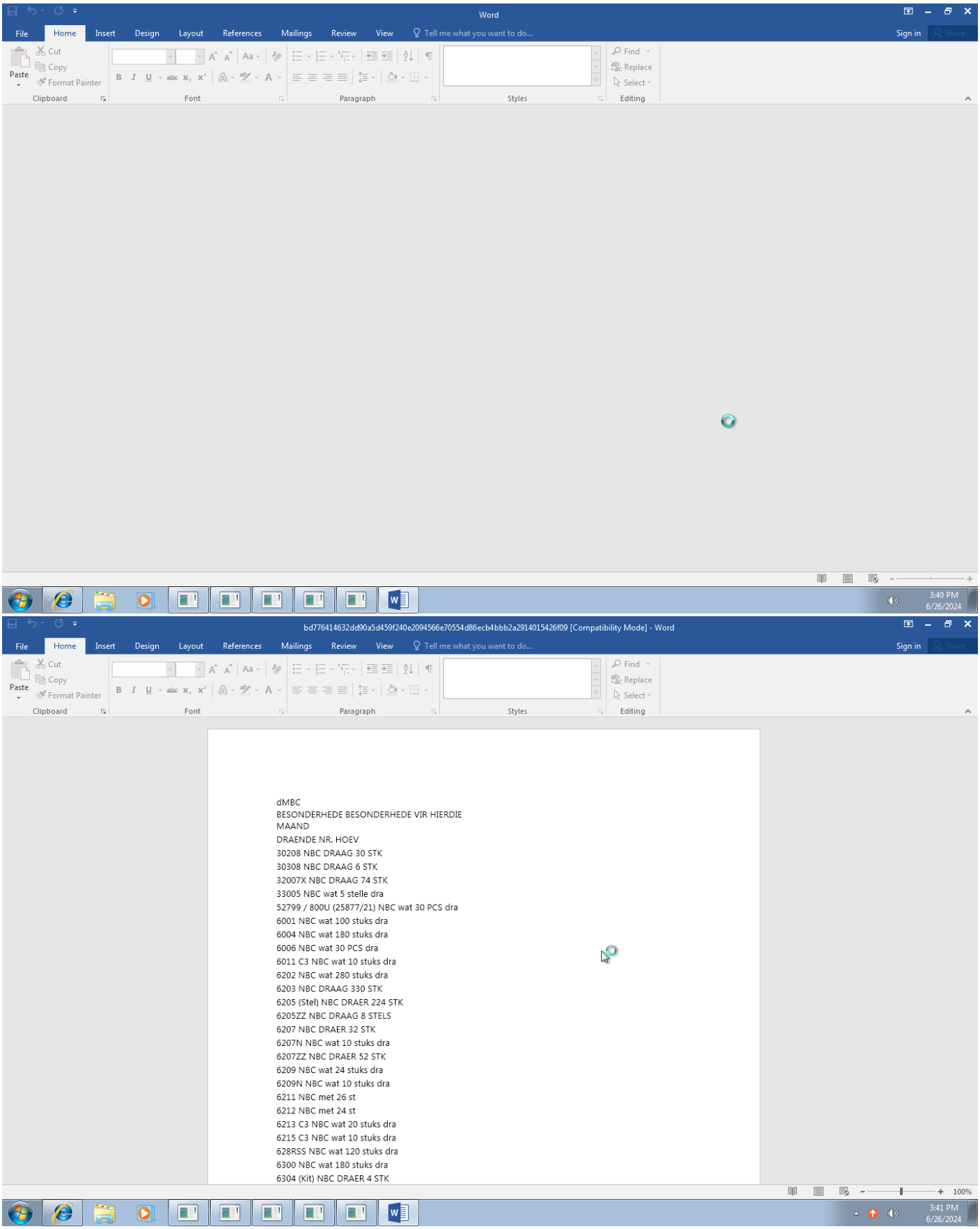
ID	#10720423
MD5	15c09feba4b5e3928f38c6637295e7b8
SHA1	0c2dec1dde335d2ea464145a5f5960d2800aaef5
SHA256	bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09
SSDeep	384:uyXG0buW+s8PL8wi4OEwH8TIbE91r2fRGJYlvibEEBvmp:ucG715P3DOqnYJQcv+EEBE
File Name	bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09.doc
File Size	16.04 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2024-06-26 13:39 (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
3:40 PM
6/26/2024


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
Downloading
Downloading: https://covid19help.top/notori.doc
Cancel
3:40 PM
6/26/2024



Screenshots truncated

NETWORK

General

84.32 KB total sent

1657.70 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, 237.13 KB sent, 2240.08 KB received

HTTP Requests

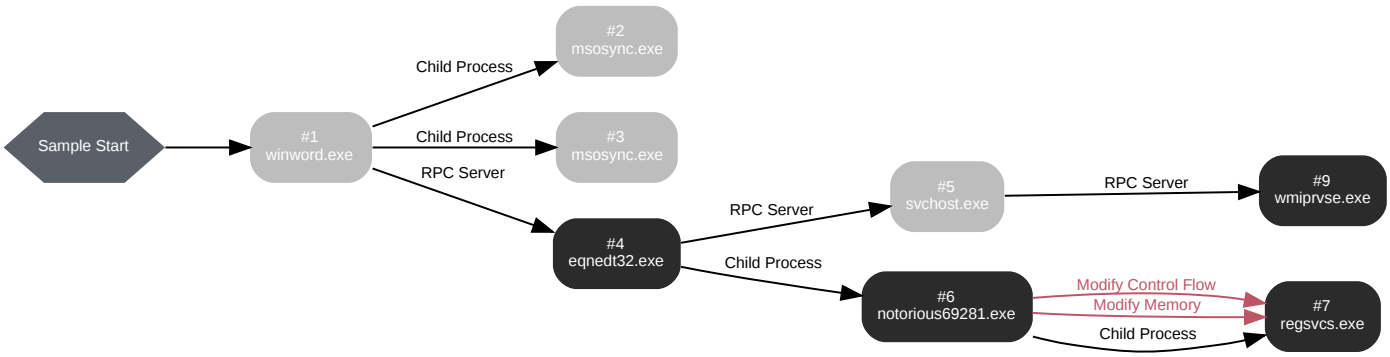
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://185[.]38[.]142[.]10:7474	-	-	-	0 bytes	MALICIOUS
GET	hxxps://covid19help[.]top/notori.doc	-	-	-	0 bytes	MALICIOUS
OPTIONS	hxxps://covid19help[.]top	-	-	-	0 bytes	MALICIOUS
GET	hxxps://api[.]ip[.]sb/geoip	-	-	-	0 bytes	MALICIOUS
GET	hxxps://covid19help[.]top/wordpad.exe	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	covid19help[.]top	NO_ERROR	104.21.83.128, 172.67.175.222	-	MALICIOUS
A	api[.]ip[.]sb, api[.]ip[.]sb[.]cdn[.]cloudflare[.]net	NO_ERROR	104.26.13.31, 172.67.75.172, 104.26.12.31	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: 51882, Reason: Analysis Target
Unmonitor End Time	End Time: 247385, Reason: Terminated
Monitor duration	195.50s
Return Code	0
PID	3656
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: 60751, Reason: Child Process
Unmonitor End Time	End Time: 66560, Reason: Terminated
Monitor duration	5.81s
Return Code	0
PID	3856
Parent PID	3656
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: 60822, Reason: Child Process
Unmonitor End Time	End Time: 294629, Reason: Terminated by timeout
Monitor duration	233.81s
Return Code	Unknown
PID	3864
Parent PID	3656
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: 71256, Reason: RPC Server
Unmonitor End Time	End Time: 83067, Reason: Terminated
Monitor duration	11.81s
Return Code	0
PID	4048
Parent PID	3656
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	1047.00 KB	a591d3d035cf90395ad1078a415a46b5b44dd813496291b702fe36cfb22dee36	✖

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: 78631, Reason: RPC Server
Unmonitor End Time	End Time: 294629, Reason: Terminated by timeout
Monitor duration	216.00s
Return Code	Unknown
PID	876
Parent PID	4048
Bitness	64 Bit

Process #6: notorious69281.exe

ID	6
File Name	c:\users\keecfmwgj\appdata\roaming\notorious69281.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 81126, Reason: Child Process
Unmonitor End Time	End Time: 100992, Reason: Terminated
Monitor duration	19.87s
Return Code	0
PID	2892
Parent PID	4048
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\aut7B6.tmp	78.10 KB	e74ef457af291610afb6c315b80bcb6f9861a7a411f3f744fa3faf1273d4df9f	✖
C:\Users\KEECFM~1\AppData\Local\Temp\brontothere	28.08 KB	423a70f3606d0d0f96d2f932614a2125dad3ff3170e2f04ff4bc3cef82bd57cd	✖
C:\Users\KEECFM~1\AppData\Local\Temp\Okeghem	95.50 KB	90f3b22bec26df402a0ab8fef7df8fbf79e5d74f9ed0f25943d1d5e7e2fe020b	✖
C:\Users\KEECFM~1\AppData\Local\Temp\aut90E.tmp	9.65 KB	6369e06e6a3e2495442d98898cfa8d51fcb272b4a54f8818e5a5804f0f029c05	✖

Host Behavior

Type	Count
System	50
Module	117
File	79
Environment	1
Registry	3
-	1
Window	2
Process	1
-	3
-	1

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\notorious69281.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 92672, Reason: Child Process
Unmonitor End Time	End Time: 294629, Reason: Terminated by timeout
Monitor duration	201.96s
Return Code	Unknown
PID	2872
Parent PID	2892
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\notorious69281.exe	0xb48	0x400000(4194304)	0x1e000	✔	1
Modify Memory	#6: c:\users\keecfmwgj\appdata\roaming\notorious69281.exe	0xb48	0x7efde008(2130567176)	0x1e000	✔	1
Modify Control Flow	#6: c:\users\keecfmwgj\appdata\roaming\notorious69281.exe	0xb48 / 0xb34	0x77a701c4(2007433668)	-	✔	1

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1762.tmp	84.11 KB	35d3caededcd7914d356eda934b67ae80aa639113dd3fe82ad710747a1c7d3f0	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17D2.tmp	83.95 KB	6a0ea337ed0e2ea66ebde9aff30194f21e6d29580a5d7b9d557d067d67e00327	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17A2.tmp	82.58 KB	12c48c1e1ec4c69b91abeb7ede43d9e33eb8770ae1cb4c16d12f4fdd057edd69	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17F2.tmp	28.80 KB	9b512d1431b193b7754be257776d63fd1cf8387bd3a6998fc5614372b423c99e	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1782.tmp	91.94 KB	d0ce547483680a7c0d261210dfce8e633fdcdbe86cd6cc0f7fecf0e0d9cac1c4	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp16F4.tmp	20.06 KB	1c8bfa0eb3e36e7d474678079efb5755ea35113cc810262af79ac07c4964df00	✖

Host Behavior

Type	Count
Module	73
Registry	273
File	257
-	12
User	3
System	191
Environment	8
-	2

Type	Count
COM	187
-	12
Keyboard	3
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: 255443, Reason: RPC Server
Unmonitor End Time	End Time: 294629, Reason: Terminated by timeout
Monitor duration	39.19s
Return Code	Unknown
PID	3344
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
System	218
Registry	2
User	2
Process	631
-	1022

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09	C:\Users\kEecfMwgj\Desktop\bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09.doc, C:\Users\kEecfMwgj\AppData\Local\Temp\tmp16F4.tmp	Sample File	16.04 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Access, Create, Delete, Read, Write	MALICIOUS
a591d3d035cf90395ad1078a415a46b5b44dd813496291b702fe36cfb22dee36	C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.exe, c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c\wordpad[1].exe	Downloaded File	1047.00 KB	application/vnd.microsoft.portable-executable	Access, Create	MALICIOUS
f0d4a7f2b4f998dfae1aac1fefa6200fe24ba37b40b04077ef0a14030fb674b7	-	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
4abd3b1898112ca3eae5c272408e91e03a0af8ac8bfc81b1b313a18915e202de	-	Downloaded File	45.38 KB	text/plain	-	CLEAN
86e88eac92b0bf840e689e4d71d66735f70c9309b82b540736b3ec50dcb11fb5	-	Downloaded File	529.34 KB	text/rtf	-	CLEAN
80dbc115aafd513275851f917754af04a502a21273e4ee8b23fd11a8d6ca16ef	-	Downloaded File	351 bytes	application/json	-	CLEAN
9e398ae77dc73d393d62430aa28c05cf1973f37ccc1ae0b803896cdd7d19cbc0	-	Extracted File	7.19 KB	image/png	-	CLEAN
e74ef457af291610afb6c315b80bcb6f9861a7a411f3f744fa3faf1273d4df9f	C:\Users\KEECFM~1\AppData\Local\Temp\aut7B6.tmp	Dropped File	78.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
90f3b22bec26df402a0ab8fef7df8fbf79e5d74f9ed0f25943d1d5e7e2fe020b	C:\Users\KEECFM~1\AppData\Local\Temp\Okeghem	Dropped File	95.50 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6369e06e6a3e2495442d98898cfa8d51fcb272b4a54f8818e5a5804f0f029c05	C:\Users\KEECFM~1\AppData\Local\Temp\aut90E.tmp	Dropped File	9.65 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
423a70f3606d0d0f96d2f932614a2125dad3ff3170e2f04ff4bc3cef82bd57cd	C:\Users\KEECFM~1\AppData\Local\Temp\brontothere	Dropped File	28.08 KB	text/plain	Access, Create, Read, Write	CLEAN
1c8bfa0eb3e36e7d474678079efb5755ea35113cc810262af79ac07c4964df00	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp16F4.tmp	Dropped File	20.06 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Access, Create, Delete, Read, Write	CLEAN
35d3caededcd7914d356eda934b67ae80aa639113dd3fe82ad710747a1c7d3f0	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1762.tmp	Dropped File	84.11 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d0ce547483680a7c0d261210dfce8e633fdcdbe86cd6cc0f7fecf0e0d9cac1c4	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1782.tmp	Dropped File	91.94 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
12c48c1e1ec4c69b91abeb7ede43d9e33eb8770ae1cb4c16d12f4fdd057edd69	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17A2.tmp	Dropped File	82.58 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
6a0ea337ed0e2ea66ebde9aff30194f21e6d29580a5d7b9d557d067d67e00327	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17D2.tmp	Dropped File	83.95 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN
9b512d1431b193b7754be257776d63fd1cf8387bd3a6998fc5614372b423c99e	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17F2.tmp	Dropped File	28.80 KB	application/zip	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\bd776414632dd90a5d459f240e2094566e70554d86ecb4bbb2a2914015426f09.doc	Accessed File, Sample File	Access	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp16F4.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c\wordpad[1].exe	Downloaded File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.exe	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\aut7B6.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\Okeghem	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\aut90E.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\brontothere	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
c:\users\keecfmwgj\appdata\local\temp\cab77f5.tmp	Downloaded File, Extracted File	-	CLEAN
c:\users\keecfmwgj\appdata\local\temp\tar77f6.tmp	Dropped File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1762.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp1782.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17A2.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17D2.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17F2.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
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\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

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://covid19help[.]top/notori.doc	Contacted, Extracted	172.67.175.222, 104.21.83.128	-	HEAD, GET	MALICIOUS
hxxp://185[.]38[.]142[.]10:7474	Contacted, Extracted	185.38.142.10	Portugal	POST	MALICIOUS
hxxps://covid19help[.]top/wordpad.exe	Contacted, Extracted	172.67.175.222, 104.21.83.128	-	GET	MALICIOUS
hxxps://covid19help[.]top	Contacted, Extracted	172.67.175.222, 104.21.83.128	-	OPTIONS	MALICIOUS
hxxps://api[.]ip[.]sb/geoip	Contacted, Extracted	104.26.12.31, 172.67.75.172, 104.26.13.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
covid19help[.]top	172.67.175.222, 104.21.83.128	-	TCP, DNS, HTTPS	MALICIOUS
api[.]ip[.]sb	104.26.12.31, 172.67.75.172, 104.26.13.31	-	TCP, DNS, HTTPS	CLEAN
api[.]ip[.]sb[.]cdn[.]cloudflare[.]net	104.26.12.31, 172.67.75.172, 104.26.13.31	-	TCP, DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.38.142.10	-	Portugal	HTTP, TCP	MALICIOUS
104.26.13.31	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net, api[.]ip[.]sb	-	TCP, DNS, HTTPS	MALICIOUS
104.21.83.128	covid19help[.]top	-	TCP, DNS, HTTPS	CLEAN
172.67.175.222	covid19help[.]top	-	DNS	CLEAN
172.67.75.172	api[.]ip[.]sb[.]cdn[.]cloudflare[.]net, api[.]ip[.]sb	-	DNS	CLEAN
104.26.12.31	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	notorious69281.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons	read, access	notorious69281.exe	CLEAN
HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt	access	notorious69281.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	read, access	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	read, access	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	read, access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	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	read, access	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	read, access	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	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	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	read, access	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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	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	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	regsvcs.exe	CLEAN
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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	regsvcs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayVersion	read, access	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	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	regsvcs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	read, access	regsvcs.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
notorious69281.exe	"C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.exe"	MALICIOUS
eqnedt32.exe	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	SUSPICIOUS
regsvcs.exe	"C:\Users\kEecfMwgj\AppData\Roaming\notorious69281.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_SOAPCommunication	RedLine Stealer SOAP response	-	-	Spyware	5/5
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

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