MALICIOUS

Classifications: Spyware | Downloader | Injector

Threat Names: Hancitor | Mal/Generic-S | Mal/HTMLGen-A | VB:Trojan.Valyria.4987 | Gen:Variant.Zusy.391704 | Gen:Variant.Doina.7190

Verdict Reason: -

Sample Type	**Word Document**
File Name	**0706_1643278086845.doc**
ID	#2469023
MD5	62b2fb380e72bc0fb12a65b2798d83e3
SHA1	d0804a455c0191585f18b9dc3e964117786858e3
SHA256	e431a1bb2efcf6000f5bac4e19673d6deb9de7997dba5f65bae7779cd19e5caf
File Size	901.00 KB
Report Created	2021-07-07 06:46 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (31 rules, 53 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• Rule "Hancitor" from ruleset "Malware" has matched on a memory dump for (process #4) rundll32.exe. • Rule "Shellcode_Loader" from ruleset "Generic" has matched on a memory dump for (process #4) rundll32.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Pidgin, WinSCP, Ethereum, Exodus Cryptocurrency Wallet.			
4/5	Defense Evasion	Sends control codes to connected devices	1	-
	• (Process #5) svchost.exe controls device "C:\Users\kEecfMwgj\Local Settings\Application Data" through API DeviceIOControl.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #4) rundll32.exe modifies memory of (process #5) svchost.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #4) rundll32.exe alters context of (process #5) svchost.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels a file which was only downloaded to memory as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "hosouggs.com/8/forum.php" which was contacted by (process #4) rundll32.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "kubantr0.ru/7gfdg5egds.exe" which was contacted by (process #4) rundll32.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "mancause.ru/8/forum.php" which was contacted by (process #4) rundll32.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Resolves known malicious domain	2	-
	• Reputation analysis labels the resolved domain "kubantr0.ru" as "Mal/HTMLGen-A". • Reputation analysis labels the resolved domain "pospvisis.com" as "Mal/HTMLGen-A".			
4/5	Heuristics	Document tries to trick users into running macros	1	-
	• Extracted text from an image embedded in C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc suggests enabling macros.			
4/5	Network Connection	Performs DNS request	1	-
	• (Process #5) svchost.exe resolves host name "pospvisis.com" to IP "92.62.115.177".			
4/5	Network Connection	Connects to remote host	1	-
	• (Process #5) svchost.exe opens an outgoing TCP connection to host "92.62.115.177:80".			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #4) rundll32.exe downloads executable via http from kubantr0.ru/7gfdg5egds.exe.			
4/5	Network Connection	Attempts to connect through HTTP	5	-

Score	Category	Operation	Count	Classification
	• (Process #4) rundll32.exe connects to "api.ipify.org/". • (Process #4) rundll32.exe connects to "mancause.ru/8/forum.php". • (Process #4) rundll32.exe connects to "kubantr0.ru/7gfdg5egds.exe". • (Process #5) svchost.exe connects to "http://api.ipify.org/?format=xml". • (Process #4) rundll32.exe failed to connect to "hosouggs.com/8/forum.php".			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #4) rundll32.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	7	-
	• Built-in AV detected a embedded file as "Gen:Variant.Zusy.391704". • Built-in AV detected the sample itself as "VB:Trojan.Valyria.4987". • Built-in AV detected the sample itself as "Gen:Variant.Zusy.391704". • Built-in AV detected a downloaded file as "Gen:Variant.Doina.7190". • Built-in AV detected "Gen:Variant.Doina.7190" in the PCAP of the analysis. • Built-in AV detected "Gen:Variant.Doina.7190" in the response data of URL "kubantr0.ru/7gfdg5egds.exe". • Built-in AV detected the dropped file c:\users\keecfmwgj\appdata\local\temp\nimb.dll as "Gen:Variant.Zusy.391704".			
3/5	Discovery	Enumerates running processes	2	-
	• (Process #4) rundll32.exe enumerates running processes. • (Process #5) svchost.exe enumerates running processes.			
3/5	Discovery	Reads system data	1	-
	• (Process #5) svchost.exe reads the cryptographic machine GUID from registry.			
3/5	Data Collection	Reads cryptocurrency wallet locations	2	-
	• (Process #5) svchost.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet". • (Process #5) svchost.exe tries to read the cryptocurrency wallet "Ethereum" for "ETH".			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #4) rundll32.exe has a thread which sleeps more than 5 minutes.			
3/5	Discovery	Checks external IP address	2	-
	• (Process #4) rundll32.exe checks external IP by asking IP info service at "api.ipify.org/". • (Process #5) svchost.exe checks external IP by asking IP info service at "http://api.ipify.org/?format=xml".			
3/5	Heuristics	Contains suspicious embedded files	1	-
	• c:\users\keecfmwgj\desktop\0706_1643278086845.doc contains an embedded file of a suspicious type.			
3/5	YARA	Suspicious content matched by YARA rules	2	-
	• Rule "Document_Contains_Embedded_PE_File" from ruleset "Malicious-Documents" has matched on a embedded file. • Rule "Document_Contains_Embedded_PE_File" from ruleset "Malicious-Documents" has matched on the sample itself.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #4) rundll32.exe reads the network adapters' addresses by API.			
2/5	Discovery	Possibly does reconnaissance	4	-

Score	Category	Operation	Count	Classification
	• (Process #5) svchost.exe tries to gather information about application "Monero" by registry. • (Process #5) svchost.exe tries to gather information about application "WinSCP" by registry. • (Process #5) svchost.exe tries to gather information about application "FileZilla" by file. • (Process #5) svchost.exe tries to gather information about application "Pidgin" by file.			
2/5	Data Collection	Reads sensitive application data	2	-
	• (Process #5) svchost.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #5) svchost.exe tries to read sensitive data of application "Pidgin" by file.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
2/5	Execution	Drops PE file	1	-
	• Drops file c:\users\keecfmwgj\appdata\local\temp\nimb.dll.			
1/5	Mutex	Creates mutex	1	-
	• (Process #5) svchost.exe creates mutex with name "serhershesrhsfesrf".			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
1/5	Heuristics	Contains known suspicious class identifier	1	-
	• Office document contains known suspicious class identifier for ActiveX object "Package" (CLSID {0003000C-0000-0000-C000-000000000046}).			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			

Mitre ATT&CK Matrix

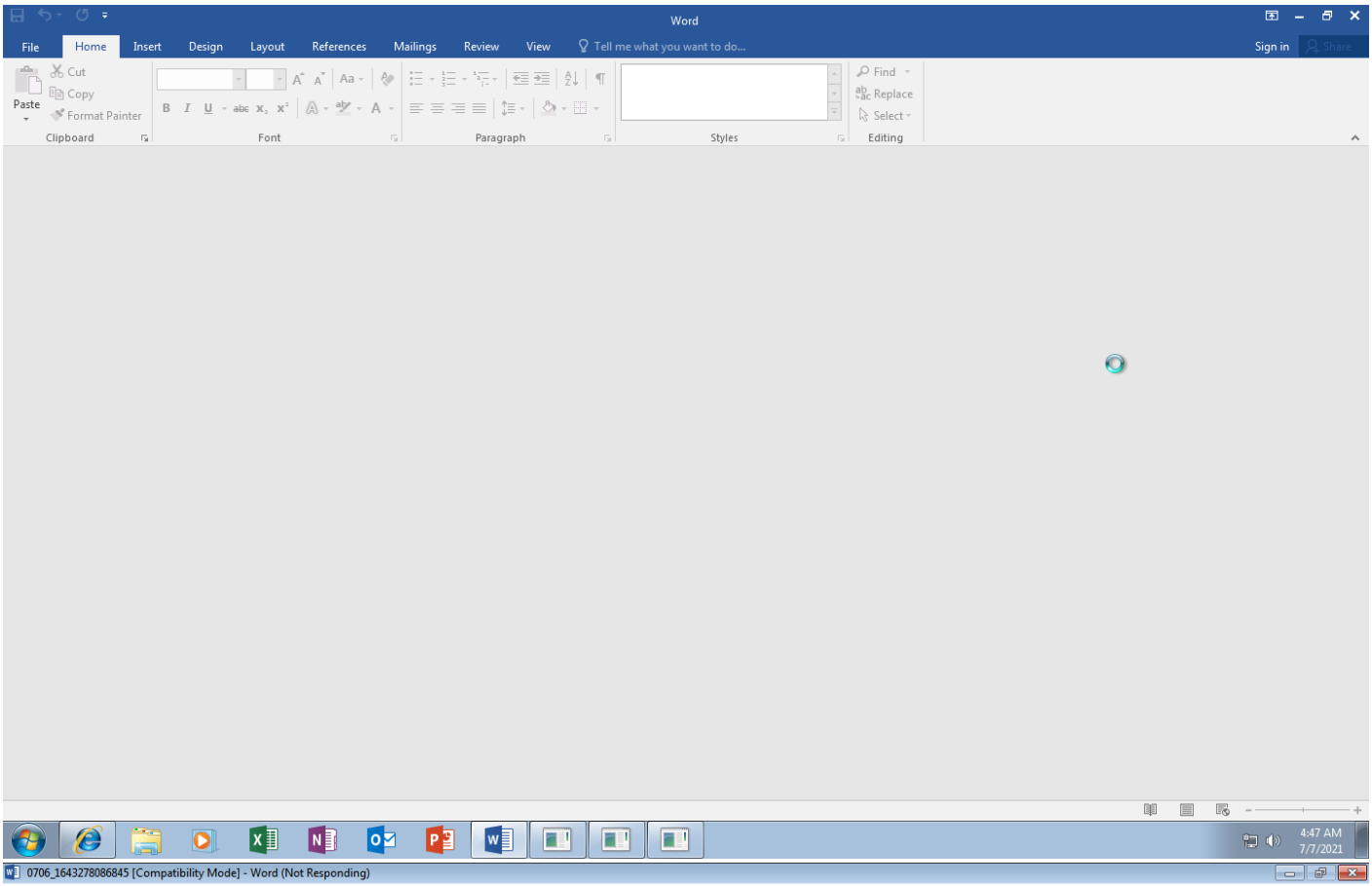
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
					#T1214 Credentials in Registry	#T1057 Process Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
						#T1082 System Information Discovery					
						#T1012 Query Registry					
						#T1083 File and Directory Discovery					

Sample Information

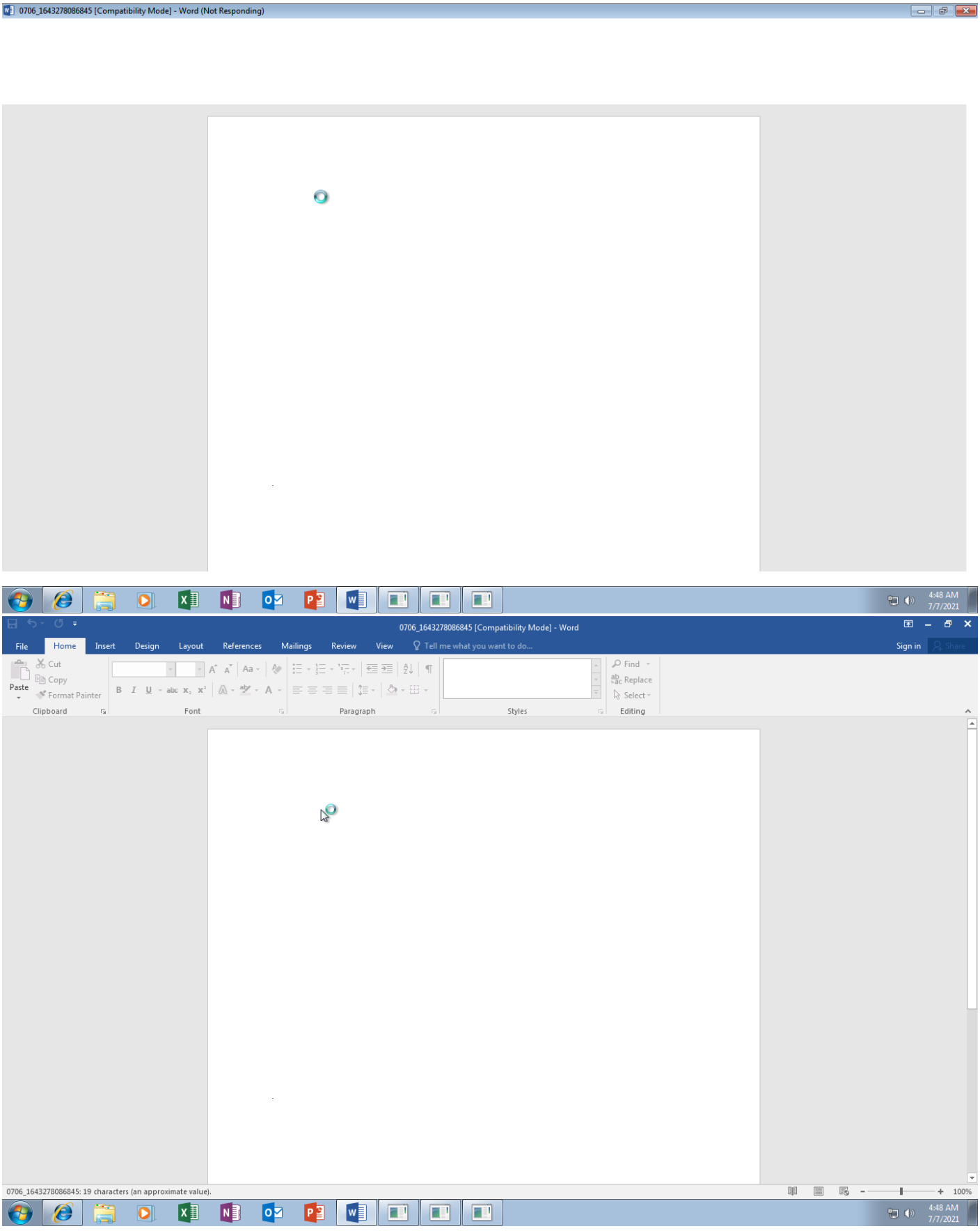
ID	#2469023
MD5	62b2fb380e72bc0fb12a65b2798d83e3
SHA1	d0804a455c0191585f18b9dc3e964117786858e3
SHA256	e431a1bb2efcf6000f5bac4e19673d6deb9de7997dba5f65bae7779cd19e5caf
SSDeep	24576:XEIZ4wA74D4SQKxZcy8gthDWP+pwmUI+:X+wJD4QZh/qWamUI+
File Name	0706_1643278086845.doc
File Size	901.00 KB
Sample Type	Word Document
Has Macros	✓

Analysis Information

Creation Time	2021-07-07 06:46 (UTC+2)
Analysis Duration	00:03:52
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
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	5
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	6


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
4:47 AM
7/7/2021
0706_1643278086845 [Compatibility Mode] - Word (Not Responding)


4:47 AM
7/7/2021



Screenshots truncated

NETWORK

General

10.33 KB total sent

277.81 KB total received

1 ports 80

6 contacted IP addresses

0 URLs extracted

8 files downloaded

0 malicious hosts detected

DNS

6 DNS requests for 5 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

5 URLs contacted, 4 servers

5 sessions, 3.45 KB sent, 277.11 KB received

HTTP Requests

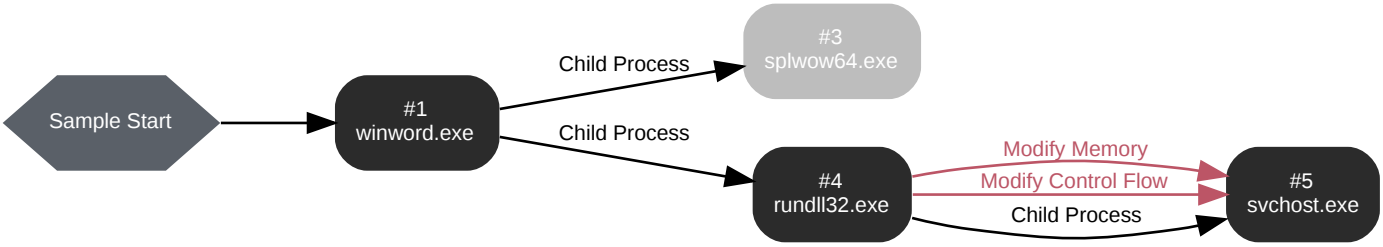
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	api.ipify.org/	-	-		0 bytes	NA
POST	mancause.ru/8/forum.php	-	-		0 bytes	NA
GET	kubantr0.ru/7gfdg5egds.exe	-	-		0 bytes	NA
GET	http://api.ipify.org/?format=xml	-	-		0 bytes	NA
POST	hosouggs.com/8/forum.php	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	NoError	54.235.88.121, 54.225.245.108, 54.225.78.40, 54.235.190.106, 50.16.216.118, 23.21.173.155, 54.235.175.90, 23.21.136.132	nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	NA
A	hosouggs.com	NoError	135.125.241.4		NA
A	mancause.ru	NoError	77.222.42.67		NA
A	kubantr0.ru	NoError	8.211.241.0		NA
A	pospvisis.com	NoError	92.62.115.177		NA

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90321, Reason: Analysis Target
Unmonitor End Time	End Time: 288586, Reason: Terminated
Monitor duration	198.26s
Return Code	0
PID	3536
Parent PID	876
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✗
-	291.50 KB	b7c0e4ca9f7e6e177ff5dc3631cb16f7fcfddd49b1536dcc9db68b0ec472dea9	✗
-	108.45 KB	f68015b98d46b026dccb4e5260d5f983362aac8dd9a26e18cf02ac914cee79d7	✗

Host Behavior

Type	Count
Module	8
Keyboard	16
Process	1

Process #3: splwow64.exe

ID	3
File Name	c:\windows\splwow64.exe
Command Line	C:\Windows\splwow64.exe 8192
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 146940, Reason: Child Process
Unmonitor End Time	End Time: 312190, Reason: Terminated by Timeout
Monitor duration	165.25s
Return Code	Unknown
PID	3804
Parent PID	3536
Bitness	64 Bit

Process #4: rundll32.exe

ID	4
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\SysWOW64\rundll32.exe c:\users\keecfmwgj\appdata\roaming\microsoft\templates\niberius.dll,UBISYAYMQSE
Initial Working Directory	C:\Users\kEecfMwgj\Documents\
Monitor Start Time	Start Time: 163891, Reason: Child Process
Unmonitor End Time	End Time: 312190, Reason: Terminated by Timeout
Monitor duration	148.30s
Return Code	Unknown
PID	3844
Parent PID	3536
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	118
Environment	3
File	3
System	29
Process	96
-	3
-	3

Network Behavior

Type	Count
HTTP	8
TCP	4

Process #5: svchost.exe

ID	5
File Name	c:\windows\syswow64\svchost.exe
Command Line	C:\Windows\SysWOW64\svchost.exe
Initial Working Directory	C:\Users\kEecfMwgj\Documents\
Monitor Start Time	Start Time: 218723, Reason: Child Process
Unmonitor End Time	End Time: 222988, Reason: Terminated
Monitor duration	4.26s
Return Code	0
PID	3956
Parent PID	3844
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\windows\syswow64\rundll32.exe	0xf08	0x400000(4194304)	0x48000	✓	1
Modify Memory	#4: c:\windows\syswow64\rundll32.exe	0xf08	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#4: c:\windows\syswow64\rundll32.exe	0xf08 / 0xf78		-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	12 bytes	fd41cd2f48623ceb8d6d4fa774c80efa5c3f22c94bfd7a7c59543772b585d9a1	✗

Host Behavior

Type	Count
System	5
Module	12
Mutex	1
File	27
Environment	13
Registry	230
-	1
Keyboard	1
Process	99

Network Behavior

Type	Count
HTTP	1
DNS	2
TCP	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e431a1bb2efcf6000f5bac4e19673d6deb9de7997dba5f65bae7779cd19e5caf	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	Sample File	901.00 KB	application/msword	-	MALICIOUS
b7c0e4ca9f7e6e177ff5dc3631cb16f7fcfddd49b1536dcc9db68b0ec472dea9	c:\users\keecfmwgj\appdata\roaming\microsoft\templates\niberius.dll, c:\users\keecfmwgj\appdata\local\temp\nimb.dll	Dropped File	291.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
dee4bb7d46bbbec6c01dc41349cb8826b27be9a0dcf39816ca8bd6e0a39c2019	-	Downloaded File	266.51 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
fc6f4f07399d011cd55104e6660dcf7d03cfcc2c6897cad9dcd6194625bfe593	nimb.dll	Embedded File	291.69 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
f68015b98d46b026dccb4e5260d5f983362aac8dd9a26e18cf02ac914cee79d7	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	108.45 KB	application/octet-stream	-	CLEAN
fd41cd2f48623ceb8d6d4fa774c80efa5c3f22c94bfd7a7c59543772b585d9a1	C:\ProgramData\kaosdma.txt	Downloaded File	12 bytes	text/plain	Read, Access, Create	CLEAN
f399cb468bfa6115311c67fb0fd53982ced5cfae574206f5a3963f6f069949b3	-	Downloaded File	121 bytes	text/plain	-	CLEAN
194bdef778576fda197959ff7b20c5bf664e91ba45c7a740b799f44d571ec868	-	Downloaded File	56 bytes	text/plain	-	CLEAN
3b7fd3df4b1eb87cf3805d83da48d2598a4ada8da008344c3fdd5dae1ab9e123	-	Downloaded File	12 bytes	text/plain	-	CLEAN
7446351edf854eae84c85b339c8e42ece360f3d3f617bc33374db7606fe2e28a	-	Downloaded File	12 bytes	text/plain	-	CLEAN
2fafb70f3c46323eb35d313ccd79b13e53933687da5a9d2733ab05741bc72660	-	Downloaded File	12 bytes	text/plain	-	CLEAN
fefa19e96290545659421d6f83c073eea44de15eaa61ce0814e0a4e5e17827fe	-	Downloaded File	12 bytes	text/plain	-	CLEAN
8f813322cdca617967768c900b3982dd0ebd753a9292a2ecffb8a966f5fff1df	0.PNG	Embedded File	551.17 KB	image/png	-	CLEAN
06b913dd62dbc9b1ae00ba33dd5bcd87e5efd5e2b56ebf7e2ea9fed37a91d5f6	2.EMF	Embedded File	4.86 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\rundll32.exe	Accessed File	Access	CLEAN
C:\ProgramData	Accessed File	Access, Create	CLEAN
C:\ProgramData\kaosdma.txt	Downloaded File	Read, Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Local Settings\Application Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Bitcoin\wallets	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Exodus\exodus.wallet	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\atomic\Local Storage\leveldb\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Electrum\wallets	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Zcash	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\bytecoin	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Ethereum\keystore	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Discord\Local Storage	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.purple\accounts.xml	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://mancause.ru/8/forum.php	-	77.222.42.67	-	POST	MALICIOUS
http://kubantr0.ru/7gfdg5egds.exe	-	8.211.241.0	-	GET	MALICIOUS
http://hosouggs.com/8/forum.php	-	135.125.241.4	-	POST	MALICIOUS
http://api.ipify.org	-	54.235.88.121	-	GET	CLEAN
http://api.ipify.org/?format=xml	-	54.235.88.121	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
kubantr0.ru	8.211.241.0	-	DNS, HTTP	MALICIOUS
pospvisis.com	92.62.115.177	-	DNS	MALICIOUS
api.ipify.org	54.235.175.90, 54.225.78.40, 50.16.216.118, 23.21.173.155, 23.21.136.132, 54.225.245.108, 54.235.88.121, 54.235.190.106	-	DNS, HTTP	CLEAN
nagano-19599.herokussl.com	54.235.175.90, 54.225.78.40, 50.16.216.118, 23.21.173.155, 23.21.136.132, 54.225.245.108, 54.235.88.121, 54.235.190.106	-	DNS	CLEAN
elb097307-934924932.us-east-1.elb.amazonaws.com	54.235.175.90, 54.225.78.40, 50.16.216.118, 23.21.173.155, 23.21.136.132, 54.225.245.108, 54.235.88.121, 54.235.190.106	-	DNS	CLEAN
hosouggs.com	135.125.241.4	-	DNS, HTTP	CLEAN
mancause.ru	77.222.42.67	-	DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
92.62.115.177	pospvisis.com	Russia	TCP, DNS	MALICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
135.125.241.4	hosouggs.com	France	TCP, DNS, HTTP	CLEAN
54.235.88.121	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	TCP, DNS, HTTP	CLEAN
8.211.241.0	kubantr0.ru	United Kingdom	TCP, DNS, HTTP	CLEAN
77.222.42.67	mancause.ru	Russia	TCP, DNS, HTTP	CLEAN
54.225.245.108	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
54.225.78.40	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
54.235.190.106	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
50.16.216.118	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
23.21.173.155	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
54.235.175.90	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
23.21.136.132	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
serhershesrhsfesrf	access	svchost.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MachineGuid	read, access	svchost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\monero-project\monero-core	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Litecoin\Litecoin-Qt	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Dash\Dash-Qt	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	svchost.exe	CLEAN

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

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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayVersion	read, access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	svchost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Valve\Steam	access	svchost.exe	CLEAN

Process

Process Name	Commandline	Verdict
rundll32.exe	C:\Windows\SysWOW64\rundll32.exe c:\users\keecfmwgj\appdata\roaming\microsoft\templates\niberius.dll,UBISYAYMQSE	SUSPICIOUS
svchost.exe	C:\Windows\SysWOW64\svchost.exe	SUSPICIOUS
winword.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n	CLEAN
splwow64.exe	C:\Windows\splwow64.exe 8192	CLEAN

YARA / AV

YARA (6)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Hancitor	Hancitor Downloader	Memory Dump	-	Downloader	5/5
Malware	Hancitor	Hancitor Downloader	Memory Dump	-	Downloader	5/5
Generic	Shellcode_Loader	Loader shellcode used by multiple malware families	Memory Dump	-	-	4/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	-	3/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	-	3/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Embedded File	nimb.dll	-	3/5

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	VB:Trojan.Valyria.4987	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	MALICIOUS
Embedded File	Gen:Variant.Zusy.391704	nimb.dll	MALICIOUS
Downloaded File	Gen:Variant.Doina.7190	-	MALICIOUS
Web Request	Gen:Variant.Doina.7190	-	MALICIOUS
Dropped File	Gen:Variant.Zusy.391704	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
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

Analyzer Information

Analyzer Version	4.2.2
Dynamic Engine Version	4.2.2 / 06/07/2021 03:43
Static Engine Version	4.2.2.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-07-07 02:05:47+00:00
AV Exceptions Version	4.2.2.13 / 2021-06-02 18:07:39
VTI Ruleset Version	4.2.2.28 / 2021-07-02 15:42:52
YARA Built-in Ruleset Version	4.2.2.18
Link Detonation Heuristics Version	-
Signature Trust Store Version	4.2.2.13 / 2021-06-02 18:07:39
Analysis Report Layout Version	10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed