MALICIOUS

Classifications: Ransomware | Injector | Downloader

Threat Names: WastedLocker | Mal/HTMLGen-A | Gen:Variant.Jacard.222844 | Trojan.GenericKD.45628116 | Generic.Mint.Zamg.3.10EEB7F3 | Gen:Variant.Razy.832814

Verdict Reason: -

Sample Type	**Word Document**
Sample Name	**0524_4109399728218.doc**
ID	#2284404
MD5	14f4c470c207e22c3b0a4efa7b4200e8
SHA1	21180195396580a9ade32b589490cf3bc94d3b5b
SHA256	0b22278ddb598d63f07eb983bcf307e0852cd3005c5bc15d4a4f26455562c8ec
File Size	1304.50 KB
Report Created	2021-05-25 06:42 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (26 rules, 47 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Ransomware
	• Rule "WastedLockerShellcode" from ruleset "Ransomware" has matched on a memory dump for (process #4) rundll32.exe.			
5/5	Injection	Writes into the memory of another running process	1	Injector
	• (Process #4) rundll32.exe modifies memory of (process #5) svchost.exe.			
5/5	Injection	Modifies control flow of another process	1	-
	• (Process #4) rundll32.exe alters context of (process #5) svchost.exe.			
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	8	-
	• Built-in AV detected the embedded file jax.k as "Gen:Variant.Jacard.222844". • Built-in AV detected the sample itself as "Gen:Variant.Jacard.222844". • Built-in AV detected a downloaded file as "Trojan.GenericKD.45628116". • Built-in AV detected "Trojan.GenericKD.45628116" in the PCAP of the analysis. • Built-in AV detected "Trojan.GenericKD.45628116" in the response data of URL "gromber6.ru/6hjusfd8.exe". • Built-in AV detected the dropped file c:\users\keecfmwgj\appdata\local\temp\jax.k as "Gen:Variant.Jacard.222844". • Built-in AV detected a memory dump of (process #4) rundll32.exe as "Generic.Mint.Zamg.3.10EEB7F3". • Built-in AV detected a memory dump of (process #4) rundll32.exe as "Gen:Variant.Razy.832814".			
4/5	Reputation	Known malicious file	1	-
	• A file which was only downloaded to memory is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "euvereginumet.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 "euvereginumet.ru" as "Mal/HTMLGen-A". • Reputation analysis labels the resolved domain "sweyblidian.com" as "Mal/HTMLGen-A".			
4/5	Network Connection	Performs DNS request	1	-
	• (Process #5) svchost.exe resolves host name "sweyblidian.com" to IP "185.100.65.29".			
4/5	Network Connection	Connects to remote host	1	-
	• (Process #5) svchost.exe opens an outgoing TCP connection to host "185.100.65.29:80".			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #4) rundll32.exe downloads executable via http from gromber6.ru/6hjusfd8.exe.			
4/5	Network Connection	Attempts to connect through HTTP	5	-

• (Process #4) rundll32.exe connects to "api.ipify.org/".
• (Process #4) rundll32.exe connects to "euvereginumet.ru/8/forum.php".
• (Process #4) rundll32.exe connects to "gromber6.ru/6hjusfd8.exe".
• (Process #5) svchost.exe connects to "http://api.ipify.org/?format=xml".
• (Process #4) rundll32.exe failed to connect to "thowerteigime.com/8/forum.php".

3/5	Discovery	Enumerates running processes	1	-

• (Process #4) rundll32.exe enumerates running processes.

3/5	Anti Analysis	Delays execution	1	-

• (Process #4) rundll32.exe has a thread which sleeps more than 5 minutes.

3/5	YARA	Suspicious content matched by YARA rules	2	-

• Rule "Document_Contains_Embedded_PE_File" from ruleset "Malicious-Documents" has matched on the embedded file "jax.k".
• Rule "Document_Contains_Embedded_PE_File" from ruleset "Malicious-Documents" has matched on the sample itself.

3/5	Heuristics	Contains suspicious embedded files	1	-

• c:\users\keecfmwgj\desktop\0524_4109399728218.doc contains an embedded file of a suspicious type.

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".

2/5	Discovery	Reads network adapter information	1	-

• (Process #4) rundll32.exe reads the network adapters' addresses by API.

2/5	Reputation	Contacts known suspicious URL	2	-

• (Process #4) rundll32.exe contacted known malicious URL "gromber6.ru/6hjusfd8.exe".
• Contacted URL "gromber6.ru" is a known suspicious URL.

2/5	Execution	Office macro uses an execute function	1	-

• Office macro uses the shell function.

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\jax.k.

1/5	Mutex	Creates mutex	7	-

• (Process #5) svchost.exe creates mutex with name "hrth".
• (Process #5) svchost.exe creates mutex with name "o;jtfytyjftyjftyjftyj;ijo;".
• (Process #5) svchost.exe creates mutex with name "ijlhlkwaftyjftyjftjftyh;joi;i".
• (Process #5) svchost.exe creates mutex with name "ah;waeh;jftyjftyjfiftfdgaf".
• (Process #5) svchost.exe creates mutex with name "hotyjftyj;afdh".
• (Process #5) svchost.exe creates mutex with name "whftyjftyjftyjtfyjtfyjtfyj;ijo;h".
• (Process #5) svchost.exe creates mutex with name "whoareyoutellmeandilltellwhoyou".

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.			

Remarks

ⓘ **Anti-Sleep Triggered (0x0200000E):** The overall sleep time of all monitored processes was truncated from "16 minutes" to "2 minutes, 40 seconds" to reveal dormant functionality.

Mitre ATT&CK Matrix

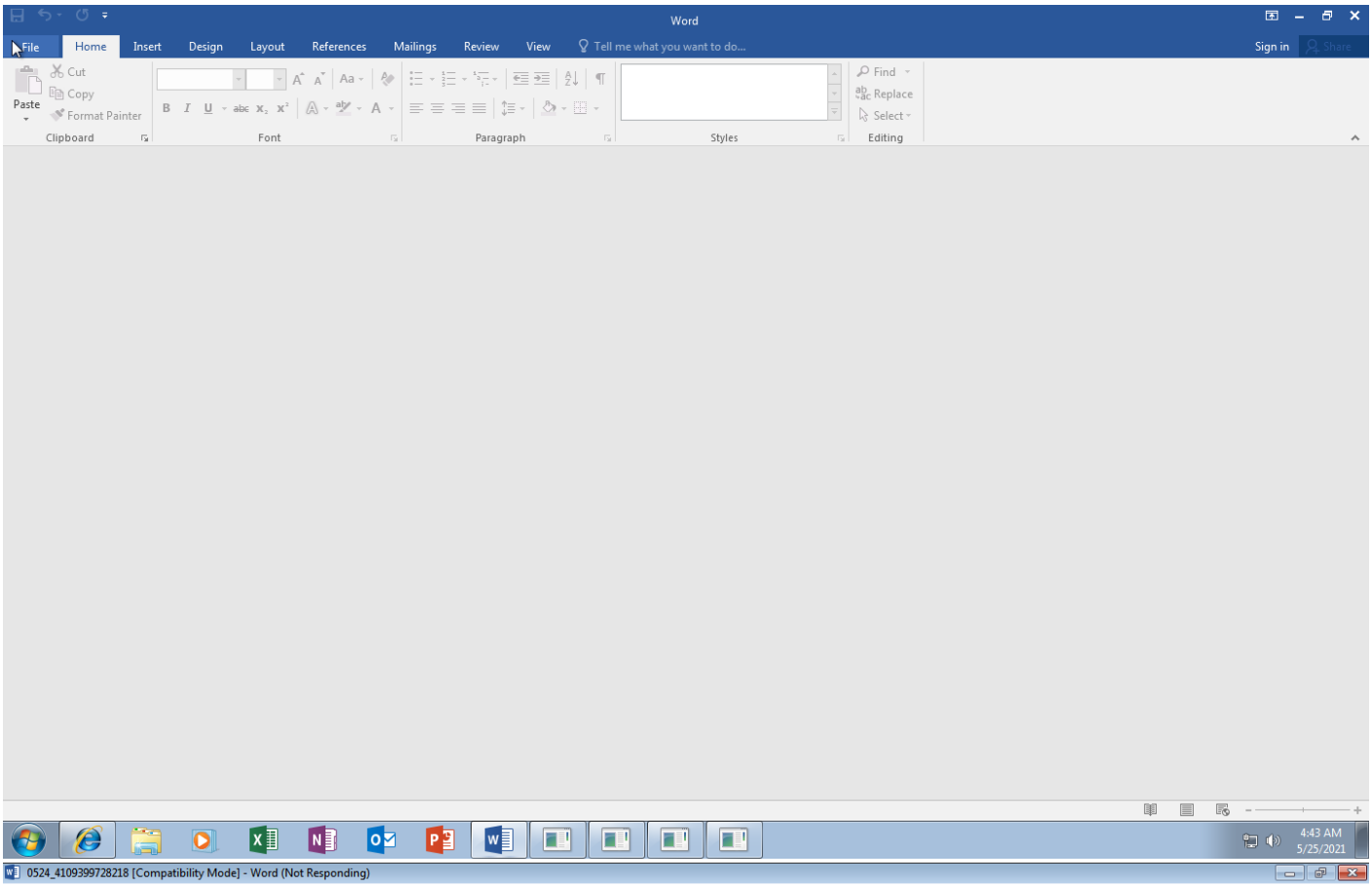
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	-	-	#T1016 System Network Configuration Discovery	-	-	-	-	-
-	-	-	-	-	-	#T1057 Process Discovery	-	-	-	-	-
-	#T1064 Scripting	-	-	#T1064 Scripting	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	#T1071 Standard Application Layer Protocol	-	-
-	-	-	-	-	-	-	#T1105 Remote File Copy	-	#T1105 Remote File Copy	-	-

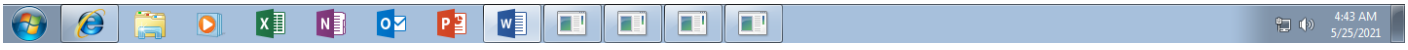
Sample Information

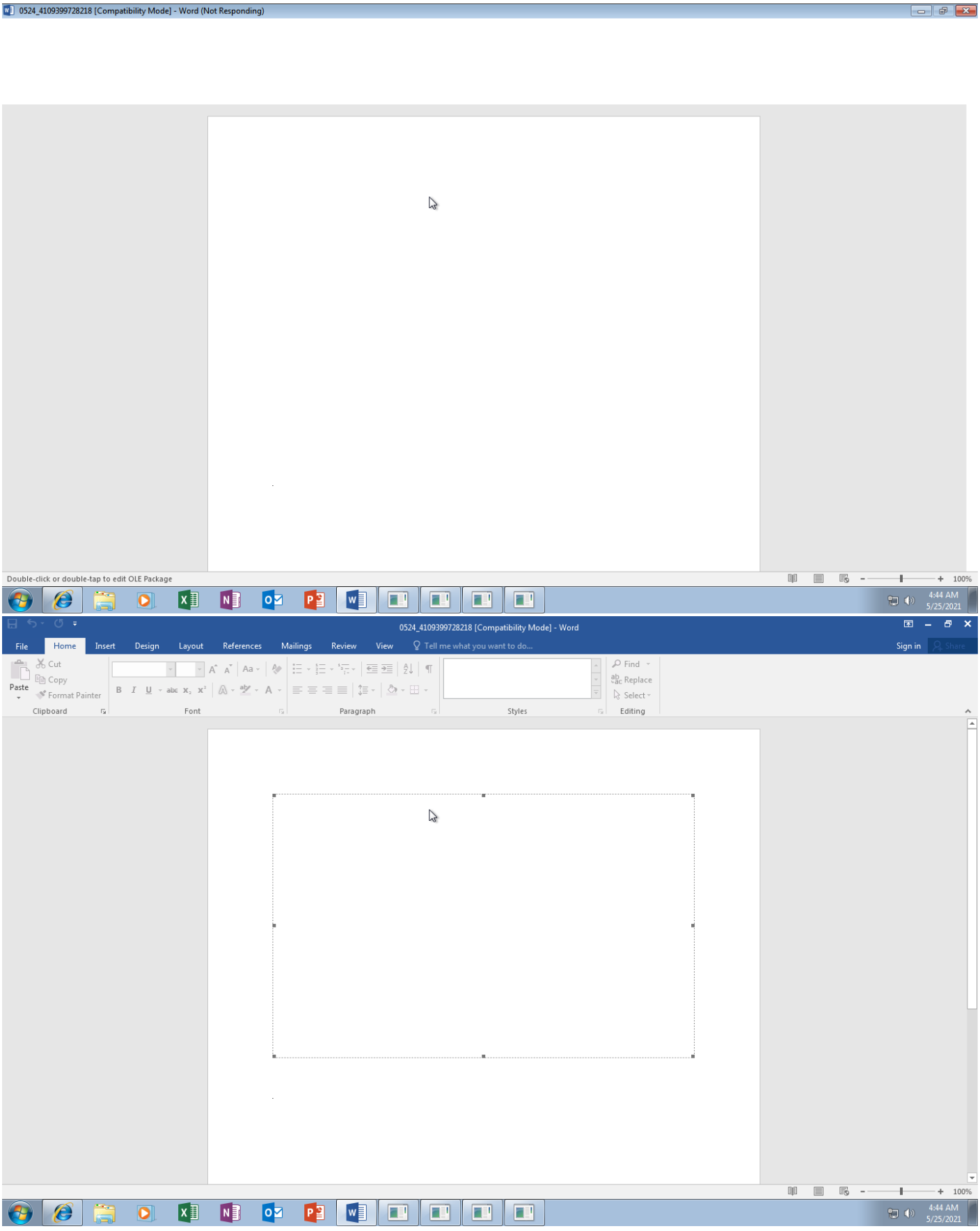
ID	6156733
MD5	14f4c470c207e22c3b0a4efa7b4200e8
SHA1	21180195396580a9ade32b589490cf3bc94d3b5b
SHA256	0b22278ddb598d63f07eb983bcf307e0852cd3005c5bc15d4a4f26455562c8ec
SSDeep	24576:nEIjrPUaphvGvGUZ93/semhXp7AsWIKHaY8k5faaboEy6r8zz1:n/jhvGvGU93097AFIKbv0WY/1
ImpHash	
Filename	0524_4109399728218.doc
File Size	1304.50 KB
Sample Type	Word Document
Has Macros	✓

Analysis Information

Creation Time	2021-05-25 06:42 (UTC+2)
Analysis Duration	00:04:09
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successfull	False
Reputation Analysis 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	7
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	4


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
4:43 AM
5/25/2021
0524_4109399728218 [Compatibility Mode] - Word (Not Responding)


4:43 AM
5/25/2021



Screenshots trunkated.

NETWORK

General

4.85 KB total sent

283.67 KB total received

1 ports 80

6 contacted IP addresses

0 URLs extracted

11 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, 4.85 KB sent, 278.79 KB recivied

DNS Requests

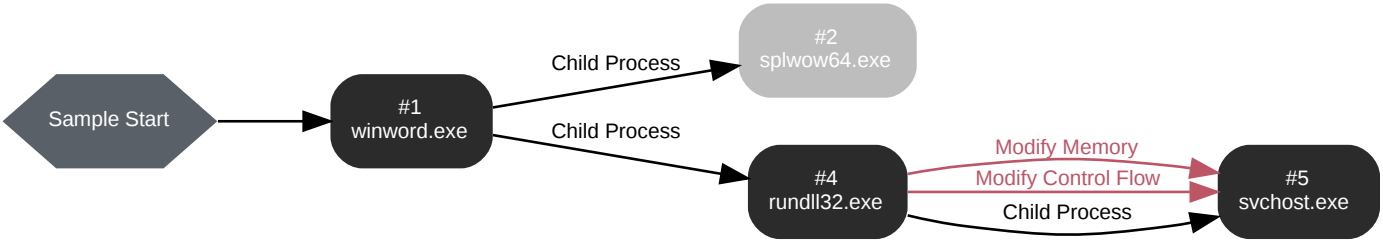
Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.ipify.org, nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	NoError	54.225.165.85, 54.235.175.90, 54.225.144.221, 50.19.252.36, 23.21.48.44, 107.22.233.72, 23.21.76.253, 50.19.96.218	nagano-19599.herokussl.com, elb097307-934924932.us-east-1.elb.amazonaws.com	N/A
A	thowerteigime.com	NoError	90.156.143.87		N/A
A	euvereginumet.ru	NoError	77.222.52.246		N/A
A	gromber6.ru	NoError	8.211.5.232		N/A
A	sweyblidian.com	NoError	185.100.65.29		N/A

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	api.ipify.org/				0 bytes	N/A
POST	euvereginumet.ru/8/forum.php				0 bytes	N/A
GET	gromber6.ru/6hjusfd8.exe				0 bytes	N/A
GET	http://api.ipify.org/?format=xml				0 bytes	N/A
POST	thowerteigime.com/8/forum.php				0 bytes	N/A

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
Filename	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: 63980, Reason: Analysis Target
Unmonitor End Time	End Time: 272548, Reason: Terminated
Monitor Duration	208.57s
Return Code	0
PID	3712
Parent PID	1112
Bitness	32 Bit

Dropped Files (3)

Filename	File Size	SHA256	YARA Match
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✕
-	704.00 KB	2a8b737a4752060a308c4312b7c0cf6c05cde5b370906286dea9cdd36f5aa613	✕
-	108.45 KB	9f0327fb7d2b24169685dc794022dcb42f351a2c277c0c6360810c268196ac67	✕

Host Behavior

Type	Count
Module	8
Keyboard	11
COM	2
Process	1

Process #2: splwow64.exe

ID	2
Filename	c:\windows\splwow64.exe
Command Line	C:\Windows\splwow64.exe 8192
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 106690, Reason: Child Process
Unmonitor End Time	End Time: 320549, Reason: Terminated by Timeout
Monitor Duration	213.86s
Return Code	Unknown
PID	3964
Parent PID	3712
Bitness	64 Bit

Process #4: rundll32.exe

ID	4
Filename	c:\windows\syswow64\rundll32.exe
Command Line	rundll32.exe c:\users\keecfmwgj\appdata\roaming\microsoft\word\startup\ket.t,EUAYKIYBPAX
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133544, Reason: Child Process
Unmonitor End Time	End Time: 320549, Reason: Terminated by Timeout
Monitor Duration	187.00s
Return Code	Unknown
PID	4044
Parent PID	3712
Bitness	32 Bit

Dropped Files (1)

Filename	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Keyboard	3
System	46
Module	176
Registry	3
-	3
Process	177
Environment	1
-	3
-	3

Network Behavior

Type	Count
HTTP	11
TCP	4

Process #5: svchost.exe

ID	5
Filename	c:\windows\syswow64\svchost.exe
Command Line	C:\Windows\SysWOW64\svchost.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 164344, Reason: Child Process
Unmonitor End Time	End Time: 320549, Reason: Terminated by Timeout
Monitor Duration	156.21s
Return Code	Unknown
PID	2852
Parent PID	4044
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	0xfd0	0x400000(4194304)	0x48000	✓	1
Modify Memory	#4: c:\windows\syswow64\rundll32.exe	0xfd0	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#4: c:\windows\syswow64\rundll32.exe	0xfd0 / 0xb28		-	✓	1

Dropped Files (1)

Filename	File Size	SHA256	YARA Match
-	12 bytes	fd41cd2f48623ceb8d6d4fa774c80efa5c3f22c94bfd7a7c59543772b585d9a1	✗

Host Behavior

Type	Count
System	3
Module	12
Mutex	77
File	5

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	2

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
0b22278ddb598d63f07eb983bcf307e0852cd3005c5bc15d4a4f26455562c8ec	C:\Users\kEecfMwgj\Desktop\0524_4109399728218.doc	Sample File	1304.50 KB	application/msword		MALICIOUS
2a8b737a4752060a308c4312b7c0cf6c05cde5b370906286dea9cdd36f5aa613	c:\users\keecfmwgj\appdata\local\temp\jax.k, c:\users\keecfmwgj\appdata\roaming\microsoft\word\startup\ket.t	Dropped File	704.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1		Downloaded File	267.01 KB	application/vnd.microsoft.portable-executable		MALICIOUS
9ce6c2ffdc33040c55cbc1ead970415494022a154b02cee02aded3727faf79d6	jax.k	Embedded File	704.17 KB	application/vnd.microsoft.portable-executable		MALICIOUS
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream		CLEAN
9f0327fb7d2b24169685dc794022dcb42f351a2c277c0c6360810c268196ac67	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
0f0408e2350bcecbe61c16cb9f083f1db2cca75be4e5f5b00be7aba408407662		Downloaded File	121 bytes	text/plain		CLEAN
ca6b8165af0d6032dabc2a818b5c08eeca3d29ed612e0deb88a64e58bae47a86		Downloaded File	52 bytes	text/plain		CLEAN
8bc8e15ebd0428201a59b41612a9da6284ace3847cae6d0711a23a176c11cbf1		Downloaded File	12 bytes	text/plain		CLEAN
dbf3eff77c45528798443b7335e45ae229f3036db4081551e1cf8456a074ac72		Downloaded File	12 bytes	text/plain		CLEAN
fdf73d5b987ef1e4a58ecee1e654161ecac8dc2f61d6f9f4fd3d17dd838ca89a		Downloaded File	12 bytes	text/plain		CLEAN
bc8b832fd2a68c177d4f5ecee42000ae6255a8445a53c6f1a4d3817226df73a2		Downloaded File	12 bytes	text/plain		CLEAN
a9f28f5c27f1d7a35858036a7775bec833b424362ebe7b630168cd096f9b1a60		Downloaded File	12 bytes	text/plain		CLEAN
99050ff7c9cd2eeb52103a3ebb1bdbbf2daad4cec2e31f09c397a1a9a93a58c7		Downloaded File	12 bytes	text/plain		CLEAN
cfa5f5b6696abeb299fa0621b62c56c14aaa2d367a0583933472f007a885874f		Downloaded File	12 bytes	text/plain		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
90229e3b878f46a7e4a2b4e89558a450d8e21578b8e57c993e3ad638df532041	0.PNG	Embedded File	551.13 KB	image/png		CLEAN
5f9b76346c88e6aa464b68e994dd0f9edd321c40b7937233c589ec8751f4fb97	2.EMF	Embedded File	4.85 KB	application/octet-stream		CLEAN

Filename

Filename	Category	Operations	Verdict
c:\users\keecfmwgj\appdata\roaming\microsoft\word\startup\ket.t	Dropped File	Access	CLEAN
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

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://euvereginumet.ru/8/forum.php		77.222.52.246		POST	MALICIOUS
http://gromber6.ru/6hjusfd8.exe		8.211.5.232		GET	SUSPICIOUS
http://api.ipify.org		54.225.165.85		GET	CLEAN
http://api.ipify.org/?format=xml		54.225.165.85		GET	CLEAN
http://thowerteigime.com/8/forum.php		90.156.143.87		POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
euvereginumet.ru	77.222.52.246		DNS, HTTP	MALICIOUS
sweyblidian.com	185.100.65.29		DNS	MALICIOUS
gromber6.ru	8.211.5.232		DNS, HTTP	SUSPICIOUS
api.ipify.org	54.225.144.221, 107.22.233.72, 23.21.48.44, 50.19.252.36, 50.19.96.218, 54.235.175.90, 54.225.165.85, 23.21.76.253		DNS, HTTP	CLEAN
nagano-19599.herokussl.com	54.225.144.221, 107.22.233.72, 23.21.48.44, 50.19.252.36, 50.19.96.218, 54.235.175.90, 54.225.165.85, 23.21.76.253		DNS	CLEAN
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.144.221, 107.22.233.72, 23.21.48.44, 50.19.252.36, 50.19.96.218, 54.235.175.90, 54.225.165.85, 23.21.76.253		DNS	CLEAN
thowerteigime.com	90.156.143.87		DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.100.65.29	sweyblidian.com	Kazakhstan	DNS, TCP	MALICIOUS
192.168.0.1		-	DNS, UDP	CLEAN
90.156.143.87	thowerteigime.com	Russia	DNS, HTTP, TCP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
54.225.165.85	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS, HTTP, TCP	CLEAN
8.211.5.232	gromber6.ru	Singapore	DNS, HTTP, TCP	CLEAN
77.222.52.246	euvereginumet.ru	Russia	DNS, HTTP, TCP	CLEAN
54.235.175.90	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
54.225.144.221	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
50.19.252.36	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
23.21.48.44	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
107.22.233.72	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
23.21.76.253	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN
50.19.96.218	elb097307-934924932.us-east-1.elb.amazonaws.com, nagano-19599.herokussl.com, api.ipify.org	United States	DNS	CLEAN

Email

-

Email Address

-

Mutex

Name	Operations	Parent Process Name	Verdict
hrth	access	svchost.exe	CLEAN
o;jtfytyjftyjftyjftyj;ijo;	access	svchost.exe	CLEAN
ijlhlkwaftyjftyjftjftyh;joi;i	access	svchost.exe	CLEAN
ah;waeh;jftyjftyjfiftfdgaf	access	svchost.exe	CLEAN
hotyjftyj;afdh	access	svchost.exe	CLEAN
whftyjftyjftyjtfyjtfyjftyj;ijo;h	access	svchost.exe	CLEAN
whoareyoutellmeandilltellwhoyou	access	svchost.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	rundll32.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	rundll32.exe	CLEAN

Process

Process Name	Commandline	Verdict
rundll32.exe	rundll32.exe c:\users\keecfmwgj\appdata\roaming\microsoft\word\startup\ket.t,EUAYKIYBPAX	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 (4)

Ruleset Name	Rule Name	Rule Description	File Type	Filename	Classification	Verdict
Ransomware	WastedLockerShellcode	WastedLocker payload decryption routine	Memory Dump	-	Ransomware	5/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0524_410939972821 8.doc		3/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0524_410939972821 8.doc		3/5
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Embedded File	jax.k		3/5

Antivirus (7)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Variant.Jacard.222844	C:\Users\kEecfMwgj\Desktop\0524_410939972 8218.doc	MALICIOUS
EMBEDDED	Gen:Variant.Jacard.222844	jax.k	MALICIOUS
DOWNLOADED	Trojan.GenericKD.45628116	-	MALICIOUS
WEB_REQUEST	Trojan.GenericKD.45628116	-	MALICIOUS
DROPPED	Gen:Variant.Jacard.222844	-	MALICIOUS
MEMORY_DUMP	Generic.Mint.Zamg.3.10EEB7F3	-	MALICIOUS
MEMORY_DUMP	Gen:Variant.Razy.832814	-	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	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-05-25 01:29:57+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
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