MALICIOUS

Classifications: Spyware

Threat Names: C2/Generic-A | Lokibot | Lokibot.v2 | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe**
ID	#6218736
MD5	9632628f4b25e22bf57a5fb1010daf4e
SHA1	339706d04fbc6c4a0e3cad9c8a12d7b88a8a0dcb
SHA256	e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe
File Size	236.42 KB
Report Created	2022-11-25 11:25 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (30 rules, 54 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Lokibot configuration was extracted	1	Spyware
	• A configuration for Lokibot was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
	• Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #4) rvtzlpyrgs.exe. • Rule "Lokibot" from ruleset "Malware" has matched on the function strings for (process #4) rvtzlpyrgs.exe. • Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #2) rvtzlpyrgs.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: WinChips, Internet Explorer / Edge, LinasFTP, Internet Explorer, Bitvise SSH Client, NCH Fling, N... ...lassic FTP, PuTTY, FAR Manager, Trojita, QtWeb Internet Browser, Total Commander, KiTTY, SecureFX, Microsoft Outlook, IncrediMail.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://sempersim.su/gm13/fre.php" which was contacted by (process #4) rvtzlpyrgs.exe as C2/Generic-A.			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "sempersim.su" as C2/Generic-A.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive browser data	4	-
	• (Process #4) rvtzlpyrgs.exe tries to read sensitive data of web browser "QtWeb Internet Browser" by registry. • (Process #4) rvtzlpyrgs.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Discovery	Searches for senstive application data	1	-
	• (Process #4) rvtzlpyrgs.exe searches for sensitive data of application "Pidgin" by file.			
2/5	Data Collection	Reads sensitive ftp data	6	-
	• (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "LinasFTP" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "Total Commander" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "FAR Manager" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "SecureFX" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "NCH Fling" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of ftp application "NCH Classic FTP" by registry.			
2/5	Discovery	Searches for senstive FTP data	3	-

Score	Category	Operation	Count	Classification
	• (Process #4) rvtzlpyrgs.exe searches for sensitive data of ftp application "FileZilla" by file. • (Process #4) rvtzlpyrgs.exe searches for sensitive data of ftp application "BlazeFTP" by file. • (Process #4) rvtzlpyrgs.exe searches for sensitive data of ftp application "FTP Navigator" by file.			
2/5	Data Collection	Reads sensitive application data	4	-
	• (Process #4) rvtzlpyrgs.exe tries to read sensitive data of application "Bitvise SSH Client" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of application "KiTTY" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of application "PuTTY" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of application "WinChips" by registry.			
2/5	Discovery	Searches for senstive mail data	2	-
	• (Process #4) rvtzlpyrgs.exe searches for sensitive data of mail application "Pocomail" by file. • (Process #4) rvtzlpyrgs.exe searches for sensitive data of mail application "Opera Mail" by file.			
2/5	Data Collection	Reads sensitive mail data	3	-
	• (Process #4) rvtzlpyrgs.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #4) rvtzlpyrgs.exe tries to read sensitive data of mail application "Trojita" by registry.			
2/5	Discovery	Searches for senstive browser data	1	-
	• (Process #4) rvtzlpyrgs.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #4) rvtzlpyrgs.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	5	-
	• (Process #2) rvtzlpyrgs.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #2) rvtzlpyrgs.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #2) rvtzlpyrgs.exe makes a direct system call to "NtResumeThread". • (Process #2) rvtzlpyrgs.exe makes a direct system call to "NtCreateSection". • (Process #2) rvtzlpyrgs.exe makes a direct system call to "NtMapViewOfSection".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #2) rvtzlpyrgs.exe modifies memory of (process #4) rvtzlpyrgs.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #2) rvtzlpyrgs.exe alters context of (process #4) rvtzlpyrgs.exe.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe starts (process #2) rvtzlpyrgs.exe with a hidden window. • (Process #2) rvtzlpyrgs.exe starts (process #4) rvtzlpyrgs.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #2) rvtzlpyrgs.exe reads from (process #4) rvtzlpyrgs.exe.			
1/5	Discovery	Reads system data	1	-
	• (Process #4) rvtzlpyrgs.exe reads the cryptographic machine GUID from registry.			

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	1	-
	• (Process #4) rvtzlpyrgs.exe creates mutex with name "B7274519EDDE9BDC8AE51348".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #4) rvtzlpyrgs.exe tries to gather information about application "NetScape" by registry. • (Process #4) rvtzlpyrgs.exe tries to gather information about application "Default Programs" by registry.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #4) rvtzlpyrgs.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #4) rvtzlpyrgs.exe resolves host name "sempersim.su" to IP "95.213.216.202".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #4) rvtzlpyrgs.exe opens an outgoing TCP connection to host "95.213.216.202:80".			
1/5	Network Connection	Downloads file	1	-
	• (Process #4) rvtzlpyrgs.exe downloads file via http from http://sempersim.su/gm13/fre.php.			
1/5	Execution	Drops PE file	1	-
	• (Process #4) rvtzlpyrgs.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe".			
-	Trusted	Known clean file	3	-
	• Embedded file "" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck" is a known clean file. • File "" is a known clean file.			

Malware Configuration: Lokibot

Metadata	Key	Extracted Value
Encryption Key	Key Tags Algorithm Mode Iv Key Tags Algorithm	+GrwTafWkea+mP09tlubezd5OJSV+VEl Encryption Key #0 3DES CBC TPh5m1q9osA= /w== Encryption Key #1 XOR
URL	Url Tags Url Tags Url Tags Url Tags Url Tags	alphastand.top/alien/fre.php Encrypted with Key #0 kbfvzoboss.bid/alien/fre.php Encrypted with Key #0 alphastand.win/alien/fre.php Encrypted with Key #0 alphastand.trade/alien/fre.php Encrypted with Key #0 http://sempersim.su/gm13/fre.php Encrypted with Key #1
Other: Version Identifier	Tags Value	Identifier in Network Packets ckav.ru

Mitre ATT&CK Matrix

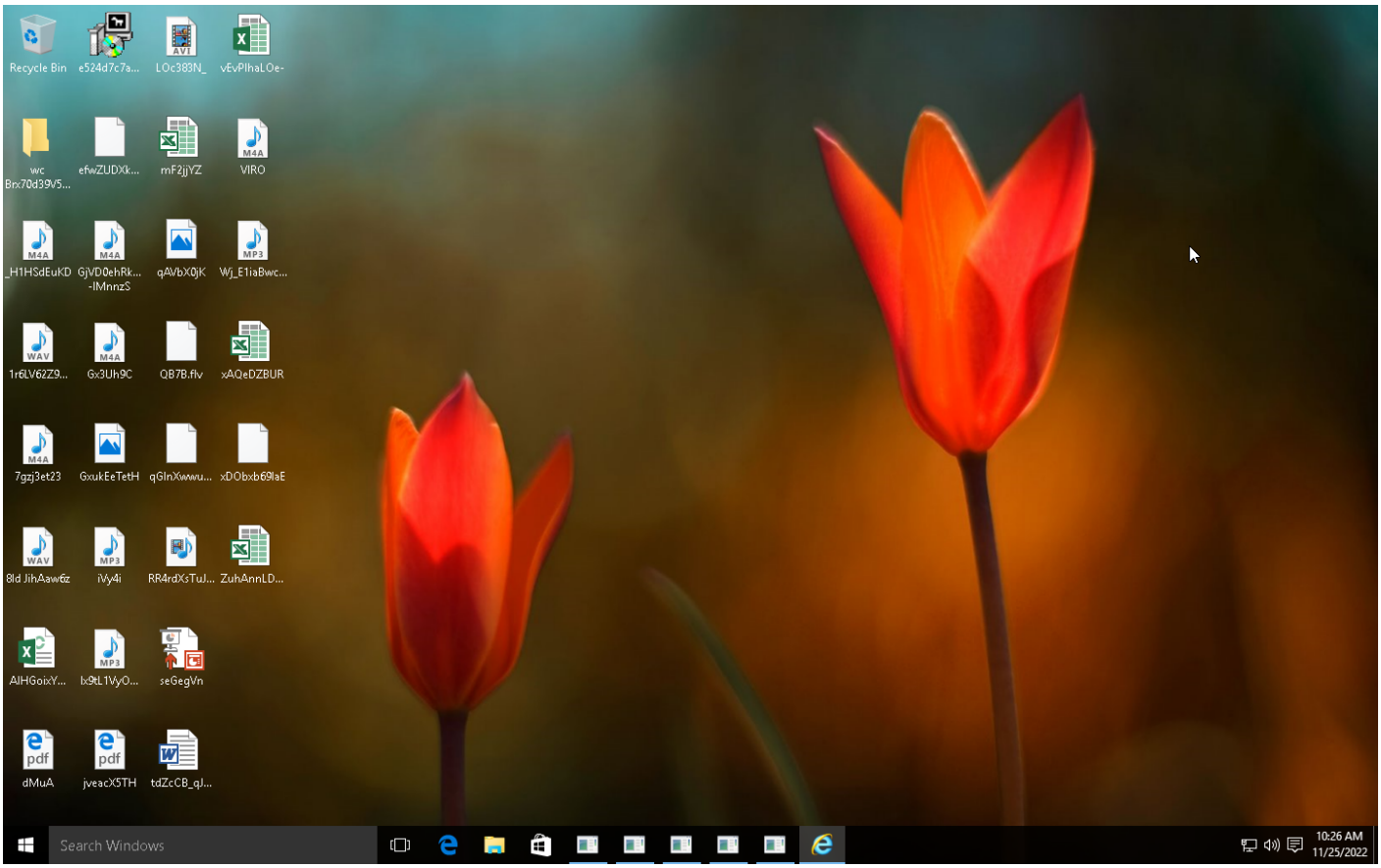
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1214 Credentials in Registry	#T1082 System Information Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
					#T1003 Credential Dumping	#T1012 Query Registry		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1081 Credentials in Files	#T1217 Browser Bookmark Discovery					
						#T1083 File and Directory Discovery					

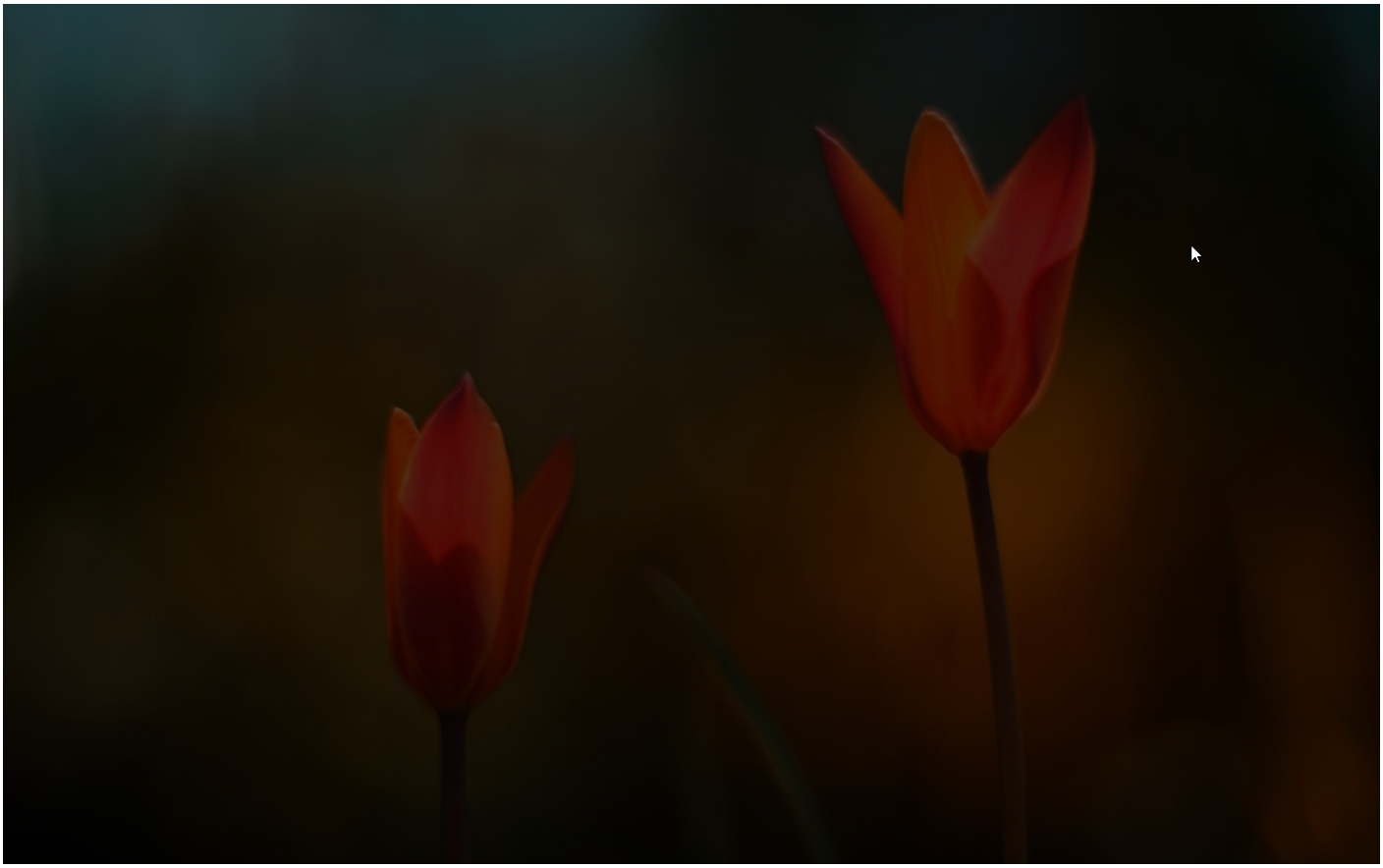
Sample Information

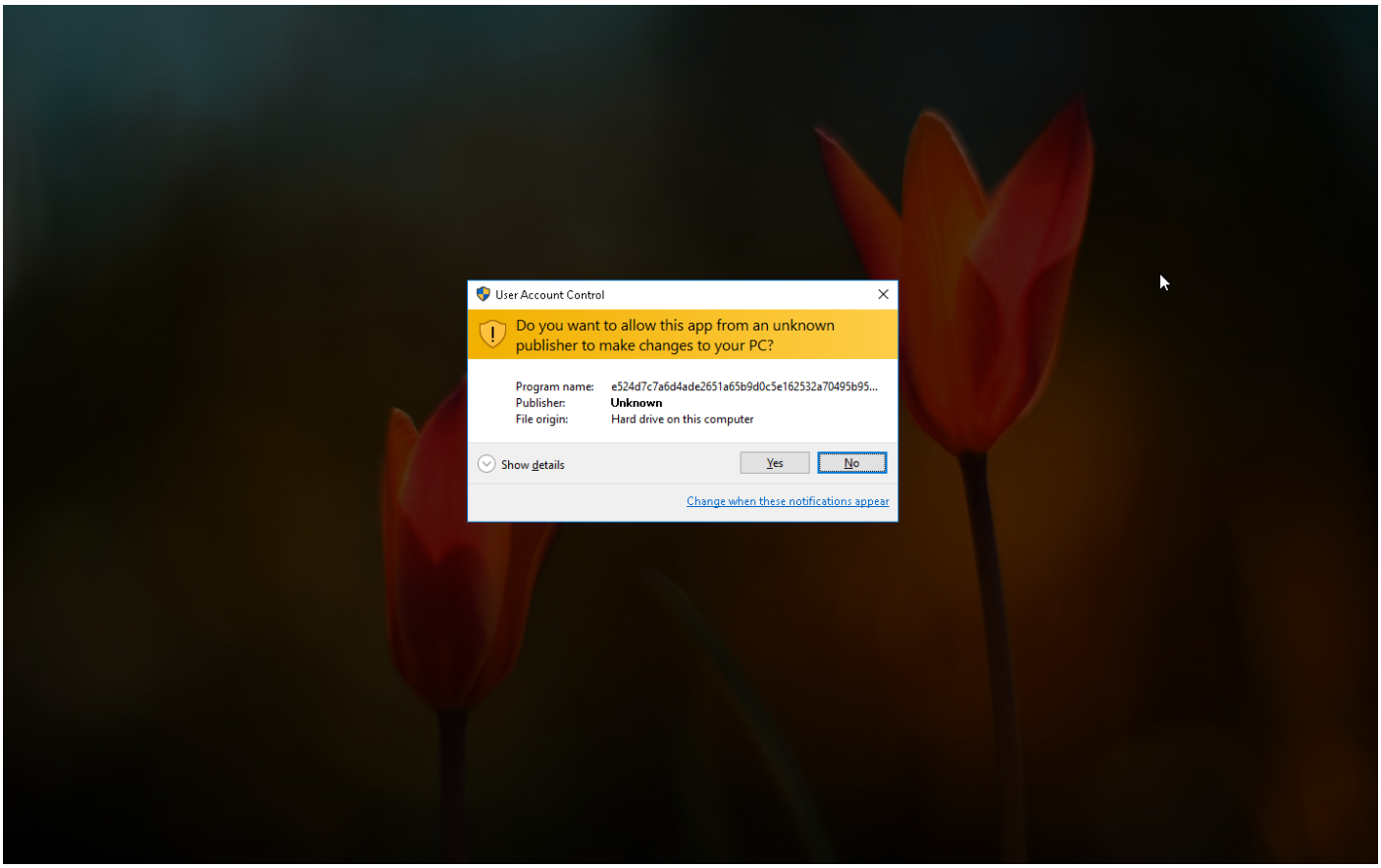
ID	#6218736
MD5	9632628f4b25e22bf57a5fb1010daf4e
SHA1	339706d04fbc6c4a0e3cad9c8a12d7b88a8a0dcb
SHA256	e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe
SSDeep	6144:QBn1PO9HgFlUgwXVH/7/Gf5emejH+PgDSD9LV9Gj4WhwW:gPOhCXVf7/GJnPFDosW
ImpHash	ab6770b0a8635b9d92a5838920cfe770
File Name	e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe
File Size	236.42 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

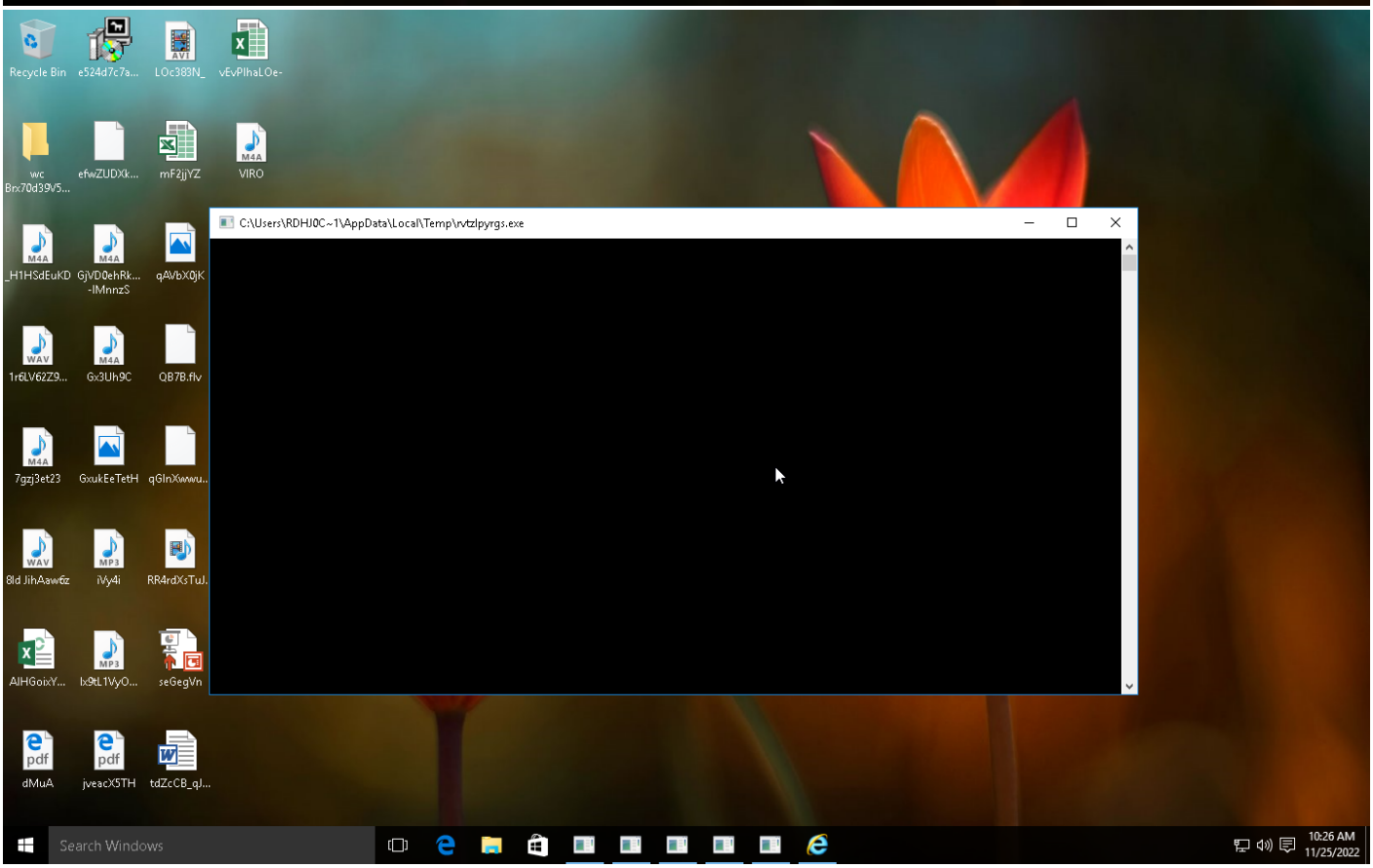
Analysis Information

Creation Time	2022-11-25 11:25 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	3
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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	21


Recycle Bin
e524d7c7a...
LOc383N_
vEvPlhaLOe-
wc Bnx70d39v5...
efwZUDXk...
mF2jjYZ
VIRO
_H1HSdEuKD
GjVD0ehRk... -IMnnzS
qAVbX0jK
Wj_E1iaBwc...
1r6LV6ZZ9...
Gx3Uh9C
QB7B.flv
xAQeDZBUR
7gzj3et23
GxukEeTetH
qGlnXwwu...
xDObxb69laE
8ld JihAaw6z
iVy4i
RR4rdXsTuJ...
ZuhAnnLD...
AIHGoixY...
lx9tL1VyO...
seGegVn
dMuA
jveacX5TH
tdZcCB_qJ...
Search Windows
10:26 AM
11/25/2022







Screenshots truncated

NETWORK

General

72.79 KB total sent

50.29 KB total received

2 ports 80, 53

2 contacted IP addresses

4 URLs extracted

5 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

114 sessions, 72.73 KB sent, 50.21 KB received

HTTP Requests

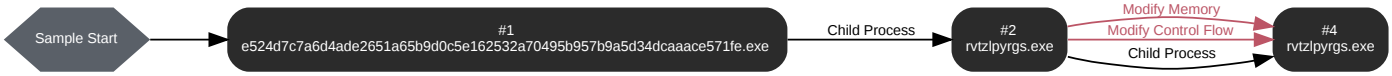
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://sempersim.su/gm13/fre.php	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	sempersim.su	NO_ERROR	95.213.216.202		NA

BEHAVIOR

Process Graph



Process #1: e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 51836, Reason: Analysis Target
Unmonitor End Time	End Time: 63872, Reason: Terminated
Monitor duration	12.04s
Return Code	2
PID	2992
Parent PID	1648
Bitness	32 Bit

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\aqqlknbytl.sm	104.00 KB	86a2b6783a599185d30db5e9a8a232d453a2310497b82d09ae7ee7601f0cafcd	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsv74D6.tmp	438.16 KB	393b378fb154a276fcdf2e8f8b9426cb3dabc0ddd63e59dd83f08e22c76d9af2	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb	5.35 KB	6b5a1ee266b6c954b473b361cbe526819de00c6d4bbfbab513ecf7ed7ec96885	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe	320.50 KB	0c49cef3f60cf1a48b60dfc066053c709b54ac83a5c39ca3f182f073d54a569e	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsg74C6.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsg75B2.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	39
Module	15
File	219
Process	1

Process #2: rvtzlpyrgs.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\rvtzlpyrgs.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 57060, Reason: Child Process
Unmonitor End Time	End Time: 62935, Reason: Terminated
Monitor duration	5.88s
Return Code	0
PID	2988
Parent PID	2992
Bitness	32 Bit

Host Behavior

Type	Count
Module	20
File	33
Environment	1
Process	1
-	3
-	2

Process #4: rvtzlpyrgs.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\rvtzlpyrgs.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 60144, Reason: Child Process
Unmonitor End Time	End Time: 292802, Reason: Terminated by timeout
Monitor duration	232.66s
Return Code	Unknown
PID	3320
Parent PID	2988
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rvtzlpyrgs.exe	0x1e0	0x400000(4194304)	0xa2000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rvtzlpyrgs.exe	0x1e0	0x214008(2179080)	0x4	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rvtzlpyrgs.exe	0x1e0 / 0x8d4	0x777d8fe0(2004717536)	-	✔	1

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	4 bytes	859ffdca62ee0971821a4b2dedfc023d0f9a021391b5ac336ddb49d53d28330e	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	320.50 KB	0c49cef3f60cf1a48b60dfc066053c709b54ac83a5c39ca3f182f073d54a569e	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	1 bytes	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	✖
-	53 bytes	353fd628b7f6e7d426e5d6a27d1bc3ac22fa7f812e7594cf2ec5ca1175785b50	✖
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✖

Host Behavior

Type	Count
Module	3934
Registry	181
Mutex	1
File	313
System	143
User	10
-	227
-	226

Network Behavior

Type	Count
HTTP	114
DNS	1
TCP	114

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe	C:\Users\RDhJ0CNFevzX\Desktop\e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe	Sample File	236.42 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
0c49cef3f60cf1a48b60dfc066053c709b54ac83a5c39ca3f182f073d54a569e	C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	Dropped File	320.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	SUSPICIOUS
859ffdca62ee0971821a4b2dedfc023d0f9a021391b5ac336ddb49d53d28330e	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	4 bytes	text/plain	Access, Create, Delete, Write	CLEAN
86a2b6783a599185d30db5e9a8a232d453a2310497b82d09ae7ee7601f0cafcd	C:\Users\RDHJ0C~1\AppData\Local\Temp\aqqlknbytl.sm	Dropped File	104.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ccf6aadc1539596860d96eaee2fbfb4d1f6f52d361be1ff807a27f814c374616	-	Downloaded File	186 bytes	application/octet-stream	-	CLEAN
b14395003e5efba733d717f89486aee8222abf00b33190ea2d34e7b68d2bca73	-	Downloaded File	15 bytes	text/plain	-	CLEAN
393b378fb154a276fcdf2e8f8b9426cb3dabc0ddd63e59dd83f08e22c76d9af2	C:\Users\RDHJ0C~1\AppData\Local\Temp\nsv74D6.tmp	Dropped File	438.16 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6b5a1ee266b6c954b473b361cbe526819de00c6d4bbfbab513ecf7ed7ec96885	C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb	Dropped File	5.35 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f158aa8b7a32a64eae6a34384322ffafbb21fa59bd7deeb7fe2a7cc7364ce8f3	-	Downloaded File	159 bytes	application/octet-stream	-	CLEAN
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	1 bytes	application/octet-stream	Access, Create, Delete, Write	CLEAN
353fd628b7f6e7d426e5d6a27d1bc3ac22fa7f812e7594cf2ec5ca1175785b50	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
c64510503435c2143bad854faba7891308b4b089d140449ceb903620fea45d6a	-	Downloaded File	23 bytes	application/octet-stream	-	CLEAN
6d8780de0d47117b257766c0da10356e59790bb7253ce479594550f975a0454a	-	Downloaded File	288 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\aqqlknbytl.sm	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsg75B2.tmp\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Accessed File, Dropped File	Access, Create, Delete, Write	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Accessed File, Dropped File	Access, Create, Delete, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsg74C6.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe	Accessed File, Dropped File	Access, Create, Delete, Write	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsv74D6.tmp	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsg75B2.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Read	CLEAN
C:\	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Access, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://kbfvzoboss.bid/alien/fre.php	-	-	-	-	MALICIOUS
http://sempersim.su/gm13/fre.php	-	95.213.216.202	-	POST	MALICIOUS
http://alphastand.trade/alien/fre.php	-	-	-	-	MALICIOUS
http://alphastand.win/alien/fre.php	-	-	-	-	MALICIOUS
http://alphastand.top/alien/fre.php	-	-	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
sempersim.su	95.213.216.202	-	DNS, TCP, HTTP	MALICIOUS
alphastand.top	-	-	-	CLEAN
kbfvzoboss.bid	-	-	-	CLEAN
alphastand.trade	-	-	-	CLEAN
alphastand.win	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
95.213.216.202	sempersim.su	Russia	DNS, TCP, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
B7274519EDDE9BDC8AE51348	access	rvtzlpyrgs.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\RegisteredApplications	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86\RootDir	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\imap.auth.pass	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup\SetupPath	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\VanDyke\SecureFX\Config Path	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities	access	rvtzlpyrgs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox\Path	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\ODBC	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Wow6432Node	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	rvtzlpyrgs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey\CurrentVersion	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Netscape	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\msa.smtp.auth.pass	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	rvtzlpyrgs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari\InstallDir	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\WinChips\UserAccounts	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\IM Providers	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\AppDataLow	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\������й��������ь�И����й��я��\9EDDE9	access, write	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings\LastPassword	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	rvtzlpyrgs.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66\Email	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Classes	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	read, access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts	access	rvtzlpyrgs.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	rvtzlpyrgs.exe	CLEAN
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient\LastUsedProfile	read, access	rvtzlpyrgs.exe	CLEAN

Process

Process Name	Commandline	Verdict
e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe	"C:\Users\RDhJ0CNFevzX\Desktop\e524d7c7a6d4ade2651a65b9d0c5e162532a70495b957b9a5d34dcaaace571fe.exe"	MALICIOUS
rvtzlpyrgs.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb	MALICIOUS
rvtzlpyrgs.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\rvtzlpyrgs.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\xdnyr.wb	SUSPICIOUS

YARA / AV

YARA (21)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Function Strings	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.1.7 / 2022-10-27 16:01:27
Link Detonation Heuristics Version	4.7.1.8 / 2022-10-30 09:01:20
Smart Memory Dumping Rules Version	4.7.1.7 / 2022-10-27 16:01:27
Config Extractors Version	4.7.1.11 / 2022-11-11 16:05:21
Signature Trust Store Version	4.7.1.8 / 2022-10-30 09:01:20
VMRay Threat Identifiers Version	4.7.1.12 / 2022-11-15 10:04:31
YARA Built-in Ruleset Version	4.7.1.10

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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows