MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe**
ID	#3277839
MD5	d62b8a5fdb90e9241ff0eef6ea035e32
SHA1	4e9e38dc4d01a649d927a933488477c5980fcb18
SHA256	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b
File Size	241.23 KB
Report Created	2022-01-14 08:29 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 62 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
	• Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe. • Rule "Lokibot" from ruleset "Malware" has matched on a memory dump for (process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe. • Rule "Lokibot" from ruleset "Malware" has matched on the function strings for (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: NCH Fling, Trojita, KiTTY, IncrediMail, FAR Manager, FTP Navigator, Microsoft Outlook, Pocomail, ...itvise SSH Client, LinasFTP, Internet Explorer / Edge, Internet Explorer, Total Commander, Opera Mail, FileZilla, NCH Classic FTP.			
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://slimpackage.com/slimfit/five/fre.php" which was contacted by (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe as "C2/Generic-A".			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "slimpackage.com" as "Mal/HTMLGen-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 #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of web browser "QtWeb Internet Browser" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive application data	5	-
	• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of application "Pidgin" by file. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of application "Bitvise SSH Client" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of application "KiTTY" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of application "PuTTY" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of application "WinChips" by registry.			
2/5	Data Collection	Reads sensitive ftp data	10	-

Score	Category	Operation	Count	Classification
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "LinasFTP" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "BlazeFTP" by file. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "BlazeFTP" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "Total Commander" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "FAR Manager" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "SecureFX" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "NCH Fling" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "NCH Classic FTP" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of ftp application "FTP Navigator" by file.		
2/5	Data Collection	Reads sensitive mail data	5	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to read sensitive data of mail application "Trojita" by registry.		
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe modifies memory of (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe.		
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe alters context of (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe.		
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	3	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe makes a direct system call to "NtResumeThread".		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe starts (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe reads from (process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Discovery	Reads system data	1	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe reads the cryptographic machine GUID from registry.		
1/5	Mutex	Creates mutex	1	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe creates mutex with name "B7274519EDDE9BDC8AE51348".		
1/5	Discovery	Possibly does reconnaissance	14	-

Score	Category	Operation	Count	Classification
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Comodo IceDragon" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Safari" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "K-Meleon" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Mozilla SeaMonkey" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Mozilla Flock" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Cyberfox" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Total Commander" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "NetScape" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Default Programs" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Bitvise SSH Client" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "SecureFX" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Postbox" by registry. • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe tries to gather information about application "Trojita" by registry.		
1/5	Privilege Escalation	Enables process privilege	1	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe enables process privilege "SeDebugPrivilege".		
1/5	Execution	Drops PE file	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp\ibqwlwmewvj.dll".		
1/5	Execution	Executes itself	1	-
		• (Process #1) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe.		
1/5	Network Connection	Performs DNS request	2	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe resolves host name "slimpackage.com" to IP "104.223.93.105". • (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe resolves host name "[illegible]" to IP "-".		
1/5	Network Connection	Connects to remote host	1	-
		• (Process #2) 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe opens an outgoing TCP connection to host "104.223.93.105:80".		
-	Trusted	Known clean file	2	-
		• File "C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck" is a known clean file. • File "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778" is a known clean file.		

Mitre ATT&CK Matrix

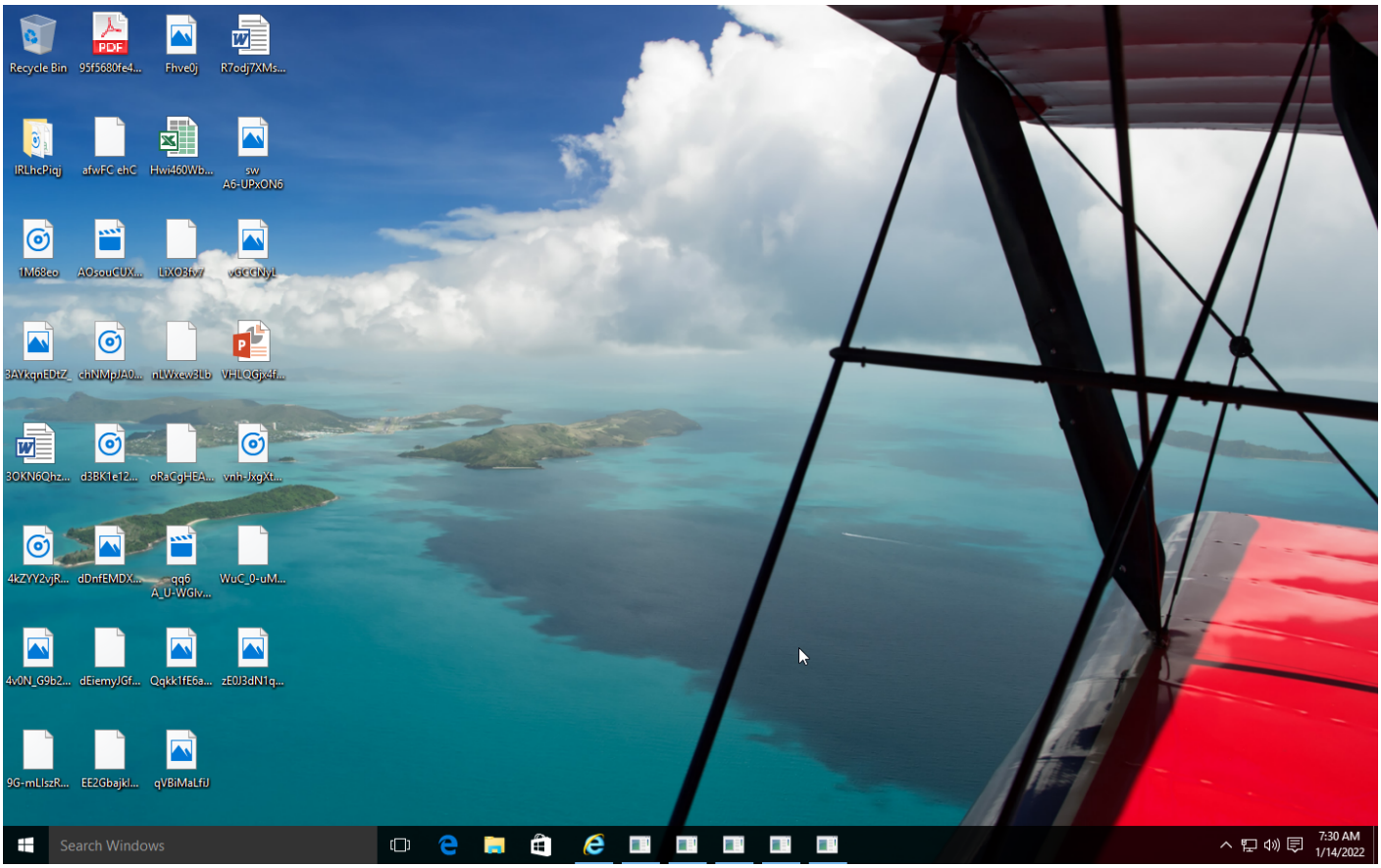
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1214 Credentials in Registry	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1045 Software Packing	#T1003 Credential Dumping	#T1012 Query Registry		#T1005 Data from Local System			
					#T1081 Credentials in Files	#T1217 Browser Bookmark Discovery					
						#T1083 File and Directory Discovery					

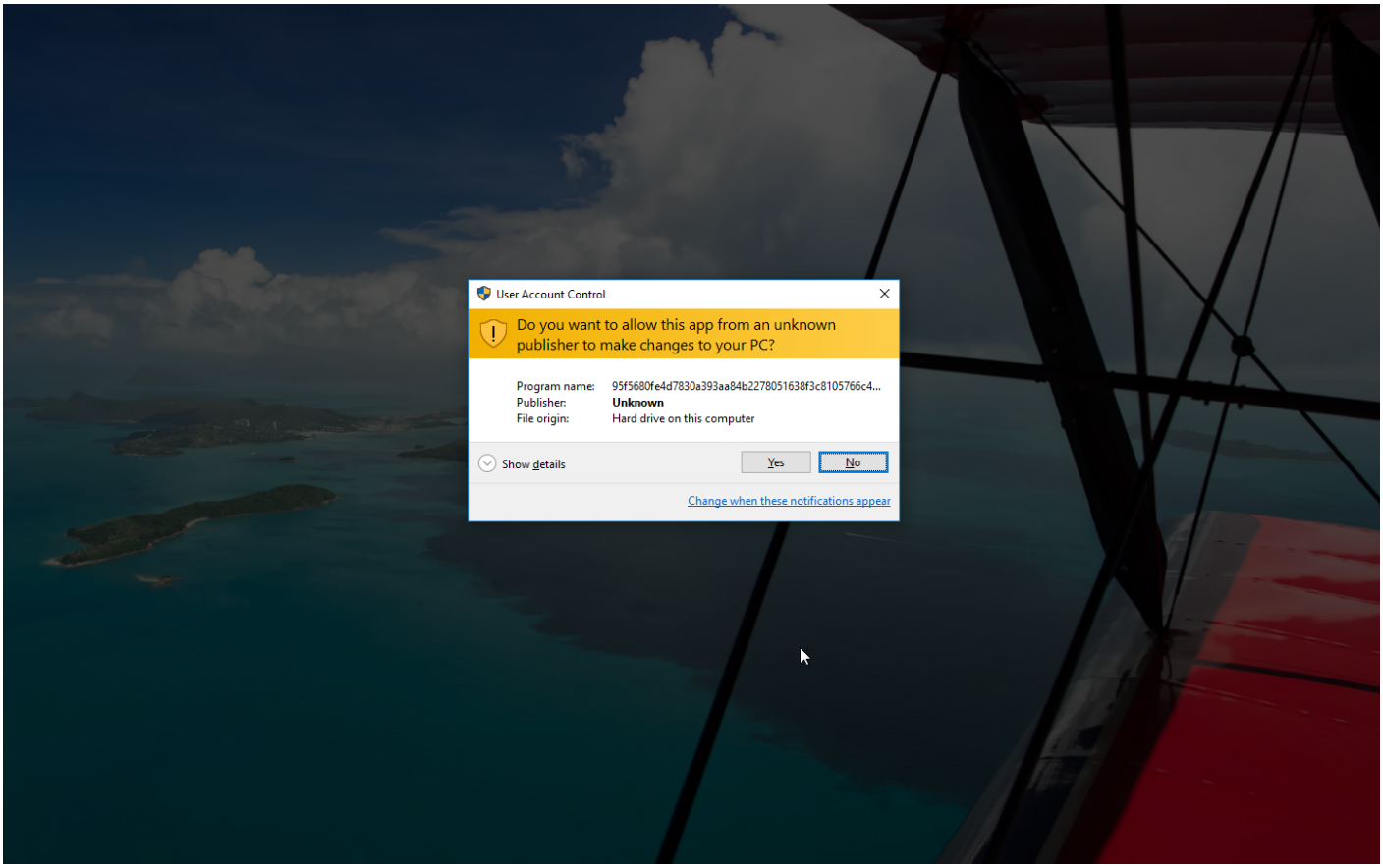
Sample Information

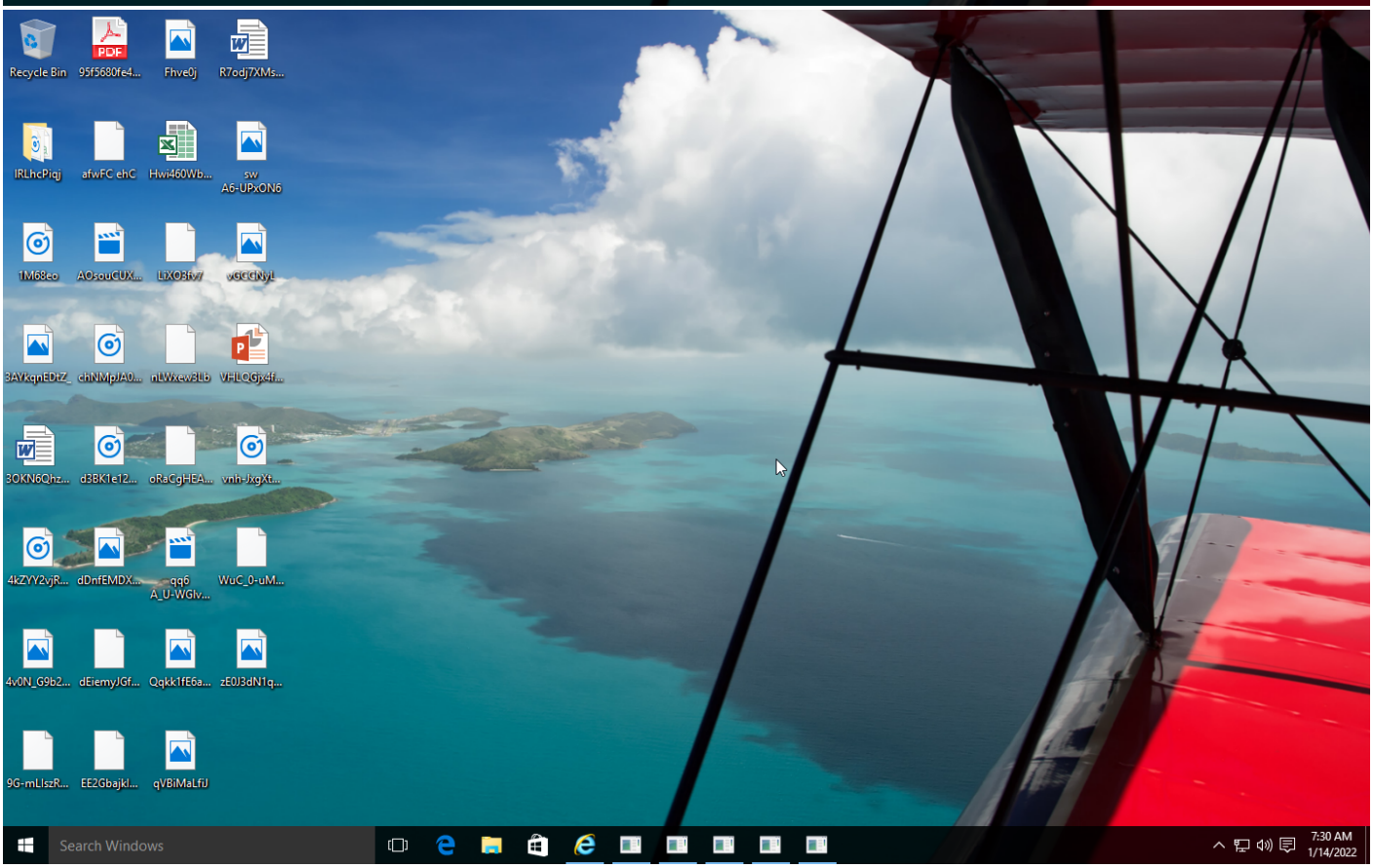
ID	#3277839
MD5	d62b8a5fdb90e9241ff0eef6ea035e32
SHA1	4e9e38dc4d01a649d927a933488477c5980fcb18
SHA256	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b
SSDeep	6144:kw/b88QHR5lvQ2urEmJzKlf78z1++UPkq4Y1ROwy:HoRbQ2ugoz87oUPkqEwy
ImpHash	099c0646ea7282d232219f8807883be0
File Name	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe
File Size	241.23 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-01-14 08:29 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
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	19


Recycle Bin
95f5680fe4...
Fhve0j
R7odj7XMs...
IRLhcPiqj
afwFC ehC
Hwi460Wb...
sw
A6-UPxON6
1M68eb
AOsouCUX...
LXO3fv7
vGCCNy1
3AYkqnEDtZ_
chNMpJA0...
nLWxew3Lb
VHLQGjx4f...
3OKN6Qhz...
d3BK1e12...
oRaCgHEA...
vnh-JxgXt...
4kZYY2vjR...
dDnfEMDX...
qq6
A_U-WGlv...
WuC_0-uM...
4v0N_G9b2...
dEiemyJGf...
Qqkk1fE6a...
zE0J3dN1q...
9G-mLIszR...
EE2GbajkI...
qVBiMaLfU
Search Windows
7:30 AM
1/14/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 95f5680fe4d7830a393aa84b2278051638f3c8105766c4...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
95f5680fe4...
Fhve0j
R7odj7XMs...
IRLhcPiqj
afwFC ehC
Hwi460Wb...
sw
A6-UPxON6
1M68eo
AOsouCUX...
LiXO3fv7
vGCCNyL
3AYkqnEDtZ_
chNMp/A0...
nLWxew3Lb
VrLQGjx4f...
3OKN6Chz...
d3BK1e12...
oRaCgHEA...
vnh-JxgXt...
4kZYY2vjR...
dDnfEMDX...
qq6
A_U-WGlv...
WuC_0-uM...
4v0N_G9b2...
dEiemyJGf...
QqkkfFE6a...
zE0J3dN1q...
9G-mLIszR...
EE2GbajkI...
qVBiMaLfU
Search Windows
7:30 AM
1/14/2022

NETWORK

General

1.75 KB total sent

325 bytes total received

1 ports 80

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 2 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

2 sessions, 1.28 KB sent, 325 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://slimpackage.com/slimfit/five/fre.php	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	slimpackage.com	NoError	104.223.93.105		NA
-	[illegible]	-			NA

BEHAVIOR

Process Graph

Process #1: 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72243, Reason: Analysis Target
Unmonitor End Time	End Time: 104640, Reason: Terminated
Monitor duration	32.40s
Return Code	0
PID	3604
Parent PID	1560
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nnrr3w4buo	213.75 KB	cd06a2c3858ac3b1bc6d06816dd2966154eabab479c4b305521a84a5b409d6d7	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\urpwvqane	4.86 KB	caf8f4ffca95fe9a5336a64b83554aea6d37586a159f467d868e25f3737b4fb4	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp\ibqwlwmewvj.dll	4.50 KB	97accd2e535507eead8da6ccdb641907134e527b19f9c64d6ef9071bfa508d66	✗

Host Behavior

Type	Count
Module	15
File	221
System	31
Process	1
-	3
-	8

Process #2: 95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 100967, Reason: Child Process
Unmonitor End Time	End Time: 323392, Reason: Terminated by Timeout
Monitor duration	222.43s
Return Code	Unknown
PID	1960
Parent PID	3604
Bitness	32 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x400000(4194304)	0x400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x401000(4198400)	0x13800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x415000(4280320)	0x4200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x41a000(4300800)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x4a0000(4849664)	0x2000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8	0x385008(3690504)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	0xdc8 / 0xd84	0x77c08fe0(2009108448)	-	✓	1

Dropped Files (4)

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

Host Behavior

Type	Count
Module	1013
Registry	180
Mutex	1
File	308
System	28
User	7

Network Behavior

Type	Count
HTTP	2
DNS	3
TCP	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b	C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	Sample File	241.23 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
cd06a2c3858ac3b1bc6d06816dd2966154eabab479c4b305521a84a5b409d6d7	C:\Users\RDHJ0C~1\AppData\Local\Temp\nnrr3w4buo	Dropped File	213.75 KB	application/octet-stream	Access, Create, Write, Read	CLEAN
caf8f4ffca95fe9a5336a64b83554aea6d37586a159f467d868e25f3737b4fb4	C:\Users\RDHJ0C~1\AppData\Local\Temp\urpwvqane	Dropped File	4.86 KB	application/octet-stream	Access, Create, Write, Read	CLEAN
97accd2e535507eead8da6ccdb641907134e527b19f9c64d6ef9071bfa508d66	C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp\ibqwlwmewvj.dll	Dropped File	4.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	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
859ffdca62ee0971821a4b2dedfc023d0f9a021391b5ac336ddb49d53d28330e	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	4 bytes	text/plain	Access, Delete, Create, Write	CLEAN
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	1 bytes	application/octet-stream	Access, Delete, Create, 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

Filename

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsp891.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	Sample File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsf8A2.tmp	Accessed File	Access, Create, Write, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nnrr3w4buo	Dropped File	Access, Create, Write, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\urpwvqane	Dropped File	Access, Create, Write, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq8E2.tmp\ibqwlwmewvj.dll	Dropped File	Access, Create, Write	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.hdb	Dropped File	Access, Delete, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\9EDDE9\9BDC8A.lck	Dropped File	Access, Delete, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://slimpackage.com/slimfit/five/fre.php	-	104.223.93.105	-	POST	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
slimpackage.com	104.223.93.105	-	DNS, HTTP	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
104.223.93.105	slimpackage.com	United States	DNS, TCP, HTTP	CLEAN
192.168.0.1	-	-	DNS, UDP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
B7274519EDDE9BDC8AE51348	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup\SetupPath	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari\InstallDir	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86\RootDir	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox\Path	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings\LastPassword	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\AppDataLow	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\IM Providers	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Netscape	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\ODBC	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\RegisteredApplications	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Wow6432Node	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Classes	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient\LastUsedProfile	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\VanDyke\SecureFX\Config Path	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail\CurrentVersion	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\WinChips\UserAccounts	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\85030200000000000c000000000000046	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\85030200000000000c000000000000046\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\imap.auth.pass	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\msa.smtp.auth.pass	access, read	95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	CLEAN

Process

Process Name	Commandline	Verdict
95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\95f5680fe4d7830a393aa84b2278051638f3c8105766c47a68c1f8981f38932b.exe"	MALICIOUS

YARA / AV

YARA (19)

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	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	Function Strings	function_strings_process_2.txt	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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
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	Not installed

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