MALICIOUS

Classifications: Spyware, Downloader

Threat Names: CryptOne, Mal/HTMLGen-A, DeepScan:Generic.SpyAgent.6.6AF37D2E, Gen:Trojan.Heur.FU.MnZ@aSAwybp

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe**
ID	#2780674
MD5	e9441b756f99ee3adf804214119c1fa1
SHA1	8fe649e6bc868401ba2a3b9bf345fc76692f53d4
SHA256	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd
File Size	1610.00 KB
Report Created	2021-09-27 20:30 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 55 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "CryptOne_Packer" from ruleset "Generic" has matched on a memory dump for (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Cyberfox, BlackHawk, Torch, Opera, 7Star, Comodo Dragon, Chromium, Kometa, Orbitum, Chedot, Epic ... ...a Firefox, Amigo, Internet Explorer / Edge, Vivaldi, FileZilla, Total Commander, Internet Explorer, Elements Browser, CentBrowser.			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected a memory dump of (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "DeepScan:Generic.SpyAgent.6.6AF37D2E". • Built-in AV detected a memory dump of (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Gen:Trojan.Heur.FU.MnZ@aSAwybp".			
4/5	Reputation	Contacts known malicious URL	6	-
	• Reputation analysis labels the URL "23.88.105.196/freebl3.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/mozglue.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/msvcp140.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/nss3.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/softokn3.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "23.88.105.196/vcruntime140.dll" which was contacted by (process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe as "Mal/HTMLGen-A".			
3/5	Hide Tracks	Deletes file after execution	1	-
	• File "c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe" deletes itself by cmd.			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe uploads 192.364KB data using HTTP POST.			
2/5	Data Collection	Reads sensitive browser data	21	-

Score	Category	Operation	Count	Classification
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Opera" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Torch" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Uran" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "7Star" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Data Collection	Reads sensitive ftp data	2	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of ftp application "Total Commander" by file.		
2/5	Data Collection	Reads sensitive mail data	1	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.		
1/5	Hide Tracks	Creates process with hidden window	2	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe starts ewygmopint90kmngfdxh with a hidden window. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe starts (process #17) cmd.exe with a hidden window.		
1/5	Discovery	Enumerates running processes	1	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe enumerates running processes.		
1/5	Discovery	Possibly does reconnaissance	6	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "Cyberfox" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "blackHawk" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "icecat" by file. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "WinSCP" by registry. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe tries to gather information about application "FileZilla" by file.		
1/5	Discovery	Reads system data	1	-
		• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe reads the cryptographic machine GUID from registry.		
1/5	Obfuscation	Resolves API functions dynamically	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe resolves 278 API functions by name.			
1/5	Crash	A monitored process crashed	1	-
	• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe crashed.			
1/5	Execution	Executes itself	1	-
	• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe.			
1/5	Network Connection	Downloads executable	6	Downloader
	• (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/freebl3.dll. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/mozglue.dll. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/msvcp140.dll. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/nss3.dll. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/softokn3.dll. • (Process #1) f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe downloads executable via http from 23.88.105.196/vcruntime140.dll.		
-	Trusted	Known clean file	7	-
	• File "Default.zip" is a known clean file. • File "C:\ProgramData\\freebl3.dll" is a known clean file. • File "C:\ProgramData\\mozglue.dll" is a known clean file. • File "C:\ProgramData\\msvcp140.dll" is a known clean file. • File "C:\ProgramData\\nss3.dll" is a known clean file. • File "C:\ProgramData\\softokn3.dll" is a known clean file. • File "C:\ProgramData\\vcruntime140.dll" is a known clean file.			
-	Trusted	Executable has a trusted signature	4	-
	• Executable C:\ProgramData\\freebl3.dll has a trusted signature. • Executable C:\ProgramData\\mozglue.dll has a trusted signature. • Executable C:\ProgramData\\nss3.dll has a trusted signature. • Executable C:\ProgramData\\softokn3.dll has a trusted signature.			

Mitre ATT&CK Matrix

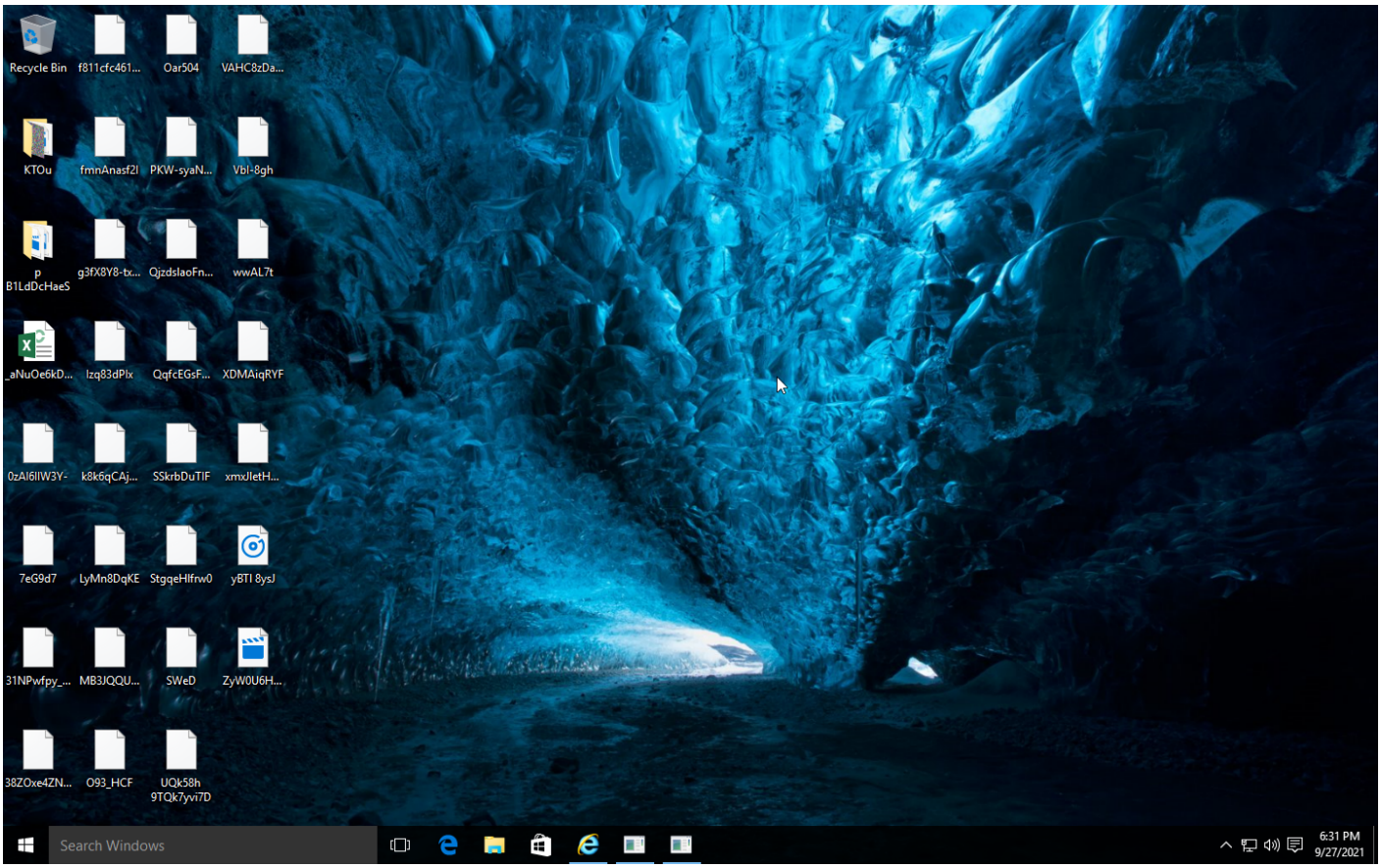
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
				#T1107 File Deletion	#T1003 Credential Dumping	#T1057 Process Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1070 Indicator Removal on Host		#T1012 Query Registry					
				#T1045 Software Packing		#T1082 System Information Discovery					

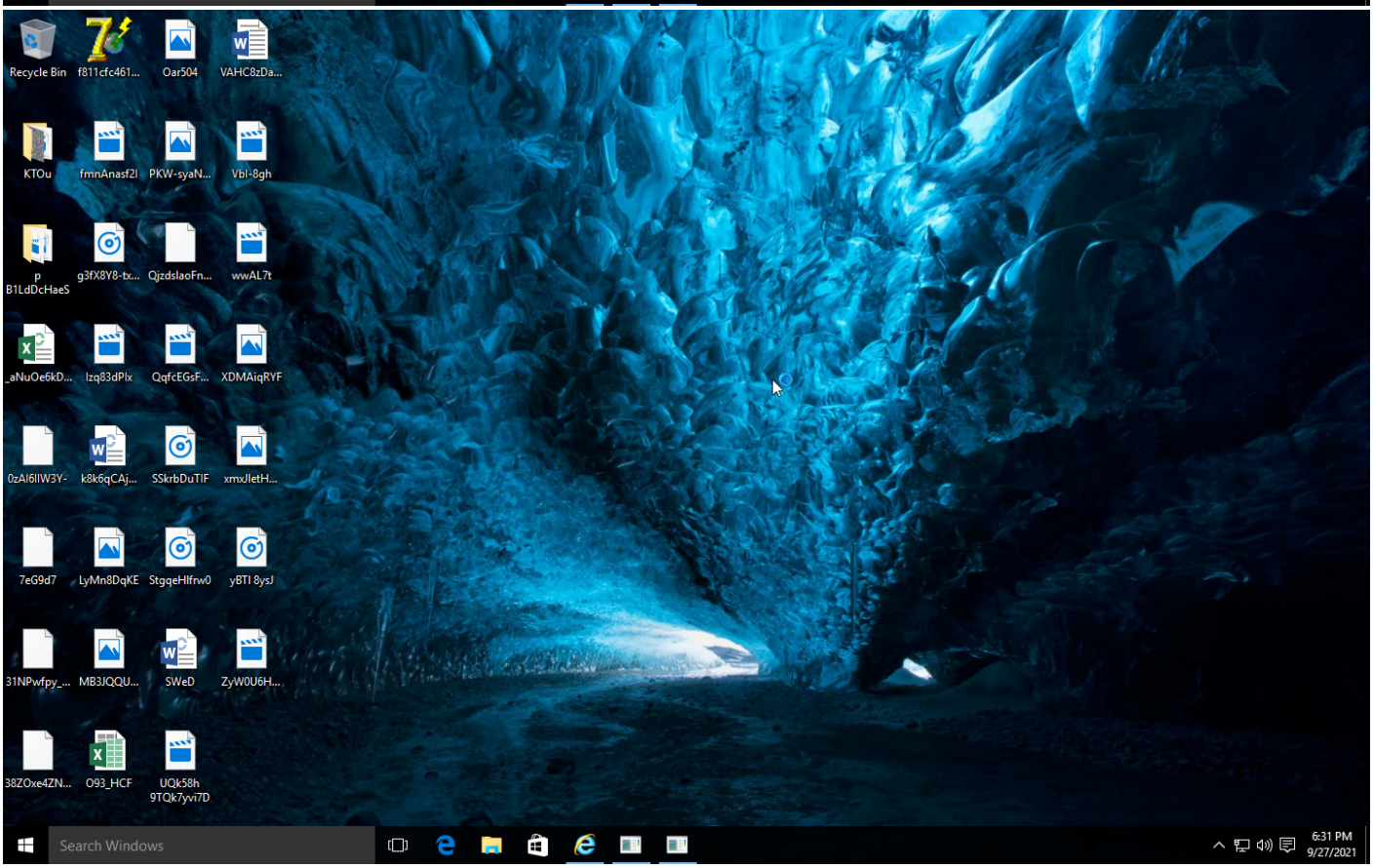
Sample Information

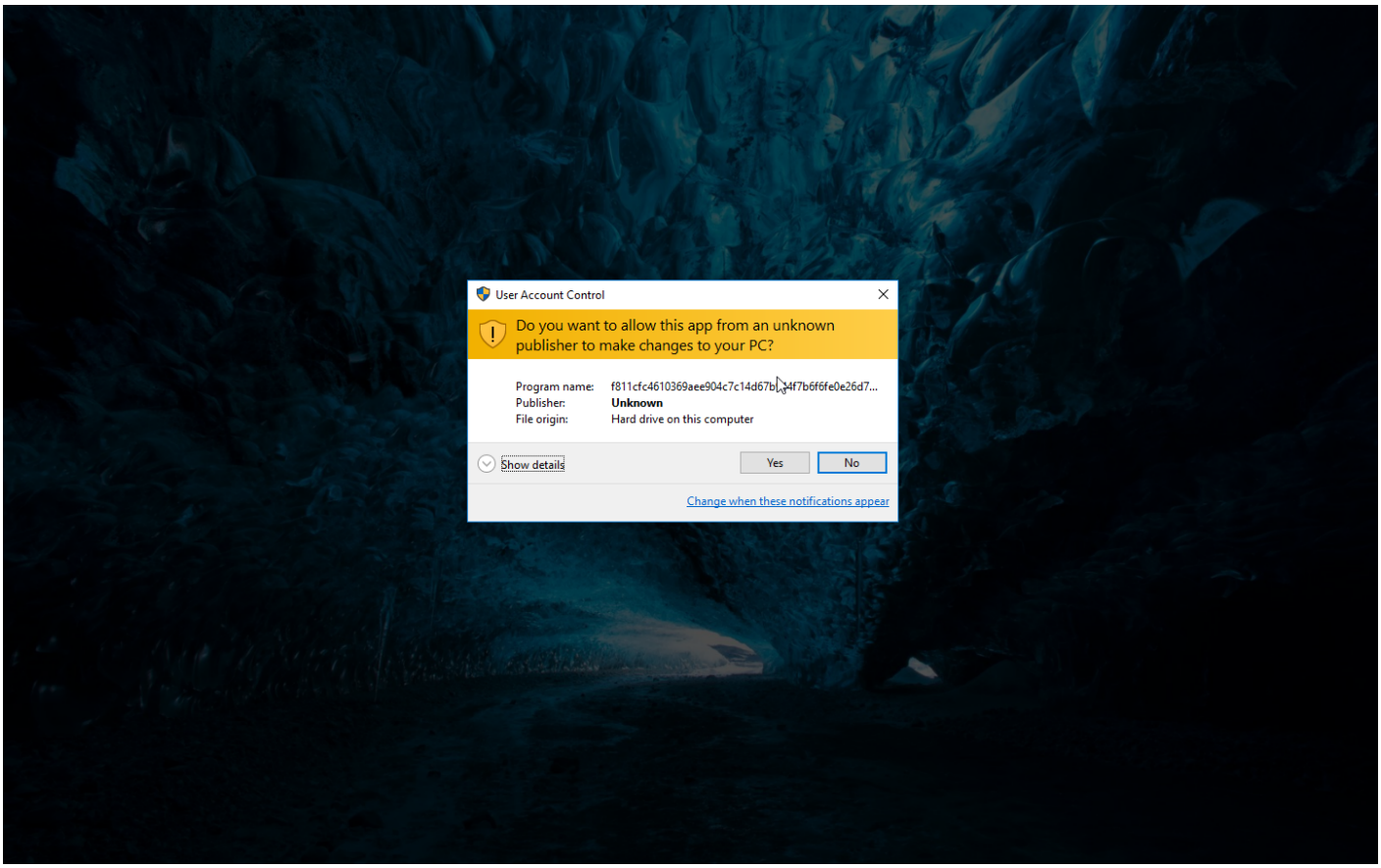
ID	#2780674
MD5	e9441b756f99ee3adf804214119c1fa1
SHA1	8fe649e6bc868401ba2a3b9bf345fc76692f53d4
SHA256	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd
SSDeep	24576:QJ6EBIZYYdVXF1EX9uOJwQ5No04Hoawhb5BJnXvxWmmq0LBPdchd:QooW9/X/vgwQ5C04lbb5BJXIVqMBPdY
ImpHash	0d4dbb56c32c47336294683fc02fb7e2
File Name	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
File Size	1610.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

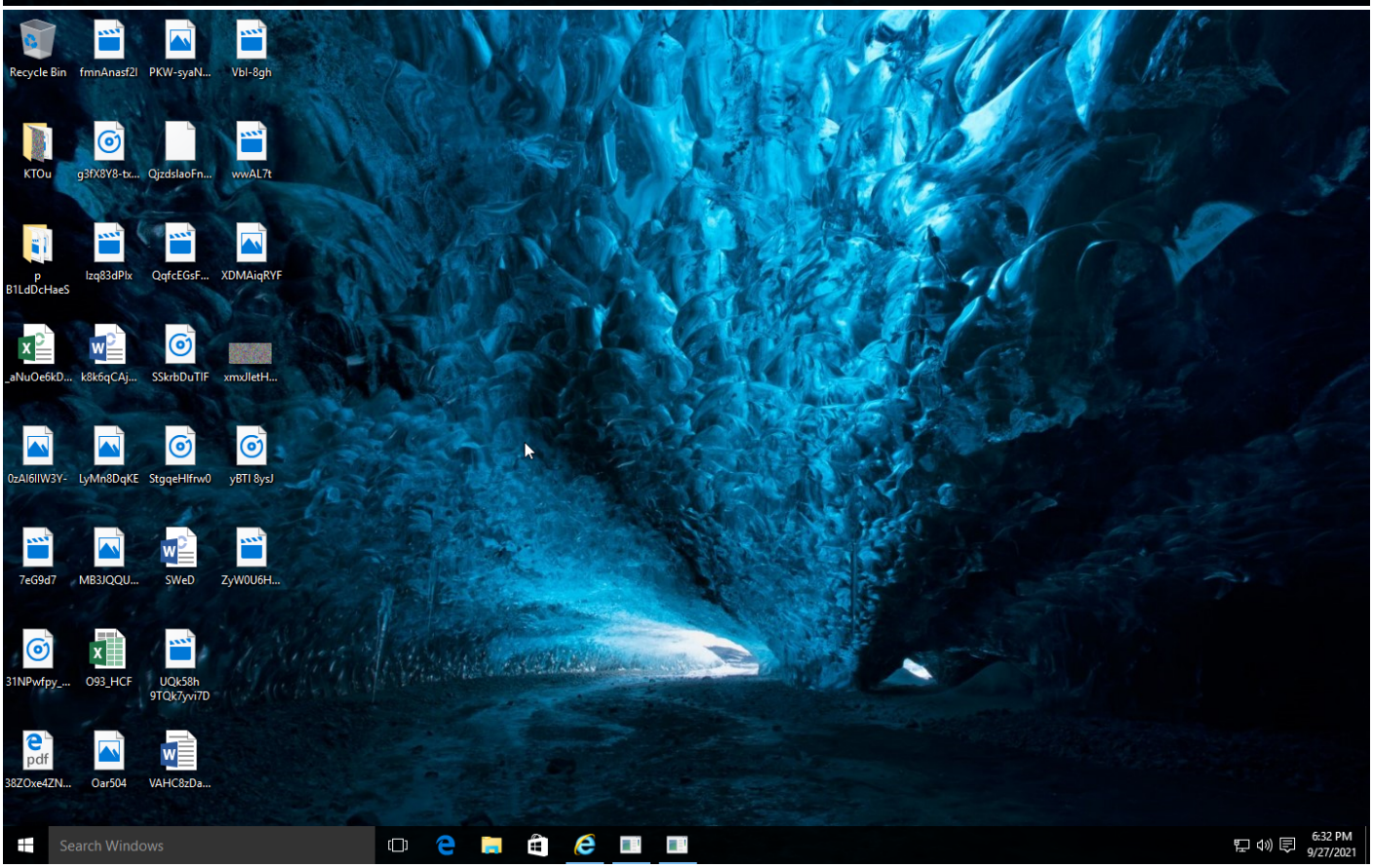
Analysis Information

Creation Time	2021-09-27 20:30 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Sample crashed
Number of Monitored Processes	18
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	30
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
f811cfc461...
Oar504
VAHC8zDa...
KTOu
fmnAnasf2I
PKW-syaN...
Vbl-8gh
p
B1LdDcHaeS
g3fX8Y8-tx...
QjzdslaoFn...
wwAL7t
_aNuOe6kD...
lzq83dPlx
QqfcEGsF...
XDMAiqRYF
0zAI6lIW3Y-
k8k6qCAj...
SSkrbDuTIF
xmxJletH...
7eG9d7
LyMn8DqKE
StgqeHlfrw0
yBTI 8ysJ
31NPwfpy_...
MB3JQQU...
SWeD
ZyW0U6H...
38ZOxe4ZN...
O93_HCF
UQk58h
9TQk7yvi7D
Search Windows
6:31 PM
9/27/2021


Recycle Bin
f811cfc461...
Oar504
VAHC8zDa...
KTOu
fmnAnasf2I
PKW-syaN...
Vbl-8gh
p
B1LdDcHaeS
g3fX8Y8-tx...
QjzdslaoFn...
wwAL7t
_aNuOe6kD...
lzq83dPlx
QqfcEGsF...
XDMAiqRYF
0zAI6lIW3Y-
k8k6qCAj...
SSkrbDuTIF
xmxJletH...
7eG9d7
LyMn8DqKE
StgqeHlfrw0
yBTI 8ysJ
31NPwfpy_...
MB3JQQU...
SWeD
ZyW0U6H...
38ZOxe4ZN...
O93_HCF
UQk58h
9TQk7yvi7D
Search Windows
6:31 PM
9/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: f811cfc4610369aee904c7c14d67b[illegible]4f7b6f6fe0e26d7...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
fmnAnasf2l
PKW-syaN...
Vbl-8gh
KTOu
g3fX8Y8-tx...
QjzdslaoFn...
wwAL7t
p
B1LdDcHaeS
lzq83dPlx
QqfcEGsF...
XDMAiqRYF
_aNuOe6kD...
k8k6qCAj...
SSkrbDuTIF
xmxJletH...
0zAI6lIW3Y-
LyMn8DqKE
StgqeHlfrw0
yBTI 8ysJ
7eG9d7
MB3JQQU...
SWeD
ZyW0U6H...
31NPwfpy_...
O93_HCF
UQk58h
9TQk7yvi7D
38ZOxe4ZN...
Oar504
VAHC8zDa...
Search Windows
6:32 PM
9/27/2021

NETWORK

General

201.14 KB total sent

2431.24 KB total received

2 ports 80, 443

3 contacted IP addresses

0 URLs extracted

7 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

10 URLs contacted, 3 servers

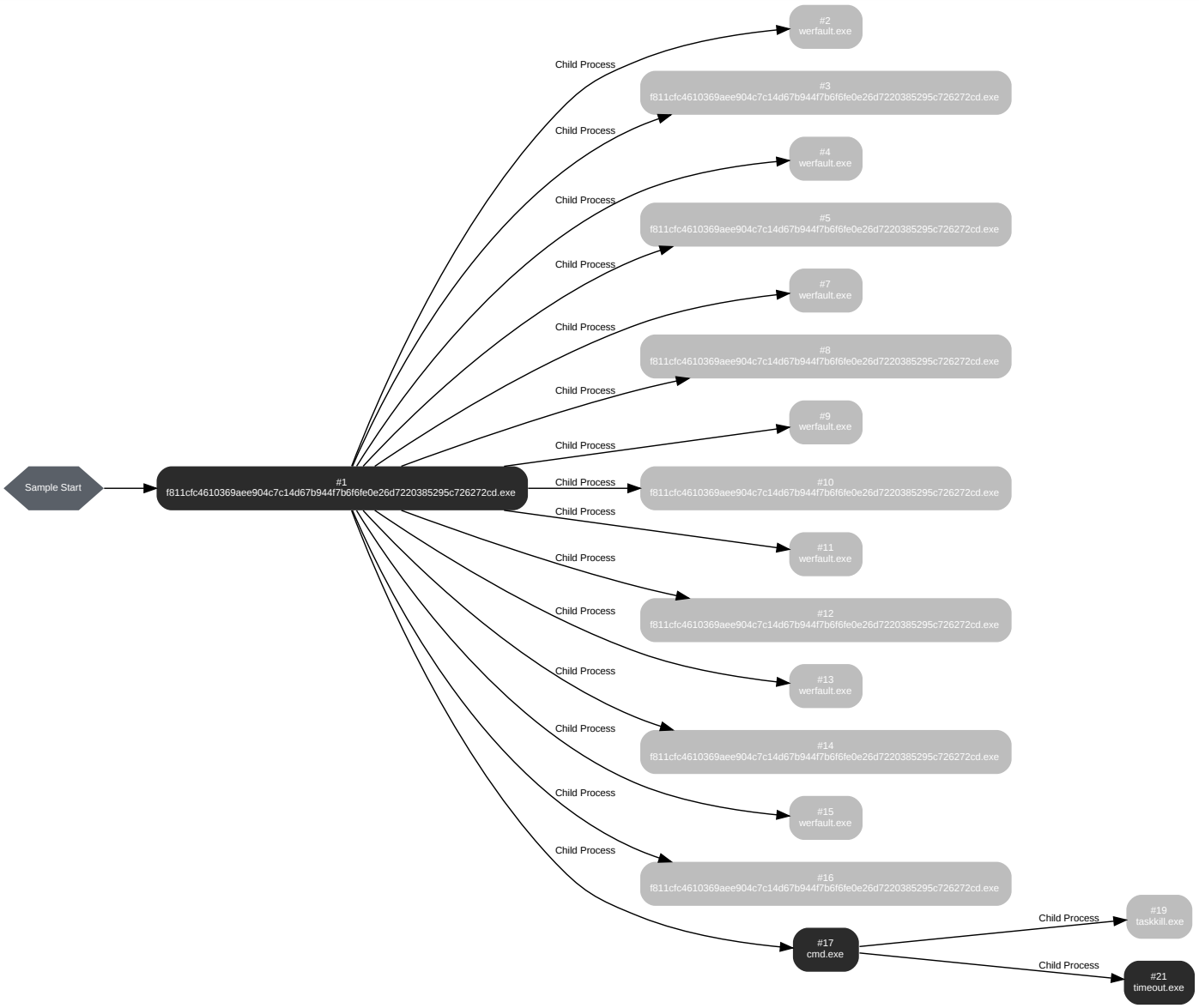
3 sessions, 201.14 KB sent, 2431.24 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	23.88.105.196/1013	-	-		0 bytes	NA
GET	23.88.105.196/freebl3.dll	-	-		0 bytes	NA
GET	23.88.105.196/mozglue.dll	-	-		0 bytes	NA
GET	23.88.105.196/msvcp140.dll	-	-		0 bytes	NA
GET	23.88.105.196/nss3.dll	-	-		0 bytes	NA
GET	23.88.105.196/softokn3.dll	-	-		0 bytes	NA
GET	23.88.105.196/vcruntime140.dll	-	-		0 bytes	NA
POST	23.88.105.196/	-	-		0 bytes	NA
GET	ok/	-	-		0 bytes	NA
GET	https://mas.to/@killern0	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 49737, Reason: Analysis Target
Unmonitor End Time	End Time: 132908, Reason: Crashed
Monitor duration	83.17s
Return Code	1
PID	1468
Parent PID	1600
Bitness	32 Bit

Dropped Files (10)

File Name	File Size	SHA256	YARA Match
-	326.45 KB	a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	✗
-	133.95 KB	3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd	✗
-	429.80 KB	334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	✗
-	1216.95 KB	e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	✗
-	141.45 KB	43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	✗
-	81.82 KB	c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	✗
files\information.txt	4.73 KB	7a67f75d9d49c23fcbbc28782d88b234701eb446f5d0464c6c0b89c8c4a79235	✗
Default.zip	22 bytes	8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85	✗
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\screenshot.jpg	185.16 KB	4efa7567f5144004bd189ac9875d6c695a9a21112c90e174d4f4a33eabfbd3b2	✗
03845cb8-7441-4a2f-8c0f-c90408af57783083953543.zip	186.94 KB	9c13f284bb92a0d27b9d3bc8500009077eb5cce01a88470b1740f0b52f906641	✗

Host Behavior

Type	Count
Module	335
Keyboard	5
System	53
Registry	169
-	3
Window	5
Process	367
File	799
Environment	1

Type	Count
User	5

Network Behavior

Type	Count
HTTP	9
HTTPS	1
TCP	3

Process #2: werfault.exe

ID	2
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 748
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 86520, Reason: Child Process
Unmonitor End Time	End Time: 92263, Reason: Terminated
Monitor duration	5.74s
Return Code	0
PID	5088
Parent PID	1468
Bitness	32 Bit

Process #3: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 88239, Reason: Child Process
Unmonitor End Time	End Time: 92352, Reason: Terminated
Monitor duration	4.11s
Return Code	259
PID	2372
Parent PID	1468
Bitness	32 Bit

Process #4: werfault.exe

ID	4
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 764
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 91545, Reason: Child Process
Unmonitor End Time	End Time: 94606, Reason: Terminated
Monitor duration	3.06s
Return Code	0
PID	2976
Parent PID	1468
Bitness	32 Bit

Process #5: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 92205, Reason: Child Process
Unmonitor End Time	End Time: 95137, Reason: Terminated
Monitor duration	2.93s
Return Code	259
PID	5092
Parent PID	1468
Bitness	32 Bit

Process #7: werfault.exe

ID	7
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 796
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 94654, Reason: Child Process
Unmonitor End Time	End Time: 97257, Reason: Terminated
Monitor duration	2.60s
Return Code	0
PID	1376
Parent PID	1468
Bitness	32 Bit

Process #8: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 95528, Reason: Child Process
Unmonitor End Time	End Time: 97627, Reason: Terminated
Monitor duration	2.10s
Return Code	259
PID	2232
Parent PID	1468
Bitness	32 Bit

Process #9: werfault.exe

ID	9
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1068
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 99638, Reason: Child Process
Unmonitor End Time	End Time: 102114, Reason: Terminated
Monitor duration	2.48s
Return Code	0
PID	2876
Parent PID	1468
Bitness	32 Bit

Process #10: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 100240, Reason: Child Process
Unmonitor End Time	End Time: 102693, Reason: Terminated
Monitor duration	2.45s
Return Code	259
PID	320
Parent PID	1468
Bitness	32 Bit

Process #11: werfault.exe

ID	11
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1332
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 103466, Reason: Child Process
Unmonitor End Time	End Time: 106425, Reason: Terminated
Monitor duration	2.96s
Return Code	0
PID	4016
Parent PID	1468
Bitness	32 Bit

Process #12: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 103751, Reason: Child Process
Unmonitor End Time	End Time: 106527, Reason: Terminated
Monitor duration	2.78s
Return Code	259
PID	4032
Parent PID	1468
Bitness	32 Bit

Process #13: werfault.exe

ID	13
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1392
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 111817, Reason: Child Process
Unmonitor End Time	End Time: 114022, Reason: Terminated
Monitor duration	2.21s
Return Code	0
PID	2060
Parent PID	1468
Bitness	32 Bit

Process #14: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 112140, Reason: Child Process
Unmonitor End Time	End Time: 114564, Reason: Terminated
Monitor duration	2.42s
Return Code	259
PID	4708
Parent PID	1468
Bitness	32 Bit

Process #15: werfault.exe

ID	15
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1348
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 114142, Reason: Child Process
Unmonitor End Time	End Time: 116891, Reason: Terminated
Monitor duration	2.75s
Return Code	0
PID	4760
Parent PID	1468
Bitness	32 Bit

Process #16: f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 114396, Reason: Child Process
Unmonitor End Time	End Time: 117082, Reason: Terminated
Monitor duration	2.69s
Return Code	259
PID	3420
Parent PID	1468
Bitness	32 Bit

Process #17: cmd.exe

ID	17
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c taskkill /im f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe /f & timeout /t... ...Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe" & del C:\ProgramData*.dll & exit
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 120007, Reason: Child Process
Unmonitor End Time	End Time: 140388, Reason: Terminated
Monitor duration	20.38s
Return Code	0
PID	1240
Parent PID	1468
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	38
Environment	27
System	1
Process	2

Process #19: taskkill.exe

ID	19
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /im f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe /f
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 127326, Reason: Child Process
Unmonitor End Time	End Time: 133888, Reason: Terminated
Monitor duration	6.56s
Return Code	0
PID	3976
Parent PID	1240
Bitness	32 Bit

Process #21: timeout.exe

ID	21
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout /t 6
Initial Working Directory	C:\ProgramData\
Monitor Start Time	Start Time: 132912, Reason: Child Process
Unmonitor End Time	End Time: 140311, Reason: Terminated
Monitor duration	7.40s
Return Code	0
PID	3104
Parent PID	1240
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
System	77
File	58

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd	C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	Sample File	1610.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
5c5a213b1a4cf1518a5da63335dd7535017d4947c21361b9641044cb8f23521e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
7a67f75d9d49c23fcbbc28782d88b234701eb446f5d0464c6c0b89c8c4a79235	C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\information.txt, information.txt, files\information.txt	Dropped File	4.73 KB	text/plain	Create, Write, Read, Access	CLEAN
8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85	C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Files\Default.zip, Files/Default.zip, Default.zip	Dropped File	22 bytes	application/zip	Access, Write, Read, Delete, Create	CLEAN
4efa7567f5144004bd189ac9875d6c695a9a21112c90e174d4f4a33eabfbd3b2	C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\screenshot.jpg, screenshot.jpg	Dropped File	185.16 KB	image/jpeg	Read, Access, Delete	CLEAN
a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	C:\ProgramData\\freebl3.dll	Downloaded File	326.45 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd	C:\ProgramData\\mozglue.dll	Downloaded File	133.95 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	C:\ProgramData\\msvcp140.dll	Downloaded File	429.80 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	C:\ProgramData\\nss3.dll	Downloaded File	1216.95 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	C:\ProgramData\\softokn3.dll	Downloaded File	141.45 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	C:\ProgramData\\vcruntime140.dll	Downloaded File	81.82 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	CLEAN
9c13f284bb92a0d27b9d3bc8500009077eb5cce01a88470b1740f0b52f906641	03845cb8-7441-4a2f-8c0f-c90408af57783083953543.zip	Downloaded File	186.94 KB	application/zip	Access, Write, Read, Delete, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	Sample File	Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1	Accessed File	Create, Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files	Accessed File	Create, Access	CLEAN
C:\ProgramData\\freebl3.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\\mozglue.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\\msvcp140.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\\nss3.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\\softokn3.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\\vcruntime140.dll	Downloaded File	Create, Write, Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Autofill	Accessed File	Create, Access, Delete	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Cookies	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\CC	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\History	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Downloads	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets	Accessed File	Create, Access, Delete	CLEAN
passwords.txt	Accessed File	Create, Access	CLEAN
Cookies\IE_Cookies.txt	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Cookies\Low\????	Accessed File	Access	CLEAN
Cookies\Edge_Cookies.txt	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies\??????	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies\???	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\..\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera GX Stable\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\\Local State	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Nichrome\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Maxthon5\Users\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\brave\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\TorBro\Profile\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Suhba\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Rafotech\Mustang\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\ \Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Browser\Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CryptoTab Browser\User Data\\Local State	Accessed File	Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Soft	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Soft\Authy	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Soft\Authy\8	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Authy Desktop\Local Storage\8	Accessed File	Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Soft\AuthyNew	Accessed File	Create, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Soft\AuthyNew\(	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Authy Desktop\Local Storage\leveldb\(	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\Profiles\..\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Telegram	Accessed File	Create, Access, Delete	CLEAN

File Name	Category	Operations	Verdict
c	Accessed File	Access, Delete	CLEAN
h	Accessed File	Access, Delete	CLEAN
files\information.txt	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Files	Accessed File	Create, Access, Delete	CLEAN
Default.zip	Dropped File	Create, Write, Access	CLEAN
03845cb8-7441-4a2f-8c0f-c90408af57783083953543.zip	Downloaded File	Access, Write, Read, Delete, Create	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Cookies\Edge_Cookies.txt	Accessed File	Read, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Cookies\IE_Cookies.txt	Accessed File	Read, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Files\Default.zip	Dropped File	Read, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\information.txt	Dropped File	Read, Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\passwords.txt	Accessed File	Read, Access	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\screenshot.jpg	Dropped File	Read, Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Atomic	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Binance	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Coinomi	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\ElectronCash	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Electrum	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\ElectrumLTC	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Exodus	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\JAXX	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Jaxx_New	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\Monero	Accessed File	Access, Delete	CLEAN
C:\ProgramData\EP87SX37HD9CG2ZMD4JQML7K1\files\Wallets\MultiDoge	Accessed File	Access, Delete	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\ProgramData	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	Accessed File	Write, Access	CLEAN
C:\ProgramData*.dll	Accessed File	Access	CLEAN
\??\C:\ProgramData\freebl3.dll	Accessed File	Write, Access	CLEAN
\??\C:\ProgramData\mozglue.dll	Accessed File	Write, Access	CLEAN
\??\C:\ProgramData\msvcp140.dll	Accessed File	Write, Access	CLEAN
\??\C:\ProgramData\nss3.dll	Accessed File	Write, Access	CLEAN
\??\C:\ProgramData\softokn3.dll	Accessed File	Write, Access	CLEAN
\??\C:\ProgramData\vcruntime140.dll	Accessed File	Write, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://23.88.105.196/freebl3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/mozglue.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/msvcp140.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/nss3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/softokn3.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/vcruntime140.dll	-	23.88.105.196	-	GET	MALICIOUS
http://23.88.105.196/1013	-	23.88.105.196	-	POST	CLEAN
http://23.88.105.196	-	23.88.105.196	-	POST	CLEAN
https://mas.to/@killern0	-	88.99.75.82	-	GET	CLEAN
http://ok	-	-	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mas.to	88.99.75.82	-	HTTPS	CLEAN
ok	, 23.88.105.196	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
88.99.75.82	mas.to	Germany	DNS, TCP, HTTPS	CLEAN
23.88.105.196	-	Germany	TCP, HTTP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe	"C:\Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe"	MALICIOUS
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 748	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 764	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 796	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1068	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1332	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1392	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1468 -s 1348	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c taskkill /im f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe /f & timeout /t... ...Users\RDhJ0CNFevzX\Desktop\f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe" & del C:\ProgramData*.dll & exit	CLEAN
taskkill.exe	taskkill /im f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd.exe /f	CLEAN
timeout.exe	timeout /t 6	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	CryptOne_Packer	Shellcode used by the CryptOne packer	Memory Dump	-	-	5/5

Antivirus (30)

File Type	Threat Name	File Name	Verdict
Memory Dump	DeepScan:Generic.SpyAgent.6.6AF37D2E	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	Gen:Trojan.Heur.FU.MnZ@aSAwybp	-	MALICIOUS
Memory Dump	DeepScan:Generic.SpyAgent.6.6AF37D2E	-	MALICIOUS

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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-27 13:37:06+00:00
Built-in AV Database Records	10469506

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