MALICIOUS

Classifications: Spyware | Injector | Downloader

Threat Names: SmokeLoader | RedNet | Mal/HTMLGen-A | C2/Generic-A | Gen:Variant.Cerbu.113972 | Generic.Andromeda.79093CCD | Gen:Variant.Razy.655877 | Generic.Andromeda.02C8F119 | Gen:Variant.Bulz.765812 | Gen:Heur.Mint.Zard.52

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe**
ID	#1133723
MD5	db2ef30e8f821c8f00456941f5944849
SHA1	01a08a69f1e8e6d822ece577a9ebe84a0c7f5f60
SHA256	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3
File Size	286.00 KB
Report Created	2021-11-10 00:13 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (40 rules, 84 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe. • Rule "Packer_RedNet" from ruleset "Generic" has matched on a memory dump for (process #8) 892f.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer / Edge, Opera, Electrum Bitcoin Wallet, Exodus Cryptocurrency Wallet, Total Commander, FileZilla, The Bat!.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe creates thread in (process #3) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	8	-
	• Built-in AV detected "Gen:Variant.Cerbu.113972" in the PCAP of the analysis. • Built-in AV detected "Gen:Variant.Cerbu.113972" in the response data of URL "host-host-file6.com/files/9985_1636488425_1340.exe". • Built-in AV detected the downloaded file C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe as "Gen:Variant.Cerbu.113972". • Built-in AV detected a memory dump of (process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe as "Generic.Andromeda.79093CCD". • Built-in AV detected a memory dump of (process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe as "Gen:Variant.Razy.655877". • Built-in AV detected a memory dump of (process #8) 892f.exe as "Generic.Andromeda.02C8F119". • Built-in AV detected a memory dump of (process #8) 892f.exe as "Gen:Variant.Bulz.765812". • Built-in AV detected a memory dump of (process #3) explorer.exe as "Gen:Heur.Mint.Zard.52".			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	4	-
	• Reputation analysis labels the URL "nalirou70.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "host-host-file6.com/files/8071_1636483658_131.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "host-host-file6.com/files/9985_1636488425_1340.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "host-host-file6.com/files/628_1636491663_2386.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 185.215.113.46 as "C2/Generic-A".			
3/5	Data Collection	Reads cryptocurrency wallet locations	2	-
	• (Process #7) 64be.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #7) 64be.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			

Score	Category	Operation	Count	Classification
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #7) 64be.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntivirusProduct".			
3/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #7) 64be.exe tries to detect anti-spyware software via WMI query: "SELECT * FROM AntiSpyWareProduct".			
3/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #7) 64be.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih". • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe".			
2/5	Discovery	Executes WMI query	7	-
	• (Process #5) 2e7b.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #7) 64be.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #7) 64be.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'. • (Process #7) 64be.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #7) 64be.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #7) 64be.exe executes WMI query: SELECT * FROM FirewallProduct. • (Process #7) 64be.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #5) 2e7b.exe queries hardware properties via WMI. • (Process #7) 64be.exe queries hardware properties via WMI.			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #5) 2e7b.exe tries to read sensitive data of ftp application "Total Commander" by file. • (Process #7) 64be.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #7) 64be.exe reads the network adapters' addresses by API.			
2/5	Discovery	Enumerates running processes	2	-
	• (Process #7) 64be.exe enumerates running processes via WMI. • (Process #3) explorer.exe enumerates running processes.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #7) 64be.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	2	-

Score	Category	Operation	Count	Classification
	• (Process #7) 64be.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #7) 64be.exe tries to read sensitive data of web browser "Opera" by file.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Logon. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Time. Task has been rescheduled by the analyzer.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe modifies memory of (process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe alters context of (process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe.			
2/5	YARA	Suspicious content matched by YARA rules	3	-
	• Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on the downloaded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe". • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) 64be.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #3) explorer.exe.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe reads from (process #2) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38".			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #3) explorer.exe starts (process #5) 2e7b.exe with a hidden window. • (Process #3) explorer.exe starts (process #7) 64be.exe with a hidden window. • (Process #3) explorer.exe starts (process #8) 892f.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #7) 64be.exe enables process privilege "SeDebugPrivilege". • (Process #8) 892f.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	1	-
	• (Process #7) 64be.exe tries to gather information about application "FileZilla" by file.			
1/5	YARA	Content matched by YARA rules	6	-

Score	Category	Operation	Count	Classification
	• Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on the downloaded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe". • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on the downloaded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe". • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) 64be.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) 64be.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #3) explorer.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #3) explorer.exe.			
1/5	Obfuscation	Resolves API functions dynamically	4	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe resolves 39 API functions by name. • (Process #8) 892f.exe resolves 108 API functions by name. • (Process #7) 64be.exe resolves 52 API functions by name. • (Process #5) 2e7b.exe resolves 48 API functions by name.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #7) 64be.exe resolves host name "api.ip.sb" to IP "104.26.12.31".			
1/5	Network Connection	Connects to remote host	4	-
	• (Process #8) 892f.exe opens an outgoing TCP connection to host "185.215.113.46:80". • (Process #7) 64be.exe opens an outgoing TCP connection to host "104.26.12.31:443". • (Process #5) 2e7b.exe opens an outgoing TCP connection to host "185.92.73.142:52097". • (Process #7) 64be.exe opens an outgoing TCP connection to host "185.198.164.33:80".			
1/5	Network Connection	Downloads executable	3	Downloader
	• (Process #3) explorer.exe downloads executable via http from host-host-file6.com/files/8071_1636483658_131.exe. • (Process #3) explorer.exe downloads executable via http from host-host-file6.com/files/9985_1636488425_1340.exe. • (Process #3) explorer.exe downloads executable via http from host-host-file6.com/files/628_1636491663_2386.exe.			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #5) 2e7b.exe tries to connect to TCP port 52097 at 185.92.73.142.			
1/5	Execution	Executes itself	2	-
	• (Process #1) 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe.			

Mitre ATT&CK Matrix

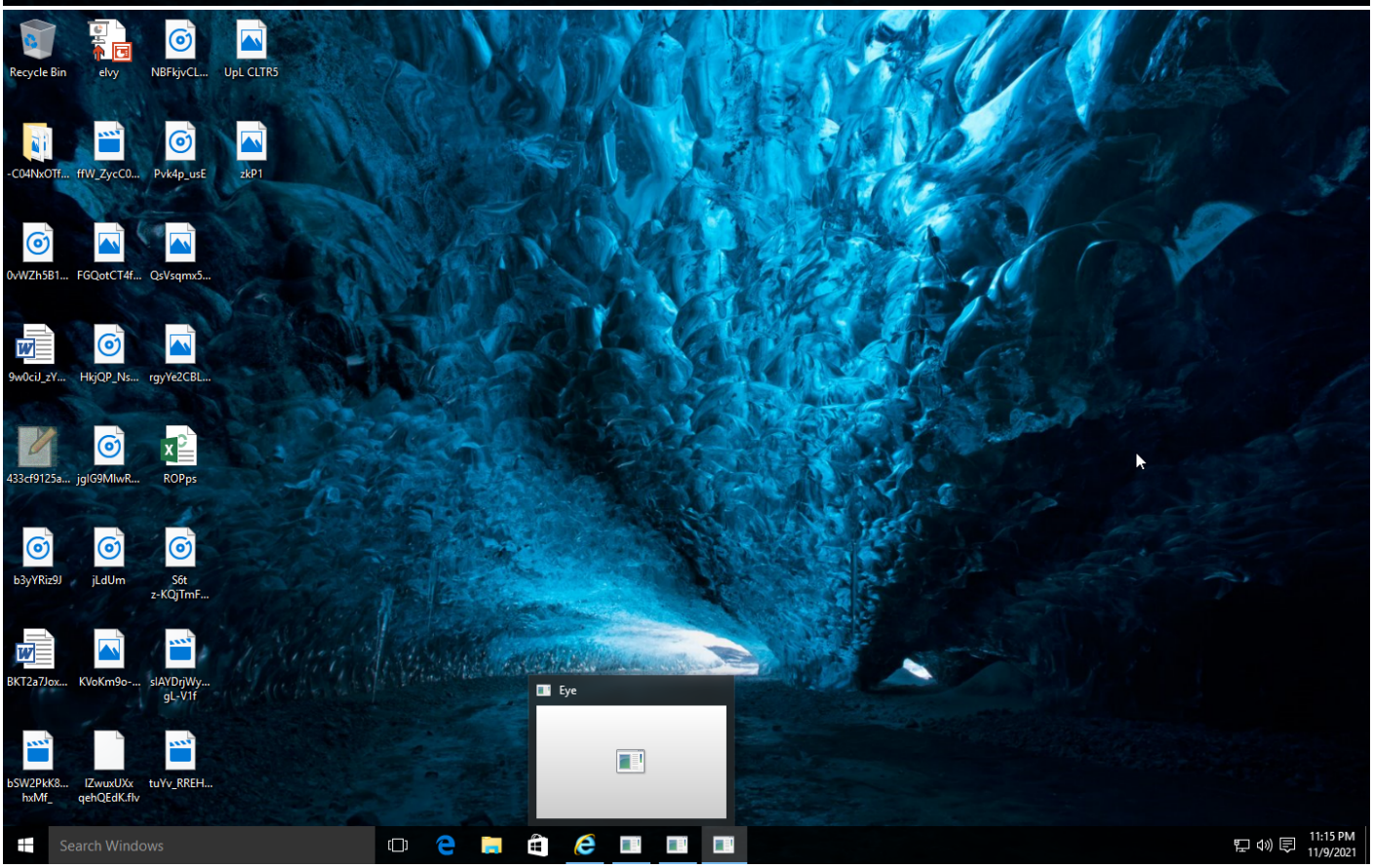
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
	#T1053 Scheduled Task			#T1096 NTFS File Attributes		#T1082 System Information Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1083 File and Directory Discovery			#T1065 Uncommonly Used Port		
						#T1016 System Network Configuration Discovery					
						#T1063 Security Software Discovery					

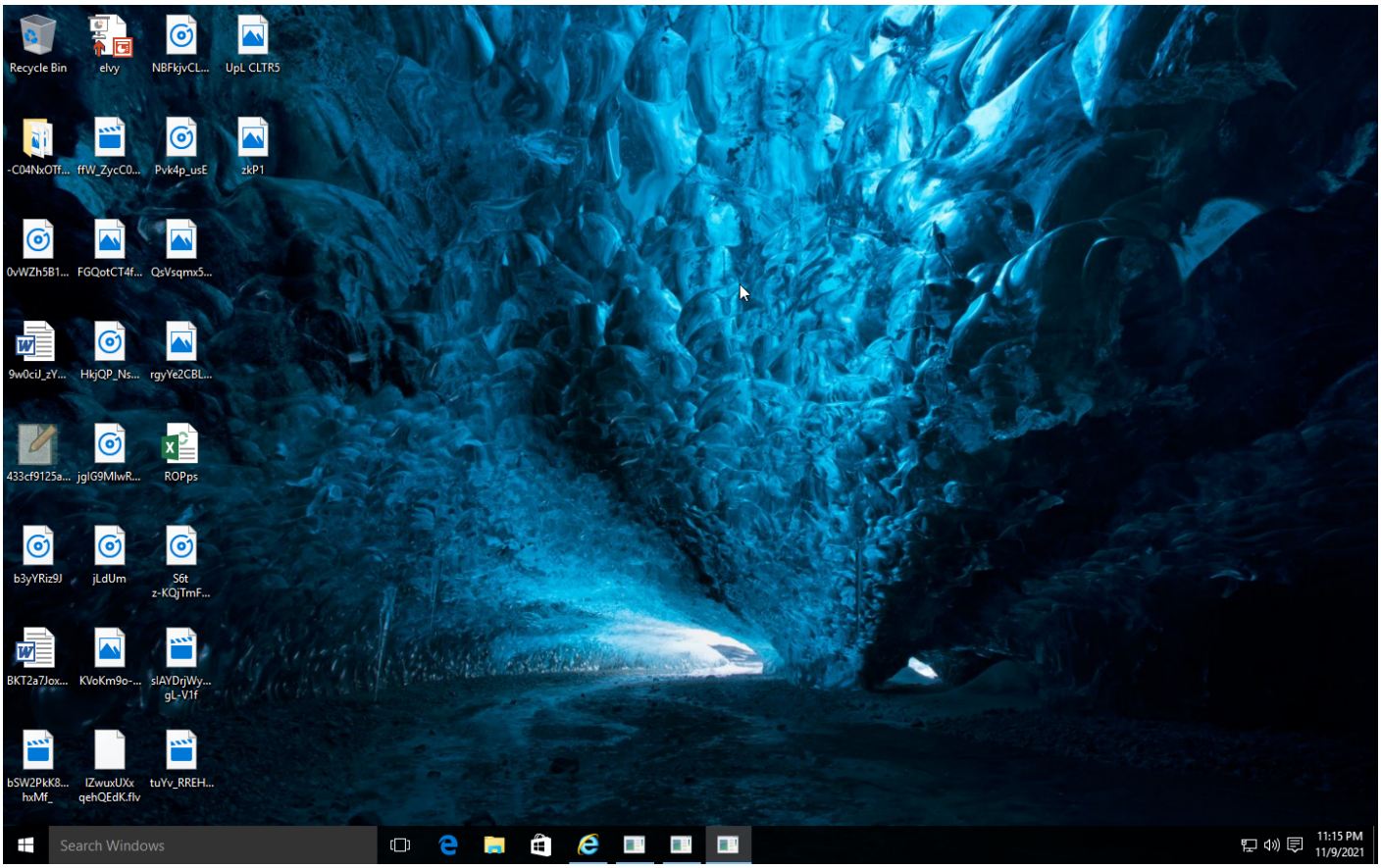
Sample Information

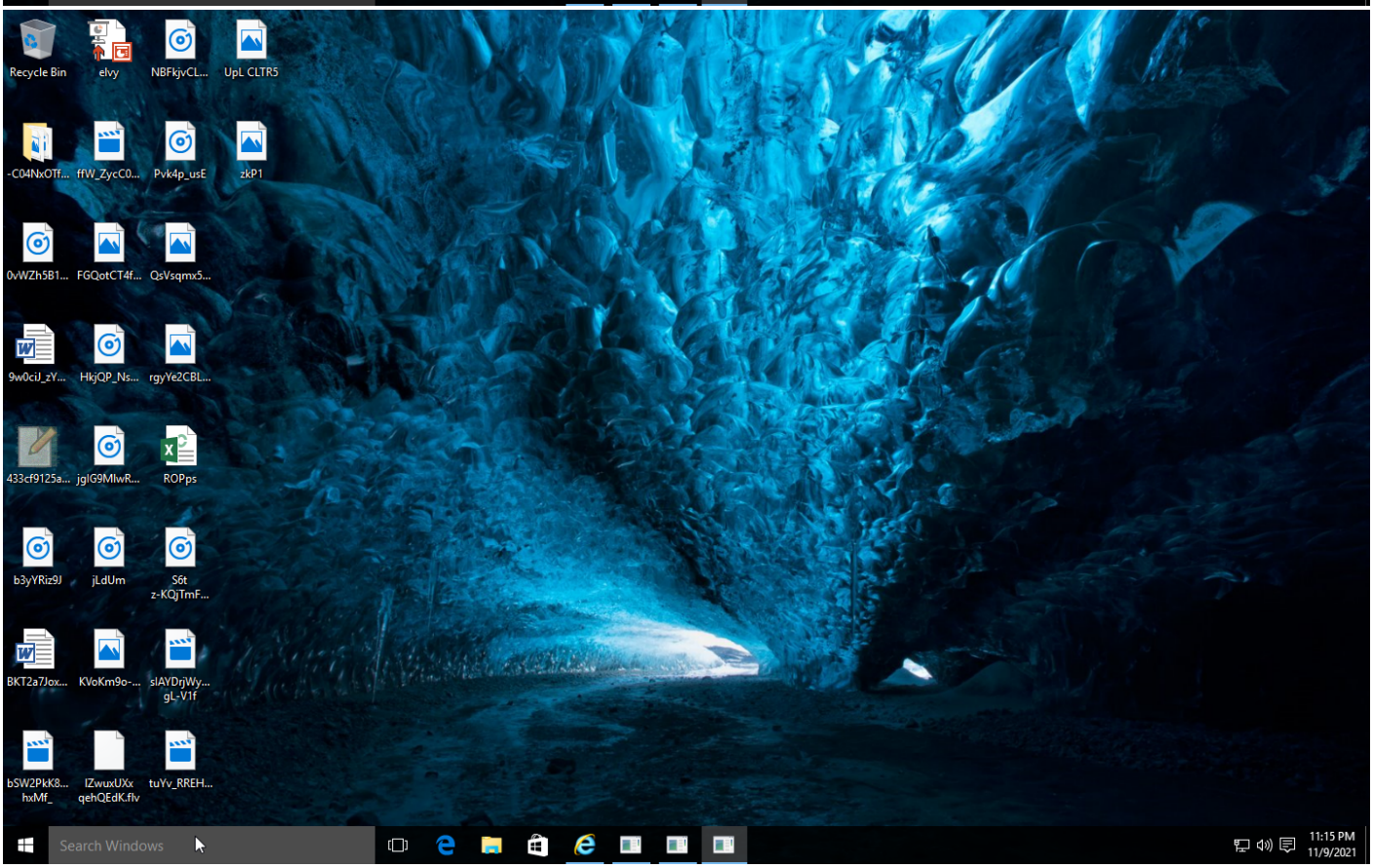
ID	#1133723
MD5	db2ef30e8f821c8f00456941f5944849
SHA1	01a08a69f1e8e6d822ece577a9ebe84a0c7f5f60
SHA256	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3
SSDeep	3072:6zyig02ASl6xXrDXa23CiVfcC5DBoLtJalC4CrraxIsgUUirwX0m5Sl5nTk5DItT:6xxXoiVfcGB0valC4CrrqR3rC0z5+k
ImpHash	a5effb4de201aefae267d5eef9a314ac
File Name	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe
File Size	286.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-11-10 00:13 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
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	7
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	15


Recycle Bin
elvy
NBFkjvCL...
UpL CLTR5
-C04NxOTf...
ffW_ZycC0...
Pvk4p_usE
zkP1
0vWZh5B1...
FGQotCT4f...
QsVsqmx5...
9w0ciJ_zY...
HkjQP_Ns...
rgyYe2CBL...
433cf9125a...
jglG9MlwR...
ROPps
b3yYRiz9J
jLdUm
S6t z-KQjTmF...
BKT2a7Jox...
KVoKm9o-...
slAYDrjWy... gL-V1f
bSW2PkK8... hxMf_
IZwuxUXx qehQEdK.flv
tuYv_RREH...
Eye
Search Windows
11:15 PM
11/9/2021





Screenshots truncated

NETWORK

General

975.42 KB total sent

1159.75 KB total received

3 ports 80, 52097, 443

6 contacted IP addresses

0 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

5 URLs contacted, 2 servers

20 sessions, 12.25 KB sent, 1138.21 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	nalirou70.top/	-	-		0 bytes	NA
GET	host-host-file6.com/files/8071_1636483658_131.exe	-	-		0 bytes	NA
GET	host-host-file6.com/files/9985_1636488425_1340.exe	-	-		0 bytes	NA
GET	host-host-file6.com/files/628_1636491663_2386.exe	-	-		0 bytes	NA
GET	https://api.ip.sb/ip	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.ip.sb, api.ip.sb.cdn.cloudflare.net	NoError	104.26.12.31, 104.26.13.31, 172.67.75.172	api.ip.sb.cdn.cloudflare.net	NA
-	api.ip.sb	-	104.26.12.31, 104.26.13.31, 172.67.75.172		NA

BEHAVIOR

Process Graph

Process #1: 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 67099, Reason: Analysis Target
Unmonitor End Time	End Time: 92035, Reason: Terminated
Monitor duration	24.94s
Return Code	0
PID	5020
Parent PID	1636
Bitness	32 Bit

Host Behavior

Type	Count
Module	51
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: 433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86316, Reason: Child Process
Unmonitor End Time	End Time: 103235, Reason: Terminated
Monitor duration	16.92s
Return Code	0
PID	380
Parent PID	5020
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0x13a0	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0x13a0	0x401000(4198400)	0x7000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0x13a0	0x2e4008(3031048)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0x13a0 / 0xd14	0x772d8fe0(1999474656)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	12
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 99642, Reason: Injection
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	208.97s
Return Code	Unknown
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0xd14	0x410000(4259840)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0xd14	0x420000(4325376)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	0xd14	0x421920(4331808)	-	✓	1

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	286.00 KB	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.exe	140.50 KB	f071bb54ef89464b10aec76d59532d8eb0087b32508a584fbf7a9e3f78cff9d0	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	554.00 KB	52f0387abaa5763ce2d9fd13388660c3c7bb256c7715c37b434abab63dda3717	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe	393.50 KB	efa0c9fc855126fffc9e80bf8de21fa10ab736e14d1956d025b450969a38450c	✗

Host Behavior

Type	Count
Module	23
System	5105
Process	10847
Mutex	1
Registry	2
File	25
User	1

Type	Count
COM	1

Network Behavior

Type	Count
HTTP	19
TCP	19

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 148703, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	159.91s
Return Code	Unknown
PID	836
Parent PID	532
Bitness	64 Bit

Process #5: 2e7b.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\2e7b.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 157397, Reason: Child Process
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	151.21s
Return Code	Unknown
PID	2568
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Environment	1
File	179
Registry	17
Module	55
Window	1
Keyboard	1
User	2
-	3
COM	5
-	1

Network Behavior

Type	Count
TCP	1

Process #6: bcatcih

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 158086, Reason: Child Process
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	150.52s
Return Code	Unknown
PID	3480
Parent PID	836
Bitness	32 Bit

Host Behavior

Type	Count
Module	7
File	3
Environment	1

Process #7: 64be.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\64be.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 171324, Reason: Child Process
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	137.28s
Return Code	Unknown
PID	1260
Parent PID	1636
Bitness	32 Bit

Host Behavior

Type	Count
Environment	12
User	3
Process	2
-	4
Module	64
System	11
File	274
Registry	31
-	106
Window	1
COM	124
-	9
Keyboard	1

Network Behavior

Type	Count
HTTPS	1
DNS	2
TCP	2

Process #8: 892f.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\892f.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 180736, Reason: Child Process
Unmonitor End Time	End Time: 308608, Reason: Terminated by Timeout
Monitor duration	127.87s
Return Code	Unknown
PID	392
Parent PID	1636
Bitness	32 Bit

Host Behavior

Type	Count
Module	200
File	25
Environment	2
System	4
User	1
Registry	2

Network Behavior

Type	Count
TCP	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3	C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	286.00 KB	application/vnd.microsoft.portable-executable	Create, Delete, Access, Write	MALICIOUS
f071bb54ef89464b10aec76d59532d8eb0087b32508a584fbf7a9e3f78cff9d0	C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.exe	Downloaded File	140.50 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	MALICIOUS
52f0387abaa5763ce2d9fd13388660c3c7bb256c7715c37b434abab63dda3717	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	Downloaded File	554.00 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	MALICIOUS
efa0c9fc855126fffc9e80bf8de21fa10ab736e14d1956d025b450969a38450c	C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe	Downloaded File	393.50 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	Sample File	Delete, Access	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	Create, Delete, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.exe	Downloaded File	Create, Access, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	Downloaded File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\2E7B.exe.config	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe	Downloaded File	Create, Access, Write	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IMM32.DLL	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\ole32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\combase.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SspiCli.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msvcr100.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\kernel.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\mscoree.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\8062d427acd64e37f4fded7b00f4a869\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\cc4e5d110dd318e8b7d61a9ed184ab74\System.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\9b645a48c9bcfc95aaadf6a069bb4ebe\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\8cd2187094ba6cade0ca0fab4f932654\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\psapi.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YaAddon	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\64BE.exe.config	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\9w0ciJ_zYUaQ.doc	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1oxP3YD.docx	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\BPGW_EoD.docx	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ideTVaRv.docx	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WZMuAsBYqfudCSlFsSG.docx	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\YdvSQ4.docx	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://nalirou70.top	-	47.74.84.15	-	POST	MALICIOUS
http://host-host-file6.com/files/8071_1636483658_131.exe	-	47.74.84.15	-	GET	MALICIOUS
http://host-host-file6.com/files/9985_1636488425_1340.exe	-	47.74.84.15	-	GET	MALICIOUS
http://host-host-file6.com/files/628_1636491663_2386.exe	-	47.74.84.15	-	GET	MALICIOUS
https://api.ip.sb/ip	-	104.26.12.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
nalirou70.top	47.74.84.15	-	HTTP	CLEAN
host-host-file6.com	47.74.84.15	-	HTTP	CLEAN
api.ip.sb	104.26.13.31, 104.26.12.31, 172.67.75.172	-	HTTPS, DNS	CLEAN
api.ip.sb.cdn.cloudflare.net	104.26.13.31, 104.26.12.31, 172.67.75.172	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.215.113.46	-	Seychelles	TCP	MALICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN
47.74.84.15	nalirou70.top, host-host-file6.com	Australia	TCP, HTTP, DNS	CLEAN
104.26.12.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	TCP, HTTPS, DNS	CLEAN
185.92.73.142	-	Netherlands	TCP	CLEAN
185.198.164.33	-	Netherlands	TCP	CLEAN
104.26.13.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN
172.67.75.172	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
FE7F15060B875FB9FB2A49F08D5D03120C287F38	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	892f.exe, 64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	892f.exe, 64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	access, read	64be.exe, 2e7b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	64be.exe	CLEAN
HKEY_CURRENT_USER	access	64be.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	64be.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	64be.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	64be.exe	CLEAN

Process

Process Name	Commandline	Verdict
433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe	"C:\Users\RDhJ0CNFevzX\Desktop\433cf9125a44e304eca2c5cf3bfe2af0b1deafd1c5e8d13d559e1bac9de711b3.exe"	MALICIOUS
2e7b.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\2E7B.exe	MALICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	MALICIOUS
64be.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	MALICIOUS
892f.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\892F.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (15)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Generic	Packer_RedNet	Packer used to distribute malware	Memory Dump	-	-	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_3.txt	Downloader	5/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Downloaded File	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Downloaded File	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Downloaded File	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5

Antivirus (7)

File Type	Threat Name	File Name	Verdict
Downloaded File	Gen:Variant.Cerbu.113972	C:\Users\RDHJ0C~1\AppData\Local\Temp\64BE.exe	MALICIOUS
Web Request	Gen:Variant.Cerbu.113972	-	MALICIOUS
Memory Dump	Generic.Andromeda.79093CCD	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Generic.Andromeda.02C8F119	-	MALICIOUS
Memory Dump	Gen:Variant.Bulz.765812	-	MALICIOUS
Memory Dump	Gen:Heur.Mint.Zard.52	-	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	4.3.1
Dynamic Engine Version	4.3.1 / 10/25/2021 03:57
Static Engine Version	4.3.1.0 / 2021-10-25 03:00:16
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.20 / 2021-11-05 16:37:21
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.20 / 2021-11-05 16:37:21
YARA Built-in Ruleset Version	4.3.1.20

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	2021-11-09 21:26:35+00:00
Built-in AV Database Records	10691573

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