MALICIOUS

Classifications: Injector, Downloader

Threat Names: SmokeLoader, Mal/HTMLGen-A, Gen:Variant.Babar.29261, Generic.Andromeda.79093CCD, Gen:Variant.Razy.655877

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe**
ID	#1170829
MD5	743f8fec87ebf7c5d6b392261ec3988f
SHA1	1bc862eecde55f2c1de69bc9e3fdd7468de373d0
SHA256	c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7
File Size	334.50 KB
Report Created	2021-11-18 12:30 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (20 rules, 36 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr".			
4/5	Injection	Writes into the memory of another process	2	Injector
	• (Process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe modifies memory of (process #3) explorer.exe. • (Process #8) cdieedr modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	2	Injector
	• (Process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe creates thread in (process #3) explorer.exe. • (Process #8) cdieedr creates thread in (process #3) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "host-file-host6.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "host-file-host0.com/files/1323_1637231617_8061.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Gen:Variant.Babar.29261". • Built-in AV detected a memory dump of (process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe as "Generic.Andromeda.79093CCD". • Built-in AV detected a memory dump of (process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe as "Gen:Variant.Razy.655877". • Built-in AV detected a memory dump of (process #8) cdieedr as "Gen:Variant.Razy.655877".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.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\keecfmwgj\appdata\roaming\cdieedr". • (Process #3) explorer.exe deletes executed executable "c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe modifies memory of (process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe. • (Process #5) cdieedr modifies memory of (process #8) cdieedr.			

Score	Category	Operation	Count	Classification
2/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-

- (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe alters context of (process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe.
- (Process #5) cdieedr alters context of (process #8) cdieedr.

Score	Category	Operation	Count	Classification
2/5	Task Scheduling	Schedules task	2	-

- Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Logon.
- Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Time. Task has been rescheduled by the analyzer.

Score	Category	Operation	Count	Classification
2/5	Reputation	Contacts known suspicious URL	1	-

- Contacted URL "host-file-host0.com" is a known suspicious URL.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-

- (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe reads from (process #2) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe.
- (Process #5) cdieedr reads from (process #8) cdieedr.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	2	-

- (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
- (Process #5) cdieedr allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.

Score	Category	Operation	Count	Classification
1/5	Discovery	Enumerates running processes	1	-

- (Process #3) explorer.exe enumerates running processes.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	1	-

- (Process #3) explorer.exe creates mutex with name "4BCD659AD8F347B5B451918CD891C8238443A5AF".

Score	Category	Operation	Count	Classification
1/5	Execution	Executes itself	3	-

- (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe.
- (Process #4) taskeng.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe.
- (Process #5) cdieedr executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	2	-

- (Process #1) c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe resolves 38 API functions by name.
- (Process #5) cdieedr resolves 38 API functions by name.

Mitre ATT&CK Matrix

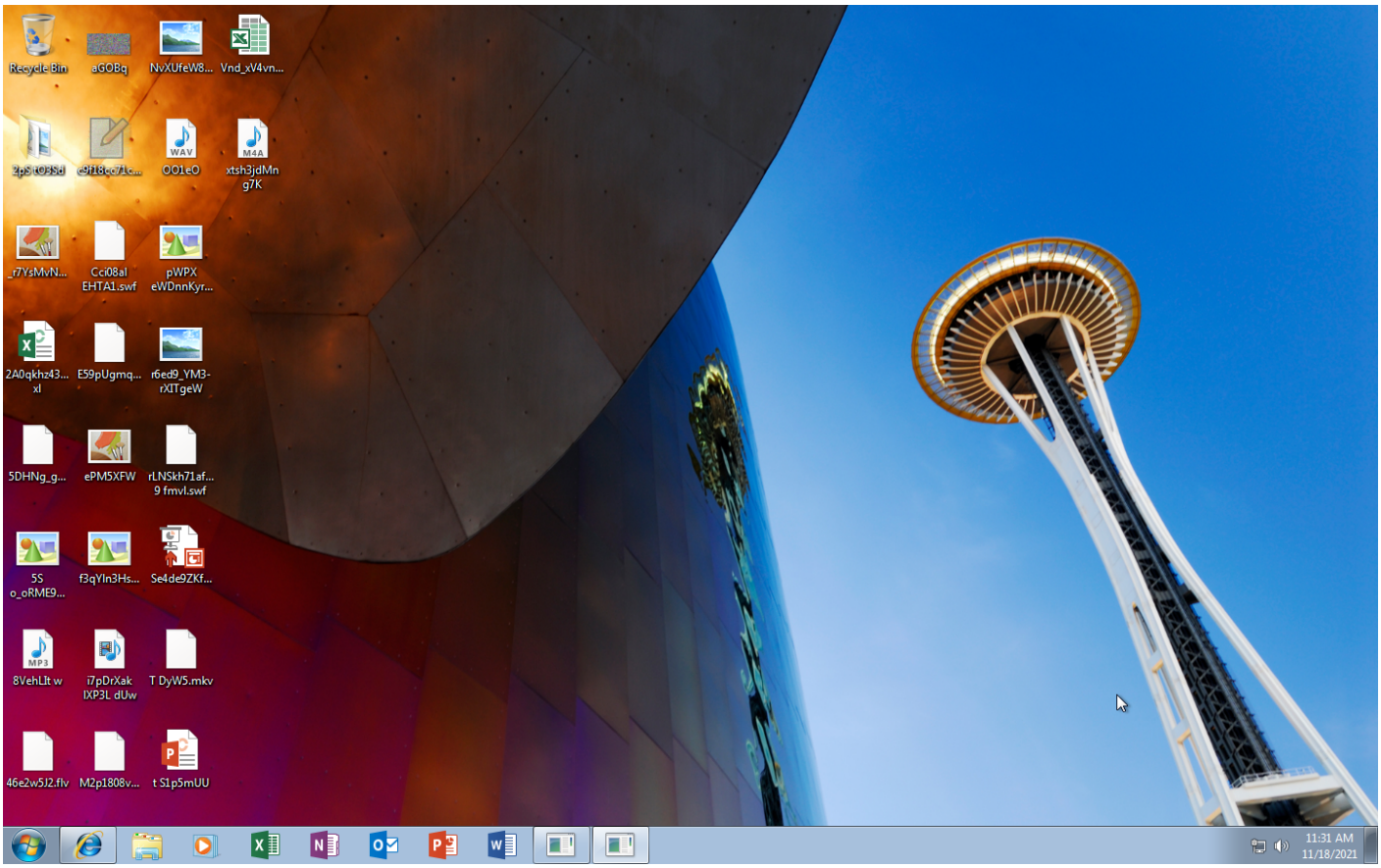
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery					
				#T1096 NTFS File Attributes							

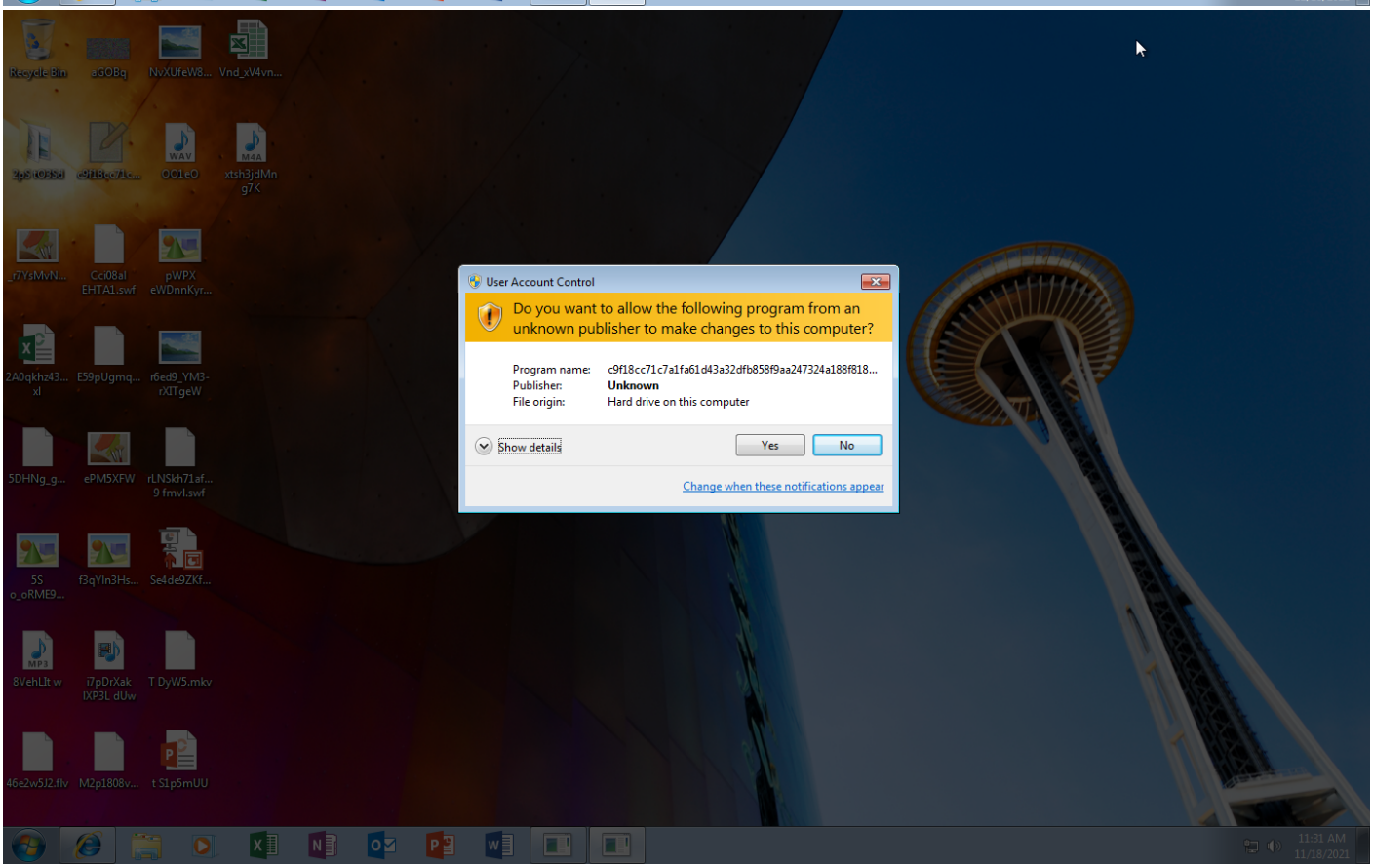
Sample Information

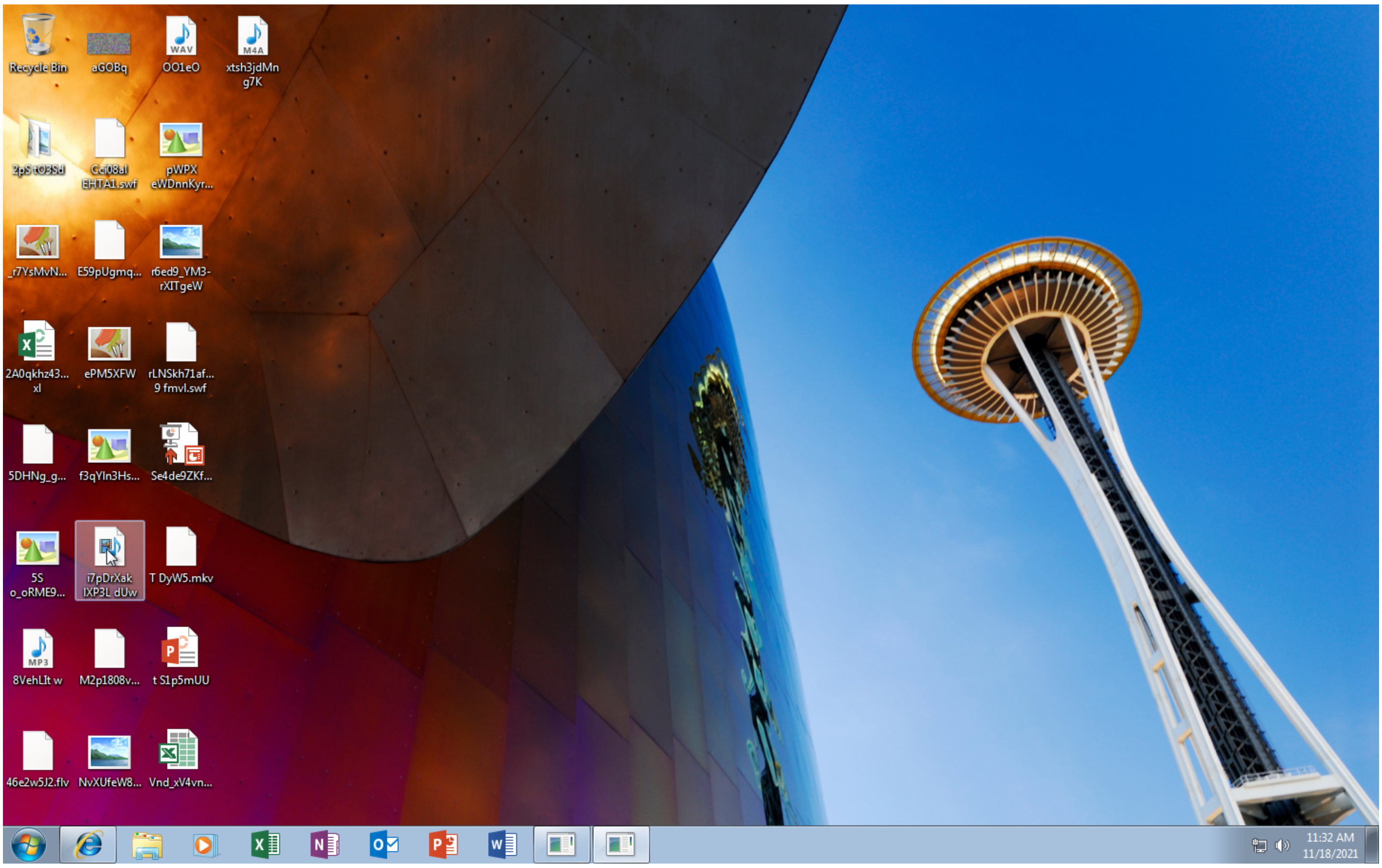
ID	#1170829
MD5	743f8fec87ebf7c5d6b392261ec3988f
SHA1	1bc862eecde55f2c1de69bc9e3fdd7468de373d0
SHA256	c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7
SSDeep	6144:B9LMytcasE/LEUZ/TPrMXiT1B18x93KX:ztcasE/L1jrMmH18x96X
ImpHash	b2e29795cf26e2405a95e142d139ea34
File Name	c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe
File Size	334.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

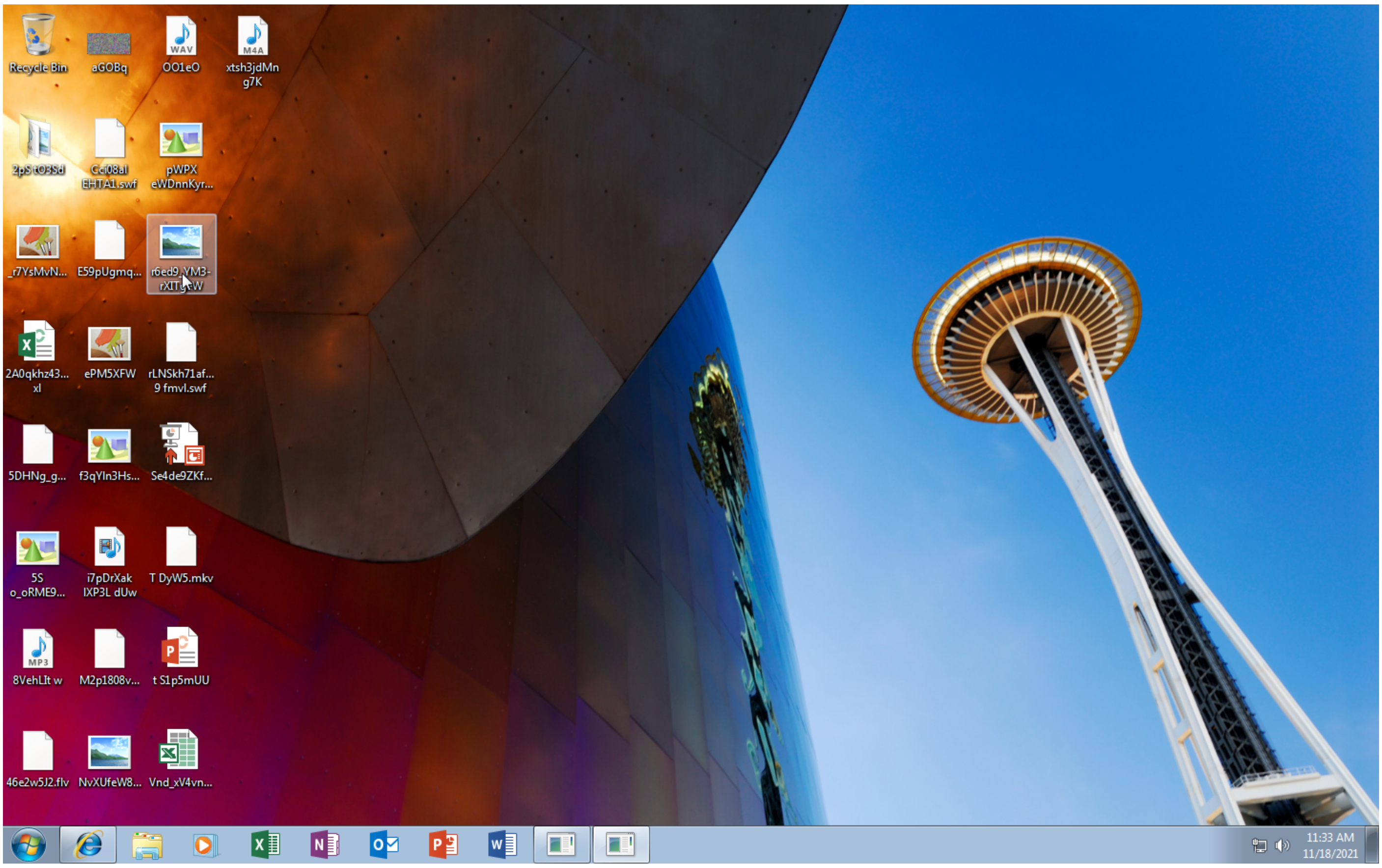
Analysis Information

Creation Time	2021-11-18 12:30 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
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	8
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f818...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
aGOBq
OO1eO
xtsh3jdMn g7K
pWPX eWDnnKyr...
_r7YsMvN...
E59pUgmq...
r6ed9_YM3- rXITgeW
2A0qkhz43... xl
ePM5XFW
rLNSkh71af... 9 fmvl.swf
5DHNg_g...
f3qYln3Hs...
Se4de9ZKf...
5S o_oRME9...
i7pDrXak IXP3L dUw
T DyW5.mkv
8VehLIt w
M2p1808v...
t S1p5mUU
46e2w5J2.flv
NvXUfeW8...
Vnd_xV4vn...
11:32 AM
11/18/2021


Recycle Bin
aGOBq
OO1eO
xtsh3jdMn g7K
pWPX eWDnnKyr...
_r7YsMvN...
E59pUgmq...
2A0qkhz43... xl
ePM5XFW
rLNSkh71af... 9 fmvl.swf
5DHNg_g...
f3qYln3Hs...
Se4de9ZKf...
5S o_oRME9...
i7pDrXak IXP3L dUw
T DyW5.mkv
8VehLIt w
M2p1808v...
t S1p5mUU
46e2w5J2.flv
NvXUfeW8...
Vnd_xV4vn...
11:33 AM
11/18/2021

NETWORK

General

8.22 KB total sent

7359.67 KB total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 1 servers

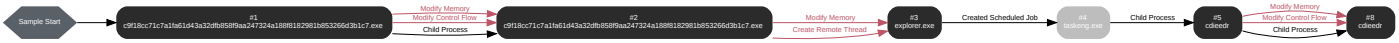
11 sessions, 8.22 KB sent, 7359.67 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	host-file-host6.com/	-	-		0 bytes	NA
GET	host-file-host0.com/files/1323_1637231617_8061.exe	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 35929, Reason: Analysis Target
Unmonitor End Time	End Time: 54203, Reason: Terminated
Monitor duration	18.27s
Return Code	0
PID	3772
Parent PID	1096
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	50
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50144, Reason: Child Process
Unmonitor End Time	End Time: 63246, Reason: Terminated
Monitor duration	13.10s
Return Code	0
PID	3800
Parent PID	3772
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xec0	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xec0	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xec0	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xec0 / 0xedc	0x770501c4(1996816836)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	18
-	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: 58770, Reason: Injection
Unmonitor End Time	End Time: 276829, Reason: Terminated by Timeout
Monitor duration	218.06s
Return Code	Unknown
PID	1096
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xedc	0x2590000(39387136)	0x5000	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xedc	0x2b90000(45678592)	0x16000	✓	1
Create Remote Thread	#2: c:\users\keecfmwgj\desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	0xedc	0x2b91930(45685040)	-	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf34	0x2bb0000(45809664)	0x5000	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf34	0x39b0000(60489728)	0x16000	✓	1
Create Remote Thread	#8: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf34	0x39b1930(60496176)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	334.50 KB	c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7	✗

Host Behavior

Type	Count
Module	31
System	6029
Process	529
Mutex	2
Registry	3
File	18
User	1

Type	Count
COM	1

Network Behavior

Type	Count
HTTP	11
TCP	11

Process #4: taskeng.exe

ID	4
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {6C20883B-C3FC-4B8C-8693-A57568CFC453} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90668, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 276829, Reason: Terminated by Timeout
Monitor duration	186.16s
Return Code	Unknown
PID	3848
Parent PID	820
Bitness	64 Bit

Process #5: cdieedr

ID	5
File Name	c:\users\keecfmwgj\appdata\roaming\cdieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 91992, Reason: Child Process
Unmonitor End Time	End Time: 103253, Reason: Terminated
Monitor duration	11.26s
Return Code	0
PID	3880
Parent PID	3848
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	50
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #8: cdieedr

ID	8
File Name	c:\users\keecfmwgj\appdata\roaming\cdieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101978, Reason: Child Process
Unmonitor End Time	End Time: 110804, Reason: Terminated
Monitor duration	8.83s
Return Code	0
PID	3888
Parent PID	3880
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf2c	0x400000(4194304)	0x200	✓	1
Modify Memory	#5: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf2c	0x401000(4198400)	0x7200	✓	1
Modify Memory	#5: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf2c	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#5: c:\users\keecfmwgj\appdata\roaming\cdieedr	0xf2c / 0xf34	0x770501c4(1996816836)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	18
-	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr, C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	Sample File	334.50 KB	application/vnd.microsoft.portable-executable	Access, Delete, Create, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	Sample File	Access, Delete	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	Sample File	Access, Delete, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\cdieedr:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\estugfj	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-file-host6.com	-	188.225.85.124	-	POST	MALICIOUS
http://host-file-host0.com/files/1323_1637231617_8061.exe	-	188.225.85.124	-	GET	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
host-file-host0.com	188.225.85.124	-	HTTP	SUSPICIOUS
host-file-host6.com	188.225.85.124	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
188.225.85.124	host-file-host0.com, host-file-host6.com	Russia	TCP, HTTP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
4BCD659AD8F347B5B451918CD891C8238443A5AF	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	cdieedr, c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	cdieedr, c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	"C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe"	MALICIOUS
cdieedr	C:\Users\kEecfMwgj\AppData\Roaming\cdieedr	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
taskeng.exe	taskeng.exe {6C20883B-C3FC-4B8C-8693-A57568CFC453} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_3.txt	Downloader	5/5

Antivirus (8)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Variant.Babar.29261	C:\Users\kEecfMwgj\Desktop\c9f18cc71c7a1fa61d43a32dfb858f9aa247324a188f8182981b853266d3b1c7.exe	MALICIOUS
Memory Dump	Generic.Andromeda.79093CCD	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.1
Dynamic Engine Version	4.3.1 / 11/09/2021 04:55
Static Engine Version	4.3.1.0 / 2021-11-09 04:00:13
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.23 / 2021-11-15 15:11:35
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.22 / 2021-11-15 15:04:23
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	2021-11-18 07:06:54+00:00
Built-in AV Database Records	10501559

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows