MALICIOUS

Classifications: Injector

Threat Names: Mal/HTMLGen-A | C2/Generic-A | Gen:Variant.Bulz.604474

Verdict Reason: -

Sample Type	**Windows DLL (x86-32)**
File Name	**31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll**
ID	#2780823
MD5	7df93445d7752cd944b727d3824ebb55
SHA1	119352f971e74f397d5f78301b144c22be8f944f
SHA256	31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898
File Size	378.00 KB
Report Created	2021-09-27 23:30 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 132 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Writes into the memory of another process	12	Injector
	• (Process #3) zcuohmv.exe modifies memory of (process #20) explorer.exe. • (Process #7) zcuohmv.exe modifies memory of (process #21) explorer.exe. • (Process #4) zcuohmv.exe modifies memory of (process #22) explorer.exe. • (Process #9) zcuohmv.exe modifies memory of (process #23) explorer.exe. • (Process #13) zcuohmv.exe modifies memory of (process #24) explorer.exe. • (Process #8) zcuohmv.exe modifies memory of (process #25) explorer.exe. • (Process #2) zcuohmv.exe modifies memory of (process #26) explorer.exe. • (Process #19) zcuohmv.exe modifies memory of (process #27) explorer.exe. • (Process #16) zcuohmv.exe modifies memory of (process #28) explorer.exe. • (Process #10) zcuohmv.exe modifies memory of (process #29) explorer.exe. • (Process #18) zcuohmv.exe modifies memory of (process #30) explorer.exe. • (Process #35) regsvr32.exe modifies memory of (process #36) explorer.exe.		
4/5	Reputation	Contacts known malicious URL	5	-
	• Reputation analysis labels the URL "https://95.77.223.148/t4" which was contacted by (process #36) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://216.201.162.158/t4" which was contacted by (process #21) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://105.198.236.99/t4" which was contacted by (process #36) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://71.74.12.34/t4" which was contacted by (process #21) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://67.165.206.193/t4" which was contacted by (process #21) explorer.exe as "Mal/HTMLGen-A".		
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 216.201.162.158 as "C2/Generic-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected a memory dump of (process #6) zcuohmv.exe as "Gen:Variant.Bulz.604474".			
3/5	Defense Evasion	Modifies Windows Defender configuration	2	-
	• (Process #37) reg.exe adds exclusion for Windows Defender. • (Process #38) reg.exe adds exclusion for Windows Defender.			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #21) explorer.exe has a thread which sleeps more than 5 minutes. • (Process #36) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #3) zcuohmv.exe creates a new explorer.exe process.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "regsvr32.exe", to be triggered by Time. Task has been rescheduled by the analyzer.			
2/5	Task Scheduling	Schedules task via schtasks	1	-
	• Schedules task "szvajmo" via the schtasks command line utility.			

Score	Category	Operation	Count	Classification
1/5	Discovery	Enumerates running processes	19	-

- (Process #7) zcuohmv.exe enumerates running processes.
- (Process #3) zcuohmv.exe enumerates running processes.
- (Process #5) zcuohmv.exe enumerates running processes.
- (Process #6) zcuohmv.exe enumerates running processes.
- (Process #13) zcuohmv.exe enumerates running processes.
- (Process #8) zcuohmv.exe enumerates running processes.
- (Process #9) zcuohmv.exe enumerates running processes.
- (Process #4) zcuohmv.exe enumerates running processes.
- (Process #2) zcuohmv.exe enumerates running processes.
- (Process #19) zcuohmv.exe enumerates running processes.
- (Process #11) zcuohmv.exe enumerates running processes.
- (Process #10) zcuohmv.exe enumerates running processes.
- (Process #15) zcuohmv.exe enumerates running processes.
- (Process #16) zcuohmv.exe enumerates running processes.
- (Process #18) zcuohmv.exe enumerates running processes.
- (Process #17) zcuohmv.exe enumerates running processes.
- (Process #14) zcuohmv.exe enumerates running processes.
- (Process #12) zcuohmv.exe enumerates running processes.
- (Process #35) regsvr32.exe enumerates running processes.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	16	-

- (Process #7) zcuohmv.exe starts (process #21) explorer.exe with a hidden window.
- (Process #3) zcuohmv.exe starts (process #20) explorer.exe with a hidden window.
- (Process #4) zcuohmv.exe starts (process #22) explorer.exe with a hidden window.
- (Process #13) zcuohmv.exe starts (process #24) explorer.exe with a hidden window.
- (Process #8) zcuohmv.exe starts (process #25) explorer.exe with a hidden window.
- (Process #9) zcuohmv.exe starts (process #23) explorer.exe with a hidden window.
- (Process #2) zcuohmv.exe starts (process #26) explorer.exe with a hidden window.
- (Process #19) zcuohmv.exe starts (process #27) explorer.exe with a hidden window.
- (Process #10) zcuohmv.exe starts (process #29) explorer.exe with a hidden window.
- (Process #16) zcuohmv.exe starts (process #28) explorer.exe with a hidden window.
- (Process #18) zcuohmv.exe starts (process #30) explorer.exe with a hidden window.
- (Process #21) explorer.exe starts (process #31) schtasks.exe with a hidden window.
- (Process #33) regsvr32.exe starts (process #35) regsvr32.exe with a hidden window.
- (Process #35) regsvr32.exe starts (process #36) explorer.exe with a hidden window.
- (Process #36) explorer.exe starts (process #37) reg.exe with a hidden window.
- (Process #36) explorer.exe starts (process #38) reg.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	10	-

- (Process #3) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #7) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #9) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #10) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #16) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #2) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #13) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #4) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #19) zcuohmv.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #35) regsvr32.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	22	-

- (Process #21) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #21) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #26) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #26) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #28) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #28) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #27) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #27) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #22) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #22) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #24) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #24) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #23) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #23) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #20) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #20) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #29) explorer.exe creates mutex with name "Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #29) explorer.exe creates mutex with name "{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}".
- (Process #21) explorer.exe creates mutex with name "{14A78D04-6F1A-4927-AECE-0EE9DEB87429}".
- (Process #36) explorer.exe creates mutex with name "Global\{F9B41FAF-4994-487E-87C0-862C1DC89AD9}".
- (Process #36) explorer.exe creates mutex with name "{F9B41FAF-4994-487E-87C0-862C1DC89AD9}".
- (Process #36) explorer.exe creates mutex with name "{14A78D04-6F1A-4927-AECE-0EE9DEB87429}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	29	-

Score	Category	Operation	Count	Classification
		• (Process #2) zcuohmv.exe resolves 96 API functions by name. • (Process #3) zcuohmv.exe resolves 99 API functions by name. • (Process #4) zcuohmv.exe resolves 96 API functions by name. • (Process #5) zcuohmv.exe resolves 99 API functions by name. • (Process #6) zcuohmv.exe resolves 99 API functions by name. • (Process #7) zcuohmv.exe resolves 99 API functions by name. • (Process #8) zcuohmv.exe resolves 96 API functions by name. • (Process #9) zcuohmv.exe resolves 96 API functions by name. • (Process #10) zcuohmv.exe resolves 96 API functions by name. • (Process #11) zcuohmv.exe resolves 96 API functions by name. • (Process #12) zcuohmv.exe resolves 96 API functions by name. • (Process #13) zcuohmv.exe resolves 96 API functions by name. • (Process #14) zcuohmv.exe resolves 96 API functions by name. • (Process #15) zcuohmv.exe resolves 96 API functions by name. • (Process #16) zcuohmv.exe resolves 96 API functions by name. • (Process #17) zcuohmv.exe resolves 96 API functions by name. • (Process #18) zcuohmv.exe resolves 96 API functions by name. • (Process #19) zcuohmv.exe resolves 99 API functions by name. • (Process #21) explorer.exe resolves 94 API functions by name. • (Process #26) explorer.exe resolves 91 API functions by name. • (Process #28) explorer.exe resolves 91 API functions by name. • (Process #29) explorer.exe resolves 91 API functions by name. • (Process #20) explorer.exe resolves 91 API functions by name. • (Process #24) explorer.exe resolves 91 API functions by name. • (Process #23) explorer.exe resolves 91 API functions by name. • (Process #22) explorer.exe resolves 91 API functions by name. • (Process #27) explorer.exe resolves 91 API functions by name. • (Process #35) regsvr32.exe resolves 92 API functions by name. • (Process #36) explorer.exe resolves 94 API functions by name.		
1/5	Network Connection	All network connection attempts failed	7	-
		• Host "68.207.102.78" is unavailable. • Host "95.77.223.148" is unavailable. • Host "216.201.162.158" is unavailable. • Host "105.198.236.99" is unavailable. • Host "71.74.12.34" is unavailable. • Host "75.107.26.196" is unavailable. • Host "67.165.206.193" is unavailable.		
1/5	Network Connection	Tries to connect using an uncommon port	2	-
		• (Process #36) explorer.exe tries to connect to TCP port 465 at 75.107.26.196. • (Process #21) explorer.exe tries to connect to TCP port 993 at 67.165.206.193.		
1/5	Execution	Drops PE file	1	-
		• (Process #20) explorer.exe drops file "C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll".		

Mitre ATT&CK Matrix

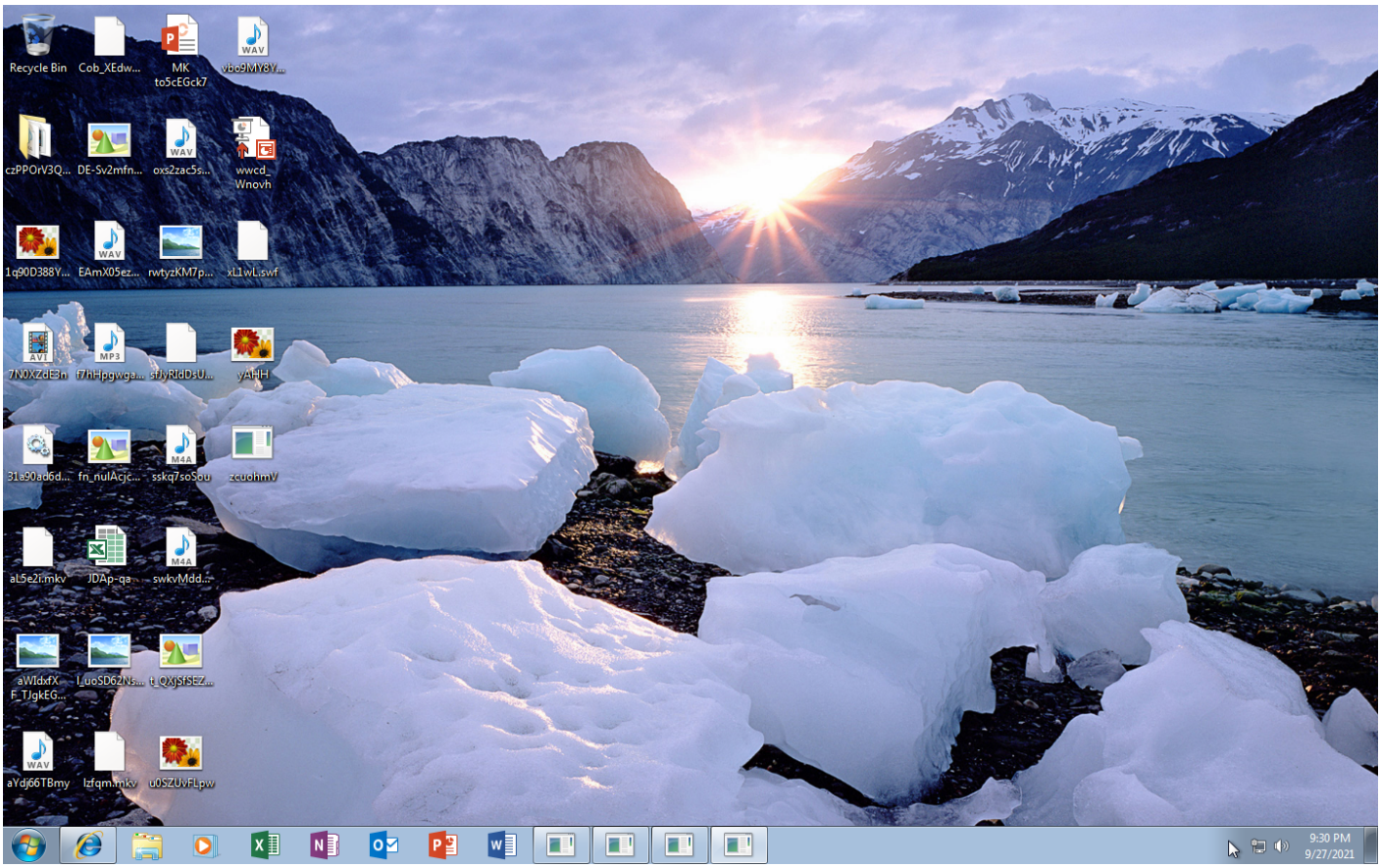
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window		#T1057 Process Discovery			#T1065 Uncommonly Used Port		
				#T1045 Software Packing							
				#T1089 Disabling Security Tools							
				#T1112 Modify Registry							

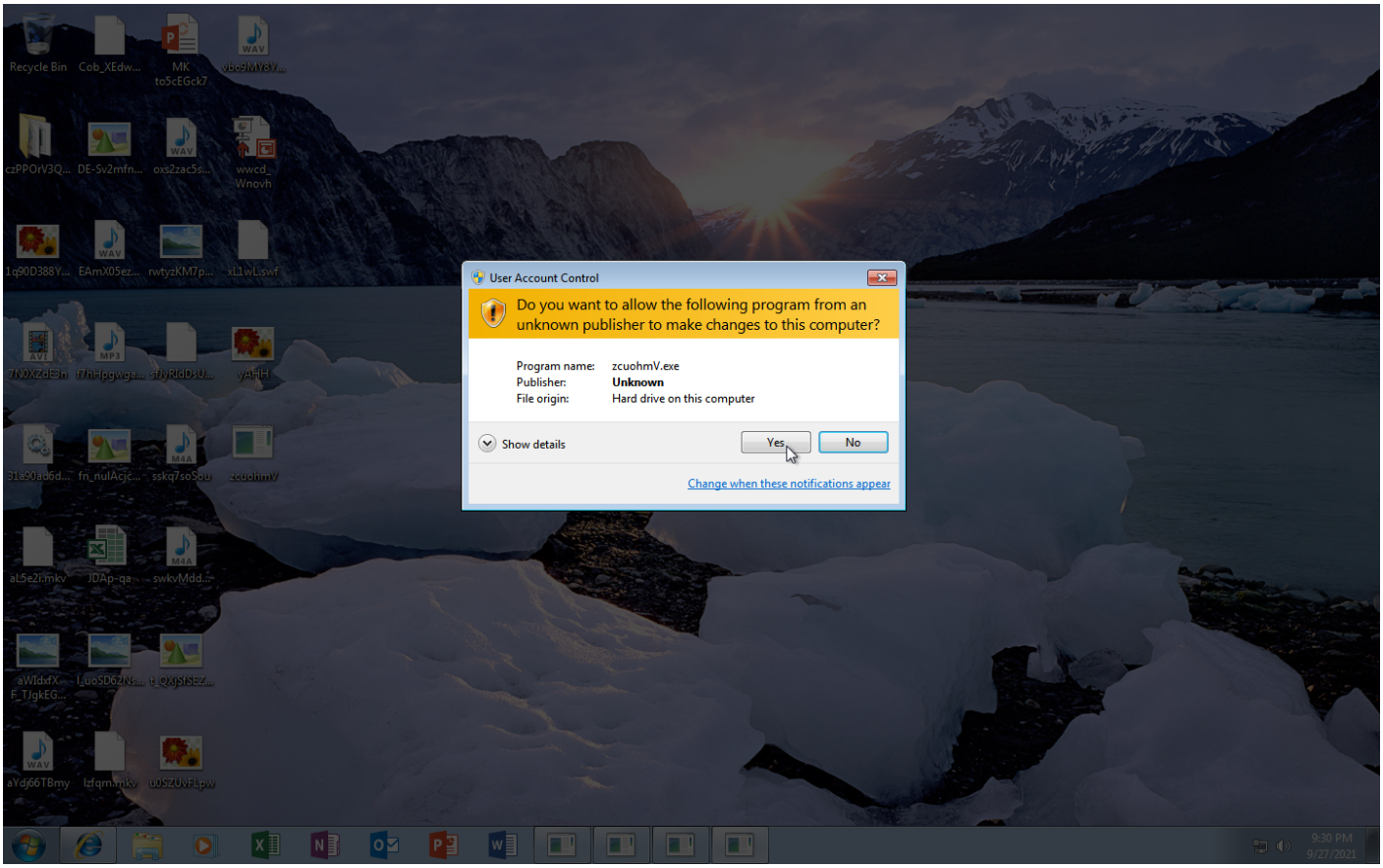
Sample Information

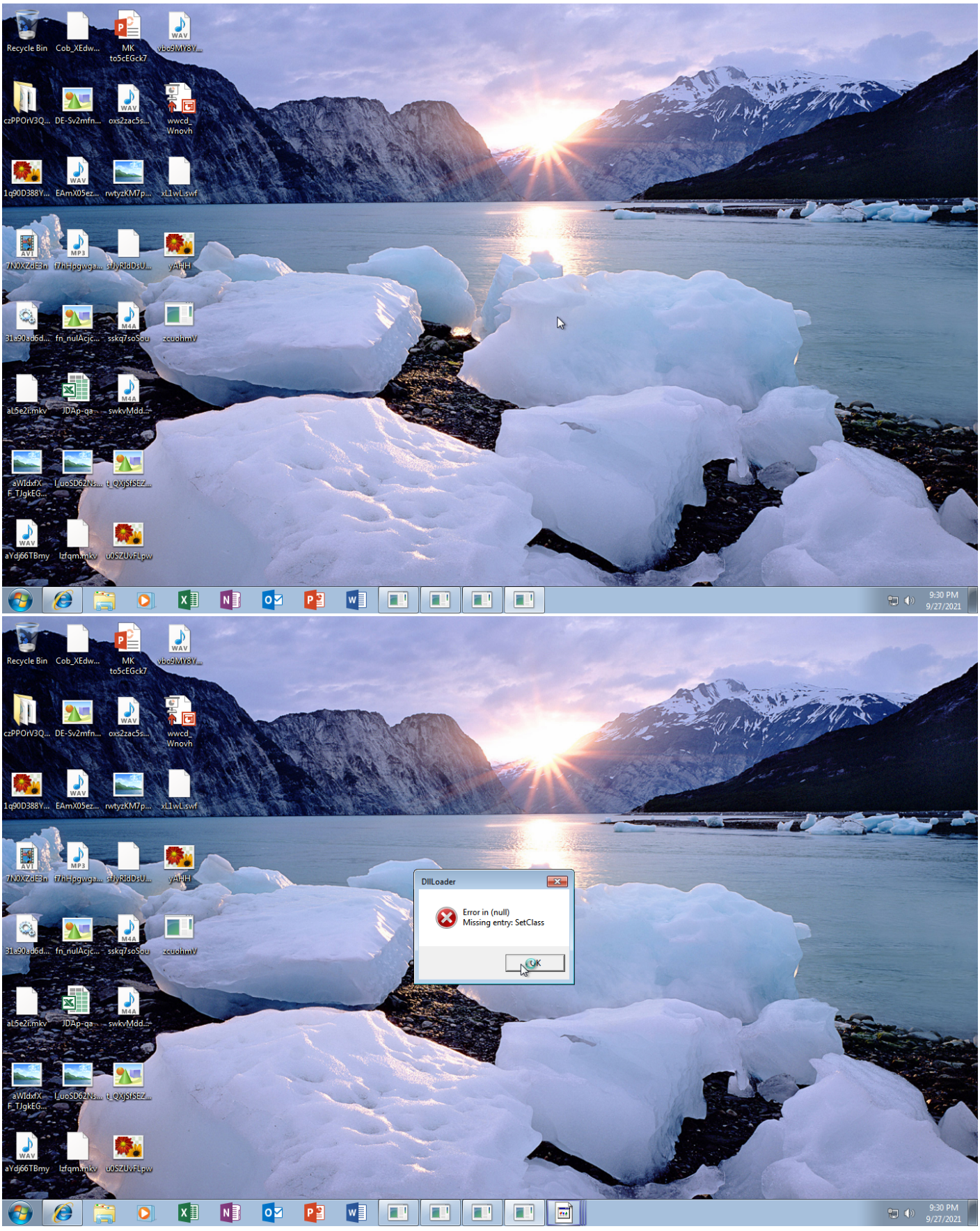
ID	#2780823
MD5	7df93445d7752cd944b727d3824ebb55
SHA1	119352f971e74f397d5f78301b144c22be8f944f
SHA256	31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898
SSDeep	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2MC:vs6Xpq0H3Jhds/9+qC/zfTPLg
ImpHash	ef258cd2a69e4871222e8a6651dd9af8
File Name	31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll
File Size	378.00 KB
Sample Type	Windows DLL (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 23:30 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	37
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0




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



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

3 ports 465, 443, 993

7 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

7 URLs contacted, 7 servers

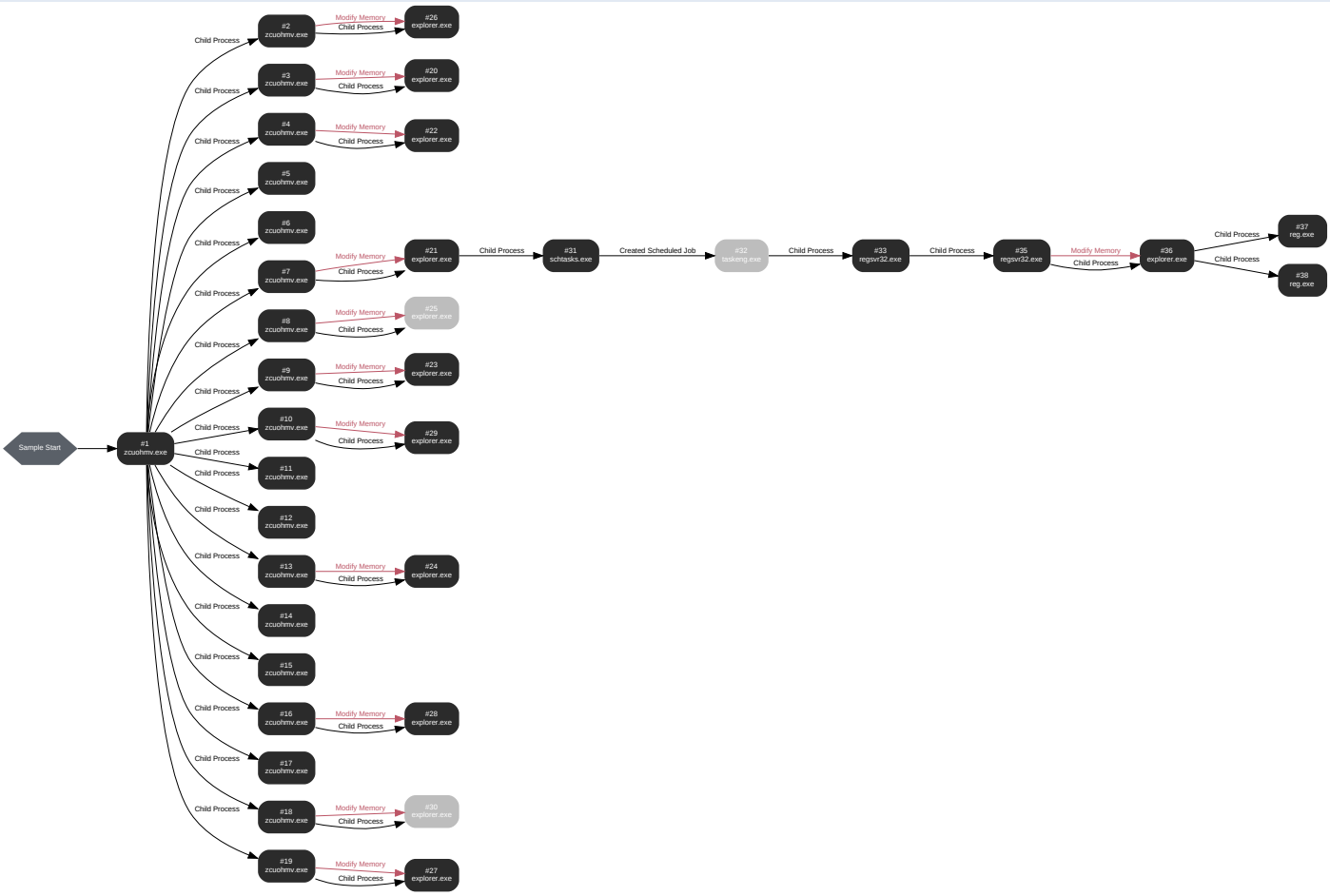
7 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	https://67.165.206.193/t4	-	-		0 bytes	NA
POST	https://68.207.102.78/t4	-	-		0 bytes	NA
POST	https://95.77.223.148/t4	-	-		0 bytes	NA
POST	https://216.201.162.158/t4	-	-		0 bytes	NA
POST	https://105.198.236.99/t4	-	-		0 bytes	NA
POST	https://71.74.12.34/t4	-	-		0 bytes	NA
POST	https://75.107.26.196/t4	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: zcuohmv.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp16u7ys_0" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 33637, Reason: Analysis Target
Unmonitor End Time	End Time: 54558, Reason: Terminated
Monitor duration	20.92s
Return Code	0
PID	3748
Parent PID	1116
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll	378.00 KB	31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898	✗
C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll	378.00 KB	17d261eaca2629ef9907d0c00fb2271201e466796f06dcb7232900d711c29330	✗

Host Behavior

Type	Count
System	2
Module	20
File	7
Environment	1
Process	18

Process #2: zcuohmv.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47254, Reason: Child Process
Unmonitor End Time	End Time: 78881, Reason: Terminated
Monitor duration	31.63s
Return Code	4294967292
PID	3772
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	5
Process	116
-	5
-	2
-	1

Process #3: zcuohmv.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47423, Reason: Child Process
Unmonitor End Time	End Time: 87034, Reason: Terminated
Monitor duration	39.61s
Return Code	4294967292
PID	3792
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	26
Module	145
File	3
Environment	5
Window	2
-	5
Process	117
-	5
-	2
-	1

Process #4: zcuohmv.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47539, Reason: Child Process
Unmonitor End Time	End Time: 83625, Reason: Terminated
Monitor duration	36.09s
Return Code	4294967292
PID	3804
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	5
Process	116
-	5
-	2
-	1

Process #5: zcuohmv.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48279, Reason: Child Process
Unmonitor End Time	End Time: 62575, Reason: Terminated
Monitor duration	14.30s
Return Code	4294967292
PID	3816
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	25
Module	141
File	4
Environment	5
Window	1
-	4
Process	21

Process #6: zcuohmv.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49211, Reason: Child Process
Unmonitor End Time	End Time: 61597, Reason: Terminated
Monitor duration	12.39s
Return Code	4294967292
PID	3828
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	14
Module	141
File	4
Environment	5
Window	1
-	4
Process	6

Process #7: zcuohmv.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49313, Reason: Child Process
Unmonitor End Time	End Time: 87584, Reason: Terminated
Monitor duration	38.27s
Return Code	4294967292
PID	3844
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	34
Module	145
File	4
Environment	5
Window	2
-	5
Process	117
-	5
-	2
-	1

Process #8: zcuohmv.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49402, Reason: Child Process
Unmonitor End Time	End Time: 74230, Reason: Terminated
Monitor duration	24.83s
Return Code	4294967292
PID	3856
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	4
Process	116
-	2

Process #9: zcuohmv.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50818, Reason: Child Process
Unmonitor End Time	End Time: 76744, Reason: Terminated
Monitor duration	25.93s
Return Code	4294967292
PID	3868
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	5
Process	116
-	5
-	2
-	1

Process #10: zcuohmv.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50950, Reason: Child Process
Unmonitor End Time	End Time: 76336, Reason: Terminated
Monitor duration	25.39s
Return Code	4294967292
PID	3880
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	4
Process	119
-	5
-	2
-	1

Process #11: zcuohmv.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51756, Reason: Child Process
Unmonitor End Time	End Time: 66748, Reason: Terminated
Monitor duration	14.99s
Return Code	4294967292
PID	3892
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	79

Process #12: zcuohmv.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52032, Reason: Child Process
Unmonitor End Time	End Time: 66501, Reason: Terminated
Monitor duration	14.47s
Return Code	4294967292
PID	3904
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	48

Process #13: zcuohmv.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52110, Reason: Child Process
Unmonitor End Time	End Time: 81501, Reason: Terminated
Monitor duration	29.39s
Return Code	4294967292
PID	3916
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	5
Process	116
-	5
-	2
-	1

Process #14: zcuohmv.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52268, Reason: Child Process
Unmonitor End Time	End Time: 66149, Reason: Terminated
Monitor duration	13.88s
Return Code	4294967292
PID	3928
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	39

Process #15: zcuohmv.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52368, Reason: Child Process
Unmonitor End Time	End Time: 66866, Reason: Terminated
Monitor duration	14.50s
Return Code	4294967292
PID	3940
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	77

Process #16: zcuohmv.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53177, Reason: Child Process
Unmonitor End Time	End Time: 76336, Reason: Terminated
Monitor duration	23.16s
Return Code	4294967292
PID	3952
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	4
Process	115
-	5
-	2
-	1

Process #17: zcuohmv.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53263, Reason: Child Process
Unmonitor End Time	End Time: 68958, Reason: Terminated
Monitor duration	15.70s
Return Code	4294967292
PID	3964
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	136
File	3
Environment	5
Window	1
-	4
Process	110

Process #18: zcuohmv.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53411, Reason: Child Process
Unmonitor End Time	End Time: 74265, Reason: Terminated
Monitor duration	20.85s
Return Code	4294967292
PID	3976
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	140
File	3
Environment	5
Window	2
-	4
Process	116
-	2

Process #19: zcuohmv.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\zcuohmv.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53513, Reason: Child Process
Unmonitor End Time	End Time: 76336, Reason: Terminated
Monitor duration	22.82s
Return Code	4294967292
PID	3988
Parent PID	3748
Bitness	32 Bit

Host Behavior

Type	Count
System	16
Module	143
File	4
Environment	5
Window	2
-	4
Process	115
-	5
-	2
-	1

Process #20: explorer.exe

ID	20
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64839, Reason: Child Process
Unmonitor End Time	End Time: 88307, Reason: Terminated
Monitor duration	23.47s
Return Code	0
PID	3348
Parent PID	3792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb4	0x70000(458752)	0x21000	✓	1
Modify Memory	#3: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb4	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#3: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb4	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	644
Registry	3
File	653
Mutex	2

Process #21: explorer.exe

ID	21
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64854, Reason: Child Process
Unmonitor End Time	End Time: 274406, Reason: Terminated by Timeout
Monitor duration	209.55s
Return Code	Unknown
PID	948
Parent PID	3844
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb8	0xb0000(720896)	0x21000	✓	1
Modify Memory	#7: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb8	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#7: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xfb8	0xfa0efa(16387834)	0x5	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗

Host Behavior

Type	Count
Module	122
Process	1
System	21939
Registry	4054
File	656
Mutex	1863
Keyboard	2
-	1
-	1
Window	1

Network Behavior

Type	Count
HTTPS	14
TCP	4

Process #22: explorer.exe

ID	22
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66749, Reason: Child Process
Unmonitor End Time	End Time: 88037, Reason: Terminated
Monitor duration	21.29s
Return Code	0
PID	2108
Parent PID	3804
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf4	0xd0000(851968)	0x21000	✓	1
Modify Memory	#4: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf4	0x70000(458752)	0x1ac4	✓	1
Modify Memory	#4: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf4	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	643
Registry	3
File	652
Mutex	2

Process #23: explorer.exe

ID	23
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66867, Reason: Child Process
Unmonitor End Time	End Time: 88307, Reason: Terminated
Monitor duration	21.44s
Return Code	0
PID	2116
Parent PID	3868
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#9: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf8	0x70000(458752)	0x21000	✓	1
Modify Memory	#9: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf8	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#9: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xaf8	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	642
Registry	3
File	651
Mutex	2

Process #24: explorer.exe

ID	24
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66978, Reason: Child Process
Unmonitor End Time	End Time: 88306, Reason: Terminated
Monitor duration	21.33s
Return Code	0
PID	2124
Parent PID	3916
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#13: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb00	0x70000(458752)	0x21000	✓	1
Modify Memory	#13: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb00	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#13: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb00	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	643
Registry	3
File	652
Mutex	2

Process #25: explorer.exe

ID	25
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67167, Reason: Child Process
Unmonitor End Time	End Time: 274406, Reason: Terminated by Timeout
Monitor duration	207.24s
Return Code	Unknown
PID	2140
Parent PID	3856
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xafc	0x70000(458752)	0x21000	✓	1
Modify Memory	#8: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xafc	0xa0000(655360)	0x1ac4	✓	1

Process #26: explorer.exe

ID	26
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67254, Reason: Child Process
Unmonitor End Time	End Time: 88306, Reason: Terminated
Monitor duration	21.05s
Return Code	0
PID	2148
Parent PID	3772
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb04	0x130000(1245184)	0x21000	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb04	0x70000(458752)	0x1ac4	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xb04	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	639
Registry	3
File	648
Mutex	2

Process #27: explorer.exe

ID	27
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67607, Reason: Child Process
Unmonitor End Time	End Time: 87993, Reason: Terminated
Monitor duration	20.39s
Return Code	0
PID	2528
Parent PID	3988
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#19: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xba8	0x70000(458752)	0x21000	✓	1
Modify Memory	#19: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xba8	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#19: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xba8	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	639
Registry	3
File	648
Mutex	2

Process #28: explorer.exe

ID	28
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67744, Reason: Child Process
Unmonitor End Time	End Time: 87842, Reason: Terminated
Monitor duration	20.10s
Return Code	0
PID	2536
Parent PID	3952
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#16: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xc18	0xb0000(720896)	0x21000	✓	1
Modify Memory	#16: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xc18	0xe0000(917504)	0x1ac4	✓	1
Modify Memory	#16: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xc18	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	639
Registry	3
File	648
Mutex	2

Process #29: explorer.exe

ID	29
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67832, Reason: Child Process
Unmonitor End Time	End Time: 88305, Reason: Terminated
Monitor duration	20.47s
Return Code	0
PID	2548
Parent PID	3880
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xa28	0x70000(458752)	0x21000	✓	1
Modify Memory	#10: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xa28	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#10: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xa28	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	640
Registry	3
File	649
Mutex	2

Process #30: explorer.exe

ID	30
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67941, Reason: Child Process
Unmonitor End Time	End Time: 274406, Reason: Terminated by Timeout
Monitor duration	206.47s
Return Code	Unknown
PID	2556
Parent PID	3976
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#18: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xc44	0x70000(458752)	0x21000	✓	1
Modify Memory	#18: c:\users\keecfmwgj\desktop\zcuohmv.exe	0xc44	0xa0000(655360)	0x1ac4	✓	1

Process #31: schtasks.exe

ID	31
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn szvajmo /tr "regsvr32.exe -s \"C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll\"" /SC ONCE /Z /ST 21:34 /ET 21:46
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87233, Reason: Child Process
Unmonitor End Time	End Time: 89578, Reason: Terminated
Monitor duration	2.35s
Return Code	0
PID	3308
Parent PID	948
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	11
COM	1
User	1
File	5

Process #32: taskeng.exe

ID	32
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {781089CD-C952-4751-ABC7-964F9BF37C7C} S-1-5-18:NT AUTHORITY\System:Service:
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 100461, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 274406, Reason: Terminated by Timeout
Monitor duration	173.94s
Return Code	Unknown
PID	2756
Parent PID	868
Bitness	64 Bit

Process #33: regsvr32.exe

ID	33
File Name	c:\windows\system32\regsvr32.exe
Command Line	regsvr32.exe -s "C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 105450, Reason: Child Process
Unmonitor End Time	End Time: 113526, Reason: Terminated
Monitor duration	8.08s
Return Code	0
PID	4004
Parent PID	2756
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Module	2
Registry	4
File	3
Process	1

Process #35: regsvr32.exe

ID	35
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	-s "C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 107324, Reason: Child Process
Unmonitor End Time	End Time: 112998, Reason: Terminated
Monitor duration	5.67s
Return Code	0
PID	4092
Parent PID	4004
Bitness	32 Bit

Host Behavior

Type	Count
System	17
Module	124
Registry	4
Window	1
-	5
File	1
Process	105
Environment	4
-	5
-	2
-	1

Process #36: explorer.exe

ID	36
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 111683, Reason: Child Process
Unmonitor End Time	End Time: 274406, Reason: Terminated by Timeout
Monitor duration	162.72s
Return Code	Unknown
PID	1720
Parent PID	4092
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#35: c:\windows\syswow64\regsvr32.exe	0x9bc	0x70000(458752)	0x21000	✓	1
Modify Memory	#35: c:\windows\syswow64\regsvr32.exe	0x9bc	0xa0000(655360)	0x1ac4	✓	1
Modify Memory	#35: c:\windows\syswow64\regsvr32.exe	0x9bc	0xfa0efa(16387834)	0x5	✓	1

Host Behavior

Type	Count
Module	122
Process	2
System	20774
Registry	3953
File	20
Mutex	1818
Keyboard	2
Environment	1
-	2
-	1
Window	1

Network Behavior

Type	Count
HTTPS	10
TCP	3

Process #37: reg.exe

ID	37
File Name	c:\windows\system32\reg.exe
Command Line	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\ProgramData\Microsoft\Cuaohnwer" /d "0"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 112312, Reason: Child Process
Unmonitor End Time	End Time: 113760, Reason: Terminated
Monitor duration	1.45s
Return Code	0
PID	3248
Parent PID	1720
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	4
File	5

Process #38: reg.exe

ID	38
File Name	c:\windows\system32\reg.exe
Command Line	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo" /d "0"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 112825, Reason: Child Process
Unmonitor End Time	End Time: 113947, Reason: Terminated
Monitor duration	1.12s
Return Code	0
PID	3276
Parent PID	1720
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	4
File	5

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898	C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll	Dropped File	378.00 KB	application/vnd.microsoft.portable-executable	Write, Access, Read, Create	MALICIOUS
17d261eaca2629ef9907d0c00fb2271201e466796f06dcb7232900d711c29330	C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll	Dropped File	378.00 KB	application/vnd.microsoft.portable-executable	Write, Access, Read, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\zcuohmV.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmp16u7ys_0	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll	Dropped File	Write, Access, Read, Create	CLEAN
C:\INTERNAL__empty	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\explorer.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\amstream.dll	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll.cfg	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo\xpgxmeky.dvv	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\regsvr32.exe	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\Cuaohnwer	Accessed File	Access, Create	CLEAN
C:\ProgramData\Microsoft\Cuaohnwer\mnqfikbirm.jdz	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://67.165.206.193/t4	-	67.165.206.193	-	POST	MALICIOUS
https://95.77.223.148/t4	-	95.77.223.148	-	POST	MALICIOUS
https://216.201.162.158/t4	-	216.201.162.158	-	POST	MALICIOUS
https://105.198.236.99/t4	-	105.198.236.99	-	POST	MALICIOUS
https://71.74.12.34/t4	-	71.74.12.34	-	POST	MALICIOUS
https://68.207.102.78/t4	-	68.207.102.78	-	POST	CLEAN
https://75.107.26.196/t4	-	75.107.26.196	-	POST	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
216.201.162.158	-	United States	TCP, HTTP	MALICIOUS

IP Address	Domains	Country	Protocols	Verdict
127.0.0.1	-	-	-	CLEAN
68.207.102.78	-	United States	TCP, HTTP	CLEAN
95.77.223.148	-	Romania	TCP, HTTP	CLEAN
105.198.236.99	-	Egypt	TCP, HTTP	CLEAN
71.74.12.34	-	United States	TCP, HTTP	CLEAN
75.107.26.196	-	United States	TCP, HTTP	CLEAN
67.165.206.193	-	United States	TCP, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}	access	explorer.exe	CLEAN
{7442EDA5-CFF3-4B3C-A3F1-B3B1E8B2325D}	access	explorer.exe	CLEAN
{14A78D04-6F1A-4927-AECE-0EE9DEB87429}	access	explorer.exe	CLEAN
Global\{F9B41FAF-4994-487E-87C0-862C1DC89AD9}	access	explorer.exe	CLEAN
{F9B41FAF-4994-487E-87C0-862C1DC89AD9}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\ProgramData\Microsoft\Cuaohnwer	write, access, read	reg.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo	write, access, read	reg.exe	SUSPICIOUS
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\ec6e59d3	write, access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-1000	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-1000\ProfileImagePath	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\d9f1899d	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\ee2f79af	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\56931eca	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\2b9b5140	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\93273625	write, access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-500	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4219442223-4223814209-3835049652-501	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\1e04810e	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\54d23eb6	write, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\a6b8e66b	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\a4f9c617	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\71b9616a	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\6b76894d	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\79c326a3	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Gyquypfdys\b40d4985	access, read	explorer.exe	CLEAN
HKEY_CLASSES_ROOT\.dll	access, read	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup	access, create	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\cee47b30	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\a1599b54	write, access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	access, create	reg.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\94c64b1a	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\a318bb28	write, access	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\1ba4dc4d	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\66ac93c7	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\de10f4a2	write, access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\53334389	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\19e5fc31	write, access	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\eb8f24ec	write, access	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\e9ce0490	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\3c8ea3ed	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\26414bca	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\34f4e424	access, read	explorer.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Microsoft\Scrhoimlunecup\f93a8b02	access, read	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\SysWOW64\explorer.exe	SUSPICIOUS
schtasks.exe	"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn szvajmo /tr "regsvr32.exe -s \"C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll\"" /SC ONCE /Z /ST 21:34 /ET 21:46	SUSPICIOUS

Process Name	Commandline	Verdict
regsvr32.exe	-s "C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll"	SUSPICIOUS
reg.exe	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\ProgramData\Microsoft\Cuaohnwer" /d "0"	SUSPICIOUS
reg.exe	C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /f /t REG_DWORD /v "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Mqloaubiwjuo" /d "0"	SUSPICIOUS
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmp16u7ys_0" /s	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="0"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="0"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="1"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="1"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="Install"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="Install"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="DefaultInstall"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="DefaultInstall"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="127.0.0.1"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="127.0.0.1"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="explorer.exe"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="explorer.exe"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="iexplore.exe"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="iexplore.exe"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=GetClass /fn_args="%Temp%\IXP000.TMP\"	CLEAN
zcuohmv.exe	"C:\Users\kEecfMwgj\Desktop\zcuohmV.exe" /dll="C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll" /fn_id=SetClass /fn_args="%Temp%\IXP000.TMP\"	CLEAN
taskeng.exe	taskeng.exe {781089CD-C952-4751-ABC7-964F9BF37C7C} S-1-5-18:NT AUTHORITY\System:Service:	CLEAN

Process Name	Commandline	Verdict
regsvr32.exe	regsvr32.exe -s "C:\Users\KEECFM~1\Desktop\31a90ad6dbe61a0a90ee10802efa1a6ea8cc5edbeb3b74e79f7d07293cd56898.dll"	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Bulz.604474	-	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	4.3.0
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 18:53:08+00:00
Built-in AV Database Records	10474020

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