MALICIOUS

Classifications: Injector

Threat Names: Trojan.GenericKD.47063473 Gen:Variant.Doina.24402

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**PO-003785GMHN.exe**
ID	#968741
MD5	4577c41fc896a87df4513f13d29ee65a
SHA1	38e76942a779e8b04cdf763cf993ceda76d049f2
SHA256	144fc8c1a922dbb8162d72a94780f8559bbd9e6b1faa9e037fd33e809126b080
File Size	985.50 KB
Report Created	2021-09-28 10:46 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 12 matches)

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.47063473". • Built-in AV detected a memory dump of (process #1) po-003785gmhn.exe as "Gen:Variant.Doina.24402". • Built-in AV detected a memory dump of (process #1) po-003785gmhn.exe as "Trojan.GenericKD.47063473".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) po-003785gmhn.exe modifies memory of (process #2) secinit.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #1) po-003785gmhn.exe creates thread in (process #2) secinit.exe.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) po-003785gmhn.exe adds "C:\Users\Public\Libraries\uxvffdU.url" to Windows startup via registry.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) po-003785gmhn.exe starts (process #2) secinit.exe with a hidden window. • (Process #1) po-003785gmhn.exe starts C:\Users\Public\Trast.bat with a hidden window.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) po-003785gmhn.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) po-003785gmhn.exe resolves 330 API functions by name.			
1/5	Crash	A monitored process crashed	1	-
	• (Process #2) secinit.exe crashed.			

Mitre ATT&CK Matrix

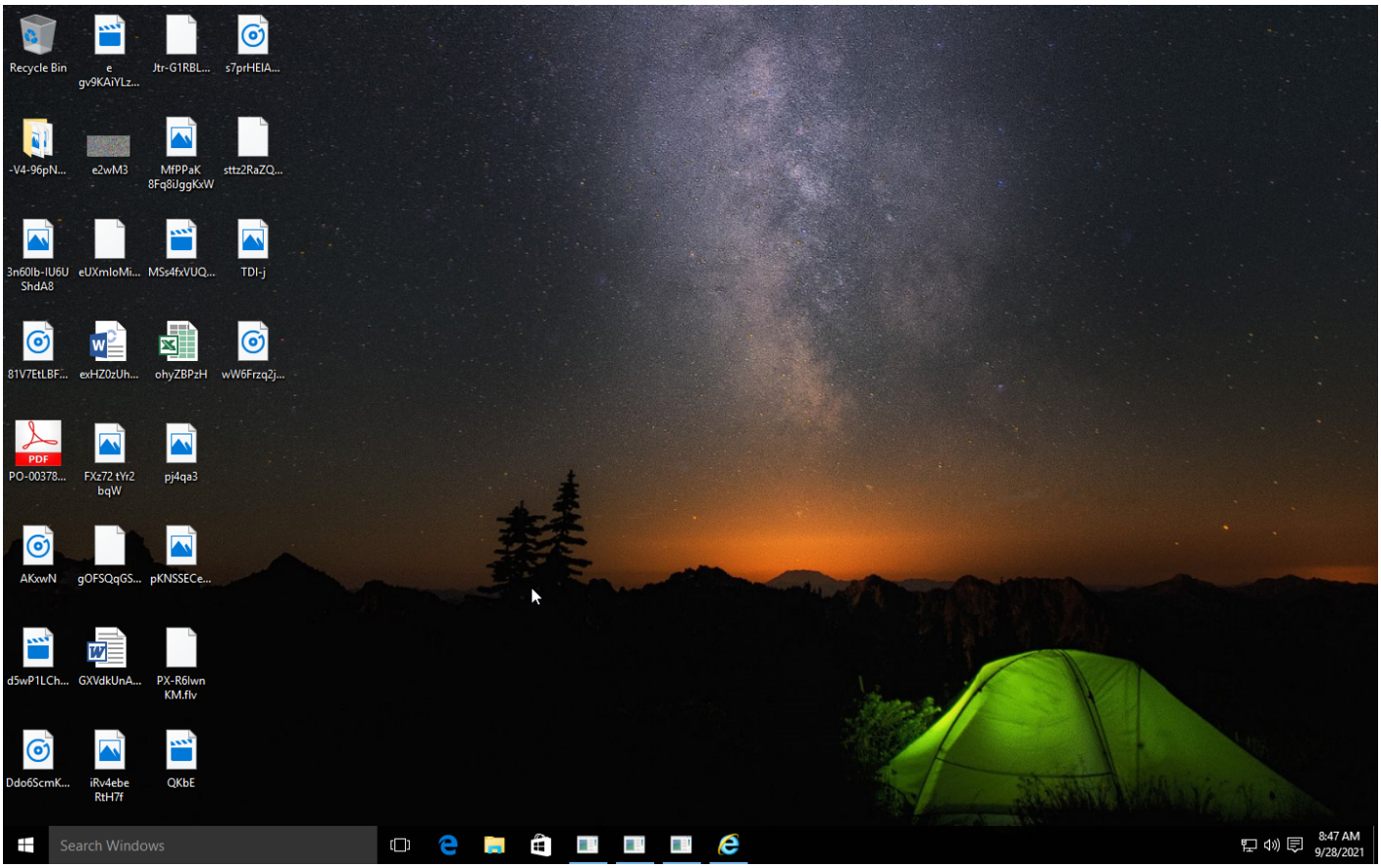
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry							
				#T1143 Hidden Window							
				#T1045 Software Packing							

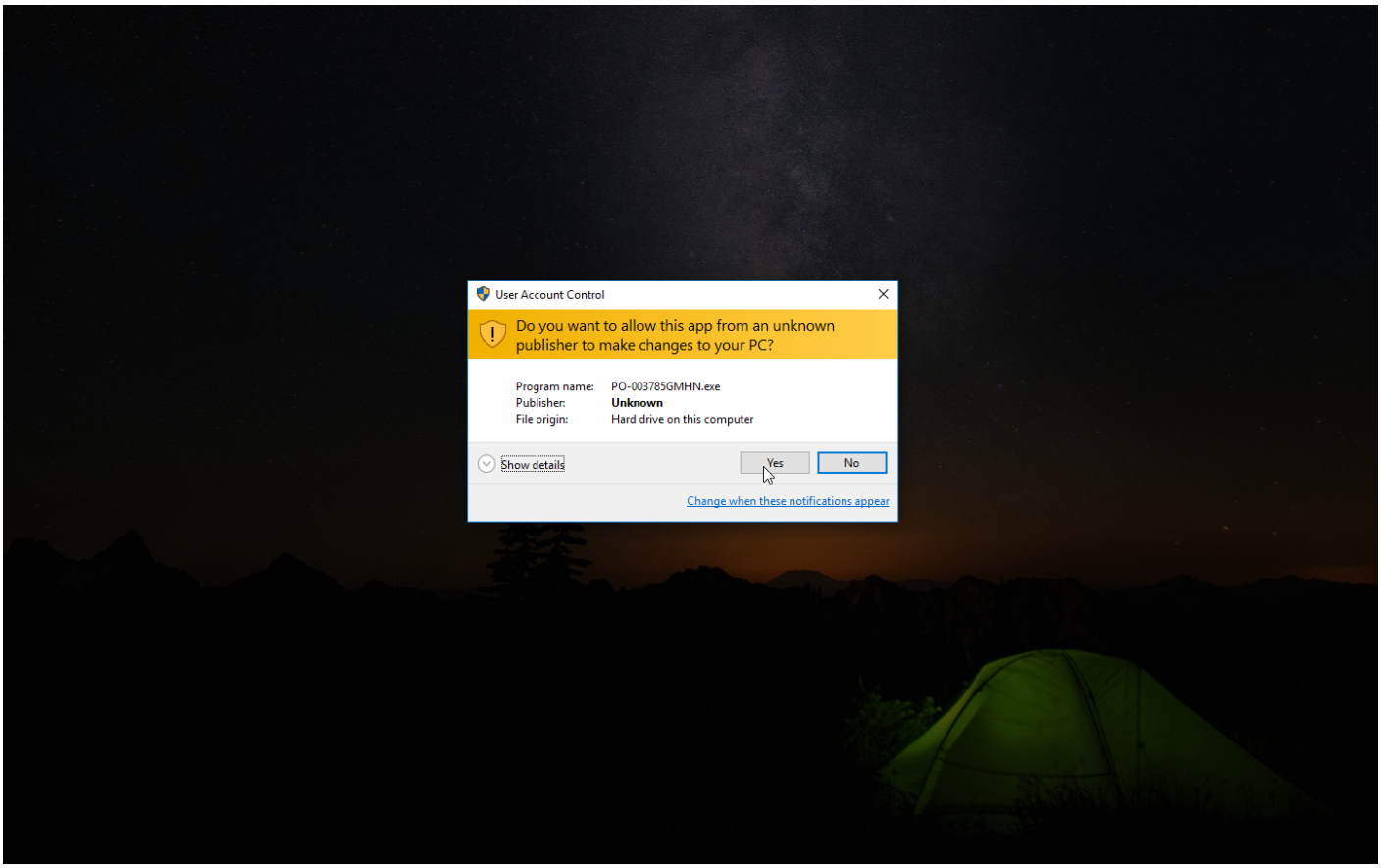
Sample Information

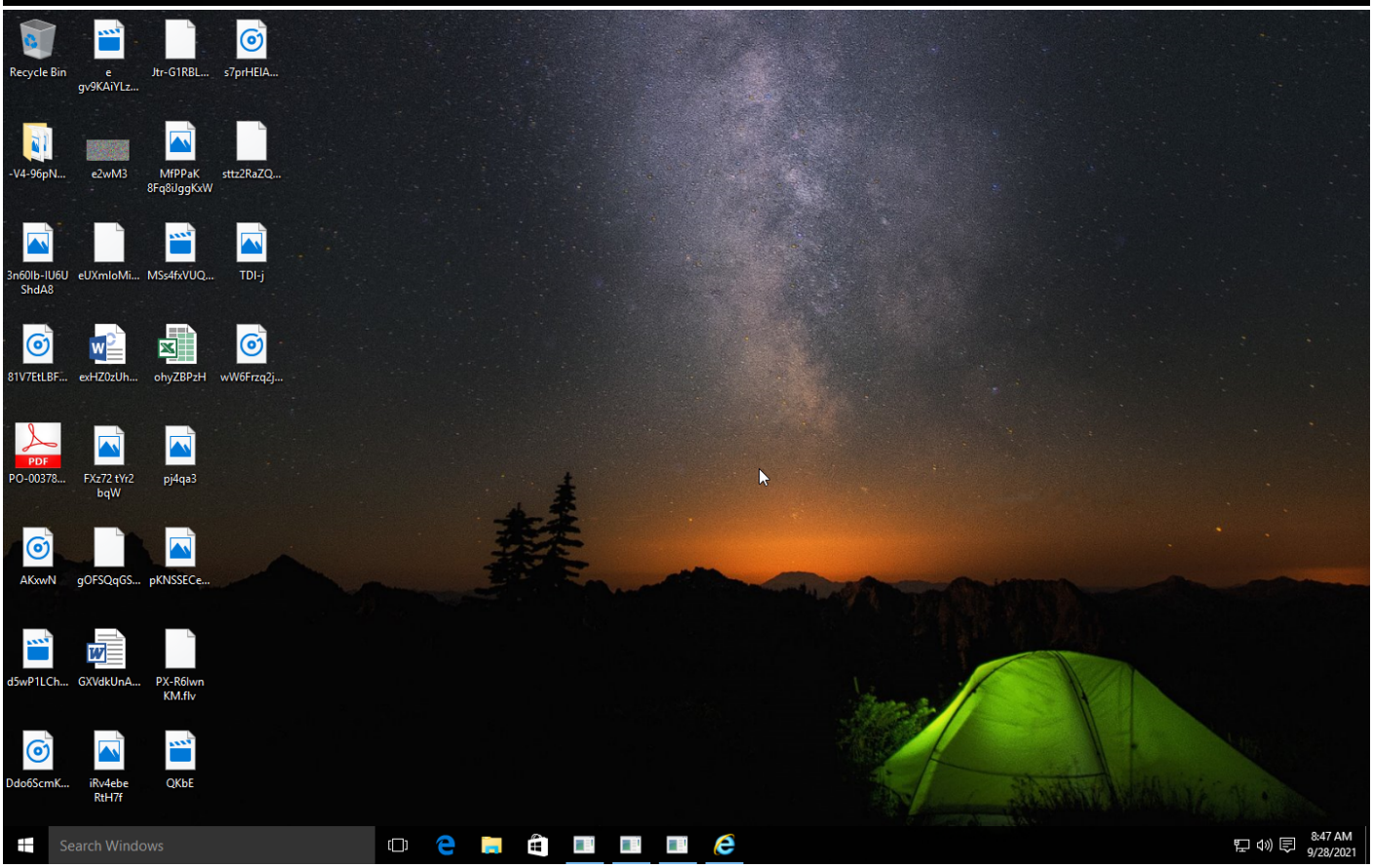
ID	#968741
MD5	4577c41fc896a87df4513f13d29ee65a
SHA1	38e76942a779e8b04cdf763cf993ceda76d049f2
SHA256	144fc8c1a922dbb8162d72a94780f8559bbd9e6b1faa9e037fd33e809126b080
SSDeep	24576:L5A8SqIkJpbDpQc6ScVHdgaHxA7VhLRYF:Lr5ZoHdgaRyzKF
ImpHash	7485e319df85e87afca01bdc77d12961
File Name	PO-003785GMHN.exe
File Size	985.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 10:46 (UTC+2)
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	3
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
e gv9KAiYLz...
Jtr-G1RBL...
s7prHEIA...
-V4-96pN...
e2wM3
MfPPaK 8Fq8UggKxW
sttz2RaZQ...
3n60lb-IU6U ShdA8
eUXmIoMi...
MSs4fxVUQ...
TDI-j
81V7EtLBF...
exHZ0zUh...
ohyZBPzH
wW6Frzq2j...
PO-00378...
FXz72 tYr2 bqW
pj4qa3
AKxwN
gOFSQqGS...
pKNSSECe...
d5wP1LCh...
GXVdkUnA...
PX-R6lwn KM.flv
Ddo6ScmK...
iRv4ebe RtH7f
QKbE
Search Windows
8:47 AM
9/28/2021





Screenshots truncated

NETWORK

General

3.63 KB total sent

624.30 KB total received

1 ports 443

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

1 URLs contacted, 1 servers

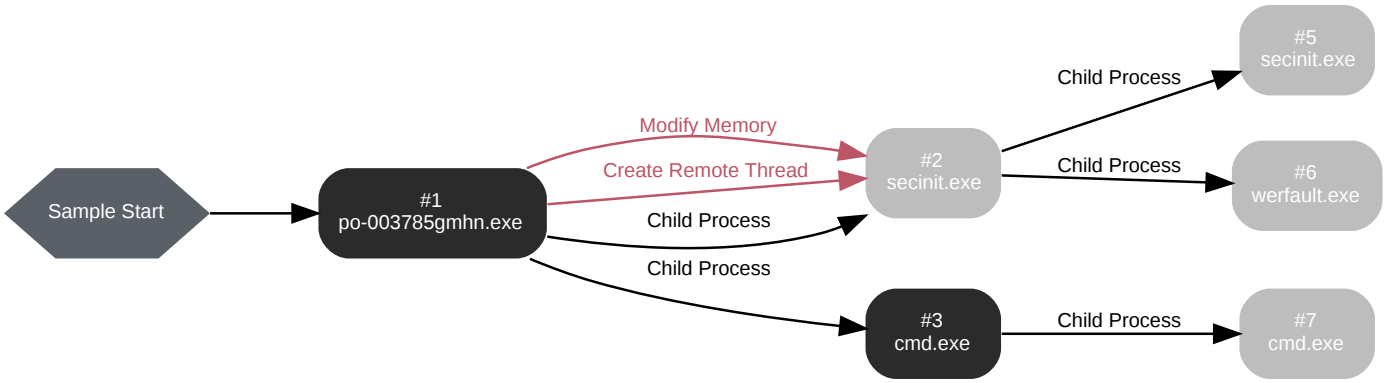
2 sessions, 3.63 KB sent, 624.30 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://maxvilletruck.com/errorserverlogrelaapirootterminationloggercongurat/Udffvxubuutfiqkrvfkzhnjdxnhxzvn	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: po-003785gmhn.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\po-003785gmhn.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PO-003785GMHN.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 56102, Reason: Analysis Target
Unmonitor End Time	End Time: 303762, Reason: Terminated by Timeout
Monitor duration	247.66s
Return Code	Unknown
PID	4792
Parent PID	1636
Bitness	32 Bit

Dropped Files (7)

File Name	File Size	SHA256	YARA Match
C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe	985.50 KB	144fc8c1a922dbb8162d72a94780f8559bbd9e6b1faa9e037fd33e809126b080	✗
-	557.50 KB	010206be3006c21251526c4f4a80436cebf9a386d959388001a44f7a883b7334	✗
C:\Users\Public\Libraries\uxvffdU.url	96 bytes	fe848db8f7ffc14387058c513f4a795b59970d992006b8602d8a27d65de0b4a9	✗
C:\Users\Public\KDECO.bat	155 bytes	37c59c8398279916cfce45f8c5e3431058248f5e3bef4d9f5c0f44a7d564f82e	✗
C:\Users\Public\UKO.bat	250 bytes	f35f2658455a2e40f151549a7d6465a836c33fa9109e67623916f889849eac56	✗
C:\Users\Public\Trast.bat	34 bytes	24222300c78180b50ed1f8361ba63cb27316ec994c1c9079708a51b4a1a9d810	✗
C:\Users\Public\nest	9 bytes	2411791a0ec8be36b9ac98b127f7458dc0cb132d9471de6e93af742b34986f27	✗

Host Behavior

Type	Count
Module	537
Keyboard	7
System	9
Registry	17
-	9
Window	6
File	25
Process	2
-	6
-	1

Network Behavior

Type	Count
HTTP	2
TCP	2

Process #2: secinit.exe

ID	2
File Name	c:\windows\syswow64\secinit.exe
Command Line	"C:\Windows\System32\secinit.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 108049, Reason: Child Process
Unmonitor End Time	End Time: 303762, Reason: Crashed
Monitor duration	195.71s
Return Code	Unknown
PID	1848
Parent PID	4792
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\po-003785gmhn.exe	0x674	0x50480000(1346895872)	0x29000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\po-003785gmhn.exe	0x674	0x110000(1114112)	0x8	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\po-003785gmhn.exe	0x674	0x120000(1179648)	0x18a	✓	1
Create Remote Thread	#1: c:\users\rdhj0cnfevzx\desktop\po-003785gmhn.exe	0x674	0x120000(1179648)	-	✓	1

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Users\Public\Trast.bat" "
Initial Working Directory	C:\Users\Public\
Monitor Start Time	Start Time: 108323, Reason: Child Process
Unmonitor End Time	End Time: 303762, Reason: Terminated by Timeout
Monitor duration	195.44s
Return Code	Unknown
PID	2068
Parent PID	4792
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	65
Environment	15
System	1
Process	1
-	1

Process #5: secinit.exe

ID	5
File Name	c:\windows\syswow64\secinit.exe
Command Line	"C:\Windows\System32\secinit.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 110753, Reason: Child Process
Unmonitor End Time	End Time: 303762, Reason: Terminated by Timeout
Monitor duration	193.01s
Return Code	Unknown
PID	1192
Parent PID	1848
Bitness	32 Bit

Process #6: werfault.exe

ID	6
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1848 -s 256
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 120235, Reason: Child Process
Unmonitor End Time	End Time: 303762, Reason: Terminated by Timeout
Monitor duration	183.53s
Return Code	Unknown
PID	2120
Parent PID	1848
Bitness	32 Bit

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat
Initial Working Directory	C:\Users\Public\
Monitor Start Time	Start Time: 131237, Reason: Child Process
Unmonitor End Time	End Time: 303762, Reason: Terminated by Timeout
Monitor duration	172.53s
Return Code	Unknown
PID	3876
Parent PID	2068
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
144fc8c1a922dbb8162d72a94780f8559bbd9e6b1faa9e037fd33e809126b080	C:\Users\RDhJ0CNFevzX\Desktop\PO-003785GMHN.exe, C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe	Sample File	985.50 KB	application/vnd.microsoft.portable-executable	Write, Read, Create, Access	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
010206be3006c21251526c4f4a80436cebf9a386d959388001a44f7a883b7334	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\fyrm0q9n\udffvxubuutfiqkrvfkzhnjdxnhxzvn[1]	Dropped File	557.50 KB	application/octet-stream	-	CLEAN
fe848db8f7ffc14387058c513f4a795b59970d992006b8602d8a27d65de0b4a9	C:\Users\Public\Libraries\uxvffdU.url	Dropped File	96 bytes	text/plain	Write, Create, Access	CLEAN
37c59c8398279916cfce45f8c5e3431058248f5e3bef4d9f5c0f44a7d564f82e	C:\Users\Public\KDECO.bat	Dropped File	155 bytes	text/plain	Write, Create, Access	CLEAN
f35f2658455a2e40f151549a7d6465a836c33fa9109e67623916f889849eac56	C:\Users\Public\UKO.bat	Dropped File	250 bytes	text/plain	Write, Create, Access	CLEAN
24222300c78180b50ed1f8361ba63cb27316ec994c1c9079708a51b4a1a9d810	C:\Users\Public\Trast.bat	Dropped File	34 bytes	text/plain	Write, Create, Access	CLEAN
2411791a0ec8be36b9ac98b127f7458dc0cb132d9471de6e93af742b34986f27	C:\Users\Public\nest	Dropped File	9 bytes	text/plain	Write, Create, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\PO-003785GMHN.exe	Sample File	Read, Access	CLEAN
3	Accessed File	Access	CLEAN
C:\Users\Public\Libraries	Accessed File	Access	CLEAN
C:\Users\Public\Libraries\Udffvxu	Accessed File	Create, Access	CLEAN
C:\Users\Public\Libraries\uxvffdU.url	Dropped File	Write, Create, Access	CLEAN
C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe	Sample File	Write, Create, Access	CLEAN
C:\Windows\System32\secinit.exe	Accessed File	Access	CLEAN
C:\Users\Public\nest	Dropped File	Write, Create, Access	CLEAN
C:\Users\Public\KDECO.bat	Dropped File	Write, Create, Access	CLEAN
C:\Users\Public\UKO.bat	Dropped File	Write, Create, Access	CLEAN
C:\Users\Public\Trast.bat	Dropped File	Write, Create, Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\Public	Accessed File	Access	CLEAN
"C:\Users\Public\Trast.bat"	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://maxvilletruck.com/errorserverlogrelaapirootterminationloggerconguration/Udffvxubuutfiqkrvfkzhnjdxnhxzvn	-	64.33.128.70	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
maxvilletruck.com	64.33.128.70	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
64.33.128.70	maxvilletruck.com	United States	DNS, HTTPS, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	po-003785gmhn.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	po-003785gmhn.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	po-003785gmhn.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	access	po-003785gmhn.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2	read, access	po-003785gmhn.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	po-003785gmhn.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Udffvxu	write, access	po-003785gmhn.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
po-003785gmhn.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PO-003785GMHN.exe"	MALICIOUS
secinit.exe	"C:\Windows\System32\secinit.exe"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Public\Trast.bat" "	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1848 -s 256	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat	CLEAN

YARA / AV

Antivirus (3)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.47063473	C:\Users\RDhJ0CNFevzX\Desktop\PO-003785GMHN.exe	MALICIOUS
Memory Dump	Gen:Variant.Doina.24402	-	MALICIOUS
Memory Dump	Trojan.GenericKD.47063473	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

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

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

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