MALICIOUS

Classifications: Backdoor

Threat Names: Netwire | C2/Generic-A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe**
ID	#5067417
MD5	e366f96c9b5c5528426a116eb49ef445
SHA1	8062220b613b56116d638b3d7f5dd043f3bc096e
SHA256	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58
File Size	1269.00 KB
Report Created	2022-08-05 13:42 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 20 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Netwire configuration was extracted	1	Backdoor
	• A configuration for Netwire was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Backdoor
	• Rule "NetWire" from ruleset "RATs" has matched on a memory dump for (process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "xman2.duckdns.org" as C2/Generic-A.			
3/5	Network Connection	Performs DNS request for known DDNS domain	1	-
	• (Process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe resolves host name "xman2.duckdns.org" of dynamic DNS provider "duckdns.org".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe modifies memory of (process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe alters context of (process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe", to be triggered by REGISTRATION.			
1/5	Mutex	Creates mutex	2	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe creates mutex with name "UGuYsqINzELkVGLDAodcCAWpBT". • (Process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe creates mutex with name "-".			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe starts (process #4) schtasks.exe with a hidden window. • (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe starts (process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe reads from (process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe.			

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe resolves host name "xman2.duckdns.org" to IP "154.53.40.254".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe opens an outgoing TCP connection to host "154.53.40.254:4433".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #7) 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe tries to connect to TCP port 4433 at 154.53.40.254.			

Malware Configuration: Netwire

Metadata	Key	Extracted Value
URL	Url	xman2.duckdns.org:4433
Credential	Password	Password
Other: Copy to Local Path	Value	✖
Other: Delete Original File	Value	✖
Other: Lock Executable	Value	✖
Other: Registry Autorun	Value	✖
Other: ActiveX Startup	Value	✖
Other: Allow Only One Instance	Value	✖
Other: Offline Keylogger	Value	✖
Other: Connection Type	Value	Direct Connection

Mitre ATT&CK Matrix

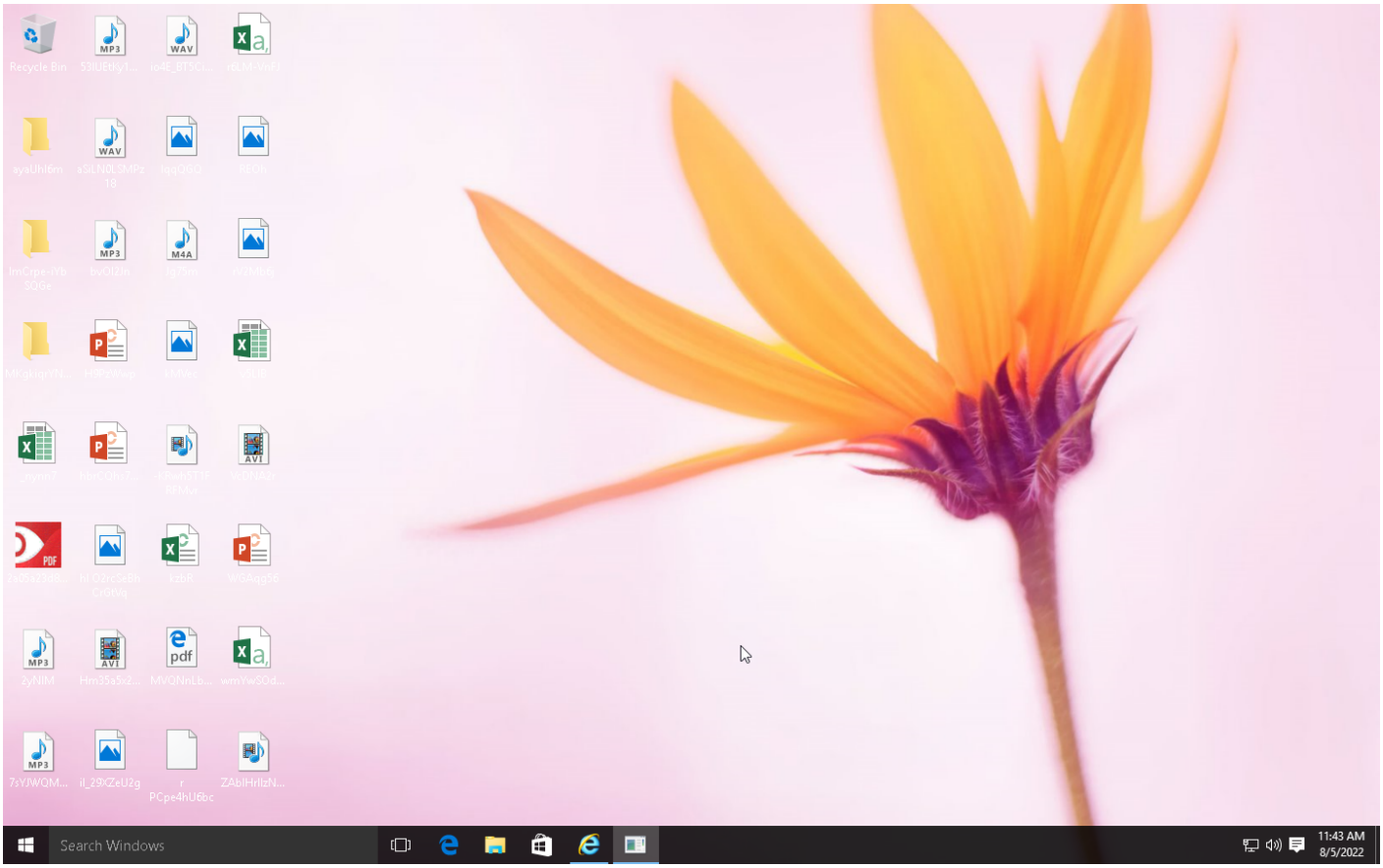
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window					#T1065 Uncommonly Used Port		
				#T1045 Software Packing							

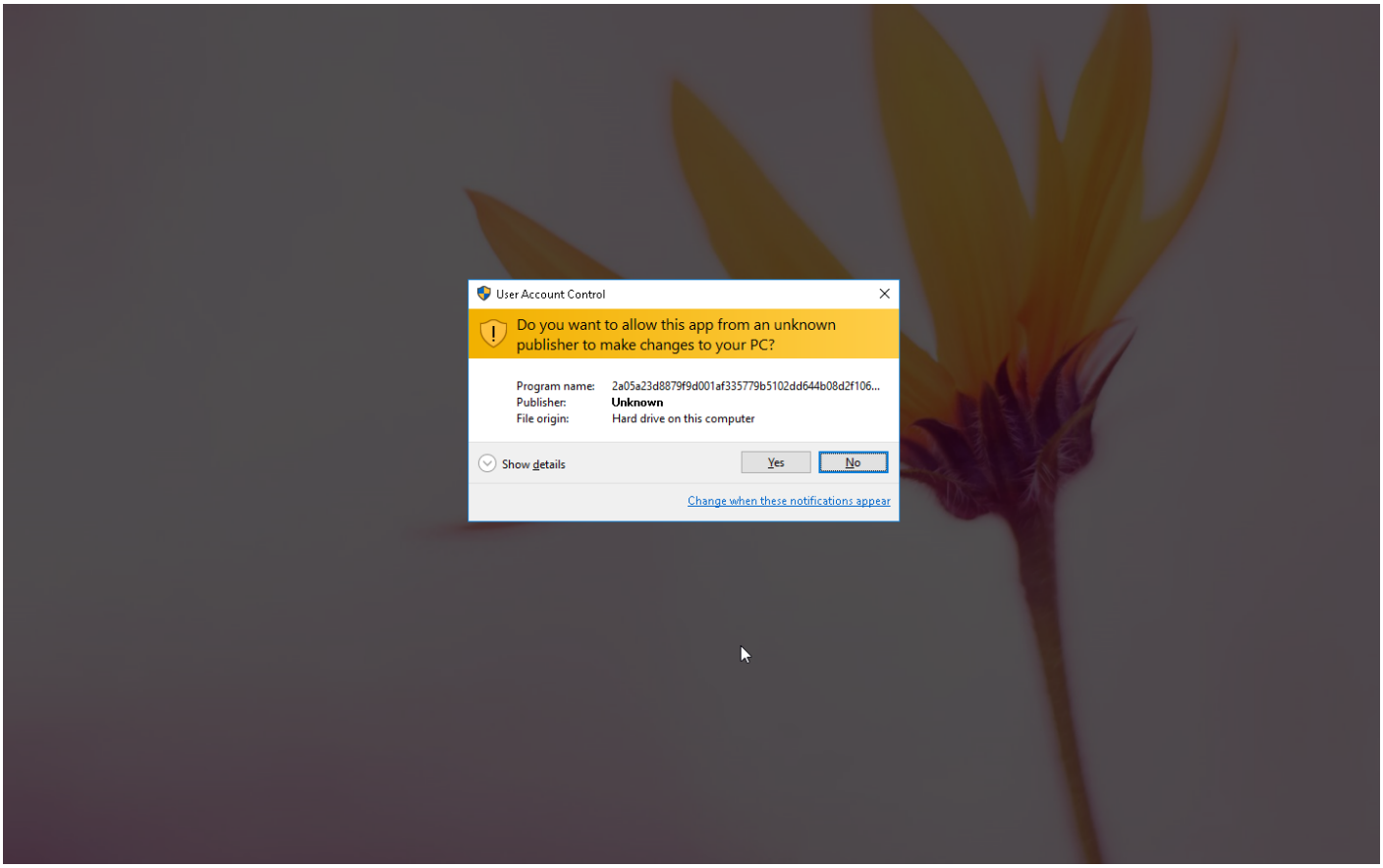
Sample Information

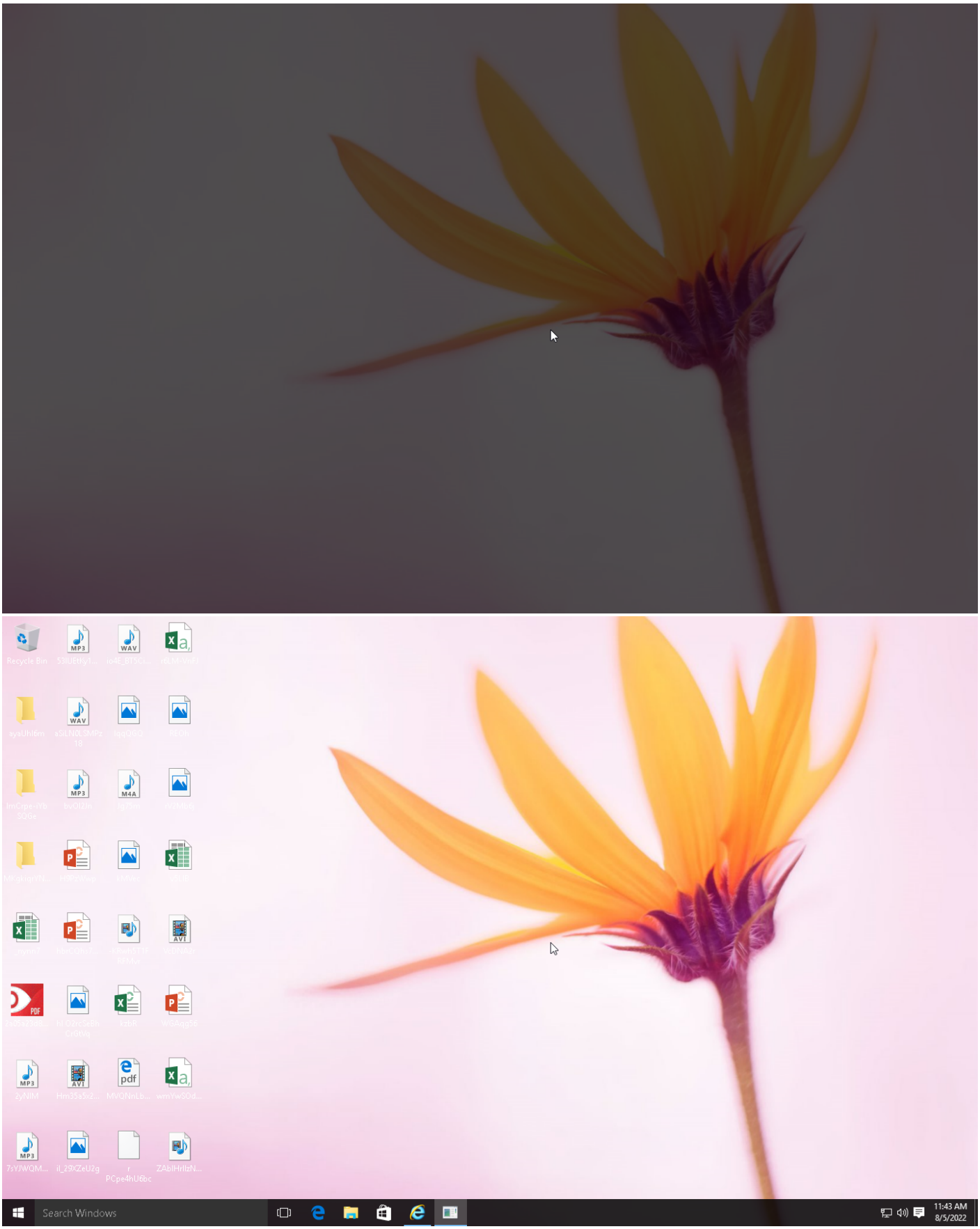
ID	#5067417
MD5	e366f96c9b5c5528426a116eb49ef445
SHA1	8062220b613b56116d638b3d7f5dd043f3bc096e
SHA256	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58
SSDeep	24576:iTJpjM7KzOkDwPN2XanQBOrOlaLlpxtRYNNHV3lSpWBb62:EjW77kQNaaQB6w+tR63AEbT
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe
File Size	1269.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 13:42 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	16


Search Windows
11:43 AM
8/5/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 2a05a23d8879f9d001af335779b5102dd644b08d2f106...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

717 bytes total sent

723 bytes total received

3 ports 4433, 53, 445

2 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

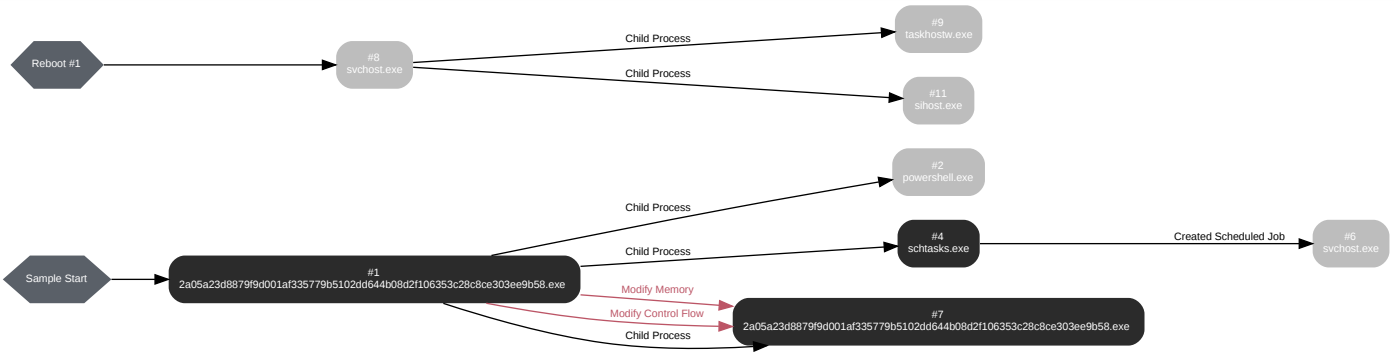
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	xman2.duckdns.org	NO_ERROR	154.53.40.254		NA

BEHAVIOR

Process Graph



Process #1: 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 67458, Reason: Analysis Target
Unmonitor End Time	End Time: 214779, Reason: Terminated
Monitor duration	147.32s
Return Code	0
PID	5020
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	1269.00 KB	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB163.tmp	1.56 KB	807607b419e72e7018fcf4f0f63effd01d5437d0e8f58143453d20b638a9f7b2	✖

Host Behavior

Type	Count
Registry	4
Module	108
Window	6
File	10
Mutex	2
User	2
System	21
Process	3
-	3
-	9

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188840, Reason: Child Process
Unmonitor End Time	End Time: 234435, Reason: Terminated
Monitor duration	45.59s
Return Code	1073807364
PID	4476
Parent PID	5020
Bitness	32 Bit

Process #4: schtasks.exe

ID	4
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rWWREmAZOgElhb" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB163.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190071, Reason: Child Process
Unmonitor End Time	End Time: 210186, Reason: Terminated
Monitor duration	20.11s
Return Code	0
PID	4480
Parent PID	5020
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	10

Process #6: svchost.exe

ID	6
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 207381, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 307478, Reason: Terminated by timeout
Monitor duration	100.10s
Return Code	Unknown
PID	864
Parent PID	4480
Bitness	64 Bit

Process #7: 2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 209675, Reason: Child Process
Unmonitor End Time	End Time: 234431, Reason: Terminated
Monitor duration	24.76s
Return Code	1073807364
PID	4540
Parent PID	5020
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x401000(4198400)	0x34200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x436000(4415488)	0xc400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x443000(4468736)	0x1400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x44c000(4505600)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x44d000(4509696)	0x2600	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0 / 0x11a0	0x41ae7b(4304507)	-	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	0x13a0	0x3bb008(3911688)	0x4	✔	1

Host Behavior

Type	Count
Module	17
File	3
Environment	1

Type	Count
System	4
Mutex	1
Registry	6
-	2

Network Behavior

Type	Count
DNS	1
TCP	1

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 262317, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 307478, Reason: Terminated by timeout
Monitor duration	45.16s
Return Code	Unknown
PID	1012
Parent PID	4480
Bitness	64 Bit

Process #9: taskhostw.exe

ID	9
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 297176, Reason: Child Process
Unmonitor End Time	End Time: 307478, Reason: Terminated by timeout
Monitor duration	10.30s
Return Code	Unknown
PID	1380
Parent PID	1012
Bitness	64 Bit

Process #11: sihost.exe

ID	11
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 304249, Reason: Child Process
Unmonitor End Time	End Time: 307478, Reason: Terminated by timeout
Monitor duration	3.23s
Return Code	Unknown
PID	1496
Parent PID	1012
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58	C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe	Sample File	1269.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
807607b419e72e7018fcf4f0f63effd01d5437d0e8f58143453d20b638a9f7b2	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB163.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB163.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe.config	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://xman2.duckdns.org:4433	-	154.53.40.254	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
xman2.duckdns.org	154.53.40.254	-	TCP, DNS	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
154.53.40.254	xman2.duckdns.org	United States	TCP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
UGuYsqlNzELkVGLDAodcCAWpBT	access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\NetWire	create, access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\NetWire\Install Date	access, write	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\NetWire\HostId	access, write	2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	CLEAN

Process

Process Name	Commandline	Verdict
2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	"C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rWWREmAZOgElhb" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB163.tmp"	SUSPICIOUS
2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe	"C:\Users\RDhJ0CNFevzX\Desktop\2a05a23d8879f9d001af335779b5102dd644b08d2f106353c28c8ce303ee9b58.exe"	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\rWWREmAZOgElhb.exe"	CLEAN
sihost.exe	sihost.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN

YARA / AV

YARA (16)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5
RATs	NetWire	NetWire RAT	Memory Dump	-	Backdoor	5/5

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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