MALICIOUS

Classifications: Injector, Spyware

Threat Names: Trojan.Agent.FNJS, Generic.Exploit.Shellcode.RDI.1.83306058, Gen:Variant.Cerbu.64651

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe**
ID	#2780765
MD5	7bb8f00948d80dc7a3936c4c1fa2b276
SHA1	e60d2828c4a5716d1d96ba1a141e239a2df374f8
SHA256	c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5
File Size	516.06 KB
Report Created	2021-09-27 22:00 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (20 rules, 44 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Total Commander, Internet Explorer, Microsoft Outlook, Google Chrome.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Trojan.Agent.FNJS". • Built-in AV detected a memory dump of (process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe as "Trojan.Agent.FNJS". • Built-in AV detected a memory dump of (process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe as "Generic.Exploit.Shellcode.RDI.1.83306058". • Built-in AV detected a memory dump of (process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe as "Gen:Variant.Cerbu.64651".			
4/5	Injection	Writes into the memory of another process	4	Injector
	• (Process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe modifies memory of (process #2) wermgr.exe. • (Process #2) wermgr.exe modifies memory of (process #5) svchost.exe. • (Process #2) wermgr.exe modifies memory of (process #7) svchost.exe. • (Process #2) wermgr.exe modifies memory of (process #8) svchost.exe.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #2) wermgr.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) wermgr.exe has a thread which sleeps more than 5 minutes.			
2/5	Data Collection	Reads sensitive browser data	2	-
	• (Process #5) svchost.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #5) svchost.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #7) svchost.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Reputation	Contacts known suspicious URL	1	-
	• (Process #2) wermgr.exe contacted known malicious URL "https://103.56.207.230/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/kps/".			
2/5	Reputation	Contacts known suspicious IP address	1	-
	• Contacted IP address 103.56.207.230 is a known suspicious IP address.			
1/5	Obfuscation	Reads from memory of another process	4	-
	• (Process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe reads from (process #2) wermgr.exe. • (Process #2) wermgr.exe reads from (process #5) svchost.exe. • (Process #2) wermgr.exe reads from (process #7) svchost.exe. • (Process #2) wermgr.exe reads from (process #8) svchost.exe.			

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	3	-

- (Process #1) c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
- (Process #2) wermgr.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
- (Process #2) wermgr.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	Privilege Escalation	Enables process privilege	4	-

- (Process #2) wermgr.exe enables process privilege "SeDebugPrivilege".
- (Process #5) svchost.exe enables process privilege "SeDebugPrivilege".
- (Process #7) svchost.exe enables process privilege "SeDebugPrivilege".
- (Process #9) svchost.exe enables process privilege "SeDebugPrivilege".

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

- (Process #2) wermgr.exe creates mutex with name "Global\{9320442D-23A5-DB07-BD98-99E92C629BA1}".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	3	-

- (Process #2) wermgr.exe starts (process #5) svchost.exe with a hidden window.
- (Process #2) wermgr.exe starts (process #7) svchost.exe with a hidden window.
- (Process #2) wermgr.exe starts (process #8) svchost.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Discovery	Enumerates running processes	2	-

- (Process #5) svchost.exe enumerates running processes.
- (Process #7) svchost.exe enumerates running processes.

Score	Category	Operation	Count	Classification
1/5	Network Connection	Performs DNS request	5	-

- (Process #2) wermgr.exe resolves host name "169.199.153.88.zen.spamhaus.org" to IP "-".
- (Process #2) wermgr.exe resolves host name "169.199.153.88.cbl.abuseat.org" to IP "-".
- (Process #2) wermgr.exe resolves host name "169.199.153.88.b.barracudacentral.org" to IP "-".
- (Process #2) wermgr.exe resolves host name "169.199.153.88.dnsbl-1.uceprotect.net" to IP "-".
- (Process #2) wermgr.exe resolves host name "169.199.153.88.spam.dnsbl.sorbs.net" to IP "-".

Score	Category	Operation	Count	Classification
1/5	Network Connection	Tries to connect using an uncommon port	1	-

- (Process #2) wermgr.exe tries to connect to TCP port 449 at 171.103.189.118.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	3	-

- (Process #5) svchost.exe resolves 191 API functions by name.
- (Process #7) svchost.exe resolves 161 API functions by name.
- (Process #8) svchost.exe resolves 65 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Discovery	Checks external IP address	1	-

- (Process #2) wermgr.exe checks external IP by asking IP info service at "wtfismyip.com/text".

Mitre ATT&CK Matrix

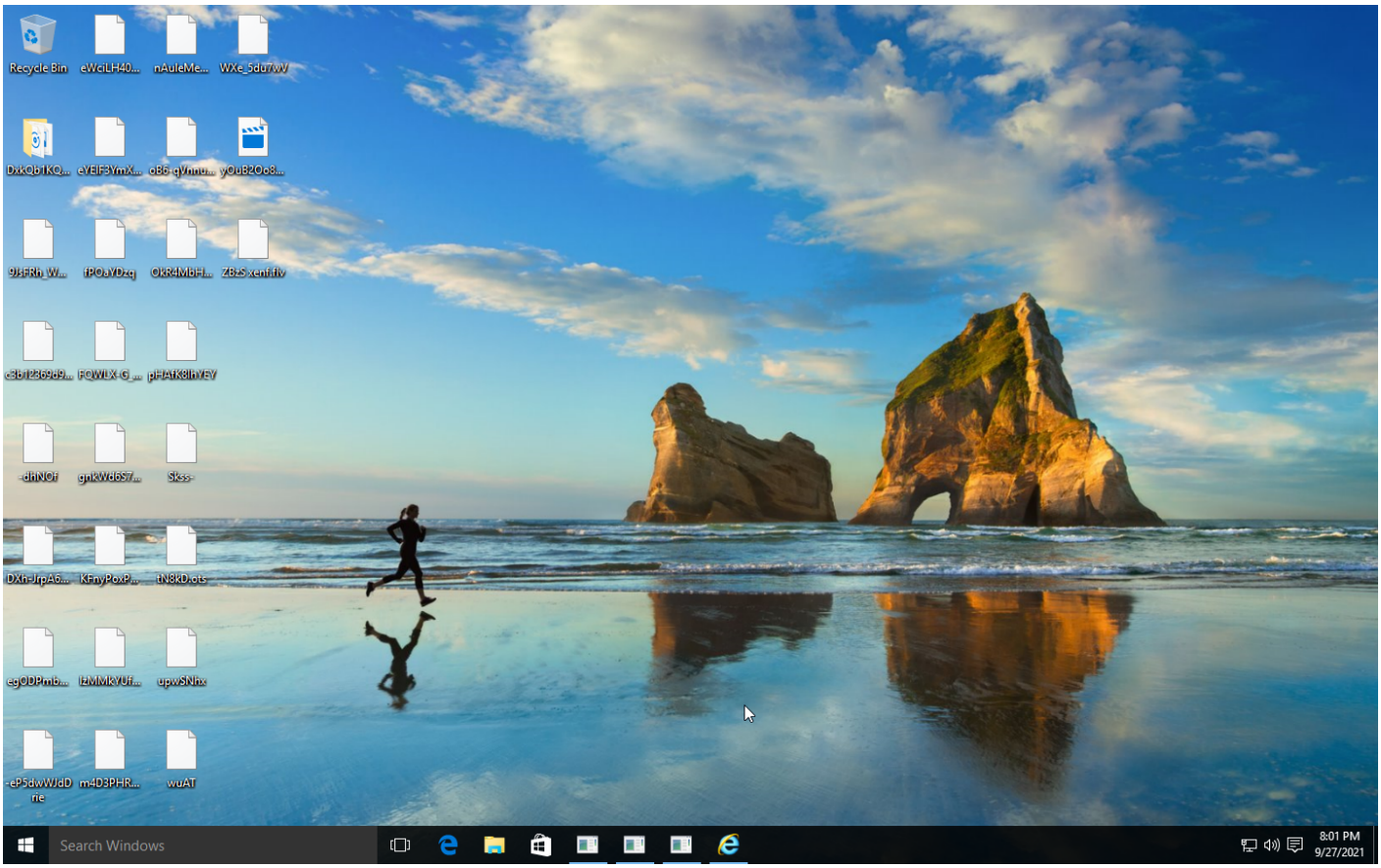
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1143 Hidden Window	#T1003 Credential Dumping	#T1057 Process Discovery		#T1005 Data from Local System			
				#T1497 Virtualization/ Sandbox Evasion	#T1214 Credentials in Registry	#T1012 Query Registry					
						#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					
						#T1016 System Network Configuration Discovery					

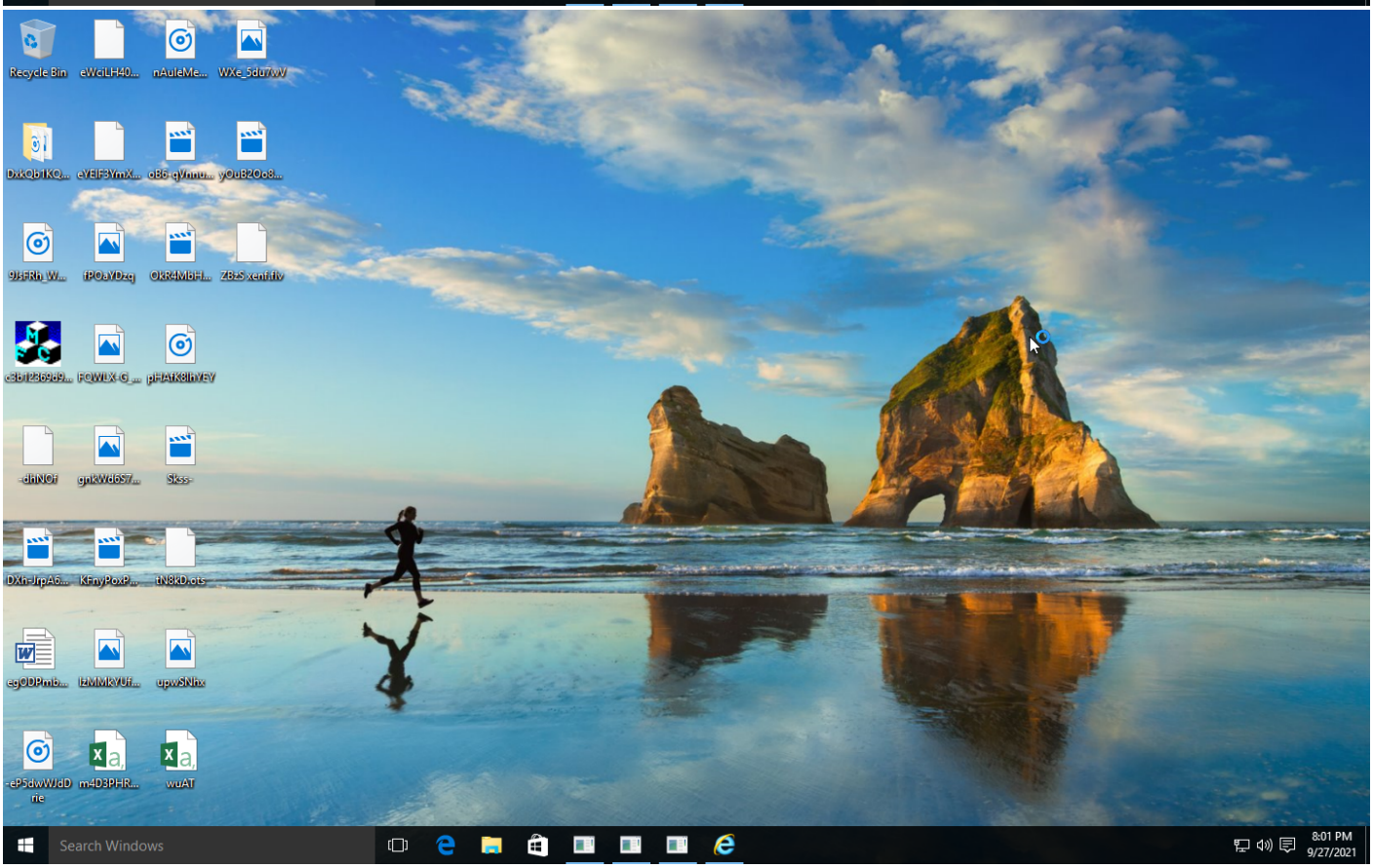
Sample Information

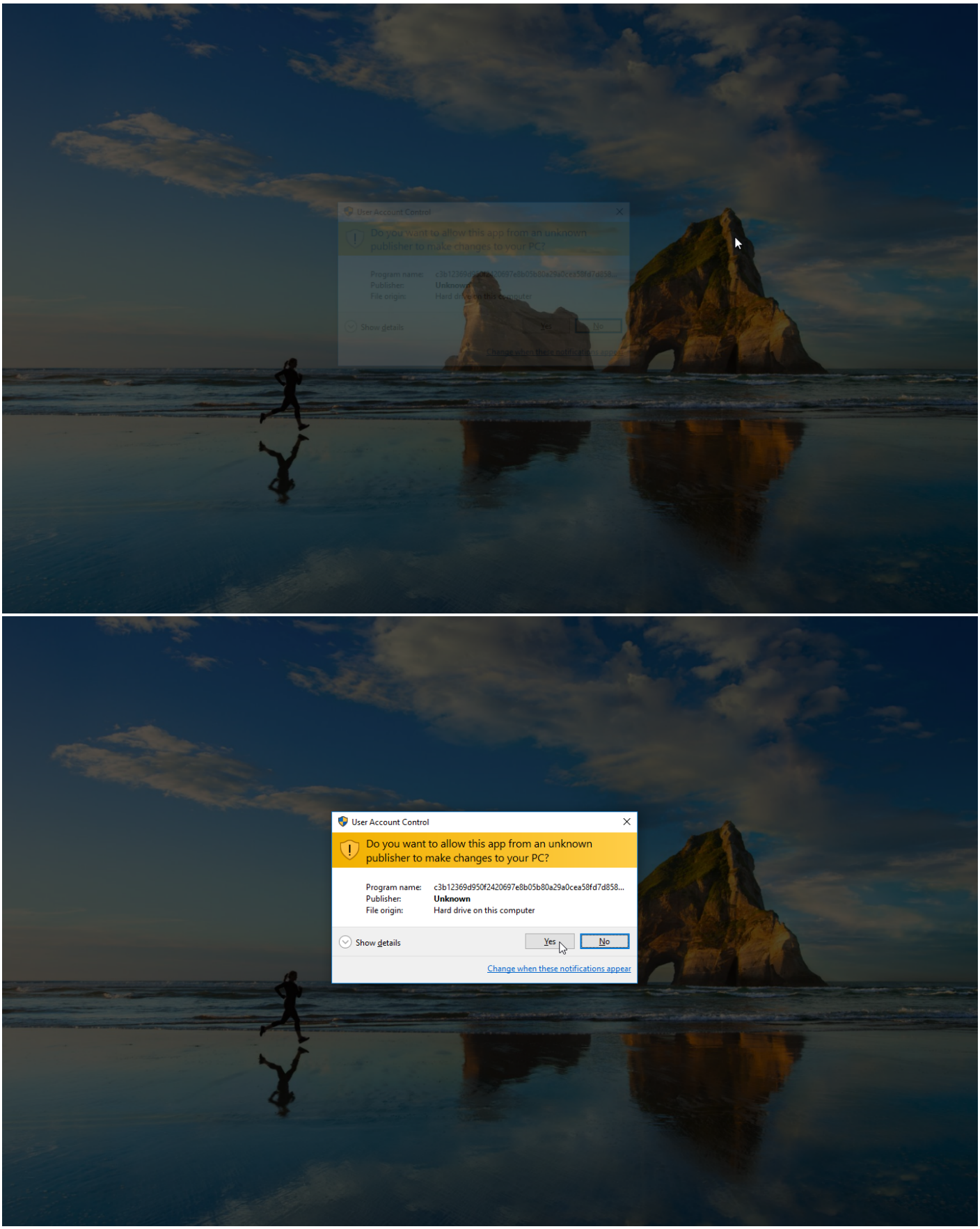
ID	#2780765
MD5	7bb8f00948d80dc7a3936c4c1fa2b276
SHA1	e60d2828c4a5716d1d96ba1a141e239a2df374f8
SHA256	c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5
SSDeep	12288:cbVMh0tRyr3W3SfniM+uwkMx8nXoTT0WJZmo:WMh0tRy73lY8X2xJZmo
ImpHash	675872e23dfc0f62ffbc2f69c316f4bc
File Name	c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe
File Size	516.06 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 22:00 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	10
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	5
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
Search Windows
8:01 PM
9/27/2021


Recycle Bin
Search Windows
8:01 PM
9/27/2021



Screenshots truncated

NETWORK

General

38.75 KB total sent

1354.05 KB total received

3 ports 80, 449, 443

6 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

6 DNS requests for 6 domains

1 nameservers contacted

2 total requests returned errors

HTTP/S

23 URLs contacted, 5 servers

14 sessions, 38.75 KB sent, 1354.05 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	wtfismyip.com/text	-	-		0 bytes	NA
POST	103.239.6.30/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/84/	-	-		0 bytes	NA
POST	103.239.6.30/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/81/	-	-		0 bytes	NA
GET	https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/pwgrabb64/	-	-		0 bytes	NA
GET	https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/pwgrabc64/	-	-		0 bytes	NA
GET	https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/networkDll64/	-	-		0 bytes	NA
GET	https://103.56.207.230/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/kps/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/kps/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/0/Windows 10 x64/1107/88.153.199.169/DEBD3DFEDF418C3E99F8759943821CA7364C37894CA12183A3519D4AA90C04E2/DrtbzVJblRThr1hHxdjxBrV7PRFhV/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/user/RDhJ0CNFevzX/0/	-	-		0 bytes	NA

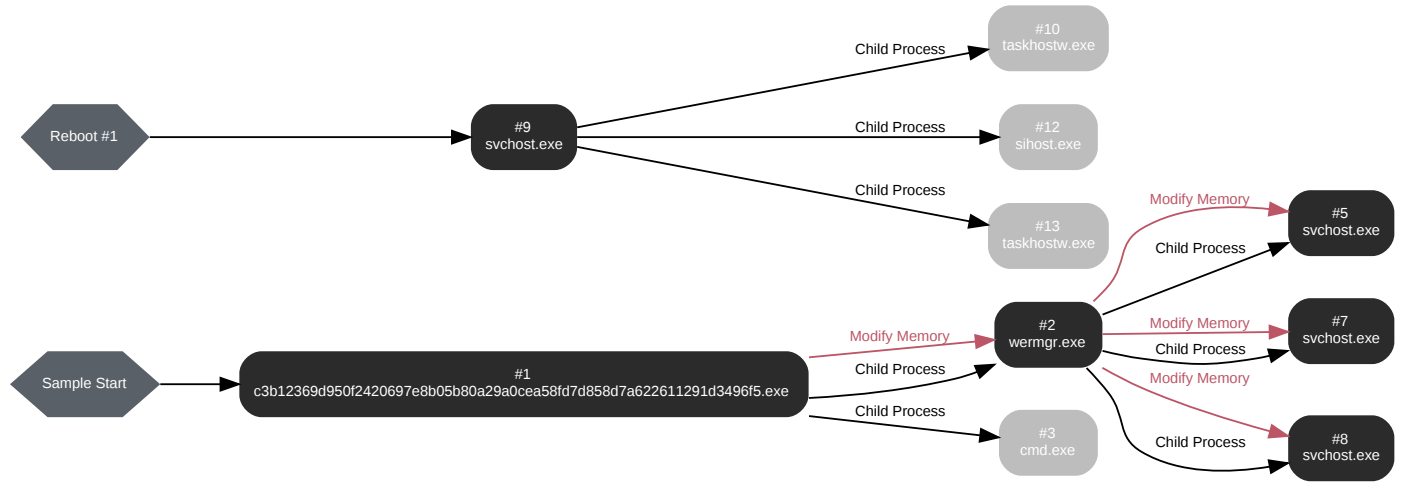
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/path/C:%5CUsers%5CRDhJ0CNFevzX%5CAppData%5CLocal%5CbrowDownload55%5Cc3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe/0/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/23/2000033/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/DNSBL/not%20listed/0/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/NAT%20status/client%20is%20behind%20NAT/0/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/dpost/	-	-		0 bytes	NA
POST	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/VERS//	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/BDPFPPJZRDXFLPBNF/1/	-	-		0 bytes	NA
POST	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/DEBG//	-	-		0 bytes	NA
POST	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/DPST//	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/HDLBFZFXPDDFJFT/1/	-	-		0 bytes	NA
POST	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabc/VERS//	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/1/1ZL1TvNZPZJdTHNBXHB/	-	-		0 bytes	NA
GET	https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/1381892/1/	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	169.199.153.88.zen.spamhaus.org	NoError			NA
A	169.199.153.88.cbl.abuseat.org	NoError			NA
A	169.199.153.88.b.barracudacentral.org	NXDomain			NA
A	169.199.153.88.dnsbl-1.uceprotect.net	NXDomain			NA
A	169.199.153.88.spam.dnsbl.sorbs.net	NoError			NA
-	xc64zb	-	fe80:0000:0000:0000:858a:31fa:02d3:471b, fe80:0000:0000:0000:2cf9:4710:a766:3856, 192.168.0.197, 2001:0000:2851:782c:2cf9:4710:a766:3856		NA

BEHAVIOR

Process Graph



Process #1: c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 52509, Reason: Analysis Target
Unmonitor End Time	End Time: 93521, Reason: Terminated
Monitor duration	41.01s
Return Code	0
PID	3692
Parent PID	1600
Bitness	32 Bit

Host Behavior

Type	Count
System	200
File	6
Environment	1
Module	51
Keyboard	1
Window	2
Process	4
-	6
-	1

Process #2: wermgr.exe

ID	2
File Name	c:\windows\system32\wermgr.exe
Command Line	C:\Windows\system32\wermgr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 78995, Reason: Child Process
Unmonitor End Time	End Time: 192116, Reason: Terminated
Monitor duration	113.12s
Return Code	1073807364
PID	1872
Parent PID	3692
Bitness	64 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	0x6a0	0x100000(1048576)	0x28db8	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	0x6a0	0x7ff6efcf8360(140698562036576)	0x10	✓	1

Host Behavior

Type	Count
System	24592
Module	638
Process	1720
User	2
Mutex	1
File	50
COM	1
-	9
-	2727
-	3

Network Behavior

Type	Count
HTTP	1
HTTPS	42
DNS	6
TCP	12

Process #3: cmd.exe

ID	3
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 79631, Reason: Child Process
Unmonitor End Time	End Time: 81318, Reason: Terminated
Monitor duration	1.69s
Return Code	0
PID	2956
Parent PID	3692
Bitness	64 Bit

Process #5: svchost.exe

ID	5
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 176116, Reason: Child Process
Unmonitor End Time	End Time: 187047, Reason: Terminated
Monitor duration	10.93s
Return Code	1073807364
PID	328
Parent PID	1872
Bitness	64 Bit

Injection Information (27)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x100000(1048576)	0x230	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x110000(1114112)	0xd8	✓	83
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x7ff6bac63980(140697672235392)	0x16	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x18	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x18	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x14	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x20	✓	79
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xf	✓	7
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1a	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xd	✓	15
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x9	✓	8
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xc	✓	11
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xa	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x15	✓	4

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x16	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x10	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xb	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x11	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x12	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x13	✓	6
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xe	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1c	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4a0000(4849664)	0x6	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4c0000(4980736)	0x204	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x5d0000(6094848)	0x400	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x5e0000(6160384)	0x80	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x8b0000(9109504)	0x58	✓	1

Host Behavior

Type	Count
Module	841
System	46
File	85
Environment	1
Process	42
User	2
Registry	13

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #7: svchost.exe

ID	7
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 184128, Reason: Child Process
Unmonitor End Time	End Time: 191992, Reason: Terminated
Monitor duration	7.86s
Return Code	1073807364
PID	1404
Parent PID	1872
Bitness	64 Bit

Injection Information (42)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x100000(1048576)	0x230	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x110000(1114112)	0xd8	✓	94
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x7ff6bac63980(140697672235392)	0x16	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1a	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x18	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xd	✓	7
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x20	✓	87
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x9	✓	7
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xc	✓	10
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xa	✓	7
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xf	✓	9
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x15	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1b	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x11	✓	7

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1c	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x6	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xe	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x16	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x14	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x26	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x8	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x18	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x12	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x17	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x19	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x10	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x13	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x7	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x180001000(6442455040)	0x5bc00	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x18005d000(6442831872)	0x1c400	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x18007a000(6442950656)	0x2a0c	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x18007a000(6442950656)	0xe00	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x18007d000(6442962944)	0x3600	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x28	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x400	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4b0000(4915200)	0x188	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4c0000(4980736)	0x50	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x6	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4c0000(4980736)	0x204	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4d0000(5046272)	0x400	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4e0000(5111808)	0x80	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x500000(5242880)	0x58	✓	1

Host Behavior

Type	Count
Module	464
System	37
File	3
Environment	1
Process	42
User	1
Registry	80

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189773, Reason: Child Process
Unmonitor End Time	End Time: 193009, Reason: Terminated
Monitor duration	3.24s
Return Code	1073807364
PID	760
Parent PID	1872
Bitness	64 Bit

Injection Information (40)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x100000(1048576)	0x230	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x110000(1114112)	0xd8	✓	78
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x7ff6bac63980(140697672235392)	0x16	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x1a	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x18	✓	10
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x15	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x20	✓	54
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xf	✓	7
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xa	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x10	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x19	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xe	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x9	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x13	✓	6

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x14	✓	6
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xb	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x6	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xc	✓	5
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0xd	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x26	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x16	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x11	✓	4
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x18	✓	3
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x12	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x20	✓	11
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x17	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x8	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x180001000(6442455040)	0x4a00	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x180006000(6442475520)	0x1c00	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x180008000(6442483712)	0x200	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x180009000(6442487808)	0x600	✓	2
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x20000(131072)	0x28	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x400	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4b0000(4915200)	0x188	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4c0000(4980736)	0x50	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x1e0000(1966080)	0x8	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4c0000(4980736)	0x204	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4d0000(5046272)	0x400	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x4e0000(5111808)	0x80	✓	1
Modify Memory	#2: c:\windows\system32\wermgr.exe	0x770	0x500000(5242880)	0x58	✓	1

Host Behavior

Type	Count
Module	76
System	39

Process #9: svchost.exe

ID	9
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: 210965, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 293251, Reason: Terminated by Timeout
Monitor duration	82.29s
Return Code	Unknown
PID	856
Parent PID	528
Bitness	64 Bit

Host Behavior

Type	Count
-	4
COM	2

Process #10: taskhostw.exe

ID	10
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 235834, Reason: Child Process
Unmonitor End Time	End Time: 293251, Reason: Terminated by Timeout
Monitor duration	57.42s
Return Code	Unknown
PID	1160
Parent PID	856
Bitness	64 Bit

Process #12: sihost.exe

ID	12
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 243688, Reason: Child Process
Unmonitor End Time	End Time: 293251, Reason: Terminated by Timeout
Monitor duration	49.56s
Return Code	Unknown
PID	1484
Parent PID	856
Bitness	64 Bit

Process #13: taskhostw.exe

ID	13
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 247809, Reason: Child Process
Unmonitor End Time	End Time: 293251, Reason: Terminated by Timeout
Monitor duration	45.44s
Return Code	Unknown
PID	1540
Parent PID	856
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5	C:\Users\RDhJ0CNFevzX\Desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	Sample File	516.06 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	Sample File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Access, Read	CLEAN
C:\Windows\system32\EN\AuthFWSnapIn.Resources.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\EN\AuthFWWizFwk.Resources.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\EN\AutoWorkplace.Resources.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\EN\fhuxpresentation.Resources.dll	Accessed File	Access, Read	CLEAN
ver.txt	Accessed File	Access	CLEAN
C:\Windows\system32\svchost.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome Beta\User Data\Default\Login Data.bak	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bak	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge Beta\User Data\Default\Login Data.bak	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCookies\2OH9TBLH.txt	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCookies\container.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCookies\TAS0OY3R.txt	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://103.56.207.230/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/kps/	-	103.56.207.230	-	GET	SUSPICIOUS
http://wtfismyip.com/text	-	95.217.228.176	-	GET	CLEAN
https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/pwgrabb64/	-	186.235.48.8	-	GET	CLEAN
https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/pwgrabc64/	-	186.235.48.8	-	GET	CLEAN
https://186.235.48.8/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/networkDll64/	-	186.235.48.8	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/kps/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/0/Windows 10 x64/1107/88.153.199.169/DEBD3DFEDF418C3E99F8759943821CA7364C37894CA12183A3519D4AA90C04E2/DrtbzVJblRThr1hHxdjxBrV7PRFhV/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/user/RDhJ0CNFevzX/0/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/path/C:%5CUsers%5CRDhJ0CNFevzX%5CAppData%5CLocal%5CbrowDownload55%5Cc3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe/0/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/23/2000033/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/DNSBL/not%20listed/0/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/14/NAT%20status/client%20is%20behind%20NAT/0/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/5/dpost/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/VERS//	-	171.103.189.118	-	POST	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/BDPFPPJZRDXFLPBNF/1/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/DEBG//	-	171.103.189.118	-	POST	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabb/DPST//	-	171.103.189.118	-	POST	CLEAN
http://103.239.6.30/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/84/	-	103.239.6.30	-	POST	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/HDLBFZFXPDDFJFT/1/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/64/pwgrabc/VERS//	-	171.103.189.118	-	POST	CLEAN
http://103.239.6.30/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/81/	-	103.239.6.30	-	POST	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/1/1ZL1TvNZPZJdTHNBXHB/	-	171.103.189.118	-	GET	CLEAN
https://171.103.189.118/tot153/XC64ZB_W10010586.FDB33F77971735B3BB3BB3B3B33B3B93/10/62/1381892/1/	-	171.103.189.118	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
wtfismyip.com	95.217.228.176	-	HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
169.199.153.88.zen.spamhaus.org	-	-	DNS	CLEAN
169.199.153.88.cbl.abuseat.org	-	-	DNS	CLEAN
169.199.153.88.b.barracudacentral.org	-	-	DNS	CLEAN
169.199.153.88.dnsbl-1.uceprotect.net	-	-	DNS	CLEAN
169.199.153.88.spam.dnsbl.sorbs.net	-	-	DNS	CLEAN
xc64zb	fe80:0000:0000:0000:2cf9:4710:a766:3856, 2001:0000:2851:782c:2cf9:4710:a766:3856, 192.168.0.197, fe80:0000:0000:0000:858a:31fa:02d3:471b	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
103.56.207.230	-	Indonesia	TLS, TCP	SUSPICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN
95.217.228.176	wtfismyip.com	Finland	TCP, HTTP, DNS	CLEAN
103.239.6.30	-	Bangladesh	TCP, HTTP	CLEAN
171.103.189.118	-	Thailand	TLS, TCP	CLEAN
186.235.48.8	-	Brazil	TCP, HTTPS	CLEAN
fe80:0000:0000:0000:858a:31fa:02d3:471b	xc64zb	-	DNS	CLEAN
fe80:0000:0000:0000:2cf9:4710:a766:3856	xc64zb	-	DNS	CLEAN
192.168.0.197	xc64zb	-	DNS	CLEAN
2001:0000:2851:782c:2cf9:4710:a766:3856	xc64zb	United Kingdom	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{9320442D-23A5-DB07-BD98-99E92C629BA1}	access	wermgr.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet	access, read	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	access, read	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Outlook\Profiles\Outlook	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	svchost.exe	CLEAN

Process

Process Name	Commandline	Verdict
c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	"C:\Users\RDhJ0CNFevzX\Desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe"	MALICIOUS
wermgr.exe	C:\Windows\system32\wermgr.exe	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe	SUSPICIOUS
cmd.exe	C:\Windows\system32\cmd.exe	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
sihost.exe	sihost.exe	CLEAN
taskhostw.exe	taskhostw.exe	CLEAN

YARA / AV

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.Agent.FNJS	C:\Users\RDhJ0CNFevzX\Desktop\c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5.exe	MALICIOUS
Memory Dump	Trojan.Agent.FNJS	-	MALICIOUS
Memory Dump	Generic.Exploit.Shellcode.RDI.1.83306058	-	MALICIOUS
Memory Dump	Gen:Variant.Cerbu.64651	-	MALICIOUS
Memory Dump	Trojan.Agent.FNJS	-	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	2021-09-27 16:34:30+00:00
Built-in AV Database Records	10473840

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