MALICIOUS

Classifications: Spyware Keylogger

Threat Names: AgentTesla

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**doc_0429191990189-3829-03-2018.INV#00399.PDF.exe**
ID	#10321178
MD5	d9d36237b5578dc9bb244d77cb8de4c4
SHA1	ef90a3b8853c84b4668375c5eda5c93ade45bb8d
SHA256	5fb2529b865460bdc505a962532260c522af1255ea05eca105fd68651c60af74
File Size	641.50 KB
Report Created	2024-04-28 10:54 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (30 rules, 67 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	6	Spyware
	• YARA detected "AgentTesla_HTML_Message" from ruleset "Malware" in memory dump data from (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe. • YARA detected "AgentTesla_StringDecryption" from ruleset "Malware" in memory dump data from (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe. • YARA detected "AgentTesla_HTML_Message" from ruleset "Malware" in memory dump data from (process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe. • YARA detected "AgentTesla_StringDecryption" from ruleset "Malware" in memory dump data from (process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe. • YARA detected "SandboxProductID" from ruleset "Generic" in memory dump data from (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe. • YARA detected "SandboxProductID" from ruleset "Generic" in memory dump data from (process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe.		
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, collects hardware information, queries network configuration and collects operating system information which indicates system fingerprinting.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe logs keys and potentially exfiltrates data.			
4/5	Masquerade	Uses a double file extension	1	-
	• File "C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe" has a double file extension.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• The sample itself is a known malicious file.			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
3/5	Anti Analysis	Modifies native system functions	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe modifies native system functions, possibly to change control flow.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe reads the network adapters' addresses by API.			
2/5	Discovery	Searches for sensitive browser data	10	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Opera" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to access sensitive data of web browser "Internet Explorer / Edge" by registry. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Flock" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Maple Studio" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Chromium" by file. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe searches for sensitive data of web browser "Torch" by file.			

Score	Category	Operation	Count	Classification
2/5	Discovery	Searches for sensitive mail data	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to access sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Discovery	Searches for sensitive application data	2	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to access sensitive data of application "WinSCP" by registry. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to access sensitive data of application "Internet Download Manager" by registry.			
2/5	Data Collection	Reads sensitive FTP data	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to read sensitive data of FTP application "CoreFTP" by registry.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe queries OS version via WMI query: select * from Win32_OperatingSystem.			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe queries hardware properties via WMI: SELECT * FROM Win32_Processor. • (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe queries hardware properties via WMI: SELECT * FROM Win32_VideoController.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe modifies memory of (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe alters context of (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe starts (process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe with a hidden window.			
1/5	Mutex	Creates mutex	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe creates mutex with name "Global\.net clr networking".			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	20	-

Score	Category	Operation	Count	Classification
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Mozilla Firefox" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "SeaMonkey" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Flock" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Postbox" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Mozilla Thunderbird" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Foxmail" by registry.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Opera Mail" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Pocomail" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Qualcomm Eudora" by registry.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "The Bat!" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "FileZilla" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "WS_FTP" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "WinSCP" by registry.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "CoreFTP" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "DynDNS" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Paltalk" by registry.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "Pidgin" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "SmartFTP" by file.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "FTP Commander" by registry.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe tries to gather information about application "No-IP DUC" by registry.		
1/5	Network Connection	Performs DNS request	2	-
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe resolves hostname "checkip.dyndns.org" to IP "132.226.8.169".		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe resolves hostname "mail.sunsealogistics.com" to IP "119.18.49.18".		
1/5	Network Connection	Connects to remote host	2	-
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe opens an outgoing TCP connection to host "119.18.49.18:587".		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe opens an outgoing TCP connection to host "132.226.8.169:80".		
1/5	Obfuscation	Resolves API functions dynamically	2	-
		• (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe resolves 41 API functions by name.		
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe resolves 136 API functions by name.		
1/5	Obfuscation	Overwrites code	1	-
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe overwrites code to possibly hide behavior.		
1/5	Discovery	Checks external IP address	1	-
		• (Process #2) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe checks external IP by asking IP info service at "http://checkip.dyndns.org".		
1/5	Obfuscation	The binary file was created with a packer	1	-
		• Memory dump of (Process #1) doc_0429191990189-3829-03-2018.inv#00399.pdf.exe is packed with "UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser".		

Mitre ATT&CK Matrix

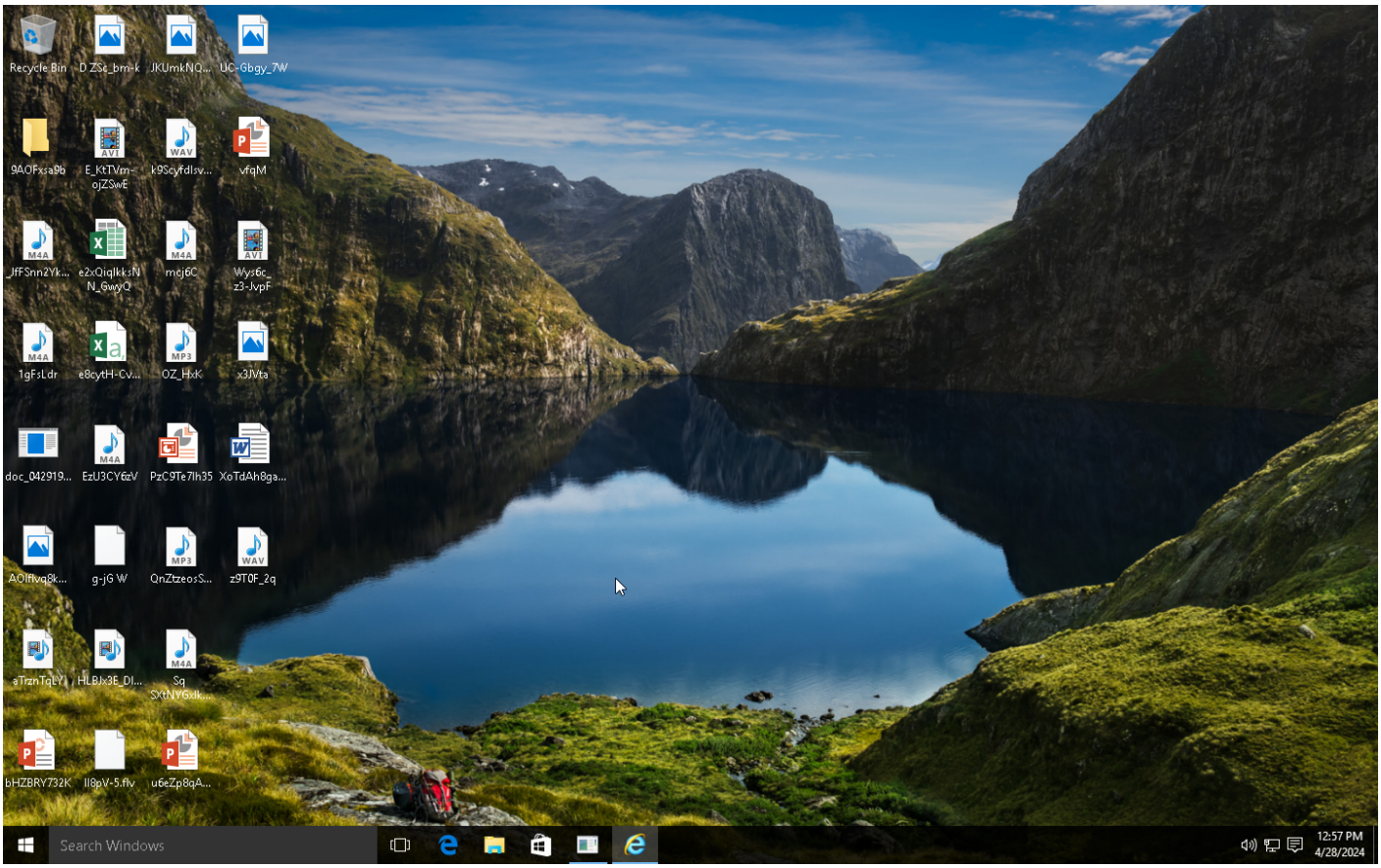
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1179 Hooking	#T1179 Hooking	#T1143 Hidden Window	#T1056 Input Capture	#T1057 Process Discovery		#T1056 Input Capture			
				#T1036 Masquerading	#T1179 Hooking	#T1016 System Network Configuration Discovery		#T1119 Automated Collection			
				#T1045 Software Packing	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1027 Obfuscated Files or Information	#T1214 Credentials in Registry	#T1012 Query Registry					
						#T1217 Browser Bookmark Discovery					
						#T1082 System Information Discovery					

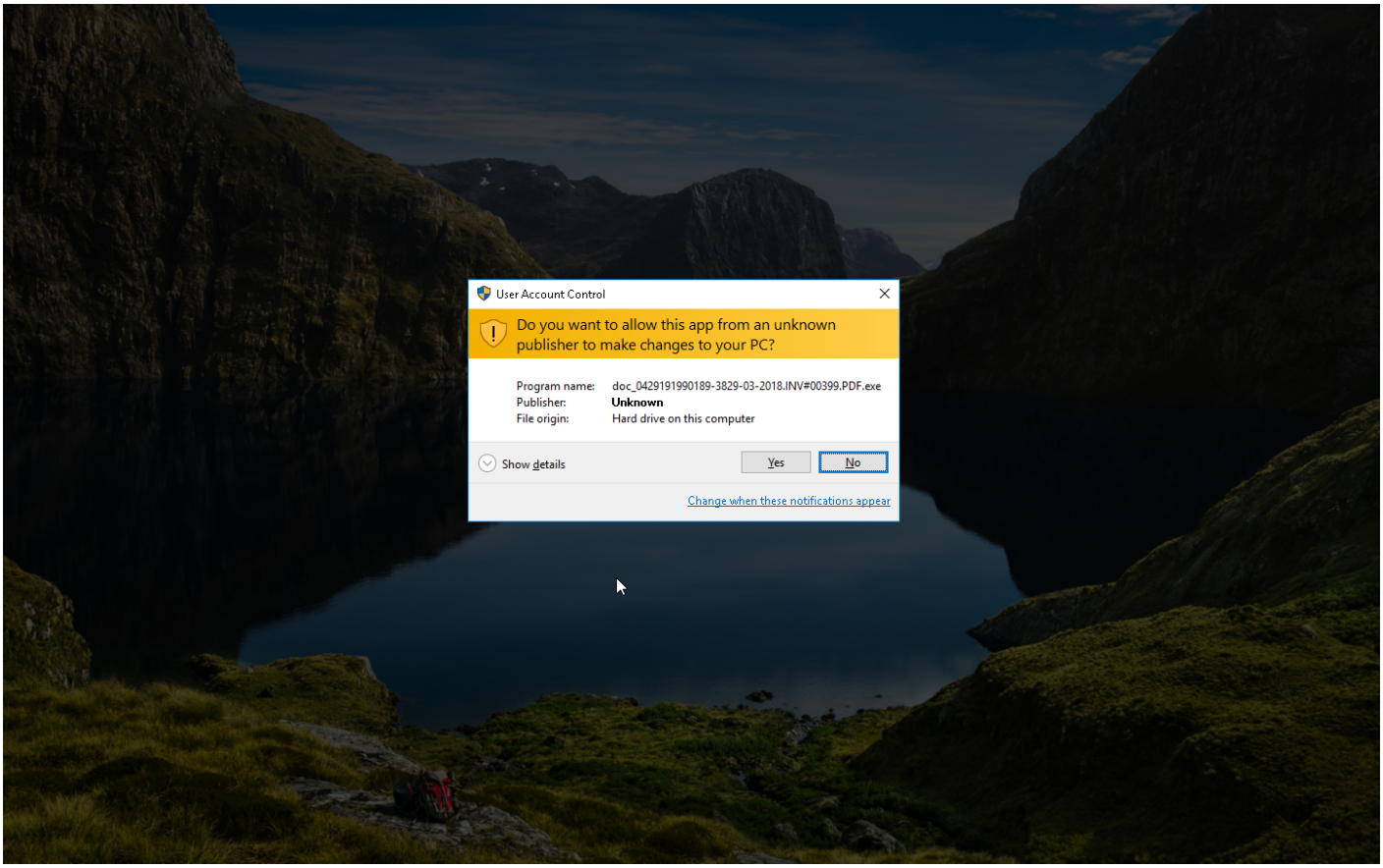
Sample Information

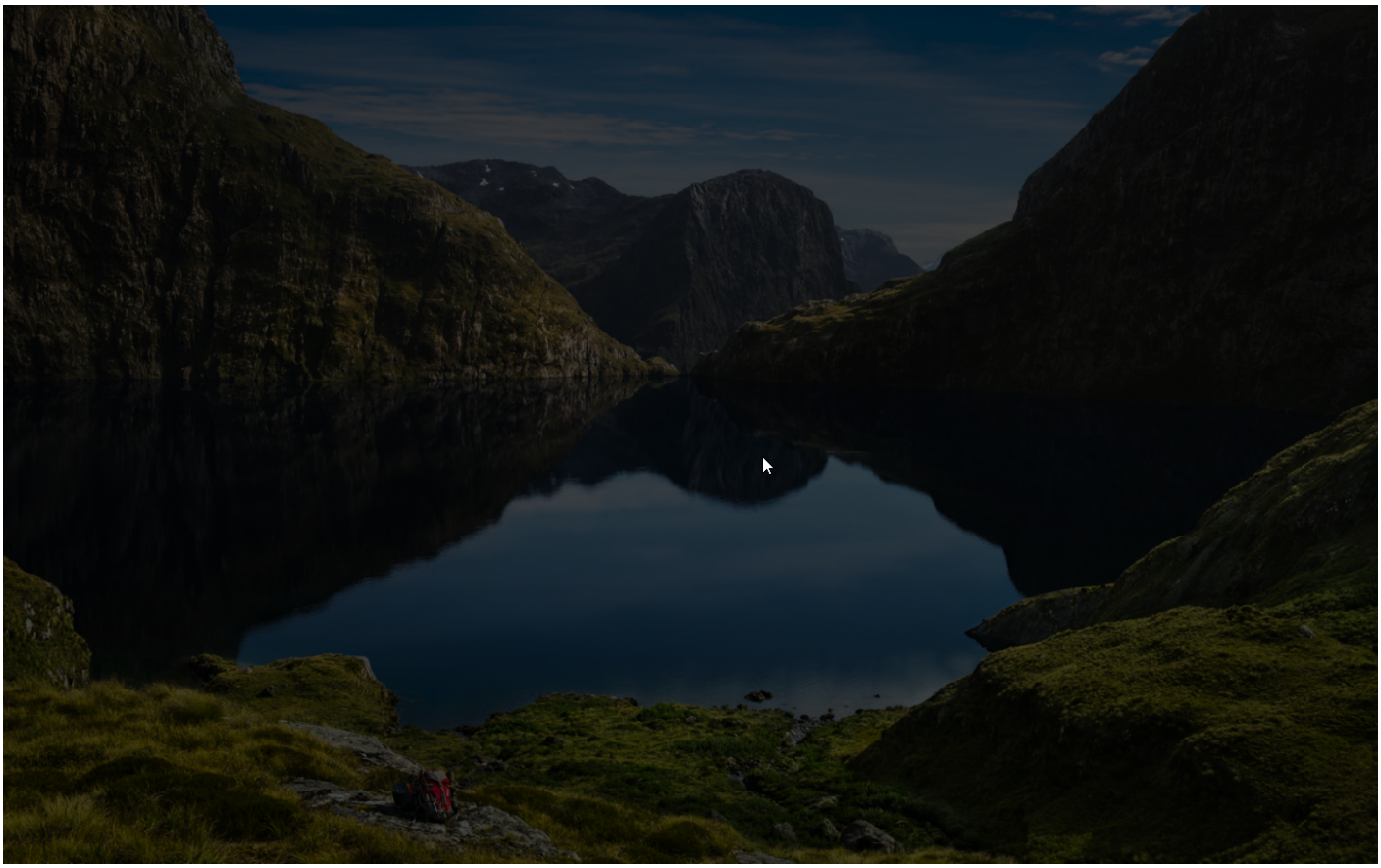
ID	#10321178
MD5	d9d36237b5578dc9bb244d77cb8de4c4
SHA1	ef90a3b8853c84b4668375c5eda5c93ade45bb8d
SHA256	5fb2529b865460bdc505a962532260c522af1255ea05eca105fd68651c60af74
SSDeep	12288:PusODY5awdTk6MHeSRzmWoQthlspcUZi3cJyLn9CETGSynk3t:W3Dn2R6DRzoMhLpEMQLQEqCd
ImpHash	9cabaf4e504448fdfc891577e902eef7
File Name	doc_0429191990189-3829-03-2018.INV#00399.PDF.exe
File Size	641.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

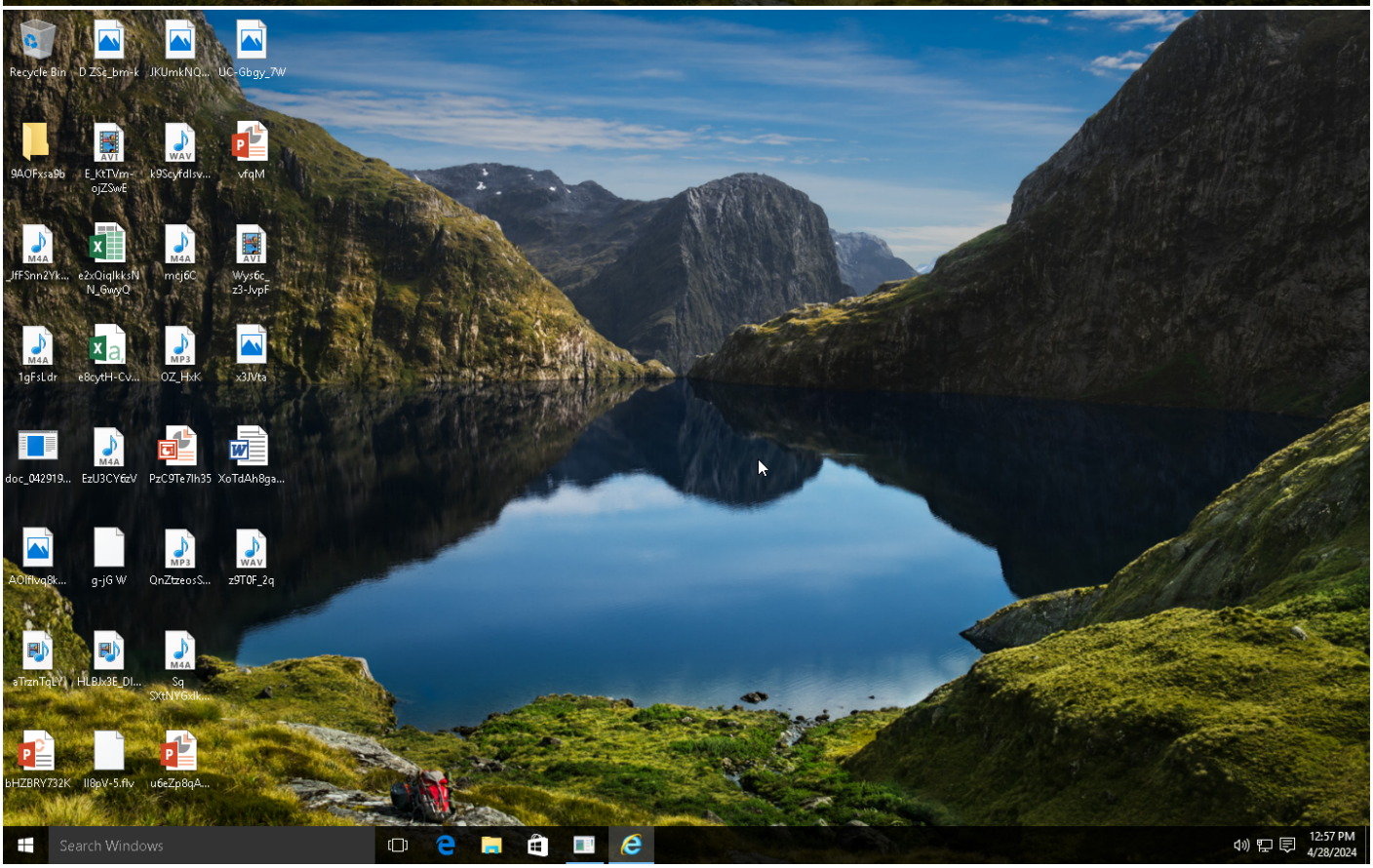
Analysis Information

Creation Time	2024-04-28 10:54 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	True
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	42


Recycle Bin
Search Windows
12:57 PM
4/28/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: doc_0429191990189-3829-03-2018.INV#00399.PDF.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Recycle Bin
Search Windows
12:57 PM
4/28/2024

NETWORK

General

906 bytes total sent

1.66 KB total received

3 ports 80, 587, 53

3 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 320 bytes sent, 534 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://checkip[.]dyndns[.]org	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	NO_ERROR	132.226.8.169, 132.226.247.73, 193.122.6.168, 158.101.44.242, 193.122.130.0	checkip[.]dyndns[.]com	CLEAN
A	mail[.]sunsealogistics[.]com, sunsealogistics[.]com	NO_ERROR	119.18.49.18	sunsealogistics[.]com	CLEAN

BEHAVIOR

Process Graph

Process #1: doc_0429191990189-3829-03-2018.inv#00399.pdf.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\doc_0429191990189-3829-03-2018.inv#00399.pdf.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 181913, Reason: Analysis Target
Unmonitor End Time	End Time: 251965, Reason: Terminated
Monitor duration	70.05s
Return Code	0
PID	4840
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	118
Keyboard	4
System	255
Registry	3
-	3
Window	2
Process	103
-	2
-	3

Process #2: doc_0429191990189-3829-03-2018.inv#00399.pdf.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\doc_0429191990189-3829-03-2018.inv#00399.pdf.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 250587, Reason: Child Process
Unmonitor End Time	End Time: 422850, Reason: Terminated by timeout
Monitor duration	172.26s
Return Code	Unknown
PID	3632
Parent PID	4840
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	0x330	0x400000(4194304)	0x75000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	0x330	0x1c0000(1835008)	0x1000	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	0x330 / 0xe44	0x778b8fe0(2005635040)	-	✔	1

Host Behavior

Type	Count
Module	243
System	147
File	106
Environment	26
Registry	235
COM	48
-	27
User	4
Mutex	24
-	2
Window	6
-	4

Network Behavior

Type	Count
HTTP	1
DNS	2
TCP	2

Process #3: svchost.exe

ID	3
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: 257681, Reason: RPC Server
Unmonitor End Time	End Time: 422850, Reason: Terminated by timeout
Monitor duration	165.17s
Return Code	Unknown
PID	1012
Parent PID	3632
Bitness	64 Bit

Process #4: wmiprvse.exe

ID	4
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 257681, Reason: RPC Server
Unmonitor End Time	End Time: 422850, Reason: Terminated by timeout
Monitor duration	165.17s
Return Code	Unknown
PID	4448
Parent PID	1012
Bitness	64 Bit

Host Behavior

Type	Count
System	10
Registry	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5fb2529b865460bdc505a962532260c522af1255ea05eca105fd68651c60af74	C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe	Sample File	641.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
e1b5f836e9fd7265fe629edbc15299565513addb2db6ed440319bbb7c3aeac7b	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b3b617419546e734d2e29c6a53356997006de5e205387af9c7df8c58c34d7d7a	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0d6155c8fb6711e0879bf22b13822eae59d2fc45442a0bd6de8005c9fa4f88f9	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3ac636366ebc0432599fc36a2533716356ac6c9c2dfa356d076f684596781d04	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
80acbdeee00fd96517643d55cc952500bec816bbd29e12ae2b698753f027c933	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
28b320860e3b1a4c522f5361a3ef01c39264de06a296e232e3919d90a065cad6	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3dc33a09f3d7ed319c3eafcc9f576c55325b00917849809a9c0d24ae88d6bd2e	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a8a0b136e82cffb404b90d52c49f15bb5202e9c004b4cd0dac28fce9146025ae	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0ce7fdd9b469c81f574d9fd2b2ebce1bcbfdde923555f4e9cb7fb16da235ec1e	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a7583e757fb1f6d8d6eabffbf819949e63ce5c0b2a89bad76e2e1af986942500	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
02ce5b762c934aadbaeb6d636913b942ab7935f7d92fc78f107a5449de5a290e	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
097fc959f8ac2431c0f569779cae599007b1c763f7f3a151898b3d883e60ce27	-	Memory Dump	468.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
531a4c72262cce558253f4bbd2024d47b740de79ade819bdf1cceed0518df5b0	-	Memory Dump	184.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a9802de51b8c3da874841f213e6eaab8cffd7c05e94f381556c70bbada17951e	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
db0dbc1c620ec521cbb57e094d3769299b671269068e02d69281764bfed3046a	-	Downloaded File	105 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Windows\Microsoft.NET\Framework\v2.0.50727\jsc.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe.config	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe.log	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v2.0.50727_32\indexaa.dat	Accessed File	Access	CLEAN
C:\Windows\system32\l_intl.nls	Accessed File	Access	CLEAN
C:\Windows\assembly\pubpol180.dat	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_32\CustomMarshalers\2.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\GAC_MSIL\System.Management\2.0.0.0__b03f5f7f11d50a3a\System.Management.dll	Accessed File	Access	CLEAN
C:\%insfolder%\%insname%	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\logins.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\logins.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\Mozilla Firefox\nss3.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\Postbox\nss3.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\Mozilla Thunderbird\nss3.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\SeaMonkey\nss3.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\Flock\nss3.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\signons3.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\signons.sqlite	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\logins.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\signons.sqlite	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\CoreFTP\sites.idx	Accessed File	Access	CLEAN
C:\ProgramData\DynDNS\Updater\config.dyndns	Accessed File	Access	CLEAN
C:\Users\All Users\AppData\Roaming\FlashFXP\3quick.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.purple\accounts.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Ftplist.txt	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://checkip[.]dyndns[.]org	Extracted, Contacted	132.226.247.73, 158.101.44.242, 132.226.8.169, 193.122.6.168, 193.122.130.0	Germany, Brazil, United States, Japan	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkip[.]dyndns[.]org	132.226.247.73, 158.101.44.242, 132.226.8.169, 193.122.6.168, 193.122.130.0	Germany, Brazil, United States, Japan	HTTP, TCP, DNS	CLEAN
checkip[.]dyndns[.]com	132.226.247.73, 158.101.44.242, 132.226.8.169, 193.122.6.168, 193.122.130.0	Germany, Brazil, United States, Japan	HTTP, TCP, DNS	CLEAN
mail[.]sunsealogistics[.]com	119.18.49.18	India	TCP, DNS	CLEAN
sunsealogistics[.]com	119.18.49.18	India	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
119.18.49.18	sunsealogistics[.]com, mail[.]sunsealogistics[.]com	India	TCP, DNS	CLEAN
132.226.8.169	checkip[.]dyndns[.]com, checkip[.]dyndns[.]org	Japan	HTTP, TCP, DNS	CLEAN
132.226.247.73	checkip[.]dyndns[.]com, checkip[.]dyndns[.]org	Brazil	DNS	CLEAN
193.122.6.168	checkip[.]dyndns[.]com, checkip[.]dyndns[.]org	Germany	DNS	CLEAN
158.101.44.242	checkip[.]dyndns[.]com, checkip[.]dyndns[.]org	United States	DNS	CLEAN
193.122.130.0	checkip[.]dyndns[.]com, checkip[.]dyndns[.]org	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\.net clr networking	access, delete	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
-	access, delete	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\InstallRoot	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\.NET	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\Library	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\IsMultiInstance	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\First Counter	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\CategoryOptions	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\FileMappingSize	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\Counter Names	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\Paltalk	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FTP Commander\UninstallString	access, read	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Vitalwerks\DUC	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	CLEAN

Process

Process Name	Commandline	Verdict
doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	"C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe"	MALICIOUS
doc_0429191990189-3829-03-2018.inv#00399.pdf.exe	"C:\Users\RDhJ0CNFevzX\Desktop\doc_0429191990189-3829-03-2018.INV#00399.PDF.exe"	MALICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (42)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_StringDecryption	Agent Tesla string decryption	Memory Dump	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5
Generic	SandboxProductID	Sandbox detection via leaked Windows product IDs	Memory Dump	-	-	4/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

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	8.0.1710.11

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