MALICIOUS

Classifications: -

Threat Names: FormBook

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**scrss.exe**
ID	#2106078
MD5	5fc986129c3d833b1c7e5ba6ff3678bc
SHA1	2ace6bc0488df9b8592e25be3de38e6c9a0c16da
SHA256	d02d076842cc94fa6612b13ff0d2f77e1ff9150d22607cfe3962da4234cf4ed5
File Size	214.30 KB
Report Created	2022-05-05 12:55 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 335 matches)

Score	Category	Operation	Count	Classification
5/5	Browser	Adds a hook to a web browser	100	Spyware

- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x5.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x6.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0xb.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x1.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x1.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0xc.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x6.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x1.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x9.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x4.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x9.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x2.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0xa.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0xb.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0xb.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x9.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x5.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x5.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x0.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0xd.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x2.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x9.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0xb.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0xb.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0xd.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x1.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x8.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x1.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x4.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x9.
- (Process #5) raserver.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0xa.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0xd.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x8.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0xd.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x5.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x0.
- (Process #5) raserver.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x5.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1e3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x109.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1a3.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x151.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x3a.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x179.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1a7.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0xcf.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x159.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1cf.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x143.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0xaf.
- (Process #5) raserver.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x171.

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	22	Spyware

- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #3) rysgtozci.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #27) absolutetelnet.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #34) flashfxp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #32) far.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #12) whatsapp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #15) thunderbird.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #17) skype.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #18) scriptftp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #28) alftp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #16) smartftp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #13) webdrive.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #5) raserver.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #33) filezilla.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #9) yahoomessenger.exe.
- Rule "FormBook" from ruleset "Malware" has matched on the function strings for (process #4) explorer.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #19) pidgin.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #22) notepad.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #14) trillian.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #20) outlook.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #21) operamail.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #31) coreftp.exe.
- Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #25) gmailnotifierpro.exe.

Score	Category	Operation	Count	Classification
4/5	Injection	Writes into the memory of another process	32	Injector

Score	Category	Operation	Count	Classification
		• (Process #3) rysgtozci.exe modifies memory of (process #4) explorer.exe. • (Process #5) raserver.exe modifies memory of (process #4) explorer.exe. • (Process #3) rysgtozci.exe modifies memory of (process #5) raserver.exe. • (Process #5) raserver.exe modifies memory of (process #8) iexplore.exe. • (Process #5) raserver.exe modifies memory of (process #9) yahoomessenger.exe. • (Process #5) raserver.exe modifies memory of (process #11) winscp.exe. • (Process #5) raserver.exe modifies memory of (process #12) whatsapp.exe. • (Process #5) raserver.exe modifies memory of (process #13) webdrive.exe. • (Process #5) raserver.exe modifies memory of (process #14) trillian.exe. • (Process #5) raserver.exe modifies memory of (process #15) thunderbird.exe. • (Process #5) raserver.exe modifies memory of (process #16) smartftp.exe. • (Process #5) raserver.exe modifies memory of (process #17) skype.exe. • (Process #5) raserver.exe modifies memory of (process #18) scriptftp.exe. • (Process #5) raserver.exe modifies memory of (process #19) pidgin.exe. • (Process #5) raserver.exe modifies memory of (process #20) outlook.exe. • (Process #5) raserver.exe modifies memory of (process #21) operamail.exe. • (Process #5) raserver.exe modifies memory of (process #22) notepad.exe. • (Process #5) raserver.exe modifies memory of (process #23) ncftp.exe. • (Process #5) raserver.exe modifies memory of (process #24) leechftp.exe. • (Process #5) raserver.exe modifies memory of (process #25) gmailnotifierpro.exe. • (Process #5) raserver.exe modifies memory of (process #26) 3dftp.exe. • (Process #5) raserver.exe modifies memory of (process #27) absolutetelnet.exe. • (Process #5) raserver.exe modifies memory of (process #28) alftp.exe. • (Process #5) raserver.exe modifies memory of (process #29) barca.exe. • (Process #5) raserver.exe modifies memory of (process #30) bitkinex.exe. • (Process #5) raserver.exe modifies memory of (process #31) coreftp.exe. • (Process #5) raserver.exe modifies memory of (process #32) far.exe. • (Process #5) raserver.exe modifies memory of (process #33) filezilla.exe. • (Process #5) raserver.exe modifies memory of (process #34) flashfxp.exe. • (Process #5) raserver.exe modifies memory of (process #35) fling.exe. • (Process #5) raserver.exe modifies memory of (process #36) icq.exe. • (Process #5) raserver.exe modifies memory of (process #37) iexplore.exe.		
4/5	Injection	Modifies control flow of another process	31	-

Score	Category	Operation	Count	Classification
		• (Process #3) rysgtozci.exe alters context of (process #4) explorer.exe. • (Process #5) raserver.exe alters context of (process #4) explorer.exe. • (Process #5) raserver.exe alters context of (process #8) iexplore.exe. • (Process #5) raserver.exe alters context of (process #9) yahoomessenger.exe. • (Process #5) raserver.exe alters context of (process #11) winscp.exe. • (Process #5) raserver.exe alters context of (process #12) whatsapp.exe. • (Process #5) raserver.exe alters context of (process #13) webdrive.exe. • (Process #5) raserver.exe alters context of (process #14) trillian.exe. • (Process #5) raserver.exe alters context of (process #15) thunderbird.exe. • (Process #5) raserver.exe alters context of (process #16) smartftp.exe. • (Process #5) raserver.exe alters context of (process #17) skype.exe. • (Process #5) raserver.exe alters context of (process #18) scriptftp.exe. • (Process #5) raserver.exe alters context of (process #19) pidgin.exe. • (Process #5) raserver.exe alters context of (process #20) outlook.exe. • (Process #5) raserver.exe alters context of (process #21) operamail.exe. • (Process #5) raserver.exe alters context of (process #22) notepad.exe. • (Process #5) raserver.exe alters context of (process #23) ncftp.exe. • (Process #5) raserver.exe alters context of (process #24) leechftp.exe. • (Process #5) raserver.exe alters context of (process #25) gmailnotifierpro.exe. • (Process #5) raserver.exe alters context of (process #26) 3dftp.exe. • (Process #5) raserver.exe alters context of (process #27) absolutetelnet.exe. • (Process #5) raserver.exe alters context of (process #28) alftp.exe. • (Process #5) raserver.exe alters context of (process #29) barca.exe. • (Process #5) raserver.exe alters context of (process #30) bitkinex.exe. • (Process #5) raserver.exe alters context of (process #31) coreftp.exe. • (Process #5) raserver.exe alters context of (process #32) far.exe. • (Process #5) raserver.exe alters context of (process #33) filezilla.exe. • (Process #5) raserver.exe alters context of (process #34) flashfxp.exe. • (Process #5) raserver.exe alters context of (process #35) fling.exe. • (Process #5) raserver.exe alters context of (process #36) icq.exe. • (Process #5) raserver.exe alters context of (process #37) iexplore.exe.		
3/5	Data Collection	Reads memory of user process	27	-

Score	Category	Operation	Count	Classification
		• (Process #5) raserver.exe reads memory of process (process #9) yahoomessenger.exe. • (Process #5) raserver.exe reads memory of process (process #11) winscp.exe. • (Process #5) raserver.exe reads memory of process (process #12) whatsapp.exe. • (Process #5) raserver.exe reads memory of process (process #13) webdrive.exe. • (Process #5) raserver.exe reads memory of process (process #14) trillian.exe. • (Process #5) raserver.exe reads memory of process (process #15) thunderbird.exe. • (Process #5) raserver.exe reads memory of process (process #16) smartftp.exe. • (Process #5) raserver.exe reads memory of process (process #17) skype.exe. • (Process #5) raserver.exe reads memory of process (process #18) scriptftp.exe. • (Process #5) raserver.exe reads memory of process (process #19) pidgin.exe. • (Process #5) raserver.exe reads memory of process (process #20) outlook.exe. • (Process #5) raserver.exe reads memory of process (process #21) operamail.exe. • (Process #5) raserver.exe reads memory of process (process #22) notepad.exe. • (Process #5) raserver.exe reads memory of process (process #23) ncftp.exe. • (Process #5) raserver.exe reads memory of process (process #24) leechftp.exe. • (Process #5) raserver.exe reads memory of process (process #25) gmailnotifierpro.exe. • (Process #5) raserver.exe reads memory of process (process #26) 3dftp.exe. • (Process #5) raserver.exe reads memory of process (process #27) absolutetelnet.exe. • (Process #5) raserver.exe reads memory of process (process #28) alftp.exe. • (Process #5) raserver.exe reads memory of process (process #29) barca.exe. • (Process #5) raserver.exe reads memory of process (process #30) bitkinex.exe. • (Process #5) raserver.exe reads memory of process (process #31) coreftp.exe. • (Process #5) raserver.exe reads memory of process (process #32) far.exe. • (Process #5) raserver.exe reads memory of process (process #33) filezilla.exe. • (Process #5) raserver.exe reads memory of process (process #34) flashfxp.exe. • (Process #5) raserver.exe reads memory of process (process #35) fling.exe. • (Process #5) raserver.exe reads memory of process (process #36) icq.exe.		
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
		• (Process #3) rysgtozci.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".		
2/5	Anti Analysis	Tries to detect debugger	1	-
		• (Process #3) rysgtozci.exe tries to detect a debugger via API "NtQueryInformationProcess".		
2/5	Hide Tracks	Deletes file after execution	1	-
		• (Process #6) cmd.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe".		
2/5	Anti Analysis	Delays execution	2	-
		• (Process #5) raserver.exe has a thread which sleeps more than 5 minutes. • (Process #4) explorer.exe has a thread which sleeps more than 5 minutes.		
2/5	Data Collection	Reads sensitive browser data	3	-
		• (Process #5) raserver.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #5) raserver.exe tries to read sensitive data of web browser "Opera" by file. • (Process #5) raserver.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	23	-

Score	Category	Operation	Count	Classification
		• (Process #3) rysgtozci.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtOpenProcessToken".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtResumeThread".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtOpenThread".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtQueryInformationToken".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtFreeVirtualMemory".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtAdjustPrivilegesToken".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtReadVirtualMemory".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtDelayExecution".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtOpenProcess".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtProtectVirtualMemory".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtMapViewOfSection".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtCreateFile".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtQueryInformationFile".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtQuerySystemInformation".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtQueryInformationProcess".		
		• (Process #2) rysgtozci.exe makes a direct system call to "NtResumeThread".		
		• (Process #2) rysgtozci.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtAllocateVirtualMemory".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtClose".		
		• (Process #2) rysgtozci.exe makes a direct system call to "NtWriteVirtualMemory".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtReadFile".		
		• (Process #3) rysgtozci.exe makes a direct system call to "NtCreateSection".		
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
		• (Process #2) rysgtozci.exe modifies memory of (process #3) rysgtozci.exe.		
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
		• (Process #2) rysgtozci.exe alters context of (process #3) rysgtozci.exe.		
1/5	Hide Tracks	Creates process with hidden window	4	-
		• (Process #1) scrss.exe starts (process #1) scrss.exe with a hidden window.		
		• (Process #2) rysgtozci.exe starts (process #2) rysgtozci.exe with a hidden window.		
		• (Process #4) explorer.exe starts (process #4) explorer.exe with a hidden window.		
		• (Process #5) raserver.exe starts (process #5) raserver.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	31	-

Score	Category	Operation	Count	Classification
		• (Process #2) rysgtozci.exe reads from (process #2) rysgtozci.exe. • (Process #3) rysgtozci.exe reads from (process #4) explorer.exe. • (Process #3) rysgtozci.exe reads from (process #5) raserver.exe. • (Process #5) raserver.exe reads from (process #9) yahoomessenger.exe. • (Process #5) raserver.exe reads from (process #11) winscp.exe. • (Process #5) raserver.exe reads from (process #12) whatsapp.exe. • (Process #5) raserver.exe reads from (process #13) webdrive.exe. • (Process #5) raserver.exe reads from (process #14) trillian.exe. • (Process #5) raserver.exe reads from (process #15) thunderbird.exe. • (Process #5) raserver.exe reads from (process #16) smartftp.exe. • (Process #5) raserver.exe reads from (process #17) skype.exe. • (Process #5) raserver.exe reads from (process #18) scriptftp.exe. • (Process #5) raserver.exe reads from (process #19) pidgin.exe. • (Process #5) raserver.exe reads from (process #20) outlook.exe. • (Process #5) raserver.exe reads from (process #21) operamail.exe. • (Process #5) raserver.exe reads from (process #22) notepad.exe. • (Process #5) raserver.exe reads from (process #23) ncftp.exe. • (Process #5) raserver.exe reads from (process #24) leechftp.exe. • (Process #5) raserver.exe reads from (process #25) gmailnotifierpro.exe. • (Process #5) raserver.exe reads from (process #26) 3dftp.exe. • (Process #5) raserver.exe reads from (process #27) absolutetelnet.exe. • (Process #5) raserver.exe reads from (process #28) alftp.exe. • (Process #5) raserver.exe reads from (process #29) barca.exe. • (Process #5) raserver.exe reads from (process #30) bitkinex.exe. • (Process #5) raserver.exe reads from (process #31) coreftp.exe. • (Process #5) raserver.exe reads from (process #32) far.exe. • (Process #5) raserver.exe reads from (process #33) filezilla.exe. • (Process #5) raserver.exe reads from (process #34) flashfxp.exe. • (Process #5) raserver.exe reads from (process #35) fling.exe. • (Process #5) raserver.exe reads from (process #36) icq.exe. • (Process #5) raserver.exe reads from (process #37) iexplore.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #2) rysgtozci.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	System Modification	Modifies operating system directory	3	-
		• (Process #3) rysgtozci.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory. • (Process #5) raserver.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory. • (Process #37) iexplore.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory.		
1/5	Mutex	Creates mutex	4	-
		• (Process #5) raserver.exe creates mutex with name "6NON26-3X60UXYXz". • (Process #5) raserver.exe creates mutex with name "-2NP6R7E2SEYA12z". • (Process #4) explorer.exe creates mutex with name "S-1-5-21-1560258-18641394712783". • (Process #8) iexplore.exe creates mutex with name "S-1-5-21-1560258-20201777346147".		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #5) raserver.exe adds "C:\Program Files (x86)\Wrvtps4_h\Cookiesclrpdxk8.exe" to Windows startup via registry.		
1/5	Discovery	Possibly does reconnaissance	2	-

Score	Category	Operation	Count	Classification
		• (Process #5) raserver.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #5) raserver.exe tries to gather information about application "Mozilla Firefox" by file.		
1/5	Network Connection	Performs DNS request	25	-
		• (Process #4) explorer.exe resolves host name "www.scovikinnovations.com" to IP "192.185.0.218". • (Process #4) explorer.exe resolves host name "www.trybes.space" to IP "-". • (Process #4) explorer.exe resolves host name "www.ilina.xyz" to IP "104.21.4.240". • (Process #4) explorer.exe resolves host name "www.konstelle.store" to IP "-". • (Process #4) explorer.exe resolves host name "www.czoqg.xyz" to IP "156.251.18.25". • (Process #4) explorer.exe resolves host name "www.thesiscoper.com" to IP "18.217.107.127". • (Process #4) explorer.exe resolves host name "www.eddrugs2018.com" to IP "204.11.56.48". • (Process #4) explorer.exe resolves host name "www.7477e.xyz" to IP "104.21.21.144". • (Process #4) explorer.exe resolves host name "www.ywfjp.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.vanessaruizwriting.com" to IP "198.54.117.218". • (Process #4) explorer.exe resolves host name "www.largestjerseysstore.com" to IP "156.245.192.153". • (Process #4) explorer.exe resolves host name "www.shishlomarket24.biz" to IP "-". • (Process #4) explorer.exe resolves host name "www.payer-breakers.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.ztzfirst.xyz" to IP "-". • (Process #4) explorer.exe resolves host name "www.monumentalmarketsllc.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.salarydetector.net" to IP "199.188.206.67". • (Process #4) explorer.exe resolves host name "www.the6figureshow.com" to IP "34.102.136.180". • (Process #4) explorer.exe resolves host name "www.lovejaclyn.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.5145.design" to IP "-". • (Process #4) explorer.exe resolves host name "www.5p6xljjse1lq.xyz" to IP "18.221.0.52". • (Process #4) explorer.exe resolves host name "www.fortitude-tech.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.10936.loan" to IP "185.216.248.42". • (Process #4) explorer.exe resolves host name "www.sdjnsbd.com" to IP "104.253.187.34". • (Process #4) explorer.exe resolves host name "www.sunwall.xyz" to IP "162.0.231.155". • (Process #4) explorer.exe resolves host name "www.dandelionfusedigital.com" to IP "198.54.117.212".		
1/5	Network Connection	Connects to remote host	15	-
		• (Process #4) explorer.exe opens an outgoing TCP connection to host "156.245.192.153:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "18.221.0.52:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "192.185.0.218:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "104.21.4.240:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "185.216.248.42:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "104.21.21.144:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "198.54.117.212:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "162.0.231.155:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "34.102.136.180:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "198.54.117.218:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "18.217.107.127:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "204.11.56.48:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "209.99.64.43:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "199.188.206.67:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "104.253.187.34:80".		
1/5	Obfuscation	Overwrites code	3	-

Score	Category	Operation	Count	Classification
	• (Process #8) iexplore.exe overwrites code to possibly hide behavior. • (Process #37) iexplore.exe overwrites code to possibly hide behavior. • (Process #4) explorer.exe overwrites code to possibly hide behavior.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe".			

Mitre ATT&CK Matrix

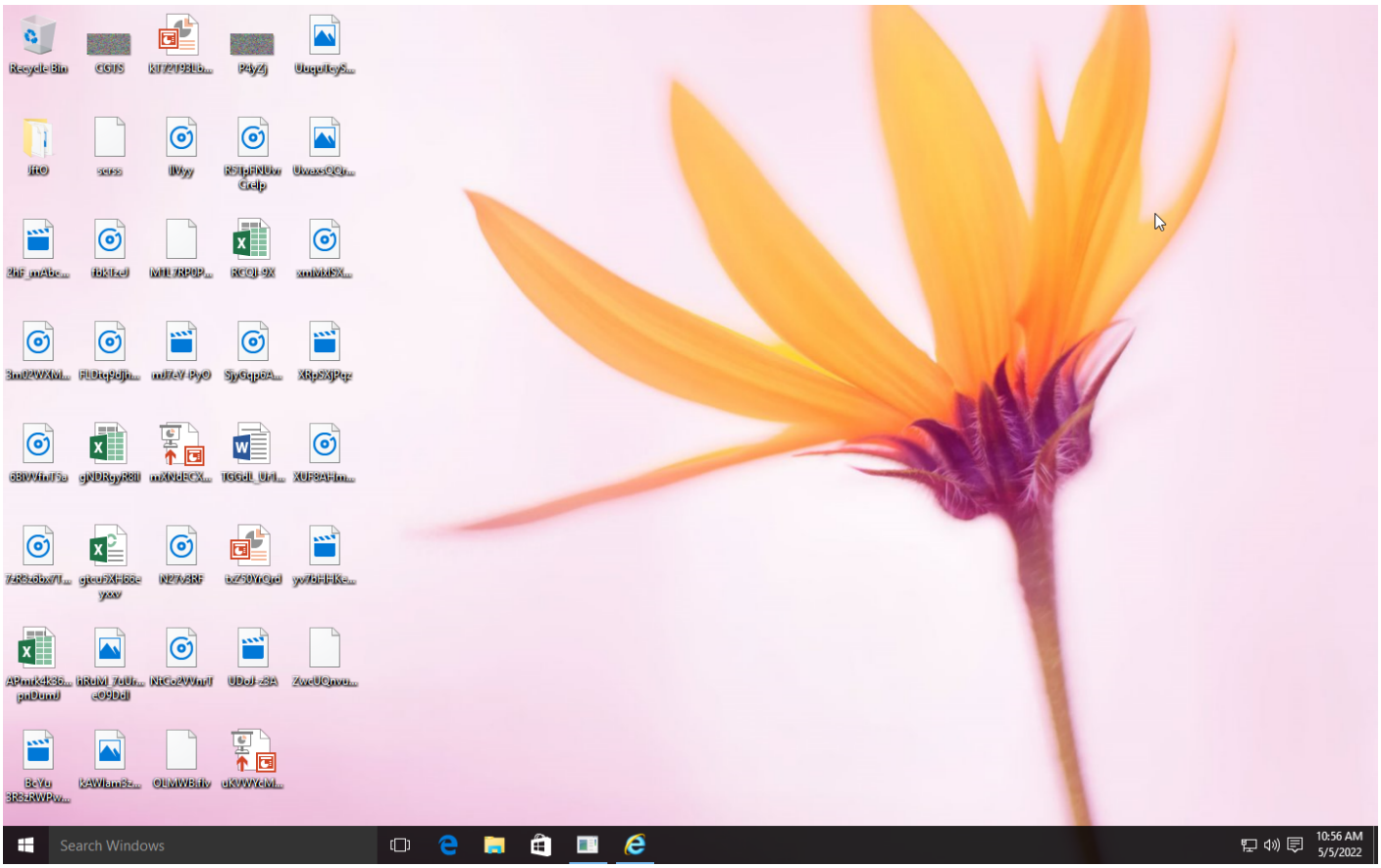
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder	#T1179 Hooking	#T1143 Hidden Window	#T1081 Credentials in Files	#T1012 Query Registry		#T1119 Automated Collection			
		#T1179 Hooking		#T1045 Software Packing	#T1003 Credential Dumping	#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1112 Modify Registry	#T1179 Hooking			#T1185 Man in the Browser			

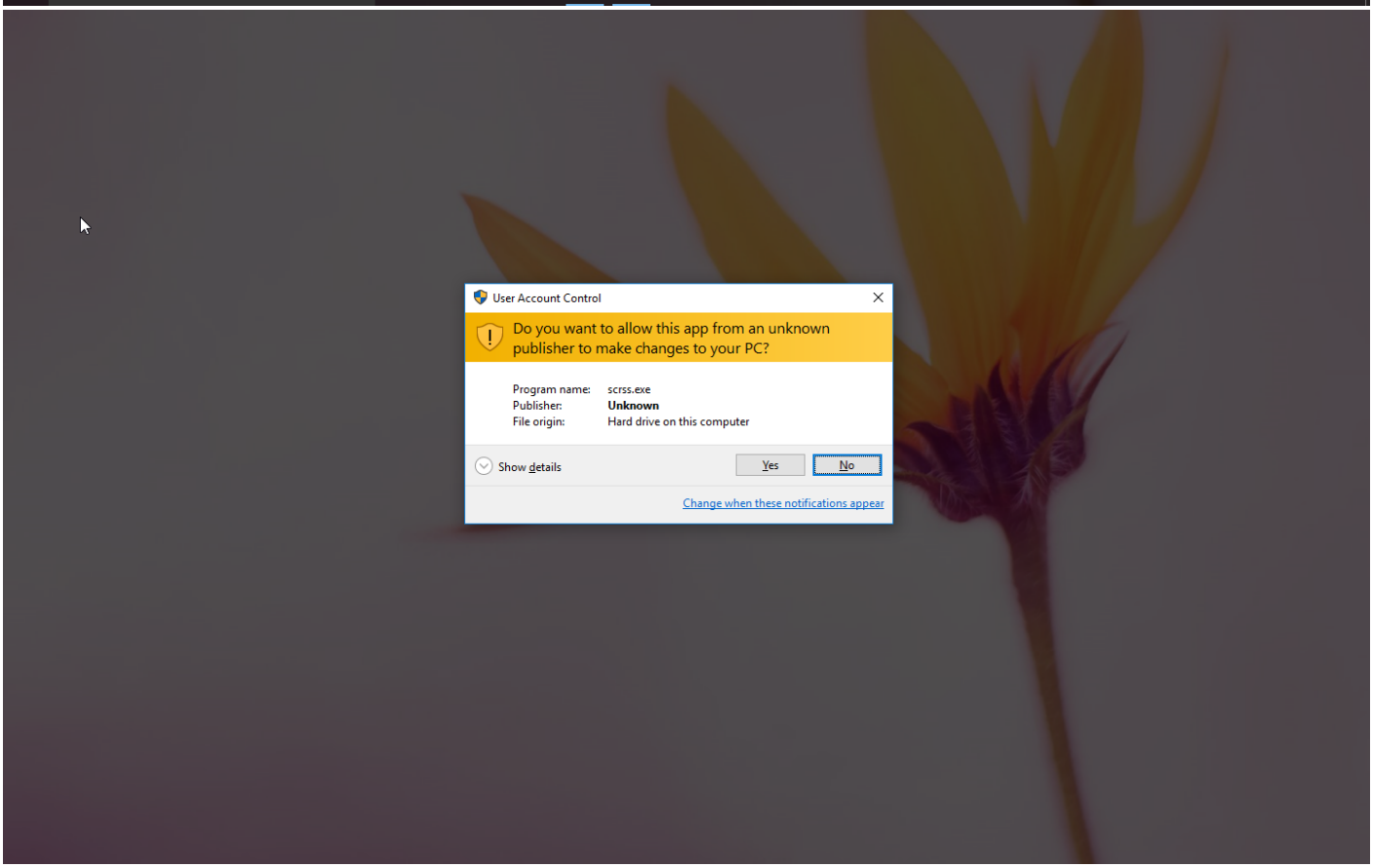
Sample Information

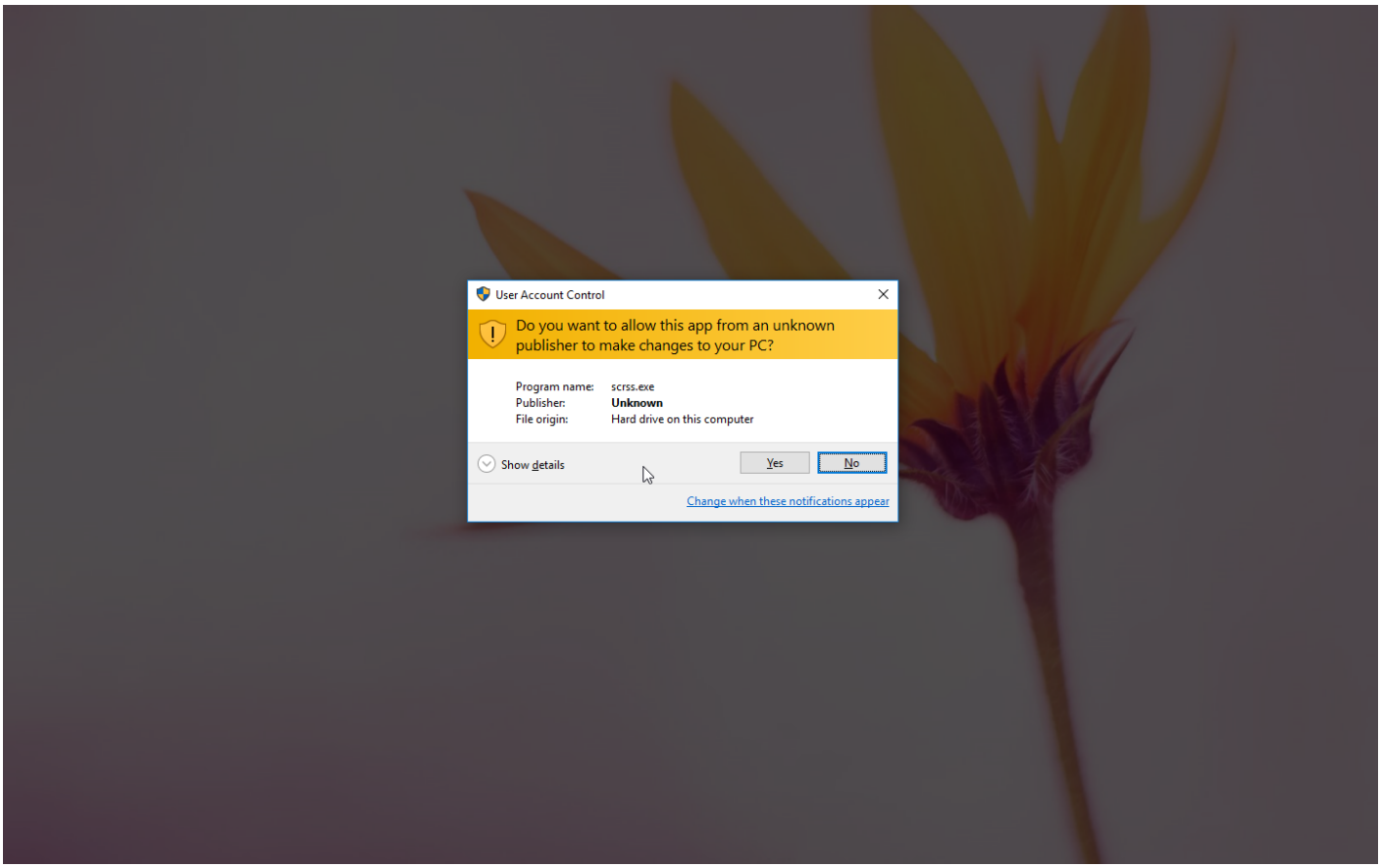
ID	#2106078
MD5	5fc986129c3d833b1c7e5ba6ff3678bc
SHA1	2ace6bc0488df9b8592e25be3de38e6c9a0c16da
SHA256	d02d076842cc94fa6612b13ff0d2f77e1ff9150d22607cfe3962da4234cf4ed5
SSDeep	3072:l1NjcVVnLpPunbD0r9X/MP5LsCIVa1aP+KQ4kFHP67DzJEhShrM/joS9zAQNgOau:HNeZmQrV/MP8XXklIiheMLPztvau
ImpHash	56a78d55f3f7af51443e58e0ce2fb5f6
File Name	scrss.exe
File Size	214.30 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-05-05 12:55 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	35
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	27


Search Windows
10:56 AM
5/5/2022


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


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

NETWORK

General

403.20 KB total sent

79.16 KB total received

3 ports 80, 53, 445

17 contacted IP addresses

32 URLs extracted

9 files downloaded

0 malicious hosts detected

DNS

38 DNS requests for 25 domains

1 nameservers contacted

20 total requests returned errors

HTTP/S

21 URLs contacted, 14 servers

6 sessions, 399.21 KB sent, 56.65 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.lovejaclyn.com/Migraine_Pain_Relief.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBK... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=19222924&ktd=0&kld=1042&kp=2	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/song_lyrics.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5MxolrF... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=26527269&ktd=0&kld=1042&kp=6	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/px.js?ch=1	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/fashion_trends.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5Mxo... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=10542279&ktd=0&kld=1042&kp=4	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/Anti_Wrinkle_Creams.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKM... ... 8je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=1919926&ktd=0&kld=1042&kp=3	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/High_Speed_Internet.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKM... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=13681481&ktd=0&kld=1042&kp=7	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/px.js?ch=2	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.lovejaclyn.com/sk-logabpstatus.php?a=VThpazQvNW1zREdRSElabWtZbDQ4YitEd2NnRlNJZENRVXhYVktOSUo0QjZmVk5ZT0dVWjM0ZDJFdzhWWFBUeGI5R0V6QXZ6NnRETVpoK09FZFl6dVhBM05YYmtEa3B4cC9VSFFRdEpXTDF2WEZjSW5hMmszSGE3TXMvQU5jVU0=&b=	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/Cheap_Air_Tickets.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5...8je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=5645746&ktd=0&kld=1042&kp=1	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com/Free_Credit_Report.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=11539660&ktd=0&kld=1042&kp=5	-	-		0 bytes	NA
GET	http://www.lovejaclyn.com	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/Anti_Wrinkle_Creams.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRb...VJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=1919926&ktd=0&kld=1061&kp=1	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/sk-privacy.php	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/find_a_tutor.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQkjIjM...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=10844596&ktd=0&kld=1061&kp=7	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/display.cfm	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/song_lyrics.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQkjIjMk...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=26527269&ktd=0&kld=1061&kp=4	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/px.js?ch=1	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/px.js?ch=2	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/10_Best_Mutual_Funds.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJR... ...9yVJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=72996&ktd=0&kld=1061&kp=5	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/Best_Penny_Stocks.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQ...VJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=3482138&ktd=0&kld=1061&kp=6	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/High_Speed_Internet.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRb...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=13681481&ktd=0&kld=1061&kp=3	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/Migraine_Pain_Relief.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJR...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=19222924&ktd=0&kld=1061&kp=2	-	-		0 bytes	NA
GET	http://www.eddrugs2018.com/sk-logabpstatus.php?a=ejBabExITVl2RFJwT3ZSV3VGME85QXFRdlo3RjJ1dWJOTzY2QWNTQVhFbE1KTVpOTmF1MzVNUTJvbUZWSWoyUUx5MVRFZ3N0U0Nwc1IxakNQREhXb1p3Si9KYVVxOG9rQXdsN3lOQUZLenBhVWw0VDNzdFAzTE5ha01lMEFyelc=&b=	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://i3.cdn-image.com/__media__/js/min.js?v2.3	-	-		0 bytes	NA
GET	http://eddrugs2018.com	-	-		0 bytes	NA
GET	http://i4.cdn-image.com/__media__/js/min.js?v2.3	-	-		0 bytes	NA
GET	http://www.buydomains.com/lander/lovejaclyn.com/?domain=lovejaclyn.com&utm_source=lovejaclyn.com&utm_campaign=skenzo&traffic_id=skenzo17&traffic_type=park	-	-		0 bytes	NA
GET	http://www.largestjerseysstore.com/fw02/?ZZI=cHF1IlzheLmJHtN59WqmKu+q3iQdAOeskIPX6LsiZG+TwEYG2vkDGRbq2lgFmRvqBs9Eeg==&elzp=TTtX	-	-		0 bytes	NA
POST	http://www.7477e.xyz/fw02/	-	-		0 bytes	NA
GET	http://www.5p6xljjse1lq.xyz/fw02/?ZZI=iY7cHZOQigy8MmRzVBkzkxJ3JOugJYILBJlwsLX+b4fBhnZGDg3yinWJ8YhLtVVSl4UJCg==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.7477e.xyz/fw02/?ZZI=hZ0UeJp6fd+b97vTasQPXH6DoCVbE/Ua0aTbzhCwqvI4iQqpMVEe8veqno3garzpF7oF0A==&oDKX=PpF0-nRHybghQp	-	-		0 bytes	NA
GET	http://www.5p6xljjse1lq.xyz/fw02/?ZZI=iY7cHZOQigy8MmRzVBkzkxJ3JOugJYILBJlwsLX+b4fBhnZGDg3yinWJ8YhLtVVSl4UJCg==&oDKX=PpF0-nRHybghQp	-	-		0 bytes	NA
POST	http://www.scovikinnovations.com/fw02/	-	-		0 bytes	NA
GET	http://www.sdjnsbd.com/fw02/?ZZI=T2HQ/5Fnw2DoAbeb93/ApdJLKQyT2yAAijSiJ6BVUO4INv+F6+csACgpZilkr+EortA9BA==&zL00dV=f6Ap5PR8IR1PV	-	-		0 bytes	NA
GET	http://www.dandelionfusedigital.com/fw02/?ZZI=FBCZxRbtofiFbuFLP5VkagDY6z5F/jU6/InmQ1C2NVKK2BsIYb7M4Im7BZBf8SVBw1WDaA==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.scovikinnovations.com/fw02/?ZZI=JW6gKnBiflfQEVztNe4Tulw1VPOJ0N5LGG9bGwyVqVadxlZXAql2YwS5UkZ1rgzw98lOgw==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.the6figureshow.com/fw02/?ZZI=eTPPPG3yBw1rXnY600nziyQrGW/kopa9XgvCJchWVR6iylbQ2Ul/sZzfUA7gGoYjKhr4+w==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.largestjerseysstore.com/fw02/?ZZI=cHF1IlzheLmJHtN59WqmKu+q3iQdAOeskIPX6LsiZG+TwEYG2vkDGRbq2lgFmRvqBs9Eeg==&oDKX=PpF0-nRHybghQp	-	-		0 bytes	NA
POST	http://www.10936.loan/fw02/	-	-		0 bytes	NA
GET	http://www.vanessaruizwriting.com/fw02/?ZZI=Ui69IaVOu1v+JLK6S5Z9JE+MP08KQpiMVt7NuF6zMG38sFvg/ehfBJlXm70TR9EtTU52bw==&elzp=TTtX	-	-		0 bytes	NA
POST	http://www.5p6xljjse1lq.xyz/fw02/	-	-		0 bytes	NA
GET	http://www.10936.loan/fw02/?ZZI=ReenpJFtiyJzDfNKFYd3YADTMMSTSUBT/El1isJ661zeWMRAYbbvuhCyy1dUowbNoPpsmw==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.ilina.xyz/fw02/?ZZI=GovV0e+2vH+6sn2WJzgIYLi9K7HJG6Hb4lAdaf5BxulWl4LHuFZ3rR7+Ae1g08nlOeWsog==&zL00dV=f6Ap5PR8IR1PV	-	-		0 bytes	NA
GET	http://www.sunwall.xyz/fw02/?ZZI=6TtO6HPce6q0Xc5JtNk8NP9HYMp6msWauevBhsRweFGL2ktJvIlk5YskpBJ7vyPDYZYfYA==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.thesiscoper.com/fw02/?ZZI=3/oBgBxwsNYyzLslzJuiywbdD1KR9wTmmpLldxkspL7D4spRMDqlE5pSL1fAhBq6YawIDg==&elzp=TTtX	-	-		0 bytes	NA
GET	http://www.10936.loan/fw02/?oDKX=PpF0-nRHybghQp&ZZI=ReenpJFtiyJzDfNKFYd3YADTMMSTSUBT/El1isJ661zeWMRAYbbvuhCyy1dUowbNoPpsmw==	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.eddrugs2018.com/fw02/?ZZI=/z6NEJ69yVJGPM1rdj5Kzq9DL/DuTIFSSAZTeAXQy8DQ5yXNPg60IHwa4EyOlGQYhiNOpw==&zL00dV=f6Ap5PR8IR1PV	-	-		0 bytes	NA
GET	http://www.salarydetector.net/fw02/?ZZI=73srvekCQLgA6VzhY0rwafKgb18eM8pr6xDuhcp4lWcnGdB1ZAXXMmsczaGk2cI0IN80/Q==&zL00dV=f6Ap5PR8IR1PV	-	-		0 bytes	NA
GET	https://www.networksolutions.com/cgi-bin/promo/domain-search?domainNames=eddrugs2018.com&search=premiumlanding&channelid=P13C100S300N0B3A1D0E0000V100	-	-		0 bytes	NA
GET	https://wildcard.hostgator.com/fw02/	-	-		0 bytes	NA
GET	https://wildcard.hostgator.com/fw02/?ZZI=JW6gKnBiflfQEVztNe4Tulw1VPOJ0N5LGG9bGwyVqVadxlZXAql2YwS5UkZ1rgzw98lOgw==&elzp=TTtX	-	-		0 bytes	NA

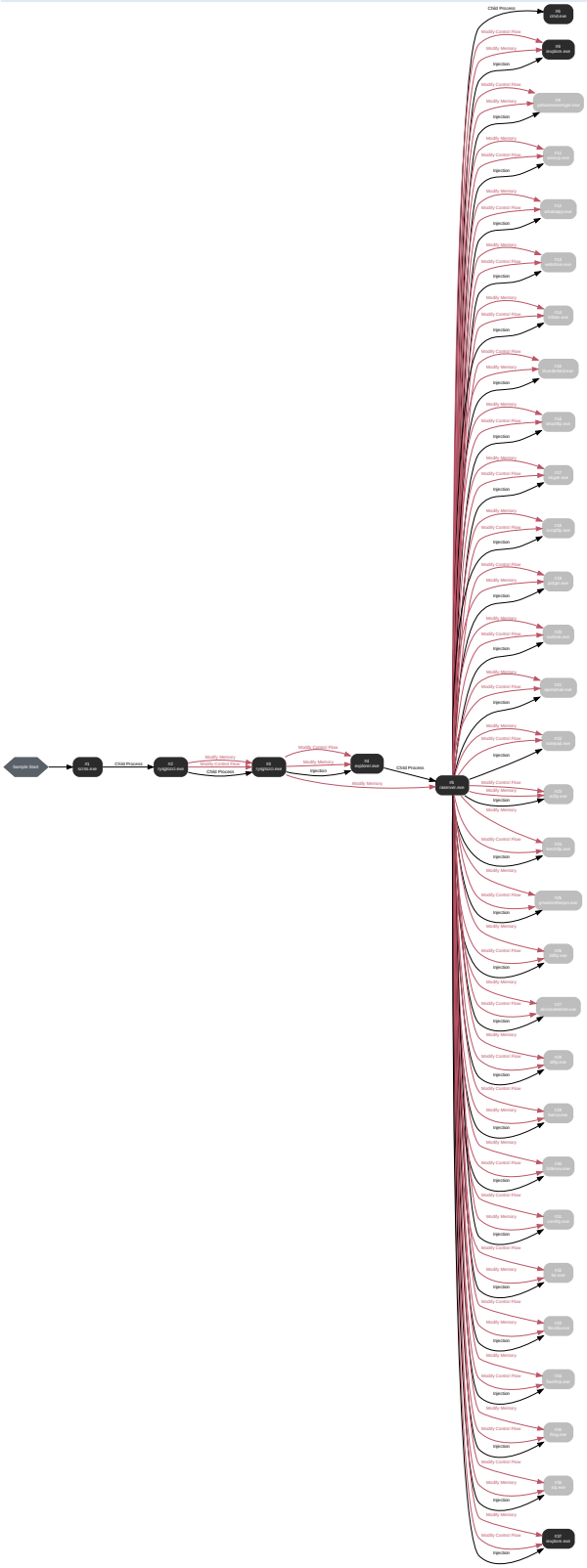
DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.scovikinnovations.com	NO_ERROR	192.185.0.218		NA
A	www.trybes.space	SERV_FAIL			NA
A	www.ywfjp.com	-			NA
A	www.ilina.xyz	NO_ERROR	104.21.4.240, 172.67.187.58		NA
A	www.konstelle.store	NX_DOMAIN			NA
A	www.czoqg.xyz	NO_ERROR	156.251.18.25		NA
A	www.thesiscoper.com	NO_ERROR	18.217.107.127		NA
A	www.eddrugs2018.com	NO_ERROR	204.11.56.48		NA
A	www.7477e.xyz	NO_ERROR	104.21.21.144, 172.67.199.31		NA
A	www.vanessaruizwriting.com, parkingpage.namecheap.com	NO_ERROR	198.54.117.218, 198.54.117.210, 198.54.117.212, 198.54.117.211, 198.54.117.216, 198.54.117.215, 198.54.117.217	parkingpage.namecheap.com	NA
A	www.largestjerseysstore.com	NO_ERROR	156.245.192.153		NA
A	www.shishlomarket24.biz	NX_DOMAIN			NA
A	www.payer-breakers.com	SERV_FAIL			NA
A	www.ztzfirst.xyz	NX_DOMAIN			NA
A	www.monumentalmarketsllc.com	NX_DOMAIN			NA
A	www.salarydetector.net, salarydetector.net	NO_ERROR	199.188.206.67	salarydetector.net	NA
A	www.the6figureshow.com, the6figureshow.com	NO_ERROR	34.102.136.180	the6figureshow.com	NA
A	www.lovejaclyn.com	NO_ERROR			NA
A	www.5145.design	NX_DOMAIN			NA
A	www.5p6xljjse1lq.xyz	NO_ERROR	18.221.0.52		NA
A	www.fortitude-tech.com	NX_DOMAIN			NA
A	www.10936.loan	NO_ERROR	185.216.248.42		NA
A	www.sdjnsbd.com	NO_ERROR	104.253.187.34		NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.sunwall.xyz	NO_ERROR	162.0.231.155		NA
A	www.dandelionfusedigital.com, parkingpage.namecheap.com	NO_ERROR	198.54.117.212, 198.54.117.211, 198.54.117.216, 198.54.117.215, 198.54.117.217, 198.54.117.218, 198.54.117.210	parkingpage.namecheap.com	NA

BEHAVIOR

Process Graph



Process #1: scrss.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\scrss.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\scrss.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64947, Reason: Analysis Target
Unmonitor End Time	End Time: 100691, Reason: Terminated
Monitor duration	35.74s
Return Code	0
PID	3984
Parent PID	1864
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg	5.25 KB	26a0ef0fe1fdab9e6dae3caecec085c3800a44d32cd5b87c182c0c0a6b559f59	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\ptcgl43g463vgbr58	185.00 KB	d0da793571aa99c98e2afca3be0f3d6850aabbacf2aca4eeab8013e4ebf77a67	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr155E.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsjFBF.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	50
File	158
Module	26
Process	1

Process #2: rysgtozci.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 94593, Reason: Child Process
Unmonitor End Time	End Time: 100958, Reason: Terminated
Monitor duration	6.37s
Return Code	0
PID	928
Parent PID	3984
Bitness	32 Bit

Host Behavior

Type	Count
Module	6
File	20
-	3
-	5
Process	1

Process #3: rysgtozci.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 98909, Reason: Child Process
Unmonitor End Time	End Time: 110943, Reason: Terminated
Monitor duration	12.03s
Return Code	0
PID	2164
Parent PID	928
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0x368	0x400000(4194304)	0x200	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0x368	0x401000(4198400)	0x2d200	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0x368	0x3b5008(3887112)	0x4	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0x368 / 0xc88	0x774d8fe0(2001571808)	-	✔	1

Host Behavior

Type	Count
System	5
-	1
-	8
Process	6
File	10
Module	14
User	1
-	3
Environment	1
-	1

Process #4: explorer.exe

ID	4
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101546, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	203.45s
Return Code	Unknown
PID	1864
Parent PID	-
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0xc88	0x7c60000(130416640)	0xfe000	✔	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0xc88 / 0x74c	0x7cbcdd9(130797017)	-	✔	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0xc88 / 0x74c	0xcedd0(847312)	-	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x100f0000(269418496)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x9ff0000(167706624)	0x173000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x74c	0xcf6b8(849592)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x74c	0xa0dddc2(168680898)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogri.ini	40 bytes	eaece2eba6310253249603033c744dd5914089b0bb26bde6685ec9813611baae	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrc.ini	1.75 KB	3f20b4605a2a543557ff9f208c286aef88fd05200f0c6150d35f1402507bd228	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrv.ini	40 bytes	6eebf968962745b2e9de2ca969af7c424916d4e3fe3cc0bb9b3d414abfce9507	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogim.jpeg	90.38 KB	e1625aa27dd1d5d658b2a743de62f8cabcf34bfb8e09c6dad9f40f9b52211b61	✖

Host Behavior

Type	Count
System	8494
Module	3
File	529

Type	Count
-	39
Process	1
Mutex	1

Network Behavior

Type	Count
HTTP	34
DNS	30
TCP	39

Process #5: raserver.exe

ID	5
File Name	c:\windows\syswow64\raserver.exe
Command Line	"C:\Windows\SysWOW64\raserver.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 105170, Reason: Child Process
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	199.83s
Return Code	Unknown
PID	1792
Parent PID	1864
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0xc88	0x110000(1114112)	0x2f000	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\rysgtozci.exe	0xc88	0x12b0000(19595264)	0x1e000	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	5163
Process	93
-	153
File	550
Registry	427
Module	160
-	28
-	1
Mutex	2
COM	1
User	1
-	1

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c del "C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 111740, Reason: Child Process
Unmonitor End Time	End Time: 116352, Reason: Terminated
Monitor duration	4.61s
Return Code	0
PID	3248
Parent PID	1792
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe	5.50 KB	874f73e2673462859967afc64c3c33c1957d7b69915124cca91ced26dcfcd5c0	✖

Host Behavior

Type	Count
File	18
Environment	11
Registry	17
System	1
Module	8

Process #8: iexplore.exe

ID	8
File Name	c:\program files\internet explorer\iexplore.exe
Command Line	"C:\Program Files\Internet Explorer\iexplore.exe" about:blank
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 120814, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	184.19s
Return Code	Unknown
PID	2020
Parent PID	1792
Bitness	64 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x6350000(104136704)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2df0000(48168960)	0x14e000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x5a0	0x2eb8dc2(48991682)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x5a0	0x2(2)	-	✔	1

Host Behavior

Type	Count
Mutex	1

Process #9: yahoomessenger.exe

ID	9
File Name	c:\program files (x86)\windows sidebar\yahoomessenger.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\yahoomessenger.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 131795, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	173.20s
Return Code	Unknown
PID	4328
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2090000(34144256)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2a60000(44433408)	0x119000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x10ec	0x2ae5717(44979991)	-	✔	1

Process #11: winscp.exe

ID	11
File Name	c:\program files (x86)\reference assemblies\winscp.exe
Command Line	"C:\Program Files (x86)\Reference Assemblies\winscp.exe"
Initial Working Directory	C:\Program Files (x86)\Reference Assemblies\
Monitor Start Time	Start Time: 137188, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.81s
Return Code	Unknown
PID	4344
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2190000(35192832)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x7a0000(7995392)	0xfe000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x10fc	0x80a717(8431383)	-	✔	1

Process #12: whatsapp.exe

ID	12
File Name	c:\program files (x86)\msbuild\whatsapp.exe
Command Line	"C:\Program Files (x86)\MSBuild\whatsapp.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 137244, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.75s
Return Code	Unknown
PID	4352
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2040000(33816576)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2a10000(44105728)	0x10a000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1104	0x2a86717(44590871)	-	✔	1

Process #13: webdrive.exe

ID	13
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: 137300, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.70s
Return Code	Unknown
PID	4368
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2070000(34013184)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2a40000(44302336)	0x154000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1114	0x2b00717(45090583)	-	✔	1

Process #14: trillian.exe

ID	14
File Name	c:\program files (x86)\microsoft.net\trillian.exe
Command Line	"C:\Program Files (x86)\Microsoft.NET\trillian.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft.NET\
Monitor Start Time	Start Time: 137363, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.64s
Return Code	Unknown
PID	4376
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2010000(33619968)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x650000(6619136)	0xe6000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x111c	0x6a2717(6956823)	-	✔	1

Process #15: thunderbird.exe

ID	15
File Name	c:\program files\windows journal\thunderbird.exe
Command Line	"C:\Program Files\Windows Journal\thunderbird.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 137571, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.43s
Return Code	Unknown
PID	4388
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x21b0000(35323904)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2b80000(45613056)	0x18d000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1128	0x2c79717(46634775)	-	✔	1

Process #16: smartftp.exe

ID	16
File Name	c:\program files\windows multimedia platform\smartftp.exe
Command Line	"C:\Program Files\Windows Multimedia Platform\smartftp.exe"
Initial Working Directory	C:\Program Files\Windows Multimedia Platform\
Monitor Start Time	Start Time: 137632, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	167.37s
Return Code	Unknown
PID	4396
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2800000(41943040)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x630000(6488064)	0xf8000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1130	0x694717(6899479)	-	✔	1

Process #17: skype.exe

ID	17
File Name	c:\program files\msbuild\skype.exe
Command Line	"C:\Program Files\MSBuild\skype.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 138014, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	166.99s
Return Code	Unknown
PID	4412
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2690000(40435712)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0xcd0000(13434880)	0x146000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1140	0xd82717(14165783)	-	✔	1

Process #18: scriptftp.exe

ID	18
File Name	c:\program files\windows multimedia platform\scriptftp.exe
Command Line	"C:\Program Files\Windows Multimedia Platform\scriptftp.exe"
Initial Working Directory	C:\Program Files\Windows Multimedia Platform\
Monitor Start Time	Start Time: 138437, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	166.56s
Return Code	Unknown
PID	4420
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x21e0000(35520512)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x5b0000(5963776)	0x131000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1148	0x64d717(6608663)	-	✔	1

Process #19: pidgin.exe

ID	19
File Name	c:\program files (x86)\internet explorer\pidgin.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\pidgin.exe"
Initial Working Directory	C:\Program Files (x86)\Internet Explorer\
Monitor Start Time	Start Time: 138534, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	166.47s
Return Code	Unknown
PID	4436
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x27b0000(41615360)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x5e0000(6160384)	0xcd000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1158	0x619717(6395671)	-	✔	1

Process #20: outlook.exe

ID	20
File Name	c:\program files\windows media player\outlook.exe
Command Line	"C:\Program Files\Windows Media Player\outlook.exe"
Initial Working Directory	C:\Program Files\Windows Media Player\
Monitor Start Time	Start Time: 138589, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	166.41s
Return Code	Unknown
PID	4444
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2270000(36110336)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2070000(34013184)	0x133000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1160	0x210f717(34666263)	-	✔	1

Process #21: operamail.exe

ID	21
File Name	c:\program files\msbuild\operamail.exe
Command Line	"C:\Program Files\MSBuild\operamail.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 138798, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	166.20s
Return Code	Unknown
PID	4460
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x20a0000(34209792)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2a70000(44498944)	0x194000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1170	0x2b70717(45549335)	-	✔	1

Process #22: notepad.exe

ID	22
File Name	c:\program files (x86)\windows portable devices\notepad.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\notepad.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 139020, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.98s
Return Code	Unknown
PID	4468
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2260000(36044800)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2090000(34144256)	0x103000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1178	0x20ff717(34600727)	-	✔	1

Process #23: ncftp.exe

ID	23
File Name	c:\program files (x86)\microsoft.net\ncftp.exe
Command Line	"C:\Program Files (x86)\Microsoft.NET\ncftp.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft.NET\
Monitor Start Time	Start Time: 139118, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.88s
Return Code	Unknown
PID	4484
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x27b0000(41615360)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x4e0000(5111808)	0xf9000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1188	0x545717(5527319)	-	✔	1

Process #24: leechftp.exe

ID	24
File Name	c:\program files (x86)\windowspowershell\leechftp.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\leechftp.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 139381, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.62s
Return Code	Unknown
PID	4492
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2210000(35717120)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2080000(34078720)	0x161000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1190	0x214d717(34920215)	-	✔	1

Process #25: gmailnotifierpro.exe

ID	25
File Name	c:\program files\windows sidebar\gmailnotifierpro.exe
Command Line	"C:\Program Files\Windows Sidebar\gmailnotifierpro.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 139535, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.46s
Return Code	Unknown
PID	4524
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x22c0000(36438016)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x650000(6619136)	0xcd000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11b0	0x689717(6854423)	-	✔	1

Process #26: 3dftp.exe

ID	26
File Name	c:\program files\common files\3dftp.exe
Command Line	"C:\Program Files\Common Files\3dftp.exe"
Initial Working Directory	C:\Program Files\Common Files\
Monitor Start Time	Start Time: 139714, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.28s
Return Code	Unknown
PID	4532
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x25c0000(39583744)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x580000(5767168)	0xef000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11b8	0x5db717(6141719)	-	✔	1

Process #27: absolutetelnet.exe

ID	27
File Name	c:\program files\common files\absolutetelnet.exe
Command Line	"C:\Program Files\Common Files\absolutetelnet.exe"
Initial Working Directory	C:\Program Files\Common Files\
Monitor Start Time	Start Time: 139770, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.23s
Return Code	Unknown
PID	4540
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2040000(33816576)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x6c0000(7077888)	0xd2000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11c0	0x6fe717(7333655)	-	✔	1

Process #28: alftp.exe

ID	28
File Name	c:\program files (x86)\windows defender\alftp.exe
Command Line	"C:\Program Files (x86)\Windows Defender\alftp.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 139833, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.17s
Return Code	Unknown
PID	4548
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2290000(36241408)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x590000(5832704)	0x13d000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11c8	0x639717(6526743)	-	✔	1

Process #29: barca.exe

ID	29
File Name	c:\program files (x86)\windows portable devices\barca.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\barca.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 139892, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	165.11s
Return Code	Unknown
PID	4556
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x20d0000(34406400)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x500000(5242880)	0xc5000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11d0	0x531717(5445399)	-	✔	1

Process #30: bitkinex.exe

ID	30
File Name	c:\program files\windows media player\bitkinex.exe
Command Line	"C:\Program Files\Windows Media Player\bitkinex.exe"
Initial Working Directory	C:\Program Files\Windows Media Player\
Monitor Start Time	Start Time: 140131, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.87s
Return Code	Unknown
PID	4564
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x21c0000(35389440)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0xc00000(12582912)	0x19e000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11d8	0xd0a717(13674263)	-	✔	1

Process #31: coreftp.exe

ID	31
File Name	c:\program files\windows portable devices\coreftp.exe
Command Line	"C:\Program Files\Windows Portable Devices\coreftp.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 140246, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.75s
Return Code	Unknown
PID	4572
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2210000(35717120)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2be0000(46006272)	0x10f000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11e0	0x2c5b717(46511895)	-	✔	1

Process #32: far.exe

ID	32
File Name	c:\program files\uninstall information\far.exe
Command Line	"C:\Program Files\Uninstall Information\far.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 140495, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.50s
Return Code	Unknown
PID	4580
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2270000(36110336)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0xba0000(12189696)	0x145000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11e8	0xc51717(12916503)	-	✔	1

Process #33: filezilla.exe

ID	33
File Name	c:\program files (x86)\windows multimedia platform\filezilla.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\filezilla.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 140576, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.42s
Return Code	Unknown
PID	4588
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2260000(36044800)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x600000(6291456)	0x112000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11f0	0x67e717(6809367)	-	✔	1

Process #34: flashfxp.exe

ID	34
File Name	c:\program files (x86)\windows portable devices\flashfxp.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\flashfxp.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 140884, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.12s
Return Code	Unknown
PID	4596
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2250000(35979264)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x580000(5767168)	0xc2000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x11f8	0x5ae717(5957399)	-	✔	1

Process #35: fling.exe

ID	35
File Name	c:\program files (x86)\windows defender\fling.exe
Command Line	"C:\Program Files (x86)\Windows Defender\fling.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 140967, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	164.03s
Return Code	Unknown
PID	4604
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x24d0000(38600704)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x600000(6291456)	0x187000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1200	0x6f3717(7288599)	-	✔	1

Process #36: icq.exe

ID	36
File Name	c:\program files\windows portable devices\icq.exe
Command Line	"C:\Program Files\Windows Portable Devices\icq.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 141045, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	163.95s
Return Code	Unknown
PID	4620
Parent PID	1792
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x2070000(34013184)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x5c0000(6029312)	0x10a000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x1210	0x636717(6514455)	-	✔	1

Process #37: iexplore.exe

ID	37
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2020 CREDAT:82945 /prefetch:2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 141091, Reason: Injection
Unmonitor End Time	End Time: 304999, Reason: Terminated by timeout
Monitor duration	163.91s
Return Code	Unknown
PID	4804
Parent PID	1792
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x8450000(138739712)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\raserver.exe	0xf20	0x8e20000(149028864)	0x194000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x12c8	0x8f20717(150079255)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\raserver.exe	0xf20 / 0x12c8	0x8f2071c(150079260)	-	✔	1

Host Behavior

Type	Count
File	1
Module	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d02d076842cc94fa6612b13ff0d2f77e1ff9150d22607cfe3962da4234cf4ed5	C:\Users\RDhJ0CNFevzX\Desktop\scrss.exe	Sample File	214.30 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
874f73e2673462859967afc64c3c33c1957d7b69915124cca91ced26dcfcd5c0	C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe, \??\C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe	Dropped File	5.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
a45a2d762e763e3b0909b33d433b0c93008cadcf392122829c92c6565ad1a85b	-	Downloaded File	1.67 KB	text/html	-	CLEAN
9e17cb15dd75bbbd5dbb984eda674863c3b10ab72613cf8a39a00c3e11a8492a	-	Downloaded File	162 bytes	text/html	-	CLEAN
2baebb84d79b7542324b5349be6504bee6e55b4baffe353f9aae1c2b585e4330	-	Downloaded File	335 bytes	text/html	-	CLEAN
5ba320b58f0e4bdca6a2e270d9f76834a157f6fd81f3ef620f5eb1a3b95ac4fc	-	Downloaded File	426 bytes	text/html	-	CLEAN
26a0ef0fe1fdab9e6dae3caecec085c3800a44d32cd5b87c182c0c0a6b559f59	C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg	Dropped File	5.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
eaece2eba6310253249603033c744dd5914089b0bb26bde6685ec9813611baae	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogri.ini	Dropped File	40 bytes	application/octet-stream	Access, Create, Read	CLEAN
3f20b4605a2a543557ff9f208c286aef88fd05200f0c6150d35f1402507bd228	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrc.ini	Dropped File	1.75 KB	application/octet-stream	Access, Create, Read	CLEAN
3eb8165a0647b8408bb41cc7414f0c46b7da04bfff19447259b1719350013d5c	-	Downloaded File	291 bytes	text/html	-	CLEAN
d0da793571aa99c98e2afca3be0f3d6850aabbacf2aca4eeab8013e4ebf77a67	C:\Users\RDHJ0C~1\AppData\Local\Temp\ptcgl43g463vgbr58	Dropped File	185.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6eebf968962745b2e9de2ca969af7c424916d4e3fe3cc0bb9b3d414abfce9507	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrv.ini	Dropped File	40 bytes	application/octet-stream	Access, Create, Read	CLEAN
e1625aa27dd1d5d658b2a743de62f8cabcf34bfb8e09c6dad9f40f9b52211b61	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogim.jpeg	Dropped File	90.38 KB	image/jpeg	Access, Create, Read	CLEAN
6fb704daa8756b1df1557d8d5ff07ea037ae792955d03c27e5662a7bcea42550	-	Downloaded File	24.42 KB	text/html	-	CLEAN
e81e05d6792762b645006a9e93c236afb8fe32bd0bd6cf9bfaad3efe205668c0	-	Downloaded File	2.15 KB	text/html	-	CLEAN
c40c4d1ac0df1ab3cf59ebad6e2490f99e292dbf17f88d599788661d0b2d0451	-	Downloaded File	277 bytes	text/html	-	CLEAN
3bbe72f3baa8ec61de17a1d767fca58704769684b7abe9161d0c4eaf4c8f0982	-	Downloaded File	707 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\scrss.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Create, Read	CLEAN

File Name	Category	Operations	Verdict
C:\	Accessed File	Access	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\ptcgl43g463vgbr58	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrc.ini	Dropped File, Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogro.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe	Accessed File	Access, Create, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr155E.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrv.ini	Accessed File	Access, Create, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlog00.ini	Accessed File	Access, Create	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrm.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrf.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access, Create	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsjFBF.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Temp\rysgtozci.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogim.jpeg	Dropped File, Accessed File	Access, Create, Read	CLEAN
\??\C:\Program Files\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
C:\Program Files (x86)\Wrvtps4_h\Cookiesclrpdxk8.exe	-	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrg.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrc.ini	Accessed File	Access, Create, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsr155E.tmp\	Accessed File	Access	CLEAN
\??\C:\Windows\SysWOW64\raserver.exe	Accessed File	Access, Create, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlog.ini	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrt.ini	Accessed File	Access, Create	CLEAN
\??\C:\Program Files (x86)\Wrvtps4_h\Cookiesclrpdxk8.exe	Accessed File	Access, Create	CLEAN
C:\Windows\System32	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\-2np6r7e\-2nlog.ini	Dropped File, Not Extracted	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogcl.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogri.ini	Dropped File, Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogri.ini	Accessed File	Access, Create, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\-2NP6R7E\-2Nlogrv.ini	Dropped File, Accessed File	Access, Create, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.lovejaclyn.com/song_lyrics.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5MxoIrF...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=26527269&ktd=0&kld=1042&kp=6	-	209.99.64.43	-	-	CLEAN
http://i3.cdn-image.com/__media__/js/min.js?v2.3	-	-	-	-	CLEAN
http://i4.cdn-image.com/__media__/js/min.js?v2.3	-	-	-	-	CLEAN
http://www.dandelionfusedigital.com/fw02/?ZZI=FBCZxRbtofiFbuFLP5VkagDY6z5F/jU6/InmQ1C2NVKK2BsIYb7M4lm7BZBf8SVBw1WDaA==&elzp=TTtX	-	198.54.117.210, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.211, 198.54.117.216, 198.54.117.215	-	GET	CLEAN
http://www.7477e.xyz/fw02/	-	172.67.199.31, 104.21.21.144	-	POST	CLEAN
http://www.lovejaclyn.com	-	209.99.64.43	-	-	CLEAN
http://www.lovejaclyn.com/Free_Credit_Report.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=11539660&ktd=0&kld=1042&kp=5	-	209.99.64.43	-	-	CLEAN
http://www.ilina.xyz/fw02/?ZZI=GovV0e+2vH+6sn2WJzglYLi9K7HJG6Hb4lAdaf5BxulWl4LHuFZ3rR7+Ae1g08nlOeWsog==&zL00dV=f6Ap5PR8IR1PV	-	104.21.4.240, 172.67.187.58	-	GET	CLEAN
http://www.eddrugs2018.com/Migraine_Pain_Relief.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJR...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=19222924&ktd=0&kld=1061&kp=2	-	204.11.56.48	-	-	CLEAN
http://www.eddrugs2018.com/fw02/?ZZI=/z6NEJ69yVJGPM1rdj5Kzq9DL/DuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw==&zL00dV=f6Ap5PR8IR1PV	-	204.11.56.48	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://www.networksolutions.com/cgi-bin/promo/domain-search?domainNames=eddrugs2018.com&search=premiumlanding&channelid=P13C100S300N0B3A1D0E0000V100	-	-	-	-	CLEAN
http://www.eddrugs2018.com/Anti_Wrinkle_Creams.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRb... ...VJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=1919926&ktd=0&kld=1061&kp=1	-	204.11.56.48	-	-	CLEAN
http://www.lovejaclyn.com/fashion_trends.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5Mxo... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=10542279&ktd=0&kld=1042&kp=4	-	209.99.64.43	-	-	CLEAN
http://www.eddrugs2018.com/sk-logabpstatus.php?a=ejBabExITVl2RFJwT3ZSV3VGME85QXFRdlo3RjJ1dWJOTzY2QWNTQVhFbE1KTVpOTmF1MzVNUTJvbUZWSWoyUUx5MVRFZ3N0U0Nwc1lxakNQREhXb1p3Si9KYVVxOG9rQXdsN3lOQUZLenBhVWw0VDNzdFAzTE5ha01lMEFyelc=&b=	-	204.11.56.48	-	-	CLEAN
http://www.eddrugs2018.com/Best_Penny_Stocks.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQ... ...VJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=3482138&ktd=0&kld=1061&kp=6	-	204.11.56.48	-	-	CLEAN
http://www.scovikinnovations.com/fw02/?ZZI=JW6gKnBiflfQEVztNe4Tulw1VPOJ0N5LGG9bGwyVqVadxlZXAql2YwS5UkZ1rgzw98IOgw==&elzp=TTtX	-	192.185.0.218	-	GET	CLEAN
http://www.vanessaruizwriting.com/fw02/?ZZI=Ui69laVOu1v+JLK6S5Z9JE+MP08KQpiMVt7NuF6zMG38sFvg/ehfBJlXm70TR9EtTU52bw==&elzp=TTtX	-	198.54.117.210, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.211, 198.54.117.216, 198.54.117.215	-	GET	CLEAN
http://www.eddrugs2018.com/10_Best_Mutual_Funds.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJR... ... 9yVJGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=72996&ktd=0&kld=1061&kp=5	-	204.11.56.48	-	-	CLEAN
http://www.eddrugs2018.com/px.js?ch=2	-	204.11.56.48	-	-	CLEAN
http://www.lovejaclyn.com/Cheap_Air_Tickets.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKMr5... ... 8je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=5645746&ktd=0&kld=1042&kp=1	-	209.99.64.43	-	-	CLEAN
http://www.largestjerseysstore.com/fw02/?ZZI=cHF1IlzheLmJHtN59WqmKu+q3iQdAOesklPX6LsiZG+TwEYG2vkDGRbq2lgFmRvqBs9Eeg==&oDKX=PpF0-nRHybghQp	-	156.245.192.153	-	GET	CLEAN
http://www.lovejaclyn.com/px.js?ch=2	-	209.99.64.43	-	-	CLEAN
http://www.eddrugs2018.com/sk-privacy.php	-	204.11.56.48	-	-	CLEAN
http://www.eddrugs2018.com/display.cfm	-	204.11.56.48	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.10936.loan/fw02/	-	185.216.248.42	-	POST	CLEAN
http://eddrugs2018.com	-	-	-	-	CLEAN
http://www.7477e.xyz/fw02/?ZZI=hZ0UeJp6fd+b97vTasQPXH6DoCVbE/Ua0aTbzhCwqvl4iQqpMVEe8veqno3garzpF7oF0A==&oDKX=PpF0-nRHybghQp	-	172.67.199.31, 104.21.21.144	-	GET	CLEAN
http://www.5p6xljjse1lq.xyz/fw02/?ZZI=iY7cHZOQigy8MmRzVBkzkxJ3JOugJYILBJlwsLX+b4fBhnZGDg3yinWJ8YhLtVVSl4UJCg==&oDKX=PpF0-nRHybghQp	-	18.221.0.52	-	GET	CLEAN
http://www.sunwall.xyz/fw02/?ZZI=6TtO6HPce6q0Xc5JtNk8NP9HYMp6msWauevBhsRweFGL2ktJvIIk5YskpBJ7vyPDYZYfYA==&elzp=TTtX	-	162.0.231.155	-	GET	CLEAN
http://www.buydomains.com/lander/lovejaclyn.com/?domain=lovejaclyn.com&utm_source=lovejaclyn.com&utm_campaign=skenzo&traffic_id=skenzo17&traffic_type=park	-	-	-	-	CLEAN
http://www.lovejaclyn.com/Anti_Wrinkle_Creams.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKM... ...8je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrlYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=1919926&ktd=0&kld=1042&kp=3	-	209.99.64.43	-	-	CLEAN
http://www.5p6xljjse1lq.xyz/fw02/	-	18.221.0.52	-	POST	CLEAN
http://www.eddrugs2018.com/find_a_tutor.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQkjIjM... ...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60lHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8lR1PV&&kt=112&&ki=10844596&ktd=0&kld=1061&kp=7	-	204.11.56.48	-	-	CLEAN
http://www.scovikinnovations.com/fw02/	-	192.185.0.218	-	POST	CLEAN
http://www.czoqg.xyz/fw02/?ZZI=i8U3GOpzdfOw2GgzvLmi5UUBcFXKNl9MVWatKm+oWi3pb1CAVMFUg5iZfze9PYgRR7t+FA==&elzp=TTtX	-	156.251.18.25	-	-	CLEAN
http://www.sdjnsbd.com/fw02/?ZZI=T2HQ/5Fnw2DoAbeb93/ApdJLKQyT2yAAijSiJ6BVUO4INv+F6+csACgpZilkr+EortA9BA==&zL00dV=f6Ap5PR8lR1PV	-	104.253.187.34	-	GET	CLEAN
http://www.10936.loan/fw02/?oDKX=PpF0-nRHybghQp&ZZI=ReenpJFtiyJzDfNKFYd3YADTMMSTSUBT/El1isJ661zeWMRAYbbvuhCyy1dUowbNoPpsmw==	-	185.216.248.42	-	GET	CLEAN
http://www.largestjerseysstore.com/fw02/?ZZI=cHF1IlzheLmJHtN59WqmKu+q3iQdAOeskIPX6LsiZG+TwEYG2vkDGRbq2lgFmRvqBs9Eeg==&elzp=TTtX	-	156.245.192.153	-	GET	CLEAN
http://www.lovejaclyn.com/High_Speed_Internet.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBKM... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrlYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=13681481&ktd=0&kld=1042&kp=7	-	209.99.64.43	-	-	CLEAN
https://wildcard.hostgator.com/fw02/?ZZI=JW6gKnBiflfQEVztNe4Tulw1VPOJ0N5LGG9bGwyVqVadxlZXAql2YwS5UkZ1rgzw98lOgw==&elzp=TTtX	-	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.lovejaclyn.com/sk-logabpstatus.php?a=VThpazQvNW1zREdRSElabWtZbDQ4YitEd2NnRlNJZENRVXhYVktOSUo0QjZmVk5ZT0dVWjM0ZDJFdzhWWFBUeGI5R0V6QXZ6NnRETVpoK09FZFI6dVhBM05YYmtEa3B4cC9VSFFRdEpXTDF2WEZjSW5hMmszSGE3TXMvQU5jVU0=&b=	-	209.99.64.43	-	-	CLEAN
http://www.eddrugs2018.com/High_Speed_Internet.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRb... ...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60IHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=13681481&ktd=0&kld=1061&kp=3	-	204.11.56.48	-	-	CLEAN
http://www.salarydetector.net/fw02/?ZZI=73srvekCQLgA6VzhY0rwafKgb18eM8pr6xDuhcp4lWcnGdB1ZAXXMmsczaGk2cl0IN80/Q==&zL00dV=f6Ap5PR8IR1PV	-	199.188.206.67	-	GET	CLEAN
http://www.lovejaclyn.com/px.js?ch=1	-	209.99.64.43	-	-	CLEAN
http://www.5p6xljjse1lq.xyz/fw02/?ZZI=iY7cHZOQigy8MmRzVBkzkxJ3JOugJYILBJlwsLX+b4fBhnZGDg3yinWJ8YhLtVVSl4UJCg==&elzp=TTtX	-	18.221.0.52	-	GET	CLEAN
http://www.10936.loan/fw02/?ZZI=ReenpJFtiyJzDfNKFYd3YADTMMSTSUBT/El1isJ661zeWMRAYbbvuhCyy1dUowbNoPpsmw==&elzp=TTtX	-	185.216.248.42	-	GET	CLEAN
http://www.thesiscoper.com/fw02/?ZZI=3/oBgBxwsNYyzLslzJuiywbdD1KR9wTmmpLIdxkspL7D4spRMDqlE5pSL1fAhBq6YawIDg==&elzp=TTtX	-	18.217.107.127	-	GET	CLEAN
http://www.eddrugs2018.com/px.js?ch=1	-	204.11.56.48	-	-	CLEAN
http://www.lovejaclyn.com/Migraine_Pain_Relief.cfm?fp=timpjPgHRCcaxOHUS%2BlkxCvG%2FNpYUy04plUXV%2F329OEOPpOpnW%2FcYpZHt%2FoXjQpXBK... ...je1hTfxmL3uEJhAV97gJwjJc9H+nJwte8UGvpeoTpTdLrIYhzbaj1d1NiBKAx5A%3D%3D&oDKX=PpF0-nRHybghQp&&kt=112&&ki=19222924&ktd=0&kld=1042&kp=2	-	209.99.64.43	-	-	CLEAN
https://wildcard.hostgator.com/fw02/	-	-	-	-	CLEAN
http://www.czoqg.xyz/fw02/?oDKX=PpF0-nRHybghQp&ZZI=i8U3GOpzdfOw2GgzvLmi5UUBcFXKNl9MVWatKm+oWi3pb1CAVMFUg5iZfze9PYgRR7t+FA==	-	156.251.18.25	-	-	CLEAN
http://www.the6figureshow.com/fw02/?ZZI=eTPPPG3yBw1rXnY600nziyQrGW/kopa9XgvCJchWVR6iyIbQ2Ul/sZzfUA7gGoYjKhr4+w==&elzp=TTtX	-	34.102.136.180	-	GET	CLEAN
http://www.eddrugs2018.com/song_lyrics.cfm?fp=3jNpvtxUpPrC4wQonWBx88BJ4X%2FS2vLDNHkeR5aKVxOC8HwDbPrI0fkqCftDV7MKhoiywrEJRbUQkjIjMk... ...JGPM1rdj5Kzq9DL%2FDuTIFSSAZTeAXQy8DQ5yXNPg60IHwa4EyOlGQYhiNOpw%3D%3D&zL00dV=f6Ap5PR8IR1PV&&kt=112&&ki=26527269&ktd=0&kld=1061&kp=4	-	204.11.56.48	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.dandelionfusedigital.com	198.54.117.210, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.211, 198.54.117.216, 198.54.117.215	-	TCP, HTTP, DNS	CLEAN
www.sdjnsbd.com	104.253.187.34	-	TCP, DNS	CLEAN
eddrugs2018.com	-	-	-	CLEAN
www.salarydetector.net	199.188.206.67	-	TCP, DNS	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.ywfjp.com	-	-	-	CLEAN
www.vanessaruizwriting.com	198.54.117.210, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.211, 198.54.117.216, 198.54.117.215	-	TCP, HTTP, DNS	CLEAN
www.ztzfirst.xyz	-	-	-	CLEAN
www.scovikinnovations.com	192.185.0.218	-	TCP, DNS	CLEAN
www.ilina.xyz	104.21.4.240, 172.67.187.58	-	TCP, DNS	CLEAN
www.monumentalmarketsllc.com	-	-	-	CLEAN
www.eddrugs2018.com	204.11.56.48	-	TCP, DNS	CLEAN
www.sunwall.xyz	162.0.231.155	-	TCP, DNS	CLEAN
www.7477e.xyz	172.67.199.31, 104.21.21.144	-	TCP, HTTP, DNS	CLEAN
i4.cdn-image.com	-	-	-	CLEAN
www.konstelle.store	-	-	-	CLEAN
wildcard.hostgator.com	-	-	-	CLEAN
www.5p6xljjse1lq.xyz	18.221.0.52	-	TCP, DNS	CLEAN
parkingpage.namecheap.com	198.54.117.210, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.211, 198.54.117.216, 198.54.117.215	-	TCP, HTTP, DNS	CLEAN
the6figureshow.com	34.102.136.180	-	TCP, DNS	CLEAN
i3.cdn-image.com	-	-	-	CLEAN
www.payer-breakers.com	-	-	-	CLEAN
www.thesiscoper.com	18.217.107.127	-	TCP, DNS	CLEAN
www.lovejaclyn.com	209.99.64.43	-	TCP, DNS	CLEAN
www.shishlomarket24.biz	-	-	-	CLEAN
www.networksolutions.com	-	-	-	CLEAN
www.fortitude-tech.com	-	-	-	CLEAN
www.largestjerseysstore.com	156.245.192.153	-	TCP, DNS	CLEAN
www.10936.loan	185.216.248.42	-	TCP, HTTP, DNS	CLEAN
salarydetector.net	199.188.206.67	-	TCP, DNS	CLEAN
www.czoqg.xyz	156.251.18.25	-	TCP, DNS	CLEAN
www.buydomains.com	-	-	-	CLEAN
www.5145.design	-	-	-	CLEAN
www.the6figureshow.com	34.102.136.180	-	TCP, DNS	CLEAN
www.trybes.space	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.216.248.42	www.10936.loan	Hong Kong	TCP, HTTP, DNS	CLEAN
156.245.192.153	www.largestjerseysstore.com	Hong Kong	TCP, DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
198.54.117.211	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	DNS	CLEAN
18.217.107.127	www.thesiscoper.com	United States	TCP, DNS	CLEAN
156.251.18.25	www.czoqg.xyz	Hong Kong	TCP, DNS	CLEAN
199.188.206.67	www.salarydetector.net, salarydetector.net	United States	TCP, DNS	CLEAN
104.253.187.34	www.sdjnsbd.com	United States	TCP, DNS	CLEAN
104.21.21.144	www.7477e.xyz	-	TCP, HTTP, DNS	CLEAN
162.0.231.155	www.sunwall.xyz	United States	TCP, DNS	CLEAN
18.221.0.52	www.5p6xljjse1lq.xyz	United States	TCP, DNS	CLEAN
172.67.199.31	www.7477e.xyz	United States	DNS	CLEAN
198.54.117.216	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	DNS	CLEAN
198.54.117.218	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	TCP, HTTP, DNS	CLEAN
198.54.117.217	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	DNS	CLEAN
192.185.0.218	www.scovikinnovations.com	United States	TCP, DNS	CLEAN
34.102.136.180	www.the6figureshow.com, the6figureshow.com	United States	TCP, DNS	CLEAN
198.54.117.215	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	DNS	CLEAN
204.11.56.48	www.eddrugs2018.com	British Virgin Islands	TCP, DNS	CLEAN
104.21.4.240	www.ilina.xyz	-	TCP, DNS	CLEAN
198.54.117.212	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	TCP, HTTP, DNS	CLEAN
198.54.117.210	www.dandelionfusedigital.com, parkingpage.namecheap.com, www.vanessaruizwriting.com	United States	DNS	CLEAN
172.67.187.58	www.ilina.xyz	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-2NP6R7E2SEYA12z	access	raserver.exe	CLEAN
6NON26-3X60UXYXz	access	raserver.exe	CLEAN
S-1-5-21-1560258-20201777346147	access	iexplore.exe	CLEAN
S-1-5-21-1560258-18641394712783	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	create, access	raserver.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook_2016	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	create, access	raserver.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	create, access	raserver.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	create, access	raserver.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	create, access	raserver.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	create, access	raserver.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	create, access	raserver.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird	create, access	raserver.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	create, access	raserver.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TDKXEFWX2TVX	write, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook	create, access	raserver.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	raserver.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	create, access	raserver.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	create, access	raserver.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
3dftp.exe	"C:\Program Files\Common Files\3dftp.exe"	SUSPICIOUS
absolutetelnet.exe	"C:\Program Files\Common Files\absolutetelnet.exe"	SUSPICIOUS
alftp.exe	"C:\Program Files (x86)\Windows Defender\alftp.exe"	SUSPICIOUS
barca.exe	"C:\Program Files (x86)\Windows Portable Devices\barca.exe"	SUSPICIOUS
bitkinex.exe	"C:\Program Files\Windows Media Player\bitkinex.exe"	SUSPICIOUS
coreftp.exe	"C:\Program Files\Windows Portable Devices\coreftp.exe"	SUSPICIOUS
far.exe	"C:\Program Files\Uninstall Information\far.exe"	SUSPICIOUS
filezilla.exe	"C:\Program Files (x86)\Windows Multimedia Platform\filezilla.exe"	SUSPICIOUS
flashfxp.exe	"C:\Program Files (x86)\Windows Portable Devices\flashfxp.exe"	SUSPICIOUS
fling.exe	"C:\Program Files (x86)\Windows Defender\fling.exe"	SUSPICIOUS

Process Name	Commandline	Verdict
icq.exe	"C:\Program Files\Windows Portable Devices\icq.exe"	SUSPICIOUS
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2020 CREDAT:82945 /prefetch:2	SUSPICIOUS
rysgtozci.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg	SUSPICIOUS
rysgtozci.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\wduqqtzg	SUSPICIOUS
raserver.exe	"C:\Windows\SysWOW64\raserver.exe"	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
cmd.exe	/c del "C:\Users\RDHJ0C~1\AppData\Local\Temp\rysgtozci.exe"	SUSPICIOUS
yahoomessenger.exe	"C:\Program Files (x86)\Windows Sidebar\yahoomessenger.exe"	SUSPICIOUS
winscp.exe	"C:\Program Files (x86)\Reference Assemblies\winscp.exe"	SUSPICIOUS
whatsapp.exe	"C:\Program Files (x86)\MSBuild\whatsapp.exe"	SUSPICIOUS
webdrive.exe	"C:\Program Files (x86)\WindowsPowerShell\webdrive.exe"	SUSPICIOUS
trillian.exe	"C:\Program Files (x86)\Microsoft.NET\trillian.exe"	SUSPICIOUS
thunderbird.exe	"C:\Program Files\Windows Journal\thunderbird.exe"	SUSPICIOUS
smartftp.exe	"C:\Program Files\Windows Multimedia Platform\smartftp.exe"	SUSPICIOUS
skype.exe	"C:\Program Files\MSBuild\skype.exe"	SUSPICIOUS
scriptftp.exe	"C:\Program Files\Windows Multimedia Platform\scriptftp.exe"	SUSPICIOUS
pidgin.exe	"C:\Program Files (x86)\Internet Explorer\pidgin.exe"	SUSPICIOUS
outlook.exe	"C:\Program Files\Windows Media Player\outlook.exe"	SUSPICIOUS
operamail.exe	"C:\Program Files\MSBuild\operamail.exe"	SUSPICIOUS
notepad.exe	"C:\Program Files (x86)\Windows Portable Devices\notepad.exe"	SUSPICIOUS
ncftp.exe	"C:\Program Files (x86)\Microsoft.NET\ncftp.exe"	SUSPICIOUS
leechftp.exe	"C:\Program Files (x86)\WindowsPowerShell\leechftp.exe"	SUSPICIOUS
gmailnotifierpro.exe	"C:\Program Files\Windows Sidebar\gmailnotifierpro.exe"	SUSPICIOUS
scrss.exe	"C:\Users\RDhJ0CNFevzX\Desktop\scrss.exe"	CLEAN
iexplore.exe	"C:\Program Files\Internet Explorer\iexplore.exe" about:blank	CLEAN

YARA / AV

YARA (27)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook	FormBook	Function Strings	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows