MALICIOUS	Classifications: -
	Threat Names: FormBook Mal/Generic-S
	Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe**
ID	#4264217
MD5	6f111b596da1ac7d71c4362b18309648
SHA1	e09f8065342a4c8664148bec4b0d9265e7e5842a
SHA256	285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96
File Size	214.18 KB
Report Created	2022-05-05 10:21 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (27 rules, 333 matches)

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

- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x9.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x1.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x5.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x8.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0xb.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x0.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x3.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x0.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x4.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x7.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x5.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x2.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0xd.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x9.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x9.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x1.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x2.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0xc.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0x3.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x7.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0x6.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x1.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0xb.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x7.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x7.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x8.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x3.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x1.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0x5.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0xd.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x5.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0xa.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x6.
- (Process #5) systray.exe adds a hook to Internet Explorer for sspicli.dll:EncryptMessage+0x4.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageA+0xb.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x5.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x9.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0xd.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x3.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:GetMessageW+0xa.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x1.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestW+0xb.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0x3.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageW+0x9.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0x7.
- (Process #5) systray.exe adds a hook to Internet Explorer for user32.dll:PeekMessageA+0xb.
- (Process #5) systray.exe adds a hook to Internet Explorer for wininet.dll:HttpSendRequestA+0xd.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x161.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x155.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x16d.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1bd.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1b3.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1a3.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0xd5.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1d1.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1e5.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x1a9.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0xc1.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0x163.
- (Process #5) systray.exe adds a hook to Internet Explorer for ntdll.dll:___guard_fids_table+0xad.

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	FormBook configuration was extracted	1	Spyware
	• A configuration for FormBook was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	15	Spyware
	• Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #3) pkypr.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #10) alftp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #14) coreftp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #21) leechftp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #5) systray.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #9) absolutetelnet.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 #20) icq.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #35) yahoomessenger.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #22) ncftp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #33) whatsapp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #27) scriptftp.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #13) bitkinex.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #24) operamail.exe. • Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #12) barca.exe.			
4/5	Injection	Writes into the memory of another process	32	Injector

Score	Category	Operation	Count	Classification
	• (Process #5) systray.exe modifies memory of (process #4) explorer.exe. • (Process #3) pkypr.exe modifies memory of (process #4) explorer.exe. • (Process #3) pkypr.exe modifies memory of (process #5) systray.exe. • (Process #5) systray.exe modifies memory of (process #8) iexplore.exe. • (Process #5) systray.exe modifies memory of (process #9) absolutetelnet.exe. • (Process #5) systray.exe modifies memory of (process #10) alftp.exe. • (Process #5) systray.exe modifies memory of (process #11) 3dftp.exe. • (Process #5) systray.exe modifies memory of (process #12) barca.exe. • (Process #5) systray.exe modifies memory of (process #13) bitkinex.exe. • (Process #5) systray.exe modifies memory of (process #14) coreftp.exe. • (Process #5) systray.exe modifies memory of (process #15) far.exe. • (Process #5) systray.exe modifies memory of (process #16) filezilla.exe. • (Process #5) systray.exe modifies memory of (process #17) flashfxp.exe. • (Process #5) systray.exe modifies memory of (process #18) fling.exe. • (Process #5) systray.exe modifies memory of (process #19) gmailnotifierpro.exe. • (Process #5) systray.exe modifies memory of (process #20) icq.exe. • (Process #5) systray.exe modifies memory of (process #21) leechftp.exe. • (Process #5) systray.exe modifies memory of (process #22) ncftp.exe. • (Process #5) systray.exe modifies memory of (process #23) notepad.exe. • (Process #5) systray.exe modifies memory of (process #24) operamail.exe. • (Process #5) systray.exe modifies memory of (process #25) outlook.exe. • (Process #5) systray.exe modifies memory of (process #26) pidgin.exe. • (Process #5) systray.exe modifies memory of (process #27) scriptftp.exe. • (Process #5) systray.exe modifies memory of (process #28) skype.exe. • (Process #5) systray.exe modifies memory of (process #29) smartftp.exe. • (Process #5) systray.exe modifies memory of (process #30) thunderbird.exe. • (Process #5) systray.exe modifies memory of (process #31) trillian.exe. • (Process #5) systray.exe modifies memory of (process #32) webdrive.exe. • (Process #5) systray.exe modifies memory of (process #33) whatsapp.exe. • (Process #5) systray.exe modifies memory of (process #34) winscp.exe. • (Process #5) systray.exe modifies memory of (process #35) yahoomessenger.exe. • (Process #5) systray.exe modifies memory of (process #36) iexplore.exe.			
4/5	Injection	Modifies control flow of another process	31	-

Score	Category	Operation	Count	Classification
	• (Process #3) pkypr.exe alters context of (process #4) explorer.exe. • (Process #5) systray.exe alters context of (process #4) explorer.exe. • (Process #5) systray.exe alters context of (process #8) iexplore.exe. • (Process #5) systray.exe alters context of (process #9) absolutetelnet.exe. • (Process #5) systray.exe alters context of (process #10) alftp.exe. • (Process #5) systray.exe alters context of (process #11) 3dftp.exe. • (Process #5) systray.exe alters context of (process #12) barca.exe. • (Process #5) systray.exe alters context of (process #13) bitkinex.exe. • (Process #5) systray.exe alters context of (process #14) coreftp.exe. • (Process #5) systray.exe alters context of (process #15) far.exe. • (Process #5) systray.exe alters context of (process #16) filezilla.exe. • (Process #5) systray.exe alters context of (process #17) flashfxp.exe. • (Process #5) systray.exe alters context of (process #18) fling.exe. • (Process #5) systray.exe alters context of (process #19) gmailnotifierpro.exe. • (Process #5) systray.exe alters context of (process #20) icq.exe. • (Process #5) systray.exe alters context of (process #21) leechftp.exe. • (Process #5) systray.exe alters context of (process #22) ncftp.exe. • (Process #5) systray.exe alters context of (process #23) notepad.exe. • (Process #5) systray.exe alters context of (process #24) operamail.exe. • (Process #5) systray.exe alters context of (process #25) outlook.exe. • (Process #5) systray.exe alters context of (process #26) pidgin.exe. • (Process #5) systray.exe alters context of (process #27) scriptftp.exe. • (Process #5) systray.exe alters context of (process #28) skype.exe. • (Process #5) systray.exe alters context of (process #29) smartftp.exe. • (Process #5) systray.exe alters context of (process #30) thunderbird.exe. • (Process #5) systray.exe alters context of (process #31) trillian.exe. • (Process #5) systray.exe alters context of (process #32) webdrive.exe. • (Process #5) systray.exe alters context of (process #33) whatsapp.exe. • (Process #5) systray.exe alters context of (process #34) winscp.exe. • (Process #5) systray.exe alters context of (process #35) yahoomessenger.exe. • (Process #5) systray.exe alters context of (process #36) iexplore.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels file "C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe" as Mal/Generic-S.			
3/5	Data Collection	Reads memory of user process	27	-

Score	Category	Operation	Count	Classification
	• (Process #5) systray.exe reads memory of process (process #9) absolutetelnet.exe. • (Process #5) systray.exe reads memory of process (process #10) alftp.exe. • (Process #5) systray.exe reads memory of process (process #11) 3dftp.exe. • (Process #5) systray.exe reads memory of process (process #12) barca.exe. • (Process #5) systray.exe reads memory of process (process #13) bitkinex.exe. • (Process #5) systray.exe reads memory of process (process #14) coreftp.exe. • (Process #5) systray.exe reads memory of process (process #15) far.exe. • (Process #5) systray.exe reads memory of process (process #16) filezilla.exe. • (Process #5) systray.exe reads memory of process (process #17) flashfxp.exe. • (Process #5) systray.exe reads memory of process (process #18) fling.exe. • (Process #5) systray.exe reads memory of process (process #19) gmailnotifierpro.exe. • (Process #5) systray.exe reads memory of process (process #20) icq.exe. • (Process #5) systray.exe reads memory of process (process #21) leechftp.exe. • (Process #5) systray.exe reads memory of process (process #22) ncftp.exe. • (Process #5) systray.exe reads memory of process (process #23) notepad.exe. • (Process #5) systray.exe reads memory of process (process #24) operamail.exe. • (Process #5) systray.exe reads memory of process (process #25) outlook.exe. • (Process #5) systray.exe reads memory of process (process #26) pidgin.exe. • (Process #5) systray.exe reads memory of process (process #27) scriptftp.exe. • (Process #5) systray.exe reads memory of process (process #28) skype.exe. • (Process #5) systray.exe reads memory of process (process #29) smartftp.exe. • (Process #5) systray.exe reads memory of process (process #30) thunderbird.exe. • (Process #5) systray.exe reads memory of process (process #31) trillian.exe. • (Process #5) systray.exe reads memory of process (process #32) webdrive.exe. • (Process #5) systray.exe reads memory of process (process #33) whatsapp.exe. • (Process #5) systray.exe reads memory of process (process #34) winscp.exe. • (Process #5) systray.exe reads memory of process (process #35) yahoomessenger.exe.			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #3) pkypr.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #3) pkypr.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\pkypr.exe".			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #5) systray.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) systray.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #5) systray.exe tries to read sensitive data of web browser "Opera" by file. • (Process #5) systray.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) pkypr.exe makes a direct system call to "NtQueryInformationToken". • (Process #3) pkypr.exe makes a direct system call to "NtReadVirtualMemory". • (Process #3) pkypr.exe makes a direct system call to "NtAdjustPrivilegesToken". • (Process #3) pkypr.exe makes a direct system call to "NtOpenThread". • (Process #3) pkypr.exe makes a direct system call to "NtClose". • (Process #3) pkypr.exe makes a direct system call to "NtProtectVirtualMemory". • (Process #3) pkypr.exe makes a direct system call to "NtQueryInformationProcess". • (Process #3) pkypr.exe makes a direct system call to "NtReadFile". • (Process #3) pkypr.exe makes a direct system call to "NtOpenProcessToken". • (Process #3) pkypr.exe makes a direct system call to "NtAllocateVirtualMemory". • (Process #3) pkypr.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #2) pkypr.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #3) pkypr.exe makes a direct system call to "NtQueryInformationFile". • (Process #3) pkypr.exe makes a direct system call to "NtOpenProcess". • (Process #3) pkypr.exe makes a direct system call to "NtFreeVirtualMemory". • (Process #3) pkypr.exe makes a direct system call to "NtCreateFile". • (Process #2) pkypr.exe makes a direct system call to "NtResumeThread". • (Process #3) pkypr.exe makes a direct system call to "NtResumeThread". • (Process #3) pkypr.exe makes a direct system call to "NtDelayExecution". • (Process #3) pkypr.exe makes a direct system call to "NtQuerySystemInformation". • (Process #2) pkypr.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #3) pkypr.exe makes a direct system call to "NtCreateSection". • (Process #3) pkypr.exe makes a direct system call to "NtMapViewOfSection".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #2) pkypr.exe modifies memory of (process #3) pkypr.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #2) pkypr.exe alters context of (process #3) pkypr.exe.			
2/5	Reputation	Resolves known suspicious domain	2	-
	• Resolved domain "www.zoommachone.xyz" is a known suspicious domain. • Resolved domain "www.portres.online" is a known suspicious domain.			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #1) 285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe starts (process #1) 285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe with a hidden window. • (Process #2) pkypr.exe starts (process #2) pkypr.exe with a hidden window. • (Process #4) explorer.exe starts (process #4) explorer.exe with a hidden window. • (Process #5) systray.exe starts (process #5) systray.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	31	-

Score	Category	Operation	Count	Classification
	• (Process #2) pkypr.exe reads from (process #2) pkypr.exe. • (Process #3) pkypr.exe reads from (process #4) explorer.exe. • (Process #3) pkypr.exe reads from (process #5) systray.exe. • (Process #5) systray.exe reads from (process #9) absolutetelnet.exe. • (Process #5) systray.exe reads from (process #10) alftp.exe. • (Process #5) systray.exe reads from (process #11) 3dftp.exe. • (Process #5) systray.exe reads from (process #12) barca.exe. • (Process #5) systray.exe reads from (process #13) bitkinex.exe. • (Process #5) systray.exe reads from (process #14) coreftp.exe. • (Process #5) systray.exe reads from (process #15) far.exe. • (Process #5) systray.exe reads from (process #16) filezilla.exe. • (Process #5) systray.exe reads from (process #17) flashfxp.exe. • (Process #5) systray.exe reads from (process #18) fling.exe. • (Process #5) systray.exe reads from (process #19) gmailnotifierpro.exe. • (Process #5) systray.exe reads from (process #20) icq.exe. • (Process #5) systray.exe reads from (process #21) leechftp.exe. • (Process #5) systray.exe reads from (process #22) ncftp.exe. • (Process #5) systray.exe reads from (process #23) notepad.exe. • (Process #5) systray.exe reads from (process #24) operamail.exe. • (Process #5) systray.exe reads from (process #25) outlook.exe. • (Process #5) systray.exe reads from (process #26) pidgin.exe. • (Process #5) systray.exe reads from (process #27) scriptftp.exe. • (Process #5) systray.exe reads from (process #28) skype.exe. • (Process #5) systray.exe reads from (process #29) smartftp.exe. • (Process #5) systray.exe reads from (process #30) thunderbird.exe. • (Process #5) systray.exe reads from (process #31) trillian.exe. • (Process #5) systray.exe reads from (process #32) webdrive.exe. • (Process #5) systray.exe reads from (process #33) whatsapp.exe. • (Process #5) systray.exe reads from (process #34) winscp.exe. • (Process #5) systray.exe reads from (process #35) yahoomessenger.exe. • (Process #5) systray.exe reads from (process #36) iexplore.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #2) pkypr.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) pkypr.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory. • (Process #5) systray.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory. • (Process #36) iexplore.exe creates file "\??\C:\Windows\SYSTEM32\ntdll.dll" in the OS directory.			
1/5	Mutex	Creates mutex	4	-
	• (Process #5) systray.exe creates mutex with name "6NON26-3X60UXYXz". • (Process #5) systray.exe creates mutex with name "5M764PD81WX9E20z". • (Process #4) explorer.exe creates mutex with name "S-1-5-21-1560258-193263778575". • (Process #8) iexplore.exe creates mutex with name "S-1-5-21-1560258-14963319274527".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #5) systray.exe adds "C:\Program Files (x86)\Lbxhx9hm\1byd2dsxipq.exe" to Windows startup via registry.			
1/5	Discovery	Possibly does reconnaissance	2	-

Score	Category	Operation	Count	Classification
	• (Process #5) systray.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #5) systray.exe tries to gather information about application "Mozilla Firefox" by file.			
1/5	Network Connection	Performs DNS request	23	-
	• (Process #4) explorer.exe resolves host name "www.palia.world" to IP "34.102.136.180". • (Process #4) explorer.exe resolves host name "www.futternmitflo.com" to IP "192.0.78.25". • (Process #4) explorer.exe resolves host name "www.tenthgenerationtorah.com" to IP "103.224.212.220". • (Process #4) explorer.exe resolves host name "www.toastpack.com" to IP "34.102.136.180". • (Process #4) explorer.exe resolves host name "www.greenlighteams.com" to IP "209.99.64.33". • (Process #4) explorer.exe resolves host name "www.digitalfactoryinstitut.com" to IP "217.70.184.50". • (Process #4) explorer.exe resolves host name "www.protocolohfresco.site" to IP "-". • (Process #4) explorer.exe resolves host name "www.sans-gluten.store" to IP "-". • (Process #4) explorer.exe resolves host name "www.bangkhacollections.com" to IP "3.108.154.143". • (Process #4) explorer.exe resolves host name "www.techkaisimi.com" to IP "70.39.125.244". • (Process #4) explorer.exe resolves host name "www.perstockholm.com" to IP "156.234.16.189". • (Process #4) explorer.exe resolves host name "www.aceites.info" to IP "82.163.176.128". • (Process #4) explorer.exe resolves host name "www.hsf777.com" to IP "23.224.102.249". • (Process #4) explorer.exe resolves host name "www.zhidao95.com" to IP "134.73.225.58". • (Process #4) explorer.exe resolves host name "www.zoommachone.xyz" to IP "85.159.66.93". • (Process #4) explorer.exe resolves host name "www.portres.online" to IP "162.213.255.214". • (Process #4) explorer.exe resolves host name "www.meredithlobrien.com" to IP "34.102.136.180". • (Process #4) explorer.exe resolves host name "www.bulkheadsrestaurantgroup.com" to IP "199.59.243.200". • (Process #4) explorer.exe resolves host name "www.apremotesamsung.com" to IP "103.224.212.222". • (Process #4) explorer.exe resolves host name "www.baigouw.com" to IP "-". • (Process #4) explorer.exe resolves host name "www.bhreselect.com" to IP "34.102.136.180". • (Process #4) explorer.exe resolves host name "www.triumphgroup.xyz" to IP "172.67.210.242". • (Process #4) explorer.exe resolves host name "www.tyrs-it.com" to IP "103.224.212.221".			
1/5	Network Connection	Connects to remote host	17	-
	• (Process #4) explorer.exe opens an outgoing TCP connection to host "3.108.154.143:80". • (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 "23.224.102.249:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "70.39.125.244:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "85.159.66.93:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "103.224.212.222:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "162.213.255.214:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "192.0.78.25:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "156.234.16.189:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "172.67.210.242:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "217.70.184.50:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "134.73.225.58:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "209.99.64.33:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "103.224.212.220:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "103.224.212.221:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "199.59.243.200:80". • (Process #4) explorer.exe opens an outgoing TCP connection to host "82.163.176.128:80".			
1/5	Obfuscation	Overwrites code	3	-

Score	Category	Operation	Count	Classification
	• (Process #36) iexplore.exe overwrites code to possibly hide behavior. • (Process #4) explorer.exe overwrites code to possibly hide behavior. • (Process #8) iexplore.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\pkypr.exe".			
-	Trusted	Known clean file	2	-
	• File "" is a known clean file. • Embedded file "" is a known clean file.			

Malware Configuration: FormBook

Metadata	Key	Extracted Value
Version	Value	4.1
Mission ID	Value	m0d4
URL	Url	www.hsf777.com/m0d4/

Other: Decoy URL	Value	prettyhairdivas.mobi
	Value	cityblocksnft.com
	Value	laraqiiz.com
	Value	mubarakdigitalmedia.com
	Value	perstockholm.com
	Value	xn--imprio-dva.site
	Value	baigouw.com
	Value	support-client-video.com
	Value	phomas.info
	Value	dengedizayn.com
	Value	zoommachone.xyz
	Value	houseoflancasterhours.com
	Value	petarungslot.website
	Value	tyrs-it.com
	Value	dalianzhuchiren.com
	Value	tenthgenerationtorah.com
	Value	portres.online
	Value	1-minute.store
	Value	shikakunazo.com
	Value	veymes.store
	Value	ruvedaj.xyz
	Value	apremotesamsung.com
	Value	palia.world
	Value	you-sayso.com
	Value	nftsofis.com
	Value	arthamandirialkesindo.com
	Value	bangkhacollections.com
	Value	digitalfactoryinstitut.com
	Value	aceites.info
	Value	altcoinwatcher.com
	Value	pearlsofgraceinc.com
	Value	xianzyw.com
	Value	gxclzs.com
	Value	greenlighteams.com
	Value	aavinya.com
	Value	sans-gluten.store
	Value	clanbeware.com
	Value	protocolohfresco.site
	Value	meredithlobrien.com
	Value	cryoablation.xyz
	Value	avicciibook.com
	Value	toastpack.com
	Value	linktosmutgoeshere.com
	Value	38289.xyz
	Value	xn--08s.com
	Value	techkaisimi.com
	Value	jllpx.com
	Value	dubaicarclinic.com
	Value	zhidao95.com
	Value	aletterboxd.com
	Value	warrantyglobe.com
	Value	mindfeed.pro
	Value	bhreselect.com
	Value	sdfijsdjidf.xyz
	Value	russetconstruction.com
	Value	futternmitflo.com
	Value	triumphgroup.xyz

Mitre ATT&CK Matrix

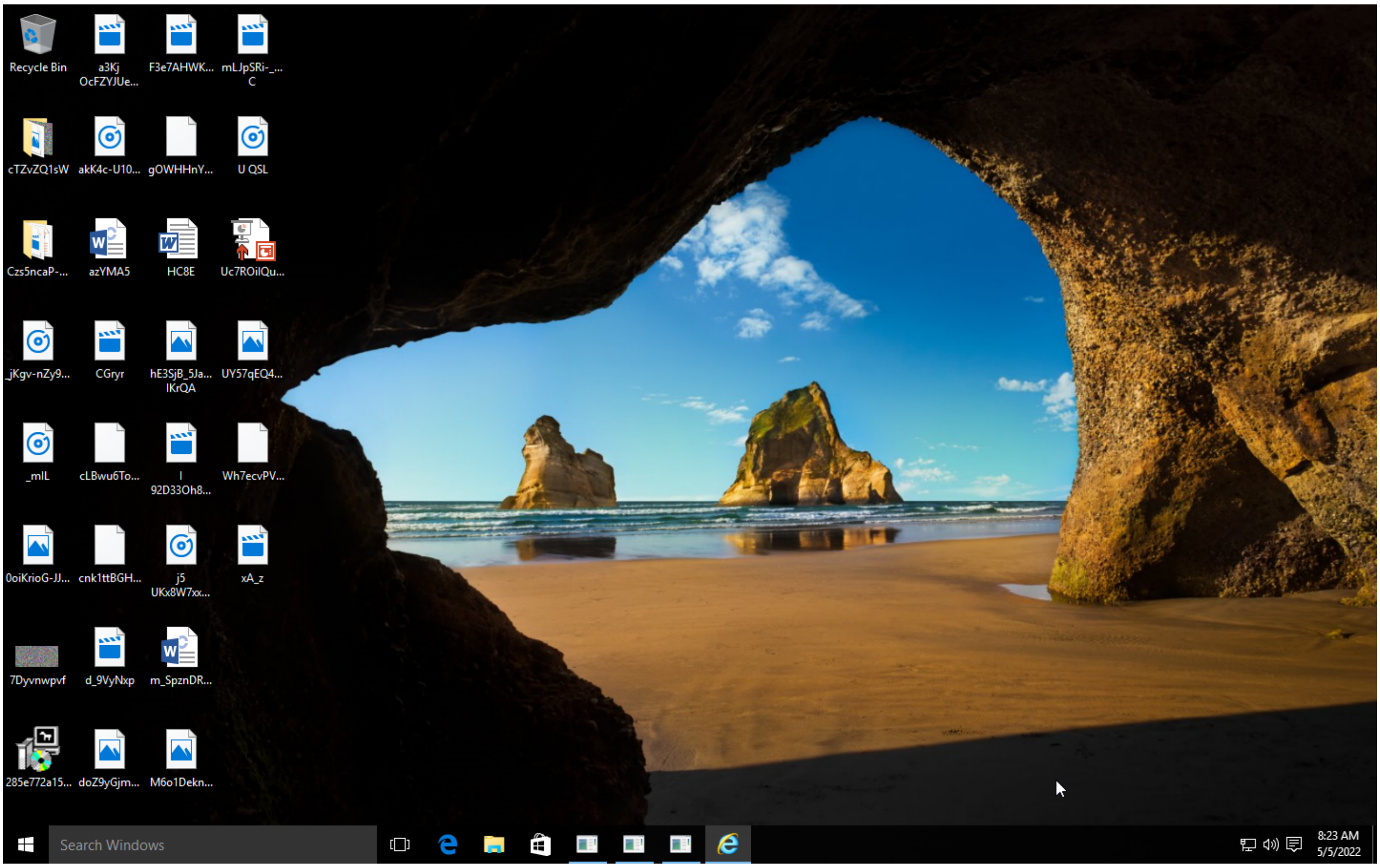
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder	#T1179 Hooking	#T1143 Hidden Window	#T1081 Credentials in Files	#T1012 Query Registry		#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			

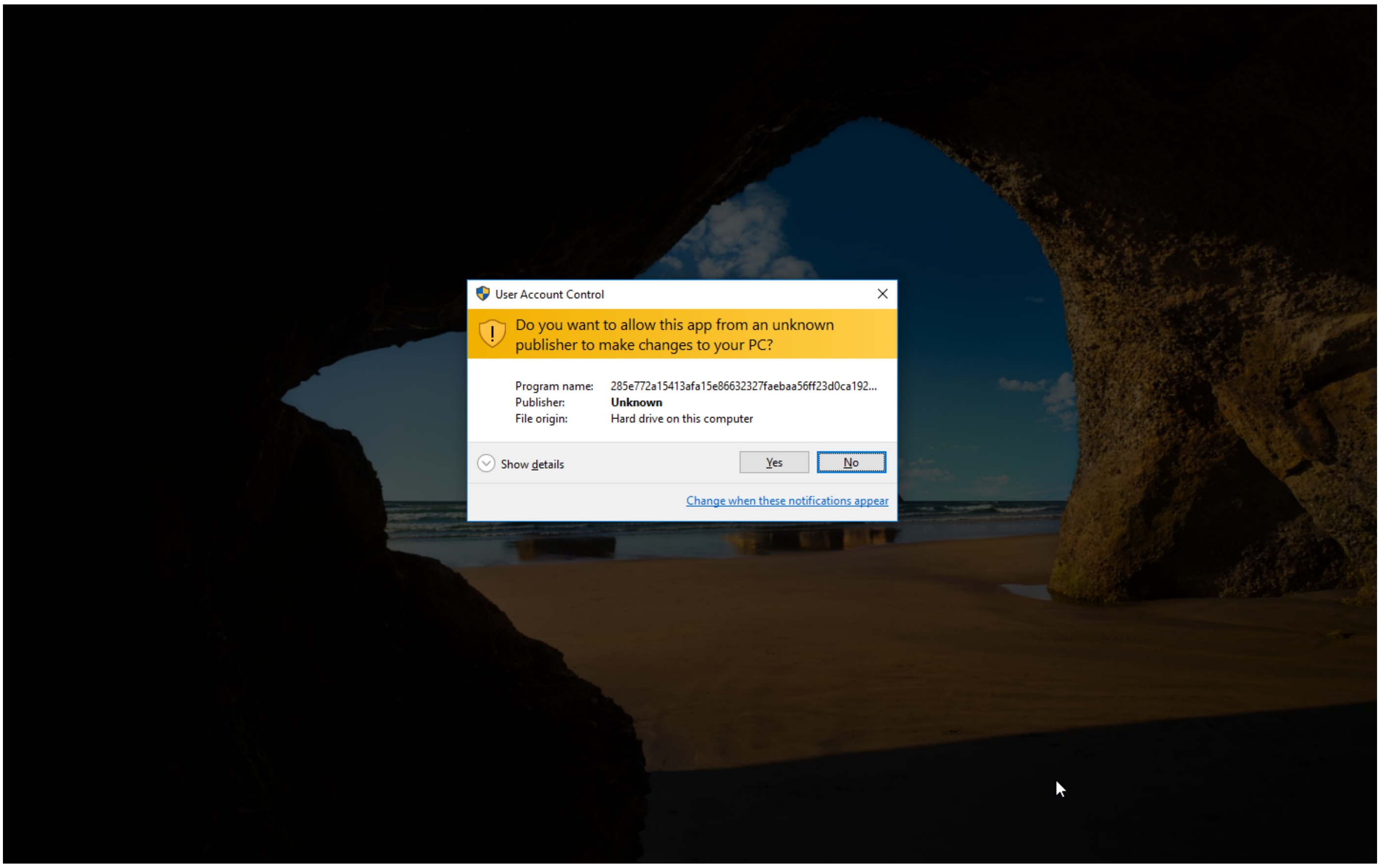
Sample Information

ID	#4264217
MD5	6f111b596da1ac7d71c4362b18309648
SHA1	e09f8065342a4c8664148bec4b0d9265e7e5842a
SHA256	285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96
SSDeep	6144:HNeZmLfHg6+reKq0Uzme51aUUTzC92gBE:HNlLvX+12auAVTzhg+
ImpHash	56a78d55f3f7af51443e58e0ce2fb5f6
File Name	285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe
File Size	214.18 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

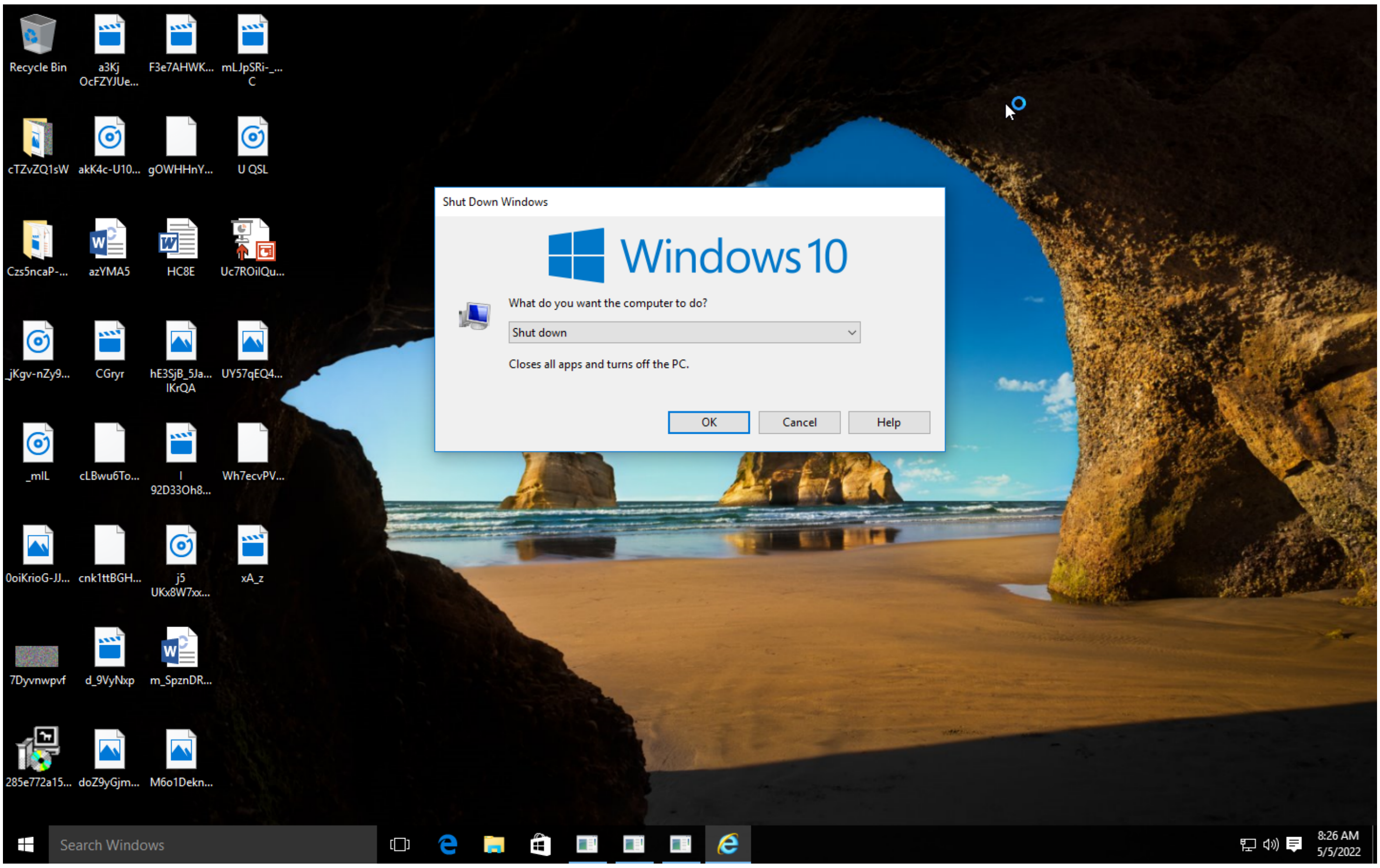
Creation Time	2022-05-05 10:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	35
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified 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	20




User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: 285e772a15413afa15e86632327faebaa56ff23d0ca192...
Publisher: **Unknown**
File origin: Hard drive on this computer



Shut Down Windows

Windows 10

What do you want the computer to do?

Shut down

Closes all apps and turns off the PC.

Screenshots truncated

NETWORK

General

12.39 KB total sent

48.36 KB total received

4 ports 80, 139, 53, 445

18 contacted IP addresses

29 URLs extracted

9 files downloaded

0 malicious hosts detected

DNS

28 DNS requests for 23 domains

1 nameservers contacted

7 total requests returned errors

HTTP/S

20 URLs contacted, 17 servers

1 sessions, 10.68 KB sent, 46.66 KB received

HTTP Requests

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://greenlighteams.com	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/Free_Credit_Report.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FH... ...As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=11539660&ktd=0&kld=1061&kp=2	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/song_lyrics.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHUo77fol... ...As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=26527269&ktd=0&kld=1061&kp=7	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/px.js?ch=2	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/sk-privacy.php	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/display.cfm	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/Best_Mortgage_Rates.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2F... ...hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=3477850&ktd=0&kld=1061&kp=6	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/sk-logabpstatus.php?a=MkcyNnhMa3RleU5FdWpNTEtGbXhuNHNGMlFNeXUxOHN3V25QUFFJdkw0ZlBxRU9XQldOUnpUWTBTRDBGNlVPblQvMGZrZndBeHcyWjhmcWJaZ3F0eDdJWEk1am9FcVlFVGROZ2RKTVladG5vZ0JVU2d4dTkvemFCek5Jdlp3S3Y=&b=	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.greenlighteams.com/10_Best_Mutual_Funds.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2......cmhAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=72996&ktd=0&kld=1061&kp=3	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/fashion_trends.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHUo77......As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=10542279&ktd=0&kld=1061&kp=4	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/Credit_Card_Application.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rd......hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=7242435&ktd=0&kld=1061&kp=5	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/px.js?ch=1	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/Best_Penny_Stocks.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHU......hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=3482138&ktd=0&kld=1061&kp=1	-	-		0 bytes	NA
GET	http://www.perstockholm.com/m0d4/?VrPHWV=O8Yh2h6&AL08=7XWYUFyABOVdAnpCCqlHgoLhtNBn8sw1plAzqMSF02fZrSrsWz8Q9PBCcJLz0Y4XBbh2Pg==	-	-		0 bytes	NA
GET	http://www.futternmitflo.com/m0d4/?VrPHWV=O8Yh2h6&AL08=hu5YyLRdsgKsg3JM32LgsQICUIcoZL968qMFJRjRR5TUyFTxWRvlKvb31X9wP6YGmle9CA==	-	-		0 bytes	NA
GET	http://www.aceites.info/m0d4/?AL08=TbollzpT9rXeZ91U9wlhpx+nZxEa9zONUu6oxAitLGSU2Wdu93eLhJ7o42pW1H17q81Ltg==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.apremotesamsung.com/m0d4/?VrPHWV=O8Yh2h6&AL08=hUVgbolmL0sCt7LaC3NHw8YP+GPS1BdzeLBlZXKVOXmYliZu5gDV6Bh8///TuT3X9hKJEw==	-	-		0 bytes	NA
GET	http://www.meredithlobrien.com/m0d4/?VrPHWV=O8Yh2h6&AL08=46O1sEyR4/wvH+bLwVUeRrKpxvMq4OD5F1CZbWpFi2lfYASfWdQWFwztdAKhmRJ+qi5Ayg==	-	-		0 bytes	NA
GET	http://www.techkaisimi.com/m0d4/?AL08=b0hNo1faq5o0ibq11tSUAJ1i6UzM7c/b3lNITCAxF7SArJmPdEQu3/RrFLto8yLoO0cRIQ==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.toastpack.com/m0d4/?AL08=C0FyLQDmOvxjZakspQ6bMYY13TbPn/9qf9RMzvcwLb2Zn1gZl3lQfiJU9Qg6oJU7QnfBxw==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.digitalfactoryinstitut.com/m0d4/?AL08=c08ZTacAukQC5NeLWtuBWKo+UaWFOcWy6CEiHhedBNHZ3tXeC1VbOKb5CJ1Nxja24KM0Hg==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.tyrs-it.com/m0d4/?AL08=EfBAPrIixbPMIKHauOAocozOgBY3ZNEx1t1yXENDBN/Y9A0rELwXOOj/ARjpOVLCDnmCVg==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.tenthgenerationtorah.com/m0d4/?AL08=mGlUdW2Hhm2PG3zh9JwTEQVxirr1ywQmw3qGssNmbrB1xVceB7WEhF7r3Lqhy6k1kXdJdA==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.zoommachone.xyz/m0d4/?AL08=/qzckqtyCc8rrPOLAqXCRRIw/xaz6fwoS3VigV0+3PEnE62ghz0EbMW68KNNy8Z877lwzg==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.palia.world/m0d4/?AL08=NmHDKYpLtOaunO6yJwQt7bjBEDSMmb6uyC2Rdc4sC+38r/w1LF5LwewBdTfUGNSbbzrJiw==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.hsf777.com/m0d4/?AL08=7Xa4BbX+EF+0bOKfkWo9GY8TeBGxHEZixmbVHdNSFZSwo63rM1BfaWFzyWRopavNogmBAQ==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.bhreselect.com/m0d4/?AL08=D3Y0Pm5nPVru/us5CxwPidK6v62Fiqkg7A+JactShsSyS/ES72bWbDUd0/Tx/17x61cBJA==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.zhidao95.com/m0d4/?VrPHWV=O8Yh2h6&AL08=NAAVMffTY9s/9fH8R/zh9xXRUU+fA/5gjMZ7rGtT7+HDshSMwhe2Brbhhu7bulHK1waO+A==	-	-		0 bytes	NA
GET	http://www.portres.online/m0d4/?AL08=5QX2iLt+pw2MYMDUfTIweWLkahJ87DwyoOP3aWzqgiacXlFD4ogajsqjANYZwMbPyx7TGQ==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.bulkheadsrestaurantgroup.com/m0d4/?VrPHWV=O8Yh2h6&AL08=ihChw7NkvHHnp4ehDSAv07TGAws7cYloqo91uq/CHYSLKFZDBb5B+puRdm5bVlmhTydU0w==	-	-		0 bytes	NA
GET	http://www.triumphgroup.xyz/m0d4/?AL08=99EE7/YJ7QYJ6gl7lR9e36EGMnrjjpKCX93zWfmkIY/R6ohvJ2OXPesLVXdNj3uSa3MFgA==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	http://www.greenlighteams.com/m0d4/?AL08=/cmhAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY/waXB8iQoULo0f16dJ4RZxCoSOnHg0Igg==&VrPHWV=O8Yh2h6	-	-		0 bytes	NA
GET	http://www.bangkhacollections.com/m0d4/?AL08=a0iJBX+S++1VW5Q9alJjR6oBYSdMg74u/0Xh/v7LWInF5XrfrQ4uI5t2H6z+dJOBGxTNhw==&FX10rv=UL00qTmpnvW	-	-		0 bytes	NA
GET	https://parking.bodiscdn.com	-	-		0 bytes	NA
GET	https://shop.gandi.net/en/domain/suggest?search=digitalfactoryinstitut.com&source=parking	-	-		0 bytes	NA
GET	https://shop.gandi.net/en/domain/transfer	-	-		0 bytes	NA
GET	https://shop.gandi.net/en	-	-		0 bytes	NA
GET	https://www.google.com	-	-		0 bytes	NA
GET	https://news.gandi.net/en	-	-		0 bytes	NA
GET	https://help.gandi.net/en	-	-		0 bytes	NA
GET	https://www.gandi.net/en/domain	-	-		0 bytes	NA
GET	https://www.gandi.net/en/security	-	-		0 bytes	NA
GET	https://www.gandi.net/en/cloud	-	-		0 bytes	NA
GET	https://www.gandi.net/en	-	-		0 bytes	NA
GET	https://www.gandi.net/en/simple-hosting	-	-		0 bytes	NA
GET	https://fonts.googleapis.com	-	-		0 bytes	NA
GET	https://whois.gandi.net/en/results?search=digitalfactoryinstitut.com	-	-		0 bytes	NA

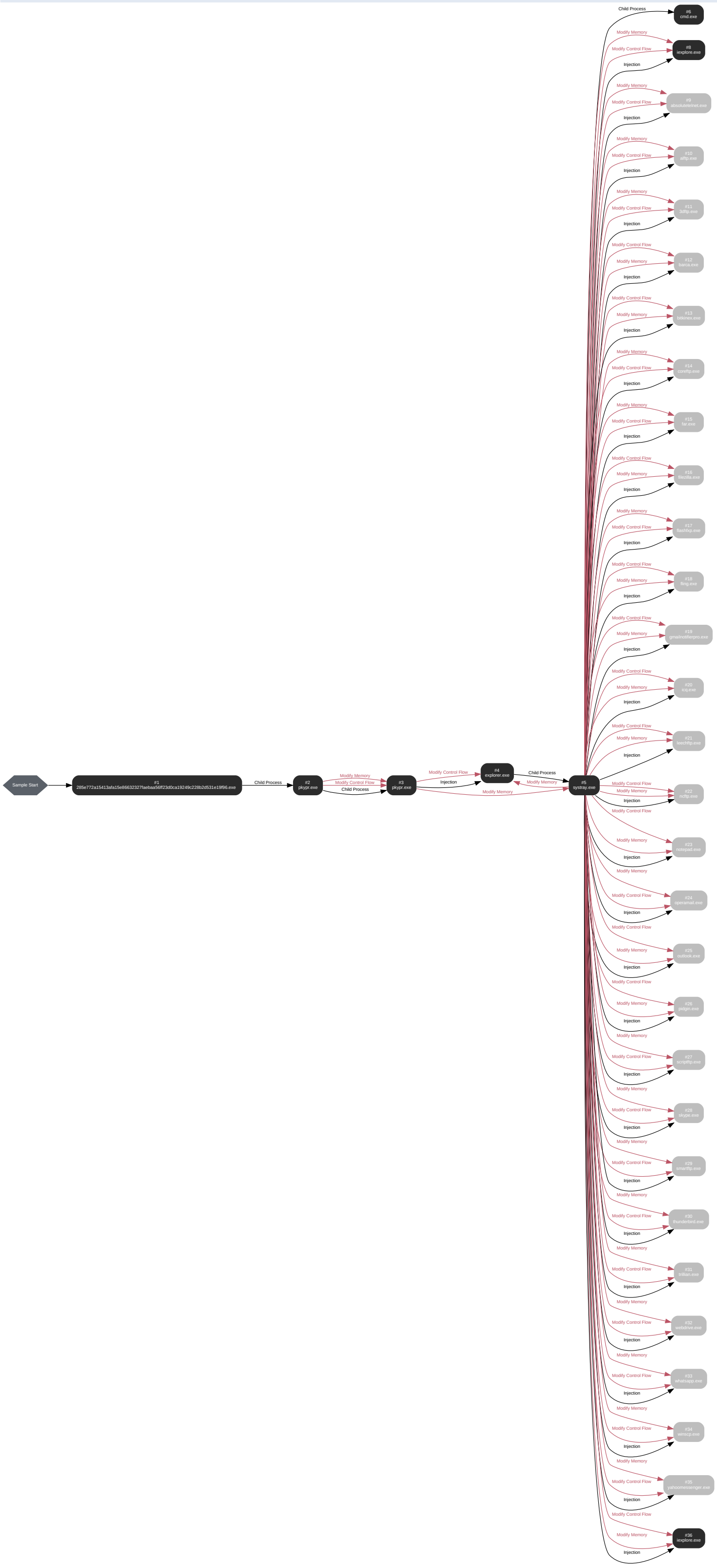
DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.baigouw.com	-			NA
A	www.palia.world, palia.world	NO_ERROR	34.102.136.180	palia.world	NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.futternmitflo.com, futternmitflo.com	NO_ERROR	192.0.78.25, 192.0.78.24	futternmitflo.com	NA
A	www.tenthgenerationtorah.com	NO_ERROR	103.224.212.220		NA
A	www.toastpack.com, toastpack.com	NO_ERROR	34.102.136.180	toastpack.com	NA
A	www.greenlighteams.com	NO_ERROR	209.99.64.33		NA
A	www.digitalfactoryinstitut.com, webredir.vip.gandi.net	NO_ERROR	217.70.184.50	webredir.vip.gandi.net	NA
A	www.protocolohfresco.site	NX_DOMAIN			NA
A	www.sans-gluten.store	NX_DOMAIN			NA
A	www.bangkhacollections.com	NO_ERROR	3.108.154.143		NA
A	www.techkaisimi.com, parking.namesilo.com	NO_ERROR	70.39.125.244, 64.32.22.102, 107.161.23.204, 209.141.38.71, 45.58.190.82, 168.235.88.209, 204.188.203.155, 192.161.187.200, 198.251.84.92, 198.251.81.30	parking.namesilo.com	NA
A	www.perstockholm.com	NO_ERROR	156.234.16.189		NA
A	www.aceites.info, aceites.info	NO_ERROR	82.163.176.128	aceites.info	NA
A	www.hsf777.com	NO_ERROR	23.224.102.249		NA
A	www.zhidao95.com	NO_ERROR	134.73.225.58		NA
A	www.zoommachone.xyz, redirect.natrocdn.com, natroredirect.natrocdn.com	NO_ERROR	85.159.66.93	redirect.natrocdn.com, natroredirect.natrocdn.com	NA
A	www.portres.online	NO_ERROR	162.213.255.214		NA
A	www.meredithlobrien.com, meredithlobrien.com	NO_ERROR	34.102.136.180	meredithlobrien.com	NA
A	www.bulkheadsrestaurantgroup.com	NO_ERROR	199.59.243.200		NA
A	www.apremotesamsung.com	NO_ERROR	103.224.212.222		NA
A	www.bhreselect.com, bhreselect.com	NO_ERROR	34.102.136.180	bhreselect.com	NA
A	www.triumphgroup.xyz	NO_ERROR	172.67.210.242, 104.21.77.185		NA
A	www.tyrs-it.com	NO_ERROR	103.224.212.221		NA

BEHAVIOR

Process Graph



Process #1: 285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 78882, Reason: Analysis Target
Unmonitor End Time	End Time: 119344, Reason: Terminated
Monitor duration	40.46s
Return Code	0
PID	2104
Parent PID	1932
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca	4.85 KB	1fbfc239148369ed5bd7713e21cf351a45f784cb79c71ec101cf31b037f58e9c	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\ow7v8lrfalu0lz3762	185.00 KB	f11f0f6d81d98dd389b02d946fe8273591ade4b3c7a6da29820449eb392186fe	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nstC98.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsa582.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
File	158
System	50
Module	26
Process	1

Process #2: pkypr.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 115011, Reason: Child Process
Unmonitor End Time	End Time: 119420, Reason: Terminated
Monitor duration	4.41s
Return Code	0
PID	3236
Parent PID	2104
Bitness	32 Bit

Host Behavior

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

Process #3: pkypr.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 117245, Reason: Child Process
Unmonitor End Time	End Time: 129171, Reason: Terminated
Monitor duration	11.93s
Return Code	0
PID	1616
Parent PID	3236
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\pkypr.exe	0x79c	0x400000(4194304)	0x200	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x79c	0x401000(4198400)	0x2d200	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x79c	0x37b008(3649544)	0x4	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x79c / 0x84	0x778a8fe0(2005569504)	-	✔	1

Host Behavior

Type	Count
System	5
Module	14
Process	6
-	8
File	10
-	3
User	1
-	1
-	1
Environment	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: 120393, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	201.95s
Return Code	Unknown
PID	1932
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\pkypr.exe	0x84	0x4e60000(82182144)	0xbf000	✔	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x84 / 0x790	0x4e7ddd9(82304473)	-	✔	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x84 / 0x790	0xcf648(849480)	-	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x120e0000(302907392)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x8260000(136708096)	0xdc000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x790	0xcfa98(850584)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x790	0x82b6dc2(137063874)	-	✔	1

Dropped Files (13)

File Name	File Size	SHA256	YARA Match
-	1.84 KB	8bafaef8f597d230d4ea25c648aaa2e1084b23a2767e9080a683e5d1809c327a	✖
-	206.50 KB	95470a8814917743eb95d5d989214e22fa20ac6512f0269af500560e8365e847	✖
-	910 bytes	e92552d87801e9701344738ed5a7cf6a1b33c55aa9ecebd29d68343bd3e716aa	✖
-	207.54 KB	8900ae8d1e0f2a1e2d8d8c086c5e362c25e4bf6a678b7e34d558ccd7df6dd76d	✖
-	210.50 KB	3d4aa9e06c956b9bb055bb3b94dceaedf97f9428ba5b7771ed8e73976553fad4	✖
-	1.11 KB	9203aed488797efdeef726a3d0ea865c2a0d53783abc6f12967f3e3d5078919b	✖
-	1.49 KB	1ce1c693075e9ff018bb82c5b5d644e773648194773b59d3f6d85d2420b192aa	✖
-	2.56 KB	2d3c9cc4880e5a8d8bb583c6be6f5826de19291405734ec9e3899eaee78e431a	✖

File Name	File Size	SHA256	YARA Match
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logim.jpeg	137.05 KB	957721a37f4c25b42bf710e139d46655a7b3c37ee6f2076c52bd7e13df7d34f1	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrv.ini	40 bytes	6eebf968962745b2e9de2ca969af7c424916d4e3fe3cc0bb9b3d414abfce9507	✖
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Lbxhx9hm\1byd2dsxipq.exe	5.00 KB	99b049d5615612c79da226823c3b8d173e66e73bb1c99d0215282274685162ed	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrc.ini	1.75 KB	3f20b4605a2a543557ff9f208c286aef88fd05200f0c6150d35f1402507bd228	✖
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logri.ini	40 bytes	eaece2eba6310253249603033c744dd5914089b0bb26bde6685ec9813611baae	✖

Host Behavior

Type	Count
System	8847
File	358
-	25
Mutex	1
COM	1
Process	1
Module	3

Network Behavior

Type	Count
HTTP	27
DNS	23
TCP	26

Process #5: systray.exe

ID	5
File Name	c:\windows\syswow64\systray.exe
Command Line	"C:\Windows\SysWOW64\systray.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 124724, Reason: Child Process
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	197.62s
Return Code	Unknown
PID	884
Parent PID	1932
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\pkypr.exe	0x84	0x110000(1114112)	0x2f000	✔	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\pkypr.exe	0x84	0x1020000(16908288)	0x6000	✔	1

Dropped Files (1)

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

Host Behavior

Type	Count
System	1881
File	272
-	153
Module	162
Process	93
Registry	150
-	28
-	1
Mutex	2
COM	1
-	1
User	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\pkypr.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 132097, Reason: Child Process
Unmonitor End Time	End Time: 137725, Reason: Terminated
Monitor duration	5.63s
Return Code	0
PID	1584
Parent PID	884
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe	5.00 KB	99b049d5615612c79da226823c3b8d173e66e73bb1c99d0215282274685162ed	✖

Host Behavior

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

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: 149577, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	172.76s
Return Code	Unknown
PID	1496
Parent PID	884
Bitness	64 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x6750000(108331008)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x600000(6291456)	0xe0000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x7b4	0x8daa8f38(2376765240)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x7b4	0x65adc2(6663618)	-	✔	1

Host Behavior

Type	Count
-	3
Mutex	1

Process #9: absolutetelnet.exe

ID	9
File Name	c:\program files (x86)\msbuild\absolutetelnet.exe
Command Line	"C:\Program Files (x86)\MSBuild\absolutetelnet.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 161414, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	160.93s
Return Code	Unknown
PID	3216
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2150000(34930688)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x1f60000(32899072)	0x1ac000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xc84	0x2078707(34047751)	-	✔	1

Process #10: alftp.exe

ID	10
File Name	c:\program files\windows portable devices\alftp.exe
Command Line	"C:\Program Files\Windows Portable Devices\alftp.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 166881, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	155.46s
Return Code	Unknown
PID	564
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2420000(37879808)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x5c0000(6029312)	0xf8000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x27c	0x624707(6440711)	-	✔	1

Process #11: 3dftp.exe

ID	11
File Name	c:\program files (x86)\windowspowershell\3dftp.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\3dftp.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 167199, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	155.14s
Return Code	Unknown
PID	560
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2740000(41156608)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0xc60000(12976128)	0x146000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xc7c	0xd12707(13707015)	-	✔	1

Process #12: barca.exe

ID	12
File Name	c:\program files (x86)\windows defender\barca.exe
Command Line	"C:\Program Files (x86)\Windows Defender\barca.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 167282, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	155.06s
Return Code	Unknown
PID	968
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x21a0000(35258368)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x600000(6291456)	0xfb000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x378	0x667707(6715143)	-	✔	1

Process #13: bitkinex.exe

ID	13
File Name	c:\program files\windows multimedia platform\bitkinex.exe
Command Line	"C:\Program Files\Windows Multimedia Platform\bitkinex.exe"
Initial Working Directory	C:\Program Files\Windows Multimedia Platform\
Monitor Start Time	Start Time: 167370, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.97s
Return Code	Unknown
PID	3532
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2160000(34996224)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2b30000(45285376)	0x1a4000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x50c	0x2c40707(46401287)	-	✔	1

Process #14: coreftp.exe

ID	14
File Name	c:\program files\internet explorer\coreftp.exe
Command Line	"C:\Program Files\Internet Explorer\coreftp.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 167643, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.70s
Return Code	Unknown
PID	3176
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2320000(36831232)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x5f0000(6225920)	0xda000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xc24	0x636707(6514439)	-	✔	1

Process #15: far.exe

ID	15
File Name	c:\program files\windows portable devices\far.exe
Command Line	"C:\Program Files\Windows Portable Devices\far.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 167725, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.61s
Return Code	Unknown
PID	2980
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x1ff0000(33488896)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x29c0000(43778048)	0x1a8000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xb9c	0x2ad4707(44910343)	-	✔	1

Process #16: filezilla.exe

ID	16
File Name	c:\program files\windowspowershell\filezilla.exe
Command Line	"C:\Program Files\WindowsPowerShell\filezilla.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 167886, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.45s
Return Code	Unknown
PID	2780
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x23e0000(37617664)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2220000(35782656)	0x145000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xda8	0x22d1707(36509447)	-	✔	1

Process #17: flashfxp.exe

ID	17
File Name	c:\program files\msbuild\flashfxp.exe
Command Line	"C:\Program Files\MSBuild\flashfxp.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 168042, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.30s
Return Code	Unknown
PID	1676
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x20b0000(34275328)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2a80000(44564480)	0x157000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xf40	0x2b43707(45364999)	-	✔	1

Process #18: fling.exe

ID	18
File Name	c:\program files (x86)\internet explorer\fling.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\fling.exe"
Initial Working Directory	C:\Program Files (x86)\Internet Explorer\
Monitor Start Time	Start Time: 168150, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.19s
Return Code	Unknown
PID	2204
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x20d0000(34406400)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x510000(5308416)	0x162000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xb94	0x5de707(6153991)	-	✔	1

Process #19: gmailnotifierpro.exe

ID	19
File Name	c:\program files (x86)\microsoft office\gmailnotifierpro.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\gmailnotifierpro.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 168274, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	154.06s
Return Code	Unknown
PID	3004
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2220000(35782656)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2040000(33816576)	0x12f000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x424	0x20db707(34453255)	-	✔	1

Process #20: icq.exe

ID	20
File Name	c:\program files\windows defender\icq.exe
Command Line	"C:\Program Files\Windows Defender\icq.exe"
Initial Working Directory	C:\Program Files\Windows Defender\
Monitor Start Time	Start Time: 168726, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	153.61s
Return Code	Unknown
PID	2508
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2620000(39976960)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0xbb0000(12255232)	0x14d000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x30c	0xc69707(13014791)	-	✔	1

Process #21: leechftp.exe

ID	21
File Name	c:\program files (x86)\msbuild\leechftp.exe
Command Line	"C:\Program Files (x86)\MSBuild\leechftp.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 168984, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	153.35s
Return Code	Unknown
PID	3792
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x20c0000(34340864)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2a90000(44630016)	0x156000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xec	0x2b52707(45426439)	-	✔	1

Process #22: ncftp.exe

ID	22
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: 169093, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	153.25s
Return Code	Unknown
PID	2576
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x21c0000(35389440)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x6c0000(7077888)	0xe8000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xeec	0x714707(7423751)	-	✔	1

Process #23: notepad.exe

ID	23
File Name	c:\program files\windows portable devices\notepad.exe
Command Line	"C:\Program Files\Windows Portable Devices\notepad.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 169407, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	152.93s
Return Code	Unknown
PID	4004
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2190000(35192832)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2b60000(45481984)	0x189000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xfa0	0x2c55707(46487303)	-	✔	1

Process #24: operamail.exe

ID	24
File Name	c:\program files (x86)\windowspowershell\operamail.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\operamail.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 169937, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	152.40s
Return Code	Unknown
PID	2580
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x26d0000(40697856)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0xc20000(12713984)	0x11a000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0xc2c	0xca6707(13264647)	-	✔	1

Process #25: outlook.exe

ID	25
File Name	c:\program files (x86)\microsoft office\outlook.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\outlook.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 170055, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	152.28s
Return Code	Unknown
PID	4008
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x21c0000(35389440)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x600000(6291456)	0x106000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x888	0x672707(6760199)	-	✔	1

Process #26: pidgin.exe

ID	26
File Name	c:\program files\windows sidebar\pidgin.exe
Command Line	"C:\Program Files\Windows Sidebar\pidgin.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 170256, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	152.08s
Return Code	Unknown
PID	4104
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2100000(34603008)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x5f0000(6225920)	0xbf000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x100c	0x61b707(6403847)	-	✔	1

Process #27: scriptftp.exe

ID	27
File Name	c:\program files\reference assemblies\scriptftp.exe
Command Line	"C:\Program Files\Reference Assemblies\scriptftp.exe"
Initial Working Directory	C:\Program Files\Reference Assemblies\
Monitor Start Time	Start Time: 170412, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	151.93s
Return Code	Unknown
PID	4112
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x21a0000(35258368)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x5e0000(6160384)	0x17c000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1014	0x6c8707(7112455)	-	✔	1

Process #28: skype.exe

ID	28
File Name	c:\program files\windows portable devices\skype.exe
Command Line	"C:\Program Files\Windows Portable Devices\skype.exe"
Initial Working Directory	C:\Program Files\Windows Portable Devices\
Monitor Start Time	Start Time: 170614, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	151.72s
Return Code	Unknown
PID	4124
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2110000(34668544)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2ae0000(44957696)	0x1a6000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1020	0x2bf2707(46081799)	-	✔	1

Process #29: smartftp.exe

ID	29
File Name	c:\program files\windows photo viewer\smartftp.exe
Command Line	"C:\Program Files\Windows Photo Viewer\smartftp.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 171043, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	151.30s
Return Code	Unknown
PID	4132
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2050000(33882112)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x640000(6553600)	0xbb000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1028	0x667707(6715143)	-	✔	1

Process #30: thunderbird.exe

ID	30
File Name	c:\program files (x86)\microsoft office\thunderbird.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\thunderbird.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 171089, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	151.25s
Return Code	Unknown
PID	4148
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x27d0000(41746432)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0xc10000(12648448)	0x163000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1038	0xcdf707(13498119)	-	✔	1

Process #31: trillian.exe

ID	31
File Name	c:\program files\windowspowershell\trillian.exe
Command Line	"C:\Program Files\WindowsPowerShell\trillian.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 171229, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	151.11s
Return Code	Unknown
PID	4156
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2010000(33619968)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x29e0000(43909120)	0x199000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1040	0x2ae5707(44979975)	-	✔	1

Process #32: webdrive.exe

ID	32
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: 171481, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	150.86s
Return Code	Unknown
PID	4172
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2170000(35061760)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2b40000(45350912)	0x156000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1050	0x2c02707(46147335)	-	✔	1

Process #33: whatsapp.exe

ID	33
File Name	c:\program files\msbuild\whatsapp.exe
Command Line	"C:\Program Files\MSBuild\whatsapp.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 171582, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	150.76s
Return Code	Unknown
PID	4180
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2140000(34865152)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x6f0000(7274496)	0xc6000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1058	0x722707(7481095)	-	✔	1

Process #34: winscp.exe

ID	34
File Name	c:\program files\windowspowershell\winscp.exe
Command Line	"C:\Program Files\WindowsPowerShell\winscp.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 171875, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	150.46s
Return Code	Unknown
PID	4196
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2410000(37814272)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x6d0000(7143424)	0xd2000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1068	0x70e707(7399175)	-	✔	1

Process #35: yahoomessenger.exe

ID	35
File Name	c:\program files (x86)\windows defender\yahoomessenger.exe
Command Line	"C:\Program Files (x86)\Windows Defender\yahoomessenger.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 172313, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	150.03s
Return Code	Unknown
PID	4204
Parent PID	884
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2120000(34734080)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x2af0000(45023232)	0x138000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1070	0x2b94707(45696775)	-	✔	1

Process #36: iexplore.exe

ID	36
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:1496 CREDAT:82945 /prefetch:2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 172868, Reason: Injection
Unmonitor End Time	End Time: 322339, Reason: Terminated by timeout
Monitor duration	149.47s
Return Code	Unknown
PID	4452
Parent PID	884
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x8ff0000(150929408)	0x9c4000	✔	1
Modify Memory	#5: c:\windows\syswow64\systray.exe	0x38c	0x99c0000(161218560)	0x14d000	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1168	0x9a79707(161978119)	-	✔	1
Modify Control Flow	#5: c:\windows\syswow64\systray.exe	0x38c / 0x1168	0x9a7970c(161978124)	-	✔	1

Host Behavior

Type	Count
Module	2
File	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96	C:\Users\RDhJ0CNFevzX\Desktop\285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe	Sample File	214.18 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
99b049d5615612c79da226823c3b8d173e66e73bb1c99d0215282274685162ed	C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe, \??\C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe, \??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Lbxhx9hm\1byd2dsxipq.exe	Dropped File	5.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
8bafaef8f597d230d4ea25c648aaa2e1084b23a2767e9080a683e5d1809c327a	-	Dropped File	1.84 KB	application/x-ms-shortcut	-	CLEAN
1fbfc239148369ed5bd7713e21cf351a45f784cb79c71ec101cf31b037f58e9c	C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca	Dropped File	4.85 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
95470a8814917743eb95d5d989214e22fa20ac6512f0269af500560e8365e847	-	Dropped File	206.50 KB	application/CDFV2	-	CLEAN
e92552d87801e9701344738ed5a7cf6a1b33c55aa9ecebd29d68343bd3e716aa	-	Dropped File	910 bytes	application/x-ms-shortcut	-	CLEAN
9e17cb15dd75bbbd5dbb984eda674863c3b10ab72613cf8a39a00c3e11a8492a	-	Downloaded File	162 bytes	text/html	-	CLEAN
63c0faa4e7a7b6cfd750c341829503f4412e6b46c01b31a7daf3a75e75476a54	-	Modified File	40.50 KB	application/CDFV2	-	CLEAN
8900ae8d1e0f2a1e2d8d8c086c5e362c25e4bf6a678b7e34d558ccd7df6dd76d	-	Dropped File	207.54 KB	application/CDFV2	-	CLEAN
3d4aa9e06c956b9bb055bb3b94dceaedf97f9428ba5b7771ed8e73976553fad4	-	Dropped File	210.50 KB	application/CDFV2	-	CLEAN
9203aed488797efdeef726a3d0ea865c2a0d53783abc6f12967f3e3d5078919b	-	Dropped File	1.11 KB	application/x-ms-shortcut	-	CLEAN
95e1144ae5faba1d6ea1ac58b29b1e8d0399125e4dbc6a17d50d0bf5cf3bdcf8	-	Downloaded File	194 bytes	text/html	-	CLEAN
1ce1c693075e9ff018bb82c5b5d644e773648194773b59d3f6d85d2420b192aa	-	Dropped File	1.49 KB	application/x-ms-shortcut	-	CLEAN
348da1db9ef660ed6dfc81f4656eacdb58af04bedbb206d3acb1804cb197cb33	-	Downloaded File	1.83 KB	text/html	-	CLEAN
2d3c9cc4880e5a8d8bb583c6be6f5826de19291405734ec9e3899eaee78e431a	-	Dropped File	2.56 KB	image/png	-	CLEAN
957721a37f4c25b42bf710e139d46655a7b3c37ee6f2076c52bd7e13df7d34f1	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logim.jpeg	Dropped File	137.05 KB	image/jpeg	Access, Create	CLEAN
3eb8165a0647b8408bb41cc7414f0c46b7da04bfff19447259b1719350013d5c	-	Downloaded File	291 bytes	text/html	-	CLEAN
20c1ab602462b7fc0d5b4cbd555cacf127b69a07a737579598ebcbc0f5b21319	-	Downloaded File	154 bytes	text/html	-	CLEAN
92972ae04dac1589bd3cb88fb591c1c4f616867532c9189150aee36dd2646e48	-	Downloaded File	1.44 KB	text/html	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6eebf968962745b2e9de2ca969af7c424916d4e3fe3cc0bb9b3d414abfce9507	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrv.ini	Dropped File	40 bytes	application/octet-stream	Access, Create	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
ab2cf504d95e65a06ce4943e83a787a00bdecb29d8fd61eaff77ec9988b73b6a	-	Downloaded File	280 bytes	text/html	-	CLEAN
3f20b4605a2a543557ff9f208c286aef88fd05200f0c6150d35f1402507bd228	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrc.ini	Dropped File	1.75 KB	application/octet-stream	Access, Create	CLEAN
f11f0f6d81d98dd389b02d946fe8273591ade4b3c7a6da29820449eb392186fe	C:\Users\RDHJ0C~1\AppData\Local\Temp\ow7v8lrfalu0lz3762	Dropped File	185.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
eaece2eba6310253249603033c744dd5914089b0bb26bde6685ec9813611baae	\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logri.ini	Dropped File	40 bytes	application/octet-stream	Access, Create	CLEAN
3b8c6e924abc18a45ee0ae926fffc0f7a0d8d4a423b7b603d9a142d121ff4588	-	Downloaded File	2.74 KB	text/html	-	CLEAN
55e2034c4a03749681ec12bf8c8b276bab78ca3586de47bdcdf2857854b23550	-	Modified File	40.50 KB	application/CDFV2	-	CLEAN
43e50400a46a0e100e2c19e20865d9099b4c0e2d12cafb8bc05dfb0592723838	-	Modified File	40.50 KB	application/CDFV2	-	CLEAN
15994fd5a549a296805c44f96216246c7869abd95683e11bb9ed05e8f8e57f81	-	Downloaded File	22.09 KB	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logro.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrg.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logri.ini	Dropped File, Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logri.ini	Accessed File	Access, Create, Write	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Lbxhx9hm\1byd2dsxipq.exe	Dropped File, Accessed File	Access, Write	CLEAN
C:\Program Files (x86)\Lbxhx9hm	-	-	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nstC98.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Modified File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\ieojvsu2 bi.lnk	Dropped File	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Temp\pkypr.exe	Accessed File	Access, Create	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access, Create	CLEAN
C:\	Accessed File	Access	CLEAN
C:\Program Files (x86)\Lbxhx9hm\1byd2dsxipq.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrm.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe	Accessed File	Access, Create, Read	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\5f7b5f1e01b83767.automaticdestinations-ms	Dropped File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\actioncentercache\{d05fbdb7-f67b-4089-8ea6-b3e4425bd309}.png	Dropped File	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7log.ini	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrt.ini	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\Lbxhx9hm	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\5m764pd8\5m7log.ini	Dropped File, Not Extracted	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\ow7v8lrfalu0lz3762	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrc.ini	Dropped File, Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\2dax7o1.lnk	Dropped File	-	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrc.ini	Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrf.ini	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\Lbxhx9hm	Accessed File	Access, Create	CLEAN
\??\C:\Program Files (x86)\Lbxhx9hm\1byd2dsxipq.exe	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\clxo0zgwz.lnk	Dropped File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Access, Create	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\1v-d31nt1cxd0.lnk	Dropped File	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logim.jpeg	Dropped File, Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsa582.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Program Files (x86)\Lbxhx9hm	Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Access, Create	CLEAN
\??\C:\Windows\SysWOW64\systray.exe	Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7log00.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrv.ini	Dropped File, Accessed File	Access, Create	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Create	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Create, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nstC98.tmp\	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logcl.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8	Accessed File	Access	CLEAN
\??\C:\Program Files\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\actioncentercache\{eea31d4d-1517-4fd0-a7fd-a3f1997ac6a3}.png	Dropped File	-	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\5M764PD8\5M7logrv.ini	Accessed File	Access, Create, Write	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.hsf777.com/m0d4/	-	23.224.102.249	-	-	MALICIOUS
http://www.greenlighteams.com/Credit_Card_Application.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rd......hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=7242435&ktd=0&kld=1061&kp=5	-	209.99.64.33	-	-	CLEAN
http://www.digitalfactoryinstitut.com/m0d4/?AL08=c08ZTacAukQC5NeLWtuBWKo+UaWFOcWy6CEiHhedBNHZ3tXeC1VbOKb5CJ1Nxja24KM0Hg==&VrPHWV=O8Yh2h6	-	217.70.184.50	-	GET	CLEAN
http://www.greenlighteams.com/display.cfm	-	209.99.64.33	-	-	CLEAN
http://www.tyrs-it.com/m0d4/?AL08=EfBAPrIixbPMIKHauOAocozOgBY3ZNEx1t1yXENDBN/Y9A0rELwXOOj/ARjpOVLCDnmCVg==&VrPHWV=O8Yh2h6	-	103.224.212.221	-	GET	CLEAN
http://www.bhreselect.com/m0d4/?AL08=D3Y0Pm5nPVru/us5CxwPidK6v62Fiqkg7A+JactShsSyS/ES72bWbDUd0/Tx/17x61cBJA==&FX10rv=UL00qTmpnvW	-	34.102.136.180	-	GET	CLEAN
http://www.zhidao95.com/m0d4/?VrPHWV=O8Yh2h6&AL08=NAAVMffTY9s/9fH8R/zh9xXRUU+fA/5gjMZ7rGtT7+HDshSMwhe2Brbhhu7bulHK1waO+A==	-	134.73.225.58	-	GET	CLEAN
https://parking.bodiscdn.com	-	-	-	-	CLEAN
https://www.gandi.net/en/security	-	-	-	-	CLEAN
http://www.bangkhacollections.com/m0d4/?AL08=a0iJBX+S++1VW5Q9alJjR6oBYSdMg74u/0Xh/v7LWInF5XrfrQ4uI5t2H6z+dJOBGxTNhw==&FX10rv=UL00qTmpnvW	-	3.108.154.143	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.greenlighteams.com/fashion_trends.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHUo77... ...As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0lgg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=10542279&ktd=0&kld=1061&kp=4	-	209.99.64.33	-	-	CLEAN
http://www.greenlighteams.com/Best_Mortgage_Rates.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2F... ...hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0lgg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=3477850&ktd=0&kld=1061&kp=6	-	209.99.64.33	-	-	CLEAN
http://www.greenlighteams.com/song_lyrics.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHUo77fol... ...As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0lgg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=26527269&ktd=0&kld=1061&kp=7	-	209.99.64.33	-	-	CLEAN
http://www.triumphgroup.xyz/m0d4/?AL08=99EE7/YJ7QYJ6gl7lR9e36EGMnrjjpKCX93zWfmkIY/R6ohvJ2OXPesLVXdNj3uSa3MFgA==&FX10rv=UL00qTmpnvW	-	172.67.210.242, 104.21.77.185	-	GET	CLEAN
http://www.hsf777.com/m0d4/?AL08=7Xa4BbX+EF+0bOKfkWo9GY8TeBGxHEZixmbVHdNSFZSwo63rM1BfaWFzyWRopavNogmBAQ==&VrPHWV=O8Yh2h6	-	23.224.102.249	-	GET	CLEAN
http://www.zoommachone.xyz/m0d4/?AL08=/qzckqtyCc8rrPOLAqXCRRIw/xaz6fwoS3VigV0+3PEnE62ghz0EbMW68KNNy8Z877lwzg==&VrPHWV=O8Yh2h6	-	85.159.66.93	-	GET	CLEAN
http://www.apremotesamsung.com/m0d4/?VrPHWV=O8Yh2h6&AL08=hUVgbolmL0sCt7LaC3NHw8YP+GPS1BdzeLBlZXKVOXmYliZu5gDV6Bh8///TuT3X9hKJEw==	-	103.224.212.222	-	GET	CLEAN
https://whois.gandi.net/en/results?search=digitalfactoryinstitut.com	-	-	-	-	CLEAN
http://www.greenlighteams.com/sk-privacy.php	-	209.99.64.33	-	-	CLEAN
https://www.gandi.net/en	-	-	-	-	CLEAN
https://news.gandi.net/en	-	-	-	-	CLEAN
https://shop.gandi.net/en/domain/suggest?search=digitalfactoryinstitut.com&source=parking	-	-	-	-	CLEAN
http://www.techkaisimi.com/m0d4/?AL08=b0hNo1faq5o0ibq11tSUAJ1i6UzM7c/b3lNITCAxF7SArJmPdEQu3/RrFLto8yLoO0cRIQ==&VrPHWV=O8Yh2h6	-	204.188.203.155, 209.141.38.71, 107.161.23.204, 168.235.88.209, 198.251.81.30, 64.32.22.102, 198.251.84.92, 192.161.187.200, 45.58.190.82, 70.39.125.244	-	GET	CLEAN
http://www.palia.world/m0d4/?AL08=NmHDKYpLtOaunO6yJwQt7bjBEDSMmb6uyC2Rdc4sC+38r/w1LF5LwewBdTfUGNSbbzrJiw==&FX10rv=UL00qTmpnvW	-	34.102.136.180	-	GET	CLEAN
http://www.greenlighteams.com/Best_Penny_Stocks.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FHU... ...hAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0lgg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=3482138&ktd=0&kld=1061&kp=1	-	209.99.64.33	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.greenlighteams.com/Free_Credit_Report.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2FH......As3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=11539660&ktd=0&kId=1061&kp=2	-	209.99.64.33	-	-	CLEAN
http://i3.cdn-image.com/__media__/js/min.js?v2.3	-	-	-	-	CLEAN
https://www.google.com	-	-	-	-	CLEAN
https://shop.gandi.net/en/domain/transfer	-	-	-	-	CLEAN
http://www.aceites.info/m0d4/?AL08=TbollzpT9rXeZ91U9wIhpx+nZxEa9zONUu6oxAitLGSU2Wdu93eLhJ7o42pW1H17q81Ltg==&FX10rv=UL00qTmpnvW	-	82.163.176.128	-	GET	CLEAN
https://www.gandi.net/en/cloud	-	-	-	-	CLEAN
https://shop.gandi.net/en	-	-	-	-	CLEAN
https://www.gandi.net/en/domain	-	-	-	-	CLEAN
http://www.greenlighteams.com/10_Best_Mutual_Funds.cfm?fp=C6Ko6tS0m791FEdtlyzy7TY22jiBV0%2B8ljiENwbi9w76FfsqEynbl3Fjnq4wKtKo4Rdg%2......cmhAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY%2FwaXB8iQoULo0f16dJ4RZxCoSOnHg0Igg%3D%3D&VrPHWV=O8Yh2h6&&kt=112&&ki=72996&ktd=0&kId=1061&kp=3	-	209.99.64.33	-	-	CLEAN
http://www.toastpack.com/m0d4/?AL08=C0FyLQDmOvxjZakspQ6bMYY13TbPn/9qf9RMzvcwLb2Zn1gZl3lQfiJU9Qg6oJU7QnfBxw==&FX10rv=UL00qTmpnvW	-	34.102.136.180	-	GET	CLEAN
http://greenlighteams.com	-	-	-	-	CLEAN
http://www.greenlighteams.com/px.js?ch=2	-	209.99.64.33	-	-	CLEAN
http://www.greenlighteams.com/px.js?ch=1	-	209.99.64.33	-	-	CLEAN
http://www.tenthgenerationtorah.com/m0d4/?AL08=mGlUdW2Hhm2PG3zh9JwTEQVxirr1ywQmw3qGssNmbrB1xVceB7WEhF7r3Lqhy6k1kXdJdA==&FX10rv=UL00qTmpnvW	-	103.224.212.220	-	GET	CLEAN
http://www.perstockholm.com/m0d4/?VrPHWV=O8Yh2h6&AL08=7XWYUFyABOVdAnpCCqlHgoLhtNBn8sw1plAzqMSF02fZrSrsWz8Q9PBCcJLz0Y4XBbh2Pg==	-	156.234.16.189	-	GET	CLEAN
http://www.portres.online/m0d4/?AL08=5QX2iLt+pw2MYMDUfTIweWLkahJ87DwyoOP3aWzqgiacXlFD4ogajsqjANYZwMbPyx7TGQ==&VrPHWV=O8Yh2h6	-	162.213.255.214	-	GET	CLEAN
https://www.gandi.net/en/simple-hosting	-	-	-	-	CLEAN
http://www.greenlighteams.com/m0d4/?AL08=/cmhAs3mhUFhowqdiCjOgaitQbNmQmqm1CrzY/waXB8iQoULo0f16dJ4RZxCoSOnHg0Igg==&VrPHWV=O8Yh2h6	-	209.99.64.33	-	GET	CLEAN
http://www.meredithlobrien.com/m0d4/?VrPHWV=O8Yh2h6&AL08=46O1sEyR4/wvH+bLwVUeRrKpxvMq4OD5F1CZbWpFi2lfYASfWdQWFwztdAKhmRJ+qi5Ayg==	-	34.102.136.180	-	GET	CLEAN
http://www.greenlighteams.com/sk-logabpstatus.php?a=MkcyNnhMa3RleU5FdWpNTEtGbXhuNHNGMlFNeXUxOHN3V25QUFFJdkw0ZlBxRU9XQldOUnpUWTBTRDBGNlVPblQvMGZrZndBeHcyWjhmcWJaZ3F0eDdJWEk1am9FcVlFVGROZ2RKTVladG5vZ0JVU2d4dTkvemFCek5Jdlp3S3Y=&b=	-	209.99.64.33	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.futternmitflo.com/m0d4/?VrPHWV=O8Yh2h6&AL08=hu5YyLRdsgKsg3JM32LgsQICUlcoZL968qMFJRjRR5TUyFTxWRvlKvb31X9wP6YGmIe9CA==	-	192.0.78.24, 192.0.78.25	-	GET	CLEAN
http://www.bulkheadsrestaurantgroup.com/m0d4/?VrPHWV=O8Yh2h6&AL08=ihChw7NkvHHnp4ehDSAv07TGAws7cYloqo91uq/CHYSLKFZDBb5B+puRdm5bVlmhTydU0w==	-	199.59.243.200	-	GET	CLEAN
https://fonts.googleapis.com	-	-	-	-	CLEAN
https://help.gandi.net/en	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.portres.online	162.213.255.214	-	DNS, TCP	SUSPICIOUS
www.zoommachone.xyz	85.159.66.93	-	DNS, TCP	SUSPICIOUS
natroredirect.natrocdn.com	85.159.66.93	-	DNS, TCP	CLEAN
www.techkaisimi.com	204.188.203.155, 209.141.38.71, 107.161.23.204, 168.235.88.209, 198.251.81.30, 64.32.22.102, 198.251.84.92, 192.161.187.200, 45.58.190.82, 70.39.125.244	-	DNS, TCP	CLEAN
www.toastpack.com	34.102.136.180	-	DNS, TCP	CLEAN
futternmitflo.com	192.0.78.24, 192.0.78.25	-	DNS, TCP	CLEAN
www.perstockholm.com	156.234.16.189	-	DNS, TCP	CLEAN
www.protocolohfresco.site	-	-	-	CLEAN
www.hsf777.com	23.224.102.249	-	DNS, TCP	CLEAN
www.meredithlobrien.com	34.102.136.180	-	DNS, TCP	CLEAN
www.sans-gluten.store	-	-	-	CLEAN
www.apremotesamsung.com	103.224.212.222	-	DNS, TCP	CLEAN
www.gandi.net	-	-	-	CLEAN
www.digitalfactoryinstitut.com	217.70.184.50	-	DNS, TCP	CLEAN
meredithlobrien.com	34.102.136.180	-	DNS, TCP	CLEAN
redirect.natrocdn.com	85.159.66.93	-	DNS, TCP	CLEAN
parking.bodiscdn.com	-	-	-	CLEAN
bhreselect.com	34.102.136.180	-	DNS, TCP	CLEAN
www.bulkheadsrestaurantgroup.com	199.59.243.200	-	DNS, TCP	CLEAN
i3.cdn-image.com	-	-	-	CLEAN
toastpack.com	34.102.136.180	-	DNS, TCP	CLEAN
www.google.com	-	-	-	CLEAN
www.tyrs-it.com	103.224.212.221	-	DNS, TCP	CLEAN
parking.namesilo.com	204.188.203.155, 209.141.38.71, 107.161.23.204, 168.235.88.209, 198.251.81.30, 64.32.22.102, 198.251.84.92, 192.161.187.200, 45.58.190.82, 70.39.125.244	-	DNS, TCP	CLEAN
whois.gandi.net	-	-	-	CLEAN
www.palia.world	34.102.136.180	-	DNS, TCP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
news.gandi.net	-	-	-	CLEAN
www.aceites.info	82.163.176.128	-	DNS, TCP, HTTP	CLEAN
help.gandi.net	-	-	-	CLEAN
webredir.vip.gandi.net	217.70.184.50	-	DNS, TCP	CLEAN
www.triumphgroup.xyz	172.67.210.242, 104.21.77.185	-	DNS, TCP	CLEAN
www.greenlighteams.com	209.99.64.33	-	DNS, TCP	CLEAN
www.zhidao95.com	134.73.225.58	-	DNS, TCP	CLEAN
greenlighteams.com	-	-	-	CLEAN
www.baigouw.com	-	-	-	CLEAN
shop.gandi.net	-	-	-	CLEAN
palia.world	34.102.136.180	-	DNS, TCP	CLEAN
www.bangkhacollections.com	3.108.154.143	-	DNS, TCP	CLEAN
www.tenthgenerationtorah.com	103.224.212.220	-	DNS, TCP	CLEAN
www.bhreselect.com	34.102.136.180	-	DNS, TCP	CLEAN
aceites.info	82.163.176.128	-	DNS, TCP, HTTP	CLEAN
www.futternmitflo.com	192.0.78.24, 192.0.78.25	-	DNS, TCP	CLEAN
fonts.googleapis.com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
204.188.203.155	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
156.234.16.189	www.perstockholm.com	Hong Kong	DNS, TCP	CLEAN
34.102.136.180	meredithlobrien.com, www.toastpack.com, toastpack.com, www.palia.world, www.bhreselect.com, palia.world, www.meredithlobrien.com, bhreselect.com	United States	DNS, TCP	CLEAN
107.161.23.204	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
199.59.243.200	www.bulkheadsrestaurantgroup.com	United States	DNS, TCP	CLEAN
70.39.125.244	parking.namesilo.com, www.techkaisimi.com	United States	DNS, TCP	CLEAN
103.224.212.221	www.tyrs-it.com	Australia	DNS, TCP	CLEAN
134.73.225.58	www.zhidao95.com	United States	DNS, TCP	CLEAN
162.213.255.214	www.portres.online	United States	DNS, TCP	CLEAN
209.141.38.71	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
172.67.210.242	www.triumphgroup.xyz	United States	DNS, TCP	CLEAN
82.163.176.128	aceites.info, www.aceites.info	United Kingdom	DNS, TCP, HTTP	CLEAN
103.224.212.220	www.tenthgenerationtorah.com	Australia	DNS, TCP	CLEAN
168.235.88.209	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
198.251.81.30	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
209.99.64.33	www.greenlighteams.com	United States	DNS, TCP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
192.161.187.200	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
64.32.22.102	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
104.21.77.185	www.triumphgroup.xyz	-	DNS	CLEAN
192.0.78.24	futternmitflo.com, www.futternmitflo.com	United States	DNS	CLEAN
198.251.84.92	parking.namesilo.com, www.techkaisimi.com	Luxembourg	DNS	CLEAN
217.70.184.50	webredir.vip.gandi.net, www.digitalfactoryinstitut.com	France	DNS, TCP	CLEAN
192.0.78.25	futternmitflo.com, www.futternmitflo.com	United States	DNS, TCP	CLEAN
85.159.66.93	www.zoommachone.xyz, redirect.natrocdn.com, natroredirect.natrocdn.com	Turkey	DNS, TCP	CLEAN
103.224.212.222	www.apremotesamsung.com	Australia	DNS, TCP	CLEAN
45.58.190.82	parking.namesilo.com, www.techkaisimi.com	United States	DNS	CLEAN
3.108.154.143	www.bangkhacollections.com	India	DNS, TCP	CLEAN
23.224.102.249	www.hsf777.com	United States	DNS, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
S-1-5-21-1560258-193263778575	access	explorer.exe	CLEAN
6NON26-3X60UXYXz	access	systray.exe	CLEAN
S-1-5-21-1560258-14963319274527	access	iexplore.exe	CLEAN
5M764PD81WX9E20z	access	systray.exe	CLEAN

Registry

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	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	create, access	systray.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	create, access	systray.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird	create, access	systray.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\JT2LG	access, write	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	create, access	systray.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	create, access	systray.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\f86ed2903a4a11cfb57e524153480001	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	create, access	systray.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_2016	create, access	systray.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	create, access	systray.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	create, access	systray.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe	"C:\Users\RDhJ0CNFevzX\Desktop\285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96.exe"	MALICIOUS
pkypr.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca	MALICIOUS
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:1496 CREDAT:82945 /prefetch:2	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
pkypr.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe C:\Users\RDHJ0C~1\AppData\Local\Temp\zpcthwca	SUSPICIOUS
systray.exe	"C:\Windows\SysWOW64\systray.exe"	SUSPICIOUS
cmd.exe	/c del "C:\Users\RDHJ0C~1\AppData\Local\Temp\pkypr.exe"	SUSPICIOUS
3dftp.exe	"C:\Program Files (x86)\WindowsPowerShell\3dftp.exe"	SUSPICIOUS
absolutetelnet.exe	"C:\Program Files (x86)\MSBuild\absolutetelnet.exe"	SUSPICIOUS
alftp.exe	"C:\Program Files\Windows Portable Devices\alftp.exe"	SUSPICIOUS
barca.exe	"C:\Program Files (x86)\Windows Defender\barca.exe"	SUSPICIOUS
bitkinex.exe	"C:\Program Files\Windows Multimedia Platform\bitkinex.exe"	SUSPICIOUS
coreftp.exe	"C:\Program Files\Internet Explorer\coreftp.exe"	SUSPICIOUS
far.exe	"C:\Program Files\Windows Portable Devices\far.exe"	SUSPICIOUS
filezilla.exe	"C:\Program Files\WindowsPowerShell\filezilla.exe"	SUSPICIOUS
flashfxp.exe	"C:\Program Files\MSBuild\flashfxp.exe"	SUSPICIOUS
fling.exe	"C:\Program Files (x86)\Internet Explorer\fling.exe"	SUSPICIOUS
gmailnotifierpro.exe	"C:\Program Files (x86)\Microsoft Office\gmailnotifierpro.exe"	SUSPICIOUS
icq.exe	"C:\Program Files\Windows Defender\icq.exe"	SUSPICIOUS
leechftp.exe	"C:\Program Files (x86)\MSBuild\leechftp.exe"	SUSPICIOUS
ncftp.exe	"C:\Program Files (x86)\Microsoft.NET\ncftp.exe"	SUSPICIOUS

Process Name	Commandline	Verdict
notepad.exe	"C:\Program Files\Windows Portable Devices\notepad.exe"	SUSPICIOUS
operamail.exe	"C:\Program Files (x86)\WindowsPowerShell\operamail.exe"	SUSPICIOUS
outlook.exe	"C:\Program Files (x86)\Microsoft Office\outlook.exe"	SUSPICIOUS
pidgin.exe	"C:\Program Files\Windows Sidebar\pidgin.exe"	SUSPICIOUS
scriptftp.exe	"C:\Program Files\Reference Assemblies\scriptftp.exe"	SUSPICIOUS
skype.exe	"C:\Program Files\Windows Portable Devices\skype.exe"	SUSPICIOUS
smartftp.exe	"C:\Program Files\Windows Photo Viewer\smartftp.exe"	SUSPICIOUS
thunderbird.exe	"C:\Program Files (x86)\Microsoft Office\thunderbird.exe"	SUSPICIOUS
trillian.exe	"C:\Program Files\WindowsPowerShell\trillian.exe"	SUSPICIOUS
webdrive.exe	"C:\Program Files (x86)\WindowsPowerShell\webdrive.exe"	SUSPICIOUS
whatsapp.exe	"C:\Program Files\MSBuild\whatsapp.exe"	SUSPICIOUS
winscp.exe	"C:\Program Files\WindowsPowerShell\winscp.exe"	SUSPICIOUS
yahoomessenger.exe	"C:\Program Files (x86)\Windows Defender\yahoomessenger.exe"	SUSPICIOUS
iexplore.exe	"C:\Program Files\Internet Explorer\iexplore.exe" about:blank	CLEAN

YARA / AV

YARA (20)

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	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
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