MALICIOUS

Classifications: Spyware | Injector

Threat Names: FormBook | Mal/Generic-S | Gen:Variant.Razy.679962

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**cc.exe**
ID	#2782517
MD5	4c70d5b1c63a468f7e0aedf64f93ca42
SHA1	c248ab00560786b7be23151597d9503a2e84602f
SHA256	83242a0f42be34e66e502e4a3a45d2470f3b24aef8a1d8484711f4439d7fe74a
File Size	1024.00 KB
Report Created	2021-09-28 12:19 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (30 rules, 160 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "FormBook" from ruleset "Malware" has matched on the function strings for (process #4) rundll32.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Opera, Internet Explorer, AbleFTP, Google Chrome.			
4/5	Injection	Writes into the memory of another process	6	Injector
	• (Process #2) cc.exe modifies memory of (process #3) explorer.exe. • (Process #4) rundll32.exe modifies memory of (process #3) explorer.exe. • (Process #2) cc.exe modifies memory of (process #4) rundll32.exe. • (Process #8) winzvg4hxq8.exe modifies memory of (process #9) explorer.exe. • (Process #10) ipconfig.exe modifies memory of (process #9) explorer.exe. • (Process #8) winzvg4hxq8.exe modifies memory of (process #10) ipconfig.exe.			
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #2) cc.exe alters context of (process #3) explorer.exe. • (Process #4) rundll32.exe alters context of (process #3) explorer.exe. • (Process #8) winzvg4hxq8.exe alters context of (process #9) explorer.exe. • (Process #10) ipconfig.exe alters context of (process #9) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected a memory dump of (process #2) cc.exe as "Gen:Variant.Razy.679962".			
3/5	Input Capture	Captures clipboard data	1	Spyware
	• (Process #3) explorer.exe reads data from clipboard.			
2/5	Anti Analysis	Tries to detect debugger	3	-
	• (Process #1) cc.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent". • (Process #1) cc.exe tries to detect a debugger via API "IsDebuggerPresent". • (Process #2) cc.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #2) cc.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #5) cmd.exe deletes executed executable "c:\users\keecfmwgj\desktop\cc.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #4) rundll32.exe has a thread which sleeps more than 5 minutes.			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive browser data	3	-
	• (Process #4) rundll32.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #4) rundll32.exe tries to read sensitive data of web browser "Opera" by file. • (Process #4) rundll32.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #4) rundll32.exe tries to read sensitive data of ftp application "AbleFTP" by file.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #1) cc.exe modifies memory of (process #2) cc.exe. • (Process #7) winzvg4hxq8.exe modifies memory of (process #8) winzvg4hxq8.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-
	• (Process #1) cc.exe alters context of (process #2) cc.exe. • (Process #7) winzvg4hxq8.exe alters context of (process #8) winzvg4hxq8.exe.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	44	-

Score	Category	Operation	Count	Classification
		• (Process #2) cc.exe makes a direct system call to "NtQuerySystemInformation".		
		• (Process #2) cc.exe makes a direct system call to "NtQueryInformationProcess".		
		• (Process #2) cc.exe makes a direct system call to "NtAllocateVirtualMemory".		
		• (Process #2) cc.exe makes a direct system call to "NtFreeVirtualMemory".		
		• (Process #2) cc.exe makes a direct system call to "NtOpenProcessToken".		
		• (Process #2) cc.exe makes a direct system call to "NtAdjustPrivilegesToken".		
		• (Process #2) cc.exe makes a direct system call to "NtClose".		
		• (Process #2) cc.exe makes a direct system call to "NtOpenDirectoryObject".		
		• (Process #2) cc.exe makes a direct system call to "NtCreateMutant".		
		• (Process #2) cc.exe makes a direct system call to "NtCreateSection".		
		• (Process #2) cc.exe makes a direct system call to "NtMapViewOfSection".		
		• (Process #2) cc.exe makes a direct system call to "NtOpenProcess".		
		• (Process #2) cc.exe makes a direct system call to "NtQueryInformationToken".		
		• (Process #2) cc.exe makes a direct system call to "NtProtectVirtualMemory".		
		• (Process #2) cc.exe makes a direct system call to "NtCreateFile".		
		• (Process #2) cc.exe makes a direct system call to "NtQueryInformationFile".		
		• (Process #2) cc.exe makes a direct system call to "NtDelayExecution".		
		• (Process #2) cc.exe makes a direct system call to "NtReadVirtualMemory".		
		• (Process #2) cc.exe makes a direct system call to "NtOpenThread".		
		• (Process #2) cc.exe makes a direct system call to "NtReadFile".		
		• (Process #2) cc.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #2) cc.exe makes a direct system call to "NtResumeThread".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtQuerySystemInformation".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtQueryInformationProcess".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtAllocateVirtualMemory".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtFreeVirtualMemory".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtOpenProcessToken".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtAdjustPrivilegesToken".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtClose".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtOpenDirectoryObject".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtCreateMutant".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtCreateSection".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtMapViewOfSection".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtOpenProcess".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtQueryInformationToken".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtProtectVirtualMemory".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtCreateFile".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtQueryInformationFile".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtDelayExecution".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtReadVirtualMemory".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtOpenThread".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtReadFile".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #8) winzvg4hxq8.exe makes a direct system call to "NtResumeThread".		
2/5	YARA	Suspicious content matched by YARA rules	6	-

Score	Category	Operation	Count	Classification
		• Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) cc.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #2) cc.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #4) rundll32.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) winzvg4hxq8.exe. • Rule "MultipleNetObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #8) winzvg4hxq8.exe.		
1/5	Privilege Escalation	Enables process privilege	2	-
		• (Process #1) cc.exe enables process privilege "SeDebugPrivilege". • (Process #7) winzvg4hxq8.exe enables process privilege "SeDebugPrivilege".		
1/5	Hide Tracks	Creates process with hidden window	7	-
		• (Process #1) cc.exe starts (process #2) cc.exe with a hidden window. • (Process #3) explorer.exe starts C:\Windows\SysWOW64\nbtstat.exe with a hidden window. • (Process #3) explorer.exe starts (process #4) rundll32.exe with a hidden window. • (Process #4) rundll32.exe starts (process #5) cmd.exe with a hidden window. • (Process #7) winzvg4hxq8.exe starts C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe with a hidden window. • (Process #9) explorer.exe starts C:\Windows\SysWOW64\taskhost.exe with a hidden window. • (Process #9) explorer.exe starts (process #10) ipconfig.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	5	-
		• (Process #1) cc.exe reads from (process #2) cc.exe. • (Process #2) cc.exe reads from (process #3) explorer.exe. • (Process #2) cc.exe reads from (process #4) rundll32.exe. • (Process #8) winzvg4hxq8.exe reads from (process #9) explorer.exe. • (Process #8) winzvg4hxq8.exe reads from (process #10) ipconfig.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #1) cc.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Mutex	Creates mutex	6	-
		• (Process #2) cc.exe creates mutex with name "62AQ09U8C34JCCAZ". • (Process #4) rundll32.exe creates mutex with name "62AQ09U8C34JCCAZ". • (Process #4) rundll32.exe creates mutex with name "O03PR-DCBVW8A2DZ". • (Process #8) winzvg4hxq8.exe creates mutex with name "62AQ09U8C34JCCAZ". • (Process #10) ipconfig.exe creates mutex with name "62AQ09U8C34JCCAZ". • (Process #10) ipconfig.exe creates mutex with name "-099ODE3WG-67X0J".		
1/5	System Modification	Modifies application directory	1	-
		• (Process #3) explorer.exe modifies "C:\Program Files (x86)\Cmrkpgp".		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #4) rundll32.exe adds "C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe" to Windows startup via registry.		
1/5	Discovery	Possibly does reconnaissance	2	-
		• (Process #4) rundll32.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #4) rundll32.exe tries to gather information about application "Mozilla Firefox" by file.		
1/5	YARA	Content matched by YARA rules	12	-

Score	Category	Operation	Count	Classification
		• Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on the sample itself. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) cc.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #1) cc.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #2) cc.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #2) cc.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #4) rundll32.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #4) rundll32.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) winzvg4hxq8.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #7) winzvg4hxq8.exe. • Rule "BabelObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #8) winzvg4hxq8.exe. • Rule "YanoObfuscatorAttributes" from ruleset "Generic" has matched on a memory dump for (process #8) winzvg4hxq8.exe.		
1/5	Network Connection	Performs DNS request	23	-
		• (Process #3) explorer.exe resolves host name "www.reemletenleafy.com" to IP "-". • (Process #3) explorer.exe resolves host name "www.esomvw.com" to IP "104.18.26.58". • (Process #3) explorer.exe resolves host name "www.deskbk.com" to IP "156.226.250.168". • (Process #3) explorer.exe resolves host name "www.anielleharris.com" to IP "23.227.38.74". • (Process #3) explorer.exe resolves host name "www.lightfootsteps.com" to IP "204.11.56.48". • (Process #3) explorer.exe resolves host name "www.jspagnier-graveur.com" to IP "23.20.208.181". • (Process #3) explorer.exe resolves host name "www.single-on-purpose.com" to IP "192.0.78.24". • (Process #3) explorer.exe resolves host name "www.totalselfconfidence.net" to IP "156.239.192.219". • (Process #3) explorer.exe resolves host name "www.medicalmanagementinc.info" to IP "-". • (Process #3) explorer.exe resolves host name "www.babybox.media" to IP "-". • (Process #3) explorer.exe resolves host name "www.wenyuexuan.com" to IP "-". • (Process #3) explorer.exe resolves host name "www.livinglovinglincoln.com" to IP "34.102.136.180". • (Process #3) explorer.exe resolves host name "www.bjjinmei.com" to IP "154.205.217.133". • (Process #3) explorer.exe resolves host name "www.murdabudz.com" to IP "160.153.136.3". • (Process #3) explorer.exe resolves host name "www.simpeltattofor.men" to IP "103.224.182.210". • (Process #3) explorer.exe resolves host name "www.1971event.com" to IP "35.206.96.200". • (Process #3) explorer.exe resolves host name "www.corlora.com" to IP "23.227.38.74". • (Process #3) explorer.exe resolves host name "www.noun-bug.com" to IP "162.0.213.105". • (Process #3) explorer.exe resolves host name "www.productprinting.online" to IP "108.179.246.105". • (Process #3) explorer.exe resolves host name "www.mabduh.com" to IP "206.189.58.26". • (Process #3) explorer.exe resolves host name "www.krveop.com" to IP "172.67.158.14". • (Process #3) explorer.exe resolves host name "www.lkkogltoyof4.xyz" to IP "150.95.255.38". • (Process #3) explorer.exe resolves host name "www.yogo7.net" to IP "156.240.160.90".		
1/5	Network Connection	Connects to remote host	18	-

Score	Category	Operation	Count	Classification
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "104.18.26.58:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "23.227.38.74:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "204.11.56.48:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "23.20.208.181:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "192.0.78.24:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "34.102.136.180:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "154.205.217.133:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "160.153.136.3:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "103.224.182.210:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "35.206.96.200:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "162.0.213.105:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "108.179.246.105:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "206.189.58.26:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "172.67.158.14:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "150.95.255.38:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "156.240.160.90:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "156.226.250.168:80". • (Process #3) explorer.exe opens an outgoing TCP connection to host "156.239.192.219:80".		
1/5	Execution	Executes itself	2	-
		• (Process #1) cc.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\cc.exe. • (Process #7) winzvg4hxq8.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\cc.exe.		

Mitre ATT&CK Matrix

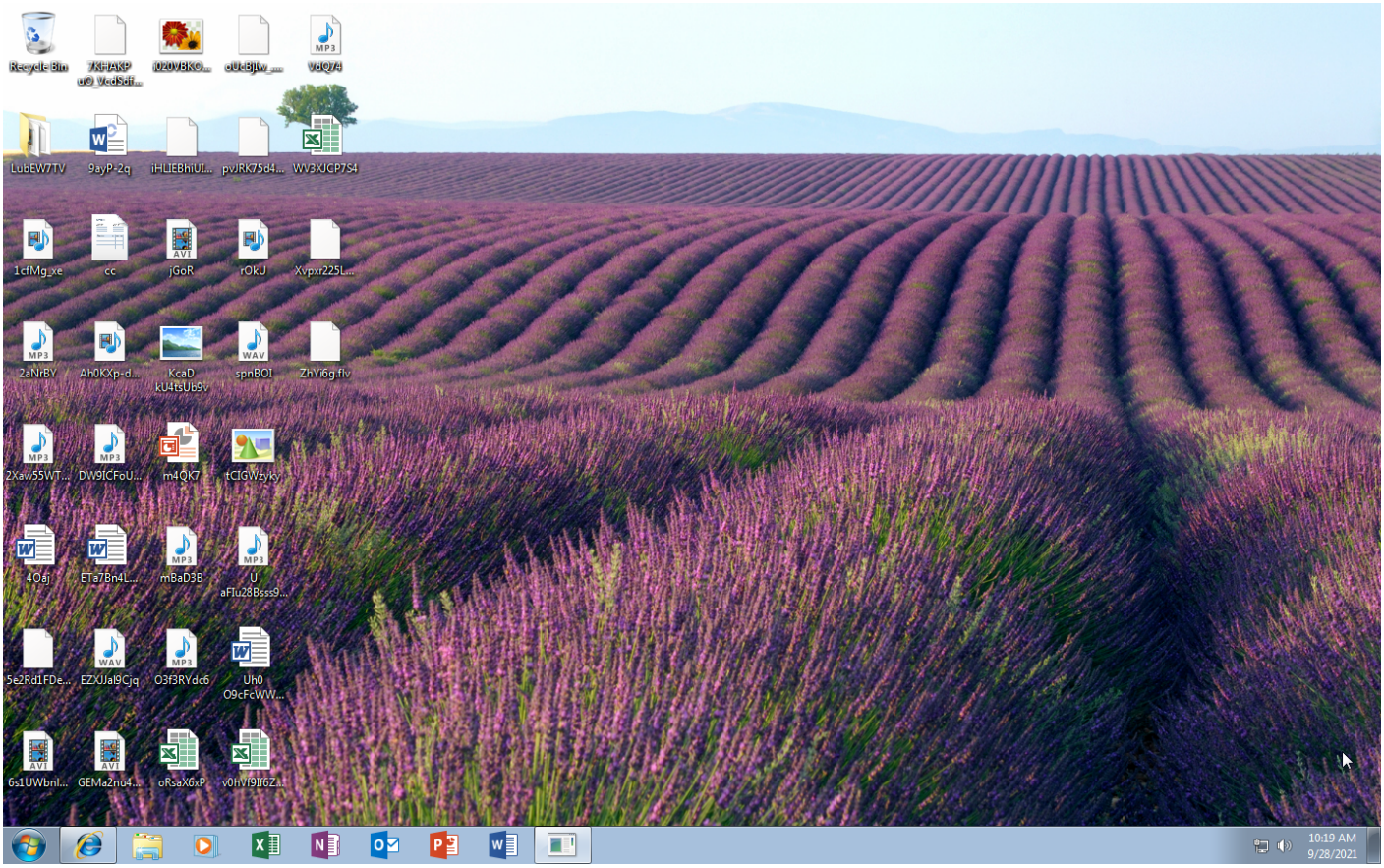
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1012 Query Registry		#T1115 Clipboard Data			
				#T1045 Software Packing	#T1003 Credential Dumping	#T1083 File and Directory Discovery		#T1119 Automated Collection			
				#T1112 Modify Registry		#T1497 Virtualization/ Sandbox Evasion		#T1005 Data from Local System			
				#T1497 Virtualization/ Sandbox Evasion		#T1124 System Time Discovery					

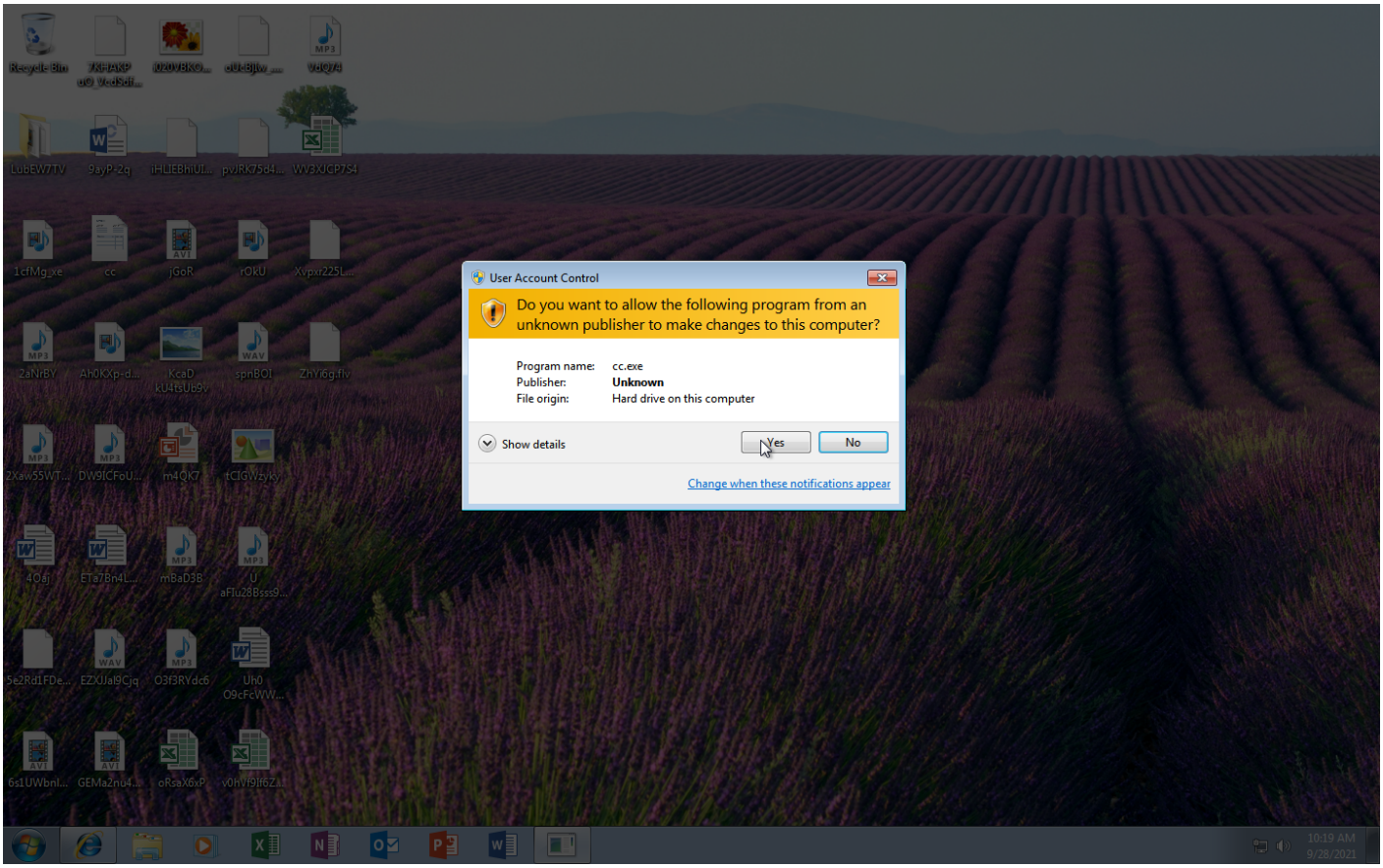
Sample Information

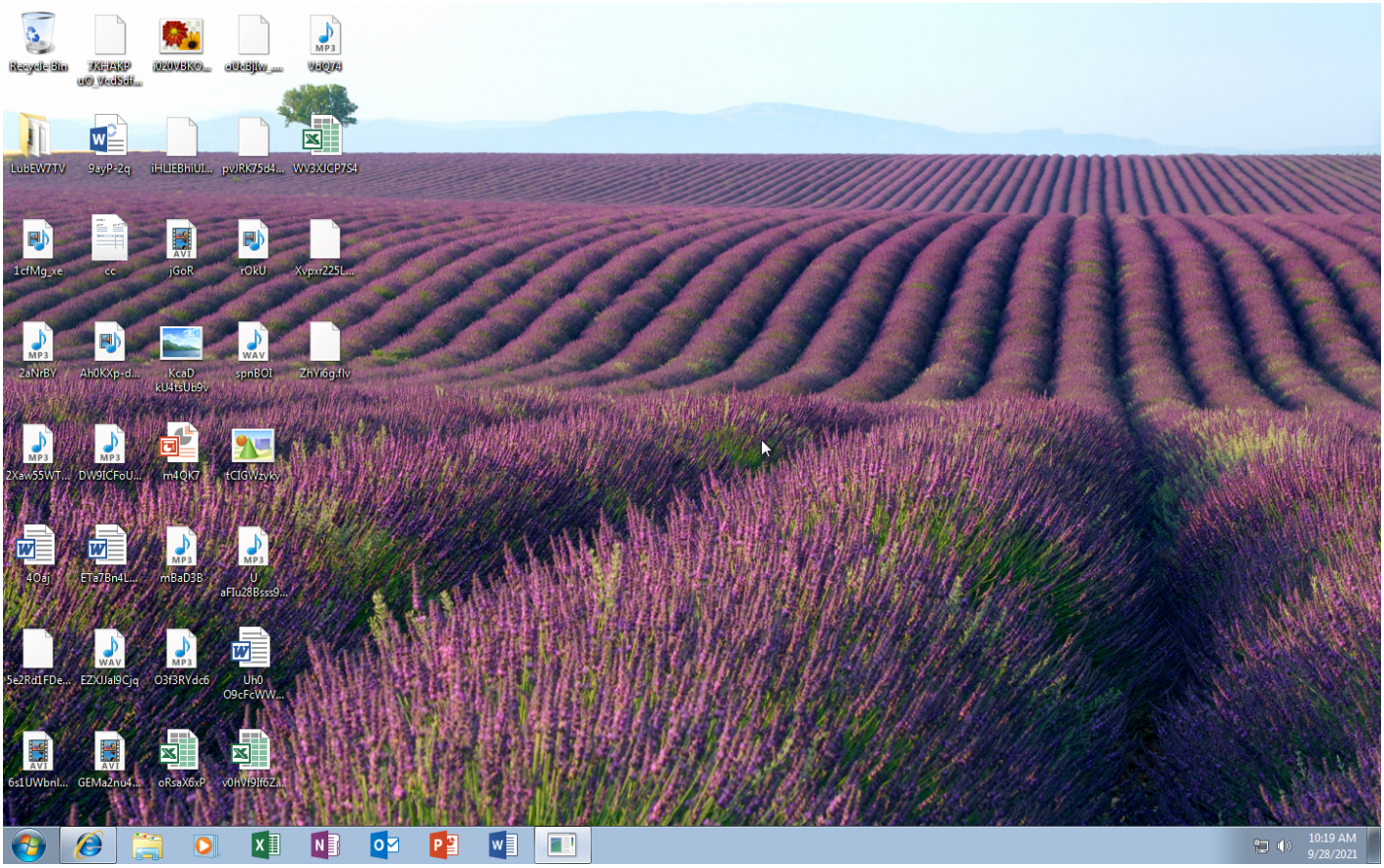
ID	#2782517
MD5	4c70d5b1c63a468f7e0aedf64f93ca42
SHA1	c248ab00560786b7be23151597d9503a2e84602f
SHA256	83242a0f42be34e66e502e4a3a45d2470f3b24aef8a1d8484711f4439d7fe74a
SSDeep	3072:EWrIy8kmoEBZBB2lrEtC1JZdDFs3sb5fkaLZ2sf2h8yezeci6x46xXX07/Bg9s9L:N/ZzLfkuS8yADi6vxU7/w8+PsFT8lw
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	cc.exe
File Size	1024.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 12:19 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	19




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



Screenshots truncated

NETWORK

General

92.49 KB total sent

127.14 KB total received

1 ports 80

19 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

34 DNS requests for 23 domains

1 nameservers contacted

15 total requests returned errors

HTTP/S

37 URLs contacted, 18 servers

45 sessions, 84.31 KB sent, 76.18 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.esomvw.com/mjyv/?MI=84GmfEOeezwjENHIvrBoemsYeWt0m/HwoH8hmSCYYDVvlSXm81Rnn8BPdG66LOse7+JH3wWm&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
POST	http://www.esomvw.com/mjyv/	-	-		0 bytes	NA
GET	http://www.deskbk.com/mjyv/?MI=elfYEudHYjWRBKVQqa1FwjnBNMNthSMPxSU2Ae2RzX6JH+Ulo+4qi3qp9hj2WZGr6rIWckf&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.anielleharris.com/mjyv/?MI=VdqIn5ATadMqw6pgyqzwjUU2K1KmNlW0QhXn4TeZ4+V516gxmgYomdsi8jTWk431wR4xkLLj&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.lightfootsteps.com/mjyv/?MI=ZaGFmHO9QjcqyRss7KbI6J403dr6bz+HcnVoXiL1W+dYgLy7T488fufqvcQ1zRSwoJw29pJ4&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.jspagnier-graveur.com/mjyv/?MI=Th83Ckvp/531Tl/GX4RX7Dh2QUTLyutGF176aUX2OVMJp6JNPI80WTgR6fQGzE7qZTwZp8ZB&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.single-on-purpose.com/mjyv/?MI=Q7OMrrPP6VpxrdE1nYHLlQBfBwjE9EOakY/k4TZPYOQ1+efX2FR/5nxasJQT51ckttjnkljO&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
POST	http://www.anielleharris.com/mjyv/	-	-		0 bytes	NA
POST	http://www.lightfootsteps.com/mjyv/	-	-		0 bytes	NA
POST	http://www.jspagnier-graveur.com/mjyv/	-	-		0 bytes	NA
POST	http://www.single-on-purpose.com/mjyv/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.totalselfconfidence.net/mjyv/?MI=7+dRD0VfrOquXVxTGZgRO8F9r9A4udAqY3P1KQFKJ8W9R0Kxy+STzHlFMkDcQByvMxKiuXRM&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.livinglovinglincoln.com/mjyv/?MI=v6+mrmg92knFd2hB4m8c7LRaoFH4FGs5nhP+0lUaaW8DwAWWNnjucsjLIXZS4yksGO7kPpSc&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.bjjinmei.com/mjyv/?MI=tK48cpM9c53SDiUBEb9HKzRmP2wH5JkMCWpRDhGyYNy0ifXLmO4jSTOPfRY6+Bx01EWV18pV&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.murdabudz.com/mjyv/?MI=hg13/nUaX9mUx8sSJlJYfgV6jTQ/W4br/c2NzJsxCbwCh/fzBEDuEbvVWcjNmMf2/7hygaPQ&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.simpeltattofor.men/mjyv/?MI=YF19Yjtl8/UPVOzf/wHjSkaABDmeFeWIIuMalRBS1oahuHz0Fdc7+ZeWTOXaxJbXSsdeR5U0&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
GET	http://www.1971event.com/mjyv/?MI=dCk/M3RqXmnriH5Dpo5+kGUPt2Tx4Jc7l1qyuUsiRnJePv/CPBZ7QEiY+Ijzn1XuWA0anRMV&MDK0g=m2MpP03h	-	-		0 bytes	NA
GET	http://www.corlora.com/mjyv/?MI=FJb0UZ1El2iZyz9b6sDaOfhvWc1+IVn9AMjAgVGnTau2aQQ7z/C35fdWtWFhzsPoN7gw81Ka&MDK0g=m2MpP03h	-	-		0 bytes	NA
POST	http://www.livinglovinglincoln.com/mjyv/	-	-		0 bytes	NA
GET	http://www.noun-bug.com/mjyv/?MI=/e6GyVavtbTeIz9m0WWy93DWNbpPODk8+8mRaUmDSGSQSMIeKfo2rpsXGYfN6k+L2XrTjDzG&gXzt_B=DN9xx4XpOBr0b	-	-		0 bytes	NA
POST	http://www.bjjinmei.com/mjyv/	-	-		0 bytes	NA
POST	http://www.murdabudz.com/mjyv/	-	-		0 bytes	NA
POST	http://www.simpeltattofor.men/mjyv/	-	-		0 bytes	NA
POST	http://www.corlora.com/mjyv/	-	-		0 bytes	NA
POST	http://www.noun-bug.com/mjyv/	-	-		0 bytes	NA
POST	http://www.productprinting.online/mjyv/	-	-		0 bytes	NA
GET	http://www.productprinting.online/mjyv/?MI=dI0EVfvGTcPWZQJTCCwwBrtyXsKLoNwUe8Jfo4lOgU2AXLHTPdQLz/5V0DEerltniF7xTL1s&MDK0g=m2MpP03h	-	-		0 bytes	NA
GET	http://www.mabduh.com/mjyv/?MI=46trCuL+qj46sXtcEXelMa5KUSrIckjmnhHha+k1BNltaPzLSYu+3DxHEUEWTfM5pLHPeQT&MDK0g=m2MpP03h	-	-		0 bytes	NA
POST	http://www.mabduh.com/mjyv/	-	-		0 bytes	NA
GET	http://www.krveop.com/mjyv/?MI=HyN26Cpbz7/YQUft90o9zs1nCJbgg4mk/6cvH3irtRilVkmclTk2bmmTD+Kmlot5gaHlkoQ3&MDK0g=m2MpP03h	-	-		0 bytes	NA
POST	http://www.lkkogltoyof4.xyz/mjyv/	-	-		0 bytes	NA
GET	http://www.lkkogltoyof4.xyz/mjyv/?MI=EAnvUfcUxKKliiQnQI88cMi+J9woX5wjkbbwLQW1UVDUs3UxvXHKg6261p2l2O3lsj46KHPB&MDK0g=m2MpP03h	-	-		0 bytes	NA
GET	http://www.yogo7.net/mjyv/?MI=jdeYqH68CS7uHwPF/IFQ000KzvKwE38RqZbU2k7yUZMS+iAtH2XF+eLlXJjI7FDVVXC+S/fz&MDK0g=m2MpP03h	-	-		0 bytes	NA
POST	http://www.krveop.com/mjyv/	-	-		0 bytes	NA
POST	http://www.yogo7.net/mjyv/	-	-		0 bytes	NA

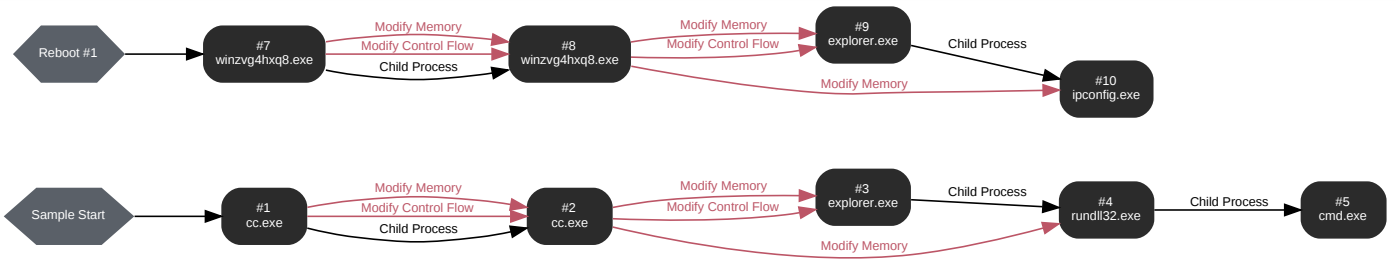
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://www.totalselfconfidence.net/mjyv/	-	-		0 bytes	NA
POST	http://www.deskbk.com/mjyv/	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.reemletenleafy.com	NXDomain			NA
A	www.esomvw.com, shops.myfunpinpin.com	NoError	104.18.26.58, 104.18.27.58	shops.myfunpinpin.com	NA
A	www.deskbk.com	NoError	156.226.250.168		NA
A	www.anielleharris.com, shops.myshopify.com	NoError	23.227.38.74	shops.myshopify.com	NA
A	www.lightfootsteps.com	NoError	204.11.56.48		NA
A	www.jspagnier-graveur.com, comingsoon.namebright.com, cdl-lb-1356093980.us-east-1.elb.amazonaws.com	NoError	23.20.208.181, 54.85.93.188	comingsoon.namebright.com, cdl-lb-1356093980.us-east-1.elb.amazonaws.com	NA
A	www.single-on-purpose.com, single-on-purpose.com	NoError	192.0.78.24, 192.0.78.25	single-on-purpose.com	NA
A	www.totalselfconfidence.net	NoError	156.239.192.219		NA
A	www.medicalmanagementinc.info	NXDomain			NA
A	www.babybox.media	NXDomain			NA
A	www.wenyuexuan.com	-			NA
A	www.livinglovinglincoln.com, livinglovinglincoln.com	NoError	34.102.136.180	livinglovinglincoln.com	NA
A	www.bjjinmei.com	NoError	154.205.217.133		NA
A	www.murdabudz.com, murdabudz.com	NoError	160.153.136.3	murdabudz.com	NA
A	www.simpeltattofor.men	NoError	103.224.182.210		NA
A	www.1971event.com	NoError	35.206.96.200		NA
A	www.corlora.com, shops.myshopify.com	NoError	23.227.38.74	shops.myshopify.com	NA
A	www.noun-bug.com	NoError	162.0.213.105		NA
A	www.productprinting.online, productprinting.online	NoError	108.179.246.105	productprinting.online	NA
A	www.mabduh.com	NoError	206.189.58.26, 206.189.50.60		NA
A	www.krveop.com	NoError	172.67.158.14, 104.21.49.26		NA
A	www.lkkogltoyof4.xyz	NoError	150.95.255.38		NA
A	www.yogo7.net	NoError	156.240.160.90		NA

BEHAVIOR

Process Graph



Process #1: cc.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\cc.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\cc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 41923, Reason: Analysis Target
Unmonitor End Time	End Time: 193829, Reason: Terminated
Monitor duration	151.91s
Return Code	1073807364
PID	3940
Parent PID	1116
Bitness	32 Bit

Host Behavior

Type	Count
Environment	3
Registry	4
User	1
Process	1
-	654
File	20
Module	13
System	3
Window	14
-	3
-	6

Process #2: cc.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\cc.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\cc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71340, Reason: Child Process
Unmonitor End Time	End Time: 81619, Reason: Terminated
Monitor duration	10.28s
Return Code	0
PID	3988
Parent PID	3940
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\cc.exe	0xf68	0x60000(393216)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\cc.exe	0xf68	0x61000(397312)	0x27c00	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\cc.exe	0xf68	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\cc.exe	0xf68 / 0xf98		-	✓	1

Host Behavior

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

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 74476, Reason: Injection
Unmonitor End Time	End Time: 196058, Reason: Terminated
Monitor duration	121.58s
Return Code	1073807364
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\cc.exe	0xf98	0x77a0000(125435904)	0x198000	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\cc.exe	0xf98 / 0x460	0x113(275)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\cc.exe	0xf98 / 0x460	0x7899909(126458121)	-	✓	1
Modify Memory	#4: c:\windows\syswow64\rundll32.exe	0xfa4	0x7f30000(133365760)	0x1b58000	✓	1
Modify Memory	#4: c:\windows\syswow64\rundll32.exe	0xfa4	0x7940000(127139840)	0x10b000	✓	1
Modify Control Flow	#4: c:\windows\syswow64\rundll32.exe	0xfa4 / 0x460	0x12f5e8(1242600)	-	✓	1
Modify Control Flow	#4: c:\windows\syswow64\rundll32.exe	0xfa4 / 0x460	0x79c58f2(127686898)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	1024.00 KB	83242a0f42be34e66e502e4a3a45d2470f3b24aef8a1d8484711f4439d7fe74a	✗

Host Behavior

Type	Count
Process	2
System	68
File	10
COM	1

Network Behavior

Type	Count
HTTP	45

Type	Count
DNS	34
TCP	70

Process #4: rundll32.exe

ID	4
File Name	c:\windows\syswow64\rundll32.exe
Command Line	"C:\Windows\SysWOW64\rundll32.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 77573, Reason: Child Process
Unmonitor End Time	End Time: 192500, Reason: Terminated
Monitor duration	114.93s
Return Code	1073807364
PID	4000
Parent PID	1116
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\keecfmwgj\desktop\cc.exe	0xf98	0x70000(458752)	0x29000	✓	1
Modify Memory	#2: c:\users\keecfmwgj\desktop\cc.exe	0xf98	0x350000(3473408)	0xe000	✓	1

Host Behavior

Type	Count
File	209
-	1
-	1
System	16841
User	1
Mutex	2
Process	5
Module	11
Registry	1814
-	6
COM	1

Process #5: cmd.exe

ID	5
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c del "C:\Users\kEecfMwgj\Desktop\cc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 81653, Reason: Child Process
Unmonitor End Time	End Time: 83398, Reason: Terminated
Monitor duration	1.75s
Return Code	0
PID	4012
Parent PID	4000
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	19

Process #7: winzvg4hxq8.exe

ID	7
File Name	c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe
Command Line	"C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 227807, Reason: Autostart
Unmonitor End Time	End Time: 283235, Reason: Terminated by Timeout
Monitor duration	55.43s
Return Code	Unknown
PID	1328
Parent PID	1108
Bitness	32 Bit

Host Behavior

Type	Count
Environment	3
Registry	4
User	1
Process	1
-	132
File	20
Module	13
System	3
Window	14
-	2
-	5

Process #8: winzvg4hxq8.exe

ID	8
File Name	c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe
Command Line	"C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 260375, Reason: Child Process
Unmonitor End Time	End Time: 269170, Reason: Terminated
Monitor duration	8.79s
Return Code	0
PID	828
Parent PID	1328
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x534	0x400000(4194304)	0x200	✓	1
Modify Memory	#7: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x534	0x401000(4198400)	0x27c00	✓	1
Modify Memory	#7: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x534	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#7: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x534 / 0x340		-	✓	1

Host Behavior

Type	Count
File	9
-	1
-	1
System	3
Module	14
User	1
Mutex	1
Environment	1
Process	6
-	8
-	3

Process #9: explorer.exe

ID	9
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 263082, Reason: Injection
Unmonitor End Time	End Time: 283235, Reason: Terminated by Timeout
Monitor duration	20.15s
Return Code	Unknown
PID	1108
Parent PID	1088
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x340	0x7530000(122880000)	0x189000	✓	1
Modify Control Flow	#8: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x340 / 0x458	0xff0e5b60(4279130976)	-	✓	1
Modify Control Flow	#8: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x340 / 0x458	0x761a909(123840777)	-	✓	1
Modify Memory	#10: c:\windows\syswow64\ipconfig.exe	0x5c4	0x9310000(154206208)	0x1b58000	✓	1
Modify Memory	#10: c:\windows\syswow64\ipconfig.exe	0x5c4	0x7120000(118620160)	0x10c000	✓	1
Modify Control Flow	#10: c:\windows\syswow64\ipconfig.exe	0x5c4 / 0x458	0x28f418(2683928)	-	✓	1
Modify Control Flow	#10: c:\windows\syswow64\ipconfig.exe	0x5c4 / 0x458	0x71a68f2(119171314)	-	✓	1

Host Behavior

Type	Count
Process	2

Process #10: ipconfig.exe

ID	10
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	"C:\Windows\SysWOW64\ipconfig.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 263565, Reason: Child Process
Unmonitor End Time	End Time: 283235, Reason: Terminated by Timeout
Monitor duration	19.67s
Return Code	Unknown
PID	848
Parent PID	1108
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x340	0x70000(458752)	0x29000	✓	1
Modify Memory	#8: c:\program files (x86)\cmrkpgp\winzvg4hxq8.exe	0x340	0x680000(6815744)	0xa000	✓	1

Host Behavior

Type	Count
File	11
-	1
-	1
System	12
User	1
Mutex	2
Registry	4
Module	10
Process	4
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
83242a0f42be34e66e502e4a3a45d2470f3b24aef8a1d8484711f4439d7fe74a	C:\Users\kEecfMwgj\Desktop\cc.exe	Sample File	1024.00 KB	application/vnd.microsoft.portable-executable	Access, Delete	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\cc.exe.config	Accessed File	Access	CLEAN
\??\C:\Windows\SysWOW64\ntdll.dll	Accessed File	Access, Read, Create	CLEAN
\??\C:\Windows\SysWOW64\rundll32.exe	Accessed File	Access, Read, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\Desktop\cc.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\Desktop\cc.exe	Accessed File	Access, Read, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\cc.exe	Sample File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop	Accessed File	Access	CLEAN
\??\C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe	Accessed File	Access, Read, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\Cmrkpgp	Accessed File	Access, Create	CLEAN
\??\C:\Users\KEECFM~1\AppData\Local\Temp\Cmrkpgp\winzvg4hxq8.exe	Accessed File	Access, Delete, Write	CLEAN
C:\Program Files (x86)\Cmrkpgp	Accessed File	Access, Write, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\179M615Q\179logrc.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\179M615Q\179logri.ini	Accessed File	Access, Create	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
\??\C:\Program Files\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\179M615Q\179logrv.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\Default\Cookies	Accessed File	Access, Create	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\Opera Software\Opera Stable\Cookies	Accessed File	Access, Create	CLEAN
\??\C:\Cookies.sqlite	Accessed File	Access, Create	CLEAN
C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe.config	Accessed File	Access	CLEAN
\??\C:\Windows\SysWOW64\ipconfig.exe	Accessed File	Access, Read, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.esomvw.com/mjyv/?MI=84GmfEOeezwjENHIvrBoemsYeWt0m/HwoH8hmSCYYDVvISXm81Rnn8BPdG66LOse7+JH3wWm&gXzt_B=DN9xx4XpOBr0b	-	104.18.26.58	-	GET	CLEAN
http://www.esomvw.com/mjyv/	-	104.18.26.58	-	POST	CLEAN
http://www.deskbk.com/mjyv/?MI=elfYEudHYjWRBKVQqa1FwjnBNMNthSMPxSU2Ae2RzX6JH+UIo+4qi3qp9hj2WZGr6riIWckf&gXzt_B=DN9xx4XpOBr0b	-	156.226.250.168	-	GET	CLEAN
http://www.anielleharris.com/mjyv/?MI=VdqIn5ATadMqw6pgyqzwjUU2K1KmNIW0QhXn4TeZ4+V516gxmgYomdsi8jTWk431wR4xkLLj&gXzt_B=DN9xx4XpOBr0b	-	23.227.38.74	-	GET	CLEAN
http://www.lightfootsteps.com/mjyv/?MI=ZaGFmHO9QjcqyRss7Kbl6J403dr6bz+HcnVoXiL1W+dYgLy7T488fufqvcQ1zRSwoJw29pJ4&gXzt_B=DN9xx4XpOBr0b	-	204.11.56.48	-	GET	CLEAN
http://www.jspagnier-graveur.com/mjyv/?MI=Th83Ckvp/531Tl/GX4RX7Dh2QUTLyutGF176aUX2OVMJp6JNPl80WTgR6fQGzE7qZTwZp8ZB&gXzt_B=DN9xx4XpOBr0b	-	23.20.208.181	-	GET	CLEAN
http://www.single-on-purpose.com/mjyv/?MI=Q7OMrrPP6VpxrdE1nYHLlQBfBwjE9EOakY/k4TZPYOQ1+efX2FR/5nxasJQT51ckttjnkljO&gXzt_B=DN9xx4XpOBr0b	-	192.0.78.24	-	GET	CLEAN
http://www.anielleharris.com/mjyv/	-	23.227.38.74	-	POST	CLEAN
http://www.lightfootsteps.com/mjyv/	-	204.11.56.48	-	POST	CLEAN
http://www.jspagnier-graveur.com/mjyv/	-	23.20.208.181	-	POST	CLEAN
http://www.single-on-purpose.com/mjyv/	-	192.0.78.24	-	POST	CLEAN
http://www.totalselfconfidence.net/mjyv/?MI=7+dRD0VfrOquXVxTGZgRO8F9r9A4udAqY3P1KQFKJ8W9R0Kxy+STzHlFMkDcQByvMxKiuXRM&gXzt_B=DN9xx4XpOBr0b	-	156.239.192.219	-	GET	CLEAN
http://www.livinglovinglincoln.com/mjyv/?MI=v6+mrmg92knFd2hB4m8c7LRaoFH4FGs5nhP+0lUaaW8DwAWWNnjucsjLIXZS4yksGO7kPpSc&gXzt_B=DN9xx4XpOBr0b	-	34.102.136.180	-	GET	CLEAN
http://www.bjjinmei.com/mjyv/?MI=tK48cpM9c53SDiUBEb9HKzRmP2wH5JkMCWpRDhGyYNy0ifXLmO4jSTOPfRY6+Bx01EWV18pV&gXzt_B=DN9xx4XpOBr0b	-	154.205.217.133	-	GET	CLEAN
http://www.murdabudz.com/mjyv/?MI=hg13/nUaX9mUx8sSJIJYfgV6jTQ/W4br/c2NzJsxCbwCh/fzBEDuEbvVWcjNmMf2/7hygaPQ&gXzt_B=DN9xx4XpOBr0b	-	160.153.136.3	-	GET	CLEAN
http://www.simpeltattofor.men/mjyv/?MI=YF19Yjtl8/UPVOzf/wHjSkaABDmeFeWIluMalRBS1oahuHz0Fdc7+ZeWTOXaxJbXSsdeR5U0&gXzt_B=DN9xx4XpOBr0b	-	103.224.182.210	-	GET	CLEAN
http://www.1971event.com/mjyv/?MI=dCk/M3RqXmnriH5Dpo5+kGUPt2Tx4Jc7I1qyuUsiRnJePv/CPBZ7QEiY+Ijzn1XuWA0anRMV&MDK0g=m2MpP03h	-	35.206.96.200	-	GET	CLEAN
http://www.corlora.com/mjyv/?MI=FJb0UZ1EIi2iZyz9b6sDaOfhvWc1+IVn9AMjAgVGnTau2aQQ7z/C35fdWtWFhzsPoN7gw81Ka&MDK0g=m2MpP03h	-	23.227.38.74	-	GET	CLEAN
http://www.livinglovinglincoln.com/mjyv/	-	34.102.136.180	-	POST	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.noun-bug.com/mjyv/?MI=/e6GyVavtbTelz9m0WWy93DWNbpPODk8+8mRaUmDSGSQSMIeKfo2rpsXGYfN6k+L2XrTjDzG&gXzt_B=DN9xx4XpOBr0b	-	162.0.213.105	-	GET	CLEAN
http://www.bjjinmei.com/mjyv/	-	154.205.217.133	-	POST	CLEAN
http://www.murdabudz.com/mjyv/	-	160.153.136.3	-	POST	CLEAN
http://www.simpeltattofor.men/mjyv/	-	103.224.182.210	-	POST	CLEAN
http://www.corlora.com/mjyv/	-	23.227.38.74	-	POST	CLEAN
http://www.noun-bug.com/mjyv/	-	162.0.213.105	-	POST	CLEAN
http://www.productprinting.online/mjyv/	-	108.179.246.105	-	POST	CLEAN
http://www.productprinting.online/mjyv/?MI=dl0EVfvGTcPWZQJTCCwwBrtyXsKLoNwUe8Jfo4lOgU2AXLHTPdQLz/5V0DEerltniF7xTL1s&MDK0g=m2MpP03h	-	108.179.246.105	-	GET	CLEAN
http://www.mabduh.com/mjyv/?MI=46trCuL+qj46sXtcEXelMa5KUSrIckjmnhHha+k1BNltaaPzLSYu+3DxHEUEWTfM5pLHPeQT&MDK0g=m2MpP03h	-	206.189.58.26	-	GET	CLEAN
http://www.mabduh.com/mjyv/	-	206.189.58.26	-	POST	CLEAN
http://www.krveop.com/mjyv/?MI=HyN26Cpbz7/YQUft90o9zs1nCJbgg4mk/6cvH3irtRiIVkmcITk2bmmTD+Kmlot5gaHIkoQ3&MDK0g=m2MpP03h	-	172.67.158.14	-	GET	CLEAN
http://www.lkkogltoyof4.xyz/mjyv/	-	150.95.255.38	-	POST	CLEAN
http://www.lkkogltoyof4.xyz/mjyv/?MI=EAnvUfcUxKKIiiQnQI88cMi+J9woX5wjkbbwLQW1UVDUs3UxvXHKg6261p2I2O3lsj46KHPB&MDK0g=m2MpP03h	-	150.95.255.38	-	GET	CLEAN
http://www.yogo7.net/mjyv/?MI=jdeYqH68CS7uHwPF/IFQ000KzvKwE38RqZbU2k7yUZMS+iAtH2XF+eLIXJjI7FDVVXC+S/fz&MDK0g=m2MpP03h	-	156.240.160.90	-	GET	CLEAN
http://www.krveop.com/mjyv/	-	172.67.158.14	-	POST	CLEAN
http://www.yogo7.net/mjyv/	-	156.240.160.90	-	POST	CLEAN
http://www.totalselfconfidence.net/mjyv/	-	156.239.192.219	-	POST	CLEAN
http://www.deskbk.com/mjyv/	-	156.226.250.168	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.reemletenleafy.com	-	-	DNS	CLEAN
www.esomvw.com	104.18.27.58, 104.18.26.58	-	HTTP, DNS	CLEAN
shops.myfunpinpin.com	104.18.27.58, 104.18.26.58	-	DNS	CLEAN
www.deskbk.com	156.226.250.168	-	HTTP, DNS	CLEAN
www.anielleharris.com	23.227.38.74	-	HTTP, DNS	CLEAN
shops.myshopify.com	23.227.38.74	-	DNS	CLEAN
www.lightfootsteps.com	204.11.56.48	-	HTTP, DNS	CLEAN
www.jspagnier-graveur.com	23.20.208.181, 54.85.93.188	-	HTTP, DNS	CLEAN
comingsoon.namebright.com	23.20.208.181, 54.85.93.188	-	DNS	CLEAN
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	23.20.208.181, 54.85.93.188	-	DNS	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.single-on-purpose.com	192.0.78.24, 192.0.78.25	-	HTTP, DNS	CLEAN
single-on-purpose.com	192.0.78.24, 192.0.78.25	-	HTTP, DNS	CLEAN
www.totalselfconfidence.net	156.239.192.219	-	HTTP, DNS	CLEAN
www.medicalmanagementinc.info	-	-	DNS	CLEAN
www.babybox.media	-	-	DNS	CLEAN
www.wenyuexuan.com	-	-	DNS	CLEAN
www.livinglovinglincoln.com	34.102.136.180	-	HTTP, DNS	CLEAN
livinglovinglincoln.com	34.102.136.180	-	HTTP, DNS	CLEAN
www.bjjinmei.com	154.205.217.133	-	HTTP, DNS	CLEAN
www.murdabudz.com	160.153.136.3	-	HTTP, DNS	CLEAN
murdabudz.com	160.153.136.3	-	HTTP, DNS	CLEAN
www.simpeltattofor.men	103.224.182.210	-	HTTP, DNS	CLEAN
www.1971event.com	35.206.96.200	-	HTTP, DNS	CLEAN
www.corlora.com	23.227.38.74	-	HTTP, DNS	CLEAN
www.noun-bug.com	162.0.213.105	-	HTTP, DNS	CLEAN
www.productprinting.online	108.179.246.105	-	HTTP, DNS	CLEAN
productprinting.online	108.179.246.105	-	HTTP, DNS	CLEAN
www.mabduh.com	206.189.50.60, 206.189.58.26	-	HTTP, DNS	CLEAN
www.krveop.com	104.21.49.26, 172.67.158.14	-	HTTP, DNS	CLEAN
www.lkkogltoyof4.xyz	150.95.255.38	-	HTTP, DNS	CLEAN
www.yogo7.net	156.240.160.90	-	HTTP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
104.18.26.58	www.esomvw.com, shops.myfunpinpin.com	-	HTTP, DNS, TCP	CLEAN
156.226.250.168	www.deskbk.com	South Africa	HTTP, DNS, TCP	CLEAN
23.227.38.74	www.anielleharris.com, www.corlora.com, shops.myshopify.com	Canada	HTTP, DNS, TCP	CLEAN
204.11.56.48	www.lightfootsteps.com	Virgin Islands	HTTP, DNS, TCP	CLEAN
23.20.208.181	comingsoon.namebright.com, www.jspagnier-graveur.com, cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States	HTTP, DNS, TCP	CLEAN
192.0.78.24	single-on-purpose.com, www.single-on-purpose.com	United States	HTTP, DNS, TCP	CLEAN
156.239.192.219	www.totalselfconfidence.net	United States	HTTP, DNS, TCP	CLEAN
34.102.136.180	www.livinglovinglincoln.com, livinglovinglincoln.com	United States	HTTP, DNS, TCP	CLEAN
154.205.217.133	www.bjjinmei.com	United States	HTTP, DNS, TCP	CLEAN
160.153.136.3	www.murdabudz.com, murdabudz.com	Netherlands	HTTP, DNS, TCP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
103.224.182.210	www.simpeltattofor.men	Australia	HTTP, DNS, TCP	CLEAN
35.206.96.200	www.1971event.com	United States	HTTP, DNS, TCP	CLEAN
162.0.213.105	www.noun-bug.com	United States	HTTP, DNS, TCP	CLEAN
108.179.246.105	productprinting.online, www.productprinting.online	United States	HTTP, DNS, TCP	CLEAN
206.189.58.26	www.mabduh.com	Germany	HTTP, DNS, TCP	CLEAN
172.67.158.14	www.krveop.com	United States	HTTP, DNS, TCP	CLEAN
150.95.255.38	www.lkkogltoyof4.xyz	Japan	HTTP, DNS, TCP	CLEAN
156.240.160.90	www.yogo7.net	Hong Kong	HTTP, DNS, TCP	CLEAN
104.18.27.58	www.esomvw.com, shops.myfunpinpin.com	-	DNS	CLEAN
54.85.93.188	comingsoon.namebright.com, www.jspagnier-graveur.com, cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States	DNS	CLEAN
192.0.78.25	single-on-purpose.com, www.single-on-purpose.com	United States	DNS	CLEAN
206.189.50.60	www.mabduh.com	Germany	DNS	CLEAN
104.21.49.26	www.krveop.com	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
62AQ09U8C34JCCAZ	access	cc.exe	CLEAN
O03PR-DCBVW8A2DZ	access	rundll32.exe	CLEAN
-099ODE3WG-67X0J	access	ipconfig.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	cc.exe, winzvg4hxq8.exe	CLEAN
HKEY_LOCAL_MACHINE	access	cc.exe, winzvg4hxq8.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	cc.exe, winzvg4hxq8.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	cc.exe, winzvg4hxq8.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	cc.exe, winzvg4hxq8.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access, create	ipconfig.exe, rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	ipconfig.exe, rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\LRQPL	access, write	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook\	access, create	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\22165c4f0be62c48b2e3e9aef6ce3db3	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\4b31ac339b3c6047a5607d10314f5a05	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\81fb1dc666658c4bb96e792ef5ce3051	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\94ba7772fb349a48ba2cc741623a1549	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\a44d88fba08a5547a1aaad50659b22d8	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\ae0727370bd4364ea1d3e75390877e70	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\c1b3326b5fa84f45970fa09da288db37	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook_2016\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\	access, create	rundll32.exe	CLEAN

Process

Process Name	Commandline	Verdict
cc.exe	"C:\Users\kEecfMwgj\Desktop\cc.exe"	MALICIOUS

Process Name	Commandline	Verdict
cc.exe	"C:\Users\kEecfMwgj\Desktop\cc.exe"	MALICIOUS
winzvg4hxq8.exe	"C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe"	MALICIOUS
winzvg4hxq8.exe	"C:\Program Files (x86)\Cmrkpgp\winzvg4hxq8.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
rundll32.exe	"C:\Windows\SysWOW64\rundll32.exe"	SUSPICIOUS
cmd.exe	/c del "C:\Users\kEecfMwgj\Desktop\cc.exe"	SUSPICIOUS
ipconfig.exe	"C:\Windows\SysWOW64\ipconfig.exe"	SUSPICIOUS

YARA / AV

YARA (19)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	FormBook	FormBook	Function Strings	function_strings_process_4.txt	Spyware	5/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Sample File	C:\Users\kEecfMwgj\Desktop\cc.exe	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	MultipleNetObfuscatorAttributes	.NET file contains multiple obfuscator attributes	Memory Dump	-	-	2/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Sample File	C:\Users\kEecfMwgj\Desktop\cc.exe	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Sample File	C:\Users\kEecfMwgj\Desktop\cc.exe	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	YanoObfuscatorAttributes	Yano Obfuscator Attributes	Memory Dump	-	-	1/5
Generic	BabelObfuscatorAttributes	Babel Obfuscator Attributes	Memory Dump	-	-	1/5

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Razy.679962	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.679962	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows