MALICIOUS

Classifications: Injector | Spyware

Threat Names: Gen:Variant.Razy.679962

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**order.exe**
ID	#2365066
MD5	4e9095ceadd56bc68a99947ab929f691
SHA1	bce676ea49fb6709dc0e9a23df2e918e05b4074b
SHA256	1fe427cfa805bbabdc371ae3f6ccea4088ca76e8b9fce9828a74885d72339020
File Size	544.50 KB
Report Created	2021-06-10 19:31 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (20 rules, 79 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #1) order.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\Desktop\order.exe\".			
4/5	Injection	Writes into the memory of another process	3	Injector
	• (Process #4) addinprocess32.exe modifies memory of (process #5) explorer.exe. • (Process #6) wininit.exe modifies memory of (process #5) explorer.exe. • (Process #4) addinprocess32.exe modifies memory of (process #6) wininit.exe.			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #4) addinprocess32.exe alters context of (process #5) explorer.exe. • (Process #6) wininit.exe alters context of (process #5) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected a memory dump of (process #4) addinprocess32.exe as "Gen:Variant.Razy.679962".			
3/5	Input Capture	Captures clipboard data	1	Spyware
	• (Process #5) explorer.exe reads data from clipboard.			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #4) addinprocess32.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #4) addinprocess32.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #7) cmd.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) order.exe modifies memory of (process #4) addinprocess32.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) order.exe alters context of (process #4) addinprocess32.exe.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	22	-

Score	Category	Operation	Count	Classification
		• (Process #4) addinprocess32.exe makes a direct system call to "NtQuerySystemInformation". • (Process #4) addinprocess32.exe makes a direct system call to "NtQueryInformationProcess". • (Process #4) addinprocess32.exe makes a direct system call to "NtAllocateVirtualMemory". • (Process #4) addinprocess32.exe makes a direct system call to "NtFreeVirtualMemory". • (Process #4) addinprocess32.exe makes a direct system call to "NtOpenProcessToken". • (Process #4) addinprocess32.exe makes a direct system call to "NtAdjustPrivilegesToken". • (Process #4) addinprocess32.exe makes a direct system call to "NtClose". • (Process #4) addinprocess32.exe makes a direct system call to "NtOpenDirectoryObject". • (Process #4) addinprocess32.exe makes a direct system call to "NtCreateMutant". • (Process #4) addinprocess32.exe makes a direct system call to "NtCreateSection". • (Process #4) addinprocess32.exe makes a direct system call to "NtMapViewOfSection". • (Process #4) addinprocess32.exe makes a direct system call to "NtOpenProcess". • (Process #4) addinprocess32.exe makes a direct system call to "NtQueryInformationToken". • (Process #4) addinprocess32.exe makes a direct system call to "NtProtectVirtualMemory". • (Process #4) addinprocess32.exe makes a direct system call to "NtCreateFile". • (Process #4) addinprocess32.exe makes a direct system call to "NtQueryInformationFile". • (Process #4) addinprocess32.exe makes a direct system call to "NtDelayExecution". • (Process #4) addinprocess32.exe makes a direct system call to "NtReadVirtualMemory". • (Process #4) addinprocess32.exe makes a direct system call to "NtOpenThread". • (Process #4) addinprocess32.exe makes a direct system call to "NtReadFile". • (Process #4) addinprocess32.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #4) addinprocess32.exe makes a direct system call to "NtResumeThread".		
1/5	Privilege Escalation	Enables process privilege	1	-
		• (Process #1) order.exe enables process privilege "SeDebugPrivilege".		
1/5	Hide Tracks	Creates process with hidden window	3	-
		• (Process #1) order.exe starts (process #4) addinprocess32.exe with a hidden window. • (Process #5) explorer.exe starts (process #5) explorer.exe with a hidden window. • (Process #6) wininit.exe starts (process #7) cmd.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	3	-
		• (Process #1) order.exe reads from (process #4) addinprocess32.exe. • (Process #4) addinprocess32.exe reads from (process #5) explorer.exe. • (Process #4) addinprocess32.exe reads from (process #6) wininit.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #1) order.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Mutex	Creates mutex	3	-
		• (Process #4) addinprocess32.exe creates mutex with name "NPL-29QSRXYEDYz9". • (Process #6) wininit.exe creates mutex with name "NPL-29QSRXYEDYz9". • (Process #6) wininit.exe creates mutex with name "K-RP6UTCADV8AHFB".		
1/5	Execution	Drops PE file	1	-
		• Drops file C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe.		
1/5	Execution	Executes dropped PE file	1	-
		• Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe".		

Score	Category	Operation	Count	Classification
1/5	Network Connection	Performs DNS request	16	-

- (Process #1) order.exe resolves host name "www.google.com" to IP "142.250.186.164".
- (Process #1) order.exe resolves host name "www.bing.com" to IP "204.79.197.200".
- (Process #5) explorer.exe resolves host name "www.chicskr.com" to IP "-".
- (Process #5) explorer.exe resolves host name "www.smshare2u.com" to IP "204.11.56.48".
- (Process #5) explorer.exe resolves host name "www.murrayburngundogs.com" to IP "192.0.78.25".
- (Process #5) explorer.exe resolves host name "www.hertsandlondonknee.com" to IP "94.136.40.51".
- (Process #5) explorer.exe resolves host name "www.tldyyl.com" to IP "141.98.163.216".
- (Process #5) explorer.exe resolves host name "www.cosmoandcocrafts.com" to IP "199.34.228.173".
- (Process #5) explorer.exe resolves host name "www.dapurbuageung.com" to IP "5.181.216.116".
- (Process #5) explorer.exe resolves host name "www.lileshop.com" to IP "107.149.24.216".
- (Process #5) explorer.exe resolves host name "www.axmpjbwqh.icu" to IP "104.252.218.228".
- (Process #5) explorer.exe resolves host name "www.mychallengeiam.com" to IP "162.210.70.10".
- (Process #5) explorer.exe resolves host name "www.roamallday.com" to IP "154.215.208.44".
- (Process #5) explorer.exe resolves host name "www.garantiservice.com" to IP "93.188.2.51".
- (Process #5) explorer.exe resolves host name "www.pakistanwholesaler.com" to IP "148.66.138.152".
- (Process #5) explorer.exe resolves host name "www.timeforbusinessblog.xyz" to IP "198.54.117.216".

Score	Category	Operation	Count	Classification
1/5	Network Connection	Connects to remote host	15	-

- (Process #1) order.exe opens an outgoing TCP connection to host "142.250.186.164:443".
- (Process #1) order.exe opens an outgoing TCP connection to host "204.79.197.200:443".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "204.11.56.48:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "192.0.78.25:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "94.136.40.51:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "141.98.163.216:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "199.34.228.173:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "5.181.216.116:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "107.149.24.216:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "104.252.218.228:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "162.210.70.10:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "93.188.2.51:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "148.66.138.152:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "154.215.208.44:80".
- (Process #5) explorer.exe opens an outgoing TCP connection to host "198.54.117.216:80".

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	1	-

- File "C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe" is a known clean file.

Mitre ATT&CK Matrix

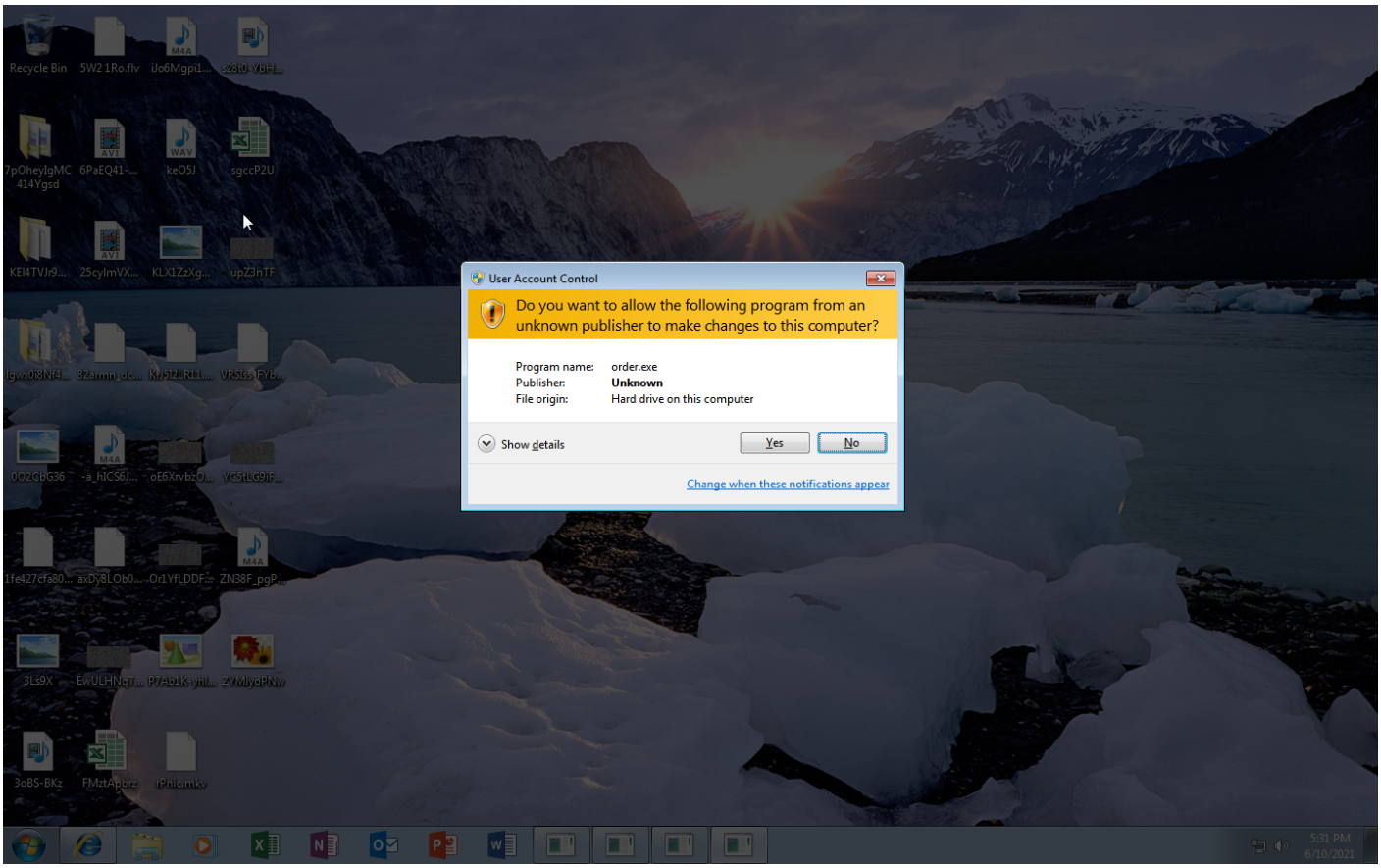
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1096 NTFS File Attributes				#T1115 Clipboard Data			
				#T1143 Hidden Window							
				#T1045 Software Packing							

Sample Information

ID	#2365066
MD5	4e9095ceadd56bc68a99947ab929f691
SHA1	bce676ea49fb6709dc0e9a23df2e918e05b4074b
SHA256	1fe427cfa805bbabdc371ae3f6ccea4088ca76e8b9fce9828a74885d72339020
SSDeep	6144:mP2KJg5YoBA4cG+qw1y/lcCcfcgjXLSua0QxCiNLd7UXm7Ej2l++7dWS9WVKBlch:m1MA4cScHfc4euixCiZiXurSkV6y
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	order.exe
File Size	544.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-06-10 19:31 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	5
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


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

NETWORK

General

31.02 KB total sent

247.11 KB total received

2 ports 80, 443

16 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

18 DNS requests for 16 domains

1 nameservers contacted

2 total requests returned errors

HTTP/S

28 URLs contacted, 15 servers

29 sessions, 28.55 KB sent, 218.12 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.smshare2u.com/sadn/?CJE=giAtDIne1Uhp38wV4thNWjg7Rtw8gtubxLwuzmJqi4rLt4OmXEVJ6rHNlmS/pZc10TbTqJyY&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.smshare2u.com/sadn/	-	-		0 bytes	NA
POST	http://www.murrayburngundogs.com/sadn/	-	-		0 bytes	NA
GET	http://www.murrayburngundogs.com/sadn/?CJE=YP0P6T22YyWwka/tlVJcwYRwU4fZn4lUdmTQUfy+EMiLuzGhRp3/KU5SB2qzYtZw8+FjVWkW&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.hertsandlondonknee.com/sadn/	-	-		0 bytes	NA
GET	http://www.hertsandlondonknee.com/sadn/?CJE=Y+EWi7LsbzESvTaYcZcVPMukst4zWC1oEWA+MhGZL1ytEBTvJ3WmD4phWWbDBPBwtRq+K+2u&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
GET	http://www.tldyyl.com/sadn/?CJE=nTdkx300uruzJeOujIJvhhpdAwnyKQR5yjJ8aY0pdBSFLsZ0CoF79kwWvpFn7N88y6QCNosF&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.tldyyl.com/sadn/	-	-		0 bytes	NA
GET	http://www.cosmoandcocrafts.com/sadn/?CJE=JDWIJLVrmA6bOrpL+RfNkAQNCXDNwF1p/RKDPBrQonnmYSh3QKWU+n5G5KLjhkgUxi8zkjNv&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.cosmoandcocrafts.com/sadn/	-	-		0 bytes	NA
GET	http://www.dapurbuageung.com/sadn/?CJE=V7KUIVAJcxUgOM1pz34t5Sn/U3PckgxFx/Wlp4wqftg7gAUUuvMLEoy5krW/UNyHXy9/5ytD&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.dapurbuageung.com/sadn/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.lileshop.com/sadn/?CJE=ikprQUWlBCZGnMKUN1xAk0NR6BrQdr6Ex/LmOk8TTE+fS067pCd7yCOYNTViNteg9/0UaDJH&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.lileshop.com/sadn/	-	-		0 bytes	NA
GET	http://www.axmpjbwqh.icu/sadn/?CJE=3iAQ4QeeKEHkIBAEVl9z1CO1O992WiwDiWM9265/nEQASGKqWPj08NBwbEnV+M3ncQk4hiZM&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.axmpjbwqh.icu/sadn/	-	-		0 bytes	NA
GET	http://www.mychallengeiam.com/sadn/?CJE=sUNOm3KXMvpSrkfMrYXNDO2+58RRmbW6BAhhLbIPcGxV1sxyut+O5mwc8ozue9dNMR5impC5&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.mychallengeiam.com/sadn/	-	-		0 bytes	NA
GET	http://www.roamallday.com/sadn/?CJE=Z99uQ+o0CUSuwDeDRQMfWXf8t2N5R94N8M0fZniL+RUkLm6FrJeUV4BmDBTmkCx+PsiTulda&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
GET	http://www.garantiservice.com/sadn/?CJE=Fp6ir5BTuXl4RAZtixBM/qJoaLMFvckFssremE4H0HjvzUBxHiu+dGw99x12wtKKNjxNlubr&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.garantiservice.com/sadn/	-	-		0 bytes	NA
GET	http://www.pakistanwholesaler.com/sadn/?CJE=0OCk9xNtdUwxJtNbaFBmeerTTDMh6YiZInCrJYbRD3/jFOOEMv7LjtPxz7TE4yJsvg4gTZ1G&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
POST	http://www.pakistanwholesaler.com/sadn/	-	-		0 bytes	NA
POST	http://www.roamallday.com/sadn/	-	-		0 bytes	NA
POST	http://www.timeforbusinessblog.xyz/sadn/	-	-		0 bytes	NA
GET	http://www.timeforbusinessblog.xyz/sadn/?CJE=tse2JoLHzdTnskMvzE3J2caKd/oSidqO/622il3VeqauHCFZRd4UF0+PwaNO6Ri7YEqo/VOQ&nnlH=u8pl2trpMphxq	-	-		0 bytes	NA
GET	https://www.google.com/	-	-		0 bytes	NA
GET	https://www.bing.com/	-	-		0 bytes	NA

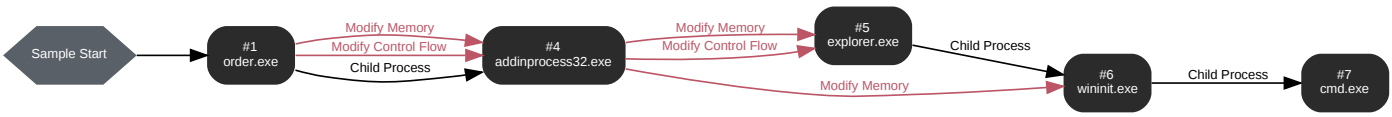
DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.google.com	NoError	142.250.186.164		NA
A	www.bing.com, a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, dual-a-0001.a-msedge.net	NoError	204.79.197.200, 13.107.21.200	a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, dual-a-0001.a-msedge.net	NA
A	www.chicskr.com	NXDomain			NA
A	www.smshare2u.com	NoError	204.11.56.48		NA
A	www.murrayburngundogs.com, murrayburngundogs.com	NoError	192.0.78.25, 192.0.78.24	murrayburngundogs.com	NA
A	www.hertsandlondonknee.com	NoError	94.136.40.51		NA
A	www.tldyyl.com	NoError	141.98.163.216		NA
A	www.cosmoandcocrafts.com	NoError	199.34.228.173		NA
A	www.dapurbuageung.com, dapurbuageung.com	NoError	5.181.216.116	dapurbuageung.com	NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.lileshop.com	NoError	107.149.24.216		NA
A	www.axmpjbwqh.icu	NoError	104.252.218.228		NA
A	www.mychallengeiam.com, mychallengeiam.com	NoError	162.210.70.10	mychallengeiam.com	NA
A	www.roamallday.com	NoError	154.215.208.44		NA
A	www.garantiservice.com	NoError	93.188.2.51		NA
A	www.pakistanwholesaler.com, pakistanwholesaler.com	NoError	148.66.138.152	pakistanwholesaler.com	NA
A	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	NoError	198.54.117.216, 198.54.117.212, 198.54.117.218, 198.54.117.217, 198.54.117.215, 198.54.117.210, 198.54.117.211	parkingpage.namecheap.com	NA
-	www.bing.com	-	204.79.197.200, 13.107.21.200		NA

BEHAVIOR

Process Graph



Process #1: order.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\order.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\order.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 39371, Reason: Analysis Target
Unmonitor End Time	End Time: 160294, Reason: Terminated
Monitor duration	120.92s
Return Code	0
PID	3664
Parent PID	876
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	153.21 KB	07fdf8bc502e6bb4cf6ae214694f45c54a53228fc2002b2f17c9a2ef64eb76f6	✗
-	58.67 KB	65830a65cb913bee83258e4ac3e140faf131e7eb084d39f7020c7acc825b0a58	✗
C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe	41.07 KB	43e96d4445fa7a451ffe1aa03c8c05df1364be2ec2f05d2cb135690a615af0cb	✗

Host Behavior

Type	Count
Registry	50
Process	1
File	25
-	11
User	1
Module	662
System	9
Environment	11
-	3
-	5

Network Behavior

Type	Count
HTTPS	3
DNS	3
TCP	3

Process #4: addinprocess32.exe

ID	4
File Name	c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150630, Reason: Child Process
Unmonitor End Time	End Time: 171596, Reason: Terminated
Monitor duration	20.97s
Return Code	0
PID	3848
Parent PID	3664
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\order.exe	0xe54	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\order.exe	0xe54	0x401000(4198400)	0x27000	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\order.exe	0xe54	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\order.exe	0xe54 / 0xf0c		-	✓	1

Host Behavior

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

Process #5: explorer.exe

ID	5
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156910, Reason: Injection
Unmonitor End Time	End Time: 281772, Reason: Terminated by Timeout
Monitor duration	124.86s
Return Code	Unknown
PID	876
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe	0xf0c	0x25e0000(39714816)	0x154000	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe	0xf0c / 0x13c	0xaebb0(715696)	-	✓	1
Modify Control Flow	#4: c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe	0xf0c / 0x13c	0x26961b9(40460729)	-	✓	1
Modify Memory	#6: c:\windows\syswow64\wininit.exe	0xf30	0xa100000(168820736)	0x1b58000	✓	1
Modify Memory	#6: c:\windows\syswow64\wininit.exe	0xf30	0x4820000(75628544)	0x177000	✓	1
Modify Control Flow	#6: c:\windows\syswow64\wininit.exe	0xf30 / 0x13c	0x3c(60)	-	✓	1
Modify Control Flow	#6: c:\windows\syswow64\wininit.exe	0xf30 / 0x13c	0x49121a2(76620194)	-	✓	1

Host Behavior

Type	Count
Process	154
System	47

Network Behavior

Type	Count
HTTP	26
DNS	15
TCP	39

Process #6: wininit.exe

ID	6
File Name	c:\windows\syswow64\wininit.exe
Command Line	"C:\Windows\SysWOW64\wininit.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 161386, Reason: Child Process
Unmonitor End Time	End Time: 281772, Reason: Terminated by Timeout
Monitor duration	120.39s
Return Code	Unknown
PID	3884
Parent PID	876
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe	0xf0c	0x70000(458752)	0x28000	✓	1
Modify Memory	#4: c:\users\keecfmwgj\appdata\local\temp\addinprocess32.exe	0xf0c	0x5d0000(6094848)	0x1a000	✓	1

Host Behavior

Type	Count
File	12
-	1
-	1
System	98
User	1
Mutex	2
Process	5
Module	10
Registry	2
-	6

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c del "C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 165513, Reason: Child Process
Unmonitor End Time	End Time: 168008, Reason: Terminated
Monitor duration	2.50s
Return Code	0
PID	3896
Parent PID	3884
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	18

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1fe427cfa805bbabdc371ae3f6ccea4088ca76e8b9fce9828a74885d72339020	C:\Users\kEecfMwgj\Desktop\order.exe	Sample File	544.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
43e96d4445fa7a451ffe1aa03c8c05df1364be2ec2f05d2cb135690a615af0cb	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe, C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe, C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe	Dropped File	41.07 KB	application/vnd.microsoft.portable-executable	Create, Delete, Access, Write	SUSPICIOUS
07fdf8bc502e6bb4cf6ae214694f45c54a53228fc2002b2f17c9a2ef64eb76f6	authroot.stl	Embedded File	153.21 KB	application/octet-stream	-	CLEAN
65830a65cb913bee83258e4ac3e140faf131e7eb084d39f7020c7acc825b0a58	c:\users\keecfmwgj\appdata\local\temp\cab66a5.tmp	Downloaded File	58.67 KB	application/vnd.ms-cab-compressed	-	CLEAN

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\order.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\order.exe	Sample File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\order.exe\:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\AddInProcess32.exe	Dropped File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe	Dropped File	Create, Delete, Access, Write	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe	Dropped File	Access	CLEAN
C:\Windows\SysWOW64\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
C:\Windows\syswow64\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\SspiCli.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
C:\Windows\system32\api-ms-win-core-synch-l1-2-0.DLL	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\syswow64\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\LPK.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\USP10.dll	Accessed File	Access	CLEAN
C:\Windows\system32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\syswow64\MSCTF.dll	Accessed File	Access	CLEAN
C:\Windows\system32\VERSION.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Windows\system32\VCRUNTIME140_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ucrtbase_clr0400.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\36eaccfde177c2e7b93b8dbdde4e012a\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\ole32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\2c3c912ea8f058f9d04c4650128feb3f\System.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\f7568d7f1b9d356f64779b4c0927cfb3\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\c9a4cbc00f690a9e3cddfc400f6e85bb\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\31fae3290fad30c31c98651462d22724\System.Core.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\df2dd09ed7c341842a104e1e668f184e\System.Data.ni.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Data\v4.0_4.0.0.0__b77a5c561934e089\System.Data.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\WS2_32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\NSI.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\CRYPT32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\MSASN1.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\15af16d373cf0528cb74fc73d365fdbf\System.Xml.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\a891970b44db9e340c3ef3efa95b793c\Microsoft.VisualBasic.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96f7edb07b12303f0ec2595c7f3778c7\System.Configuration.ni.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\shell32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\profapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\psapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rasapi32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rasman.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rtutils.dll	Accessed File	Access	CLEAN
C:\Windows\system32\mswsock.dll	Accessed File	Access	CLEAN
C:\Windows\System32\wshtcpip.dll	Accessed File	Access	CLEAN
C:\Windows\System32\wship6.dll	Accessed File	Access	CLEAN
C:\Windows\system32\winhttp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\webio.dll	Accessed File	Access	CLEAN
C:\Windows\system32\credssp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\IPHLPAPI.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\WINNSI.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\dhcpcsvc6.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\dhcpcsvc.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\RpcRtRemote.dll	Accessed File	Access	CLEAN
C:\Windows\system32\DNSAPI.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rasadhlp.dll	Accessed File	Access	CLEAN
C:\Windows\System32\fwpuclnt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\secur32.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schannel.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ncrypt.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\bcryptprimitives.dll	Accessed File	Access	CLEAN
C:\Windows\system32\USERENV.dll	Accessed File	Access	CLEAN
C:\Windows\system32\GPAPI.dll	Accessed File	Access	CLEAN
C:\Windows\system32\cryptnet.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\WLDAP32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\SensApi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\Cabinet.dll	Accessed File	Access	CLEAN
C:\Windows\system32\DEVRTL.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\e114780fd3ea5727401c06ea4f22ef35\System.Management.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Serv759bfb78#\434d944356ef49383de75240670cd55f\System.ServiceProcess.ni.dll	Accessed File	Access	CLEAN
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\gdiplus.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsCodecs.dll	Accessed File	Access	CLEAN
\??\C:\Windows\SysWOW64\ntdll.dll	Accessed File	Create, Access	CLEAN
\??\C:\Windows\SysWOW64\wininit.exe	Accessed File	Create, Access, Read	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Roaming\Temp\AddInProcess32.exe	Accessed File	Create, Access	CLEAN
\??\C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe	Accessed File	Create, Access, Read	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\ADDINP~1.EXE	Accessed File	Delete, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.smshare2u.com/sadn/?CJE=giAtDIne1Uhp38wV4thNWjg7Rtw8gtubxLwuzmJqi4rLt4OmXEVJ6rHNImS/pZc10TbTqJyY&nnlH=u8pl2trpMphxq	-	204.11.56.48	-	GET	CLEAN
http://www.smshare2u.com/sadn/	-	204.11.56.48	-	POST	CLEAN
http://www.murrayburngundogs.com/sadn/	-	192.0.78.25	-	POST	CLEAN
http://www.murrayburngundogs.com/sadn/?CJE=YP0P6T22YyWwka/tlVJcwYRwU4fZn4lUdmTQUfy+EMiLuzGhRp3/KU5SB2qzYtZw8+FjVWkW&nnlH=u8pl2trpMphxq	-	192.0.78.25	-	GET	CLEAN
http://www.hertsandlondonknee.com/sadn/	-	94.136.40.51	-	POST	CLEAN
http://www.hertsandlondonknee.com/sadn/?CJE=Y+EWi7LsbzESvTaYcZcVPMukst4zWC1oEWA+MhGZL1ytEBTvJ3WmD4phWWbDBPBwtRq+K+2u&nnlH=u8pl2trpMphxq	-	94.136.40.51	-	GET	CLEAN
http://www.tldyyl.com/sadn/?CJE=nTdkx300uruzJeOujIJvhhpdAwnyKQR5yjJ8aY0pdBSFLsZ0CoF79kwWvpFn7N88y6QCNosF&nnlH=u8pl2trpMphxq	-	141.98.163.216	-	GET	CLEAN
http://www.tldyyl.com/sadn/	-	141.98.163.216	-	POST	CLEAN
http://www.cosmoandcocrafts.com/sadn/?CJE=JDWIJLVrmA6bOrpL+RfNkAQNCXDNwF1p/RKDPBrQonnmYSh3QKWU+n5G5KLjhkgUxi8zkjNv&nnlH=u8pl2trpMphxq	-	199.34.228.173	-	GET	CLEAN
http://www.cosmoandcocrafts.com/sadn/	-	199.34.228.173	-	POST	CLEAN
http://www.dapurbuageung.com/sadn/?CJE=V7KUIVAJcxUgOM1pz34t5Sn/U3PckgxFx/Wlp4wqftg7gAUUuvMLEoy5krW/UNyHXy9/5ytD&nnlH=u8pl2trpMphxq	-	5.181.216.116	-	GET	CLEAN
http://www.dapurbuageung.com/sadn/	-	5.181.216.116	-	POST	CLEAN
http://www.lileshop.com/sadn/?CJE=ikprQUWIBCZGnMKUN1xAk0NR6BrQdr6Ex/LmOk8TTE+fS067pCd7yCOYNTViNteg9/0UaDJH&nnlH=u8pl2trpMphxq	-	107.149.24.216	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.lileshop.com/sadn/	-	107.149.24.216	-	POST	CLEAN
http://www.axmpjbwqh.icu/sadn/?CJE=3iAQ4QeeKEHkIBAEVl9z1CO1O992WiwDiWM9265/nEQASGKqWPj08NBwbEnV+M3ncQk4hiZM&nnlH=u8pl2trpMphxq	-	104.252.218.228	-	GET	CLEAN
http://www.axmpjbwqh.icu/sadn/	-	104.252.218.228	-	POST	CLEAN
http://www.mychallengeiam.com/sadn/?CJE=sUNOm3KXMvpSrkfMrYXNDO2+58RRmbW6BAhhLbIPcGxV1sxyut+O5mwc8ozue9dNMR5impC5&nnlH=u8pl2trpMphxq	-	162.210.70.10	-	GET	CLEAN
http://www.mychallengeiam.com/sadn/	-	162.210.70.10	-	POST	CLEAN
http://www.roamallday.com/sadn/?CJE=Z99uQ+o0CUSuwDeDRQMfWXf8t2N5R94N8M0fZniL+RUkLm6FrJeUV4BmDBTmkCx+PsiTulda&nnlH=u8pl2trpMphxq	-	154.215.208.44	-	GET	CLEAN
http://www.garantiservice.com/sadn/?CJE=Fp6ir5BTuXl4RAZtixBM/qJoaLMFvckFssremE4H0HjvzUBxHiu+dGw99x12wtKKNjxNIubr&nnlH=u8pl2trpMphxq	-	93.188.2.51	-	GET	CLEAN
http://www.garantiservice.com/sadn/	-	93.188.2.51	-	POST	CLEAN
http://www.pakistanwholesaler.com/sadn/?CJE=0OCk9xNtdUwxJtNbaFBmeerTTDMh6YiZInCrJYbRD3/jFOOEMv7LjtPxz7TE4yJsvg4gTZ1G&nnlH=u8pl2trpMphxq	-	148.66.138.152	-	GET	CLEAN
http://www.pakistanwholesaler.com/sadn/	-	148.66.138.152	-	POST	CLEAN
http://www.roamallday.com/sadn/	-	154.215.208.44	-	POST	CLEAN
http://www.timeforbusinessblog.xyz/sadn/	-	198.54.117.216	-	POST	CLEAN
http://www.timeforbusinessblog.xyz/sadn/?CJE=tse2JoLHzdTnskMvzE3J2caKd/oSidqO/622iI3VeqauHCFZRd4UF0+PwaNO6Ri7YEqo/VOQ&nnlH=u8pl2trpMphxq	-	198.54.117.216	-	GET	CLEAN
https://www.google.com	-	142.250.186.164	-	GET	CLEAN
https://www.bing.com	-	204.79.197.200	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.google.com	142.250.186.164	-	HTTPS, DNS	CLEAN
www.bing.com	13.107.21.200, 204.79.197.200	-	HTTPS, DNS	CLEAN
a-0001.a-afdentry.net.trafficmanager.net	13.107.21.200, 204.79.197.200	-	DNS	CLEAN
www-bing-com.dual-a-0001.a-msedge.net	13.107.21.200, 204.79.197.200	-	DNS	CLEAN
dual-a-0001.a-msedge.net	13.107.21.200, 204.79.197.200	-	DNS	CLEAN
www.chicskr.com	-	-	DNS	CLEAN
www.smshare2u.com	204.11.56.48	-	HTTP, DNS	CLEAN
www.murrayburngundogs.com	192.0.78.24, 192.0.78.25	-	HTTP, DNS	CLEAN
murrayburngundogs.com	192.0.78.24, 192.0.78.25	-	HTTP, DNS	CLEAN
www.hertsandlondonknee.com	94.136.40.51	-	HTTP, DNS	CLEAN
www.tldyyl.com	141.98.163.216	-	HTTP, DNS	CLEAN
www.cosmoandcocrafts.com	199.34.228.173	-	HTTP, DNS	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.dapurbuageung.com	5.181.216.116	-	HTTP, DNS	CLEAN
dapurbuageung.com	5.181.216.116	-	HTTP, DNS	CLEAN
www.lileshop.com	107.149.24.216	-	HTTP, DNS	CLEAN
www.axmpjbwqh.icu	104.252.218.228	-	HTTP, DNS	CLEAN
www.mychallengeiam.com	162.210.70.10	-	HTTP, DNS	CLEAN
mychallengeiam.com	162.210.70.10	-	HTTP, DNS	CLEAN
www.roamallday.com	154.215.208.44	-	HTTP, DNS	CLEAN
www.garantiservice.com	93.188.2.51	-	HTTP, DNS	CLEAN
www.pakistanwholesaler.com	148.66.138.152	-	HTTP, DNS	CLEAN
pakistanwholesaler.com	148.66.138.152	-	HTTP, DNS	CLEAN
www.timeforbusinessblog.xyz	198.54.117.218, 198.54.117.212, 198.54.117.211, 198.54.117.216, 198.54.117.217, 198.54.117.215, 198.54.117.210	-	HTTP, DNS	CLEAN
parkingpage.namecheap.com	198.54.117.218, 198.54.117.212, 198.54.117.211, 198.54.117.216, 198.54.117.217, 198.54.117.215, 198.54.117.210	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
204.79.197.200	www.bing.com, dual-a-0001.a-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, a-0001.a-afdentry.net.trafficmanager.net	United States	HTTPS, DNS, TCP	CLEAN
142.250.186.164	www.google.com	United States	HTTPS, DNS, TCP	CLEAN
204.11.56.48	www.smshare2u.com	Virgin Islands	HTTP, DNS, TCP	CLEAN
192.0.78.25	www.murrayburngundogs.com, murrayburngundogs.com	United States	HTTP, DNS, TCP	CLEAN
94.136.40.51	www.hertsandlondonknee.com	United Kingdom	HTTP, DNS, TCP	CLEAN
141.98.163.216	www.tldyyl.com	United States	HTTP, DNS, TCP	CLEAN
199.34.228.173	www.cosmoandcocrafts.com	United States	HTTP, DNS, TCP	CLEAN
5.181.216.116	dapurbuageung.com, www.dapurbuageung.com	Germany	HTTP, DNS, TCP	CLEAN
107.149.24.216	www.lileshop.com	United States	HTTP, DNS, TCP	CLEAN
104.252.218.228	www.axmpjbwqh.icu	United States	HTTP, DNS, TCP	CLEAN
162.210.70.10	www.mychallengeiam.com, mychallengeiam.com	United States	HTTP, DNS, TCP	CLEAN
154.215.208.44	www.roamallday.com	Hong Kong	HTTP, DNS, TCP	CLEAN
93.188.2.51	www.garantiservice.com	Sweden	HTTP, DNS, TCP	CLEAN
148.66.138.152	pakistanwholesaler.com, www.pakistanwholesaler.com	Singapore	HTTP, DNS, TCP	CLEAN
198.54.117.216	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	HTTP, DNS, TCP	CLEAN
13.107.21.200	www.bing.com, dual-a-0001.a-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, a-0001.a-afdentry.net.trafficmanager.net	United States	DNS	CLEAN
192.0.78.24	www.murrayburngundogs.com, murrayburngundogs.com	United States	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
198.54.117.212	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.218	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.217	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.215	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.210	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.211	www.timeforbusinessblog.xyz, parkingpage.namecheap.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
NPL-29QSRXYEDYz9	access	addinprocess32.exe	CLEAN
K-RP6UTCADV8AHFB	access	wininit.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	order.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	access, read	order.exe	CLEAN
HKEY_CURRENT_USER	access	order.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	order.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	order.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	create, access	wininit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	wininit.exe	CLEAN

Process

Process Name	Commandline	Verdict
order.exe	"C:\Users\kEecfMwgj\Desktop\order.exe"	MALICIOUS
addinprocess32.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe"	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
wininit.exe	"C:\Windows\SysWOW64\wininit.exe"	SUSPICIOUS
cmd.exe	/c del "C:\Users\KEECFM~1\AppData\Local\Temp\AddInProcess32.exe"	SUSPICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
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

Analyzer Information

Analyzer Version	4.2.2
Dynamic Engine Version	4.2.2 / 06/07/2021 03:43
Static Engine Version	4.2.2.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-06-10 12:49:14+00:00
AV Exceptions Version	4.2.2.13 / 2021-06-02 18:07:39
VTI Ruleset Version	4.2.2.19 / 2021-06-10 11:54:46
YARA Built-in Ruleset Version	4.2.2.0
Link Detonation Heuristics Version	-
Signature Trust Store Version	4.2.2.13 / 2021-06-02 18:07:39
Analysis Report Layout Version	10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed