MALICIOUS

Classifications: Downloader | Spyware

Threat Names: Mal/HTMLGen-A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe**
ID	#5068248
MD5	005297e7c0d555822b5a6f31fcdc7661
SHA1	9d5f9d90a1574c333ec68dbc800cb70397a1826d
SHA256	6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0
File Size	12674.00 KB
Report Created	2022-08-05 17:13 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (23 rules, 46 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Takes screenshot	1	-
	• (Process #2) 2.0.0-beta2.cps.exe takes a screenshot using BitBlt API.			
5/5	_data_collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer / Edge, Electrum-LTC Litecoin Wallet, Exodus Cryptocurrency Wallet, Windows Mail, Electron Cash Bitcoin Cash Wallet, Electrum Bitcoin Wallet, The Bat!.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #2) 2.0.0-beta2.cps.exe takes screenshots and potentially exfiltrates data.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll" which was contacted by (process #2) 2.0.0-beta2.cps.exe as Mal/HTMLGen-A.			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #2) 2.0.0-beta2.cps.exe hides thread via API "NtSetInformationThread".			
3/5	_data_collection	Reads cryptocurrency wallet locations	4	-
	• (Process #2) 2.0.0-beta2.cps.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet". • (Process #2) 2.0.0-beta2.cps.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #2) 2.0.0-beta2.cps.exe tries to read the cryptocurrency wallet "Electrum-LTC Litecoin Wallet" for "LTC". • (Process #2) 2.0.0-beta2.cps.exe tries to read the cryptocurrency wallet "Electron Cash Bitcoin Cash Wallet" for "BCH".			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #2) 2.0.0-beta2.cps.exe uploads 158.443KB data using HTTP POST.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 2.0.0-beta2.cps.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #2) 2.0.0-beta2.cps.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #2) 2.0.0-beta2.cps.exe tries to detect "Sandboxie" by checking for existence of module "sbiedll.dll".			
2/5	_data_collection	Reads sensitive browser data	1	-
	• (Process #2) 2.0.0-beta2.cps.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	_data_collection	Reads sensitive mail data	2	-

Score	Category	Operation	Count	Classification
	• (Process #2) 2.0.0-beta2.cps.exe tries to read sensitive data of mail application "Windows Mail" by file. • (Process #2) 2.0.0-beta2.cps.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #2) 2.0.0-beta2.cps.exe is possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	10	-
	• (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtClose". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtMapViewOfSection". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtQueryInformationProcess". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtCreateSection". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtProtectVirtualMemory". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtQueryVirtualMemory". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtSetInformationThread". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtQuerySystemInformation". • (Process #2) 2.0.0-beta2.cps.exe makes a direct system call to "NtOpenFile".		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #3) a1photo-&-art-enhancer_search&patch_activation.exe starts (process #3) a1photo-&-art-enhancer_search&patch_activation.exe with a hidden window.			
1/5	Mutex	Creates mutex	1	-
	• (Process #2) 2.0.0-beta2.cps.exe creates mutex with name "CCOYS///hdr".			
1/5	Discovery	Reads system data	1	-
	• (Process #2) 2.0.0-beta2.cps.exe reads the cryptographic machine GUID from registry.			
1/5	Network Connection	Downloads executable	7	Downloader
	• (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll. • (Process #2) 2.0.0-beta2.cps.exe downloads Windows executable via http from http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll.		
1/5	Obfuscation	Overwrites code	1	-
	• (Process #2) 2.0.0-beta2.cps.exe overwrites code to possibly hide behavior.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #2) 2.0.0-beta2.cps.exe resolves 133 API functions by name. • (Process #4) a1photo-&-art-enhancer_search&patch_activation.tmp resolves 95 API functions by name.			
1/5	Execution	Drops PE file	2	-
	• (Process #3) a1photo-&-art-enhancer_search&patch_activation.exe drops file "C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp". • (Process #4) a1photo-&-art-enhancer_search&patch_activation.tmp drops file "C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup_setup64.tmp".			
1/5	Execution	Executes dropped PE file	3	-

Score	Category	Operation	Count	Classification
	• Executes dropped file "C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp". • Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe". • Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe".			
-	Trusted	Known clean file	5	-
	• Embedded file "" is a known clean file. • Embedded file "C:\Users\kEecfMwgj\AppData\LocalLow\mozglue.dll" is a known clean file. • Embedded file "C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup_setup64.tmp" is a known clean file. • Embedded file "C:\Users\kEecfMwgj\AppData\LocalLow\sqlite3.dll" is a known clean file. • Embedded file "C:\Users\kEecfMwgj\AppData\LocalLow\nss3.dll" is a known clean file.			
-	Trusted	Executable has a trusted signature	3	-
	• Executable C:\Users\kEecfMwgj\AppData\LocalLow\mozglue.dll has a trusted signature. • Executable has a trusted signature. • Executable C:\Users\kEecfMwgj\AppData\LocalLow\nss3.dll has a trusted signature.			

Mitre ATT&CK Matrix

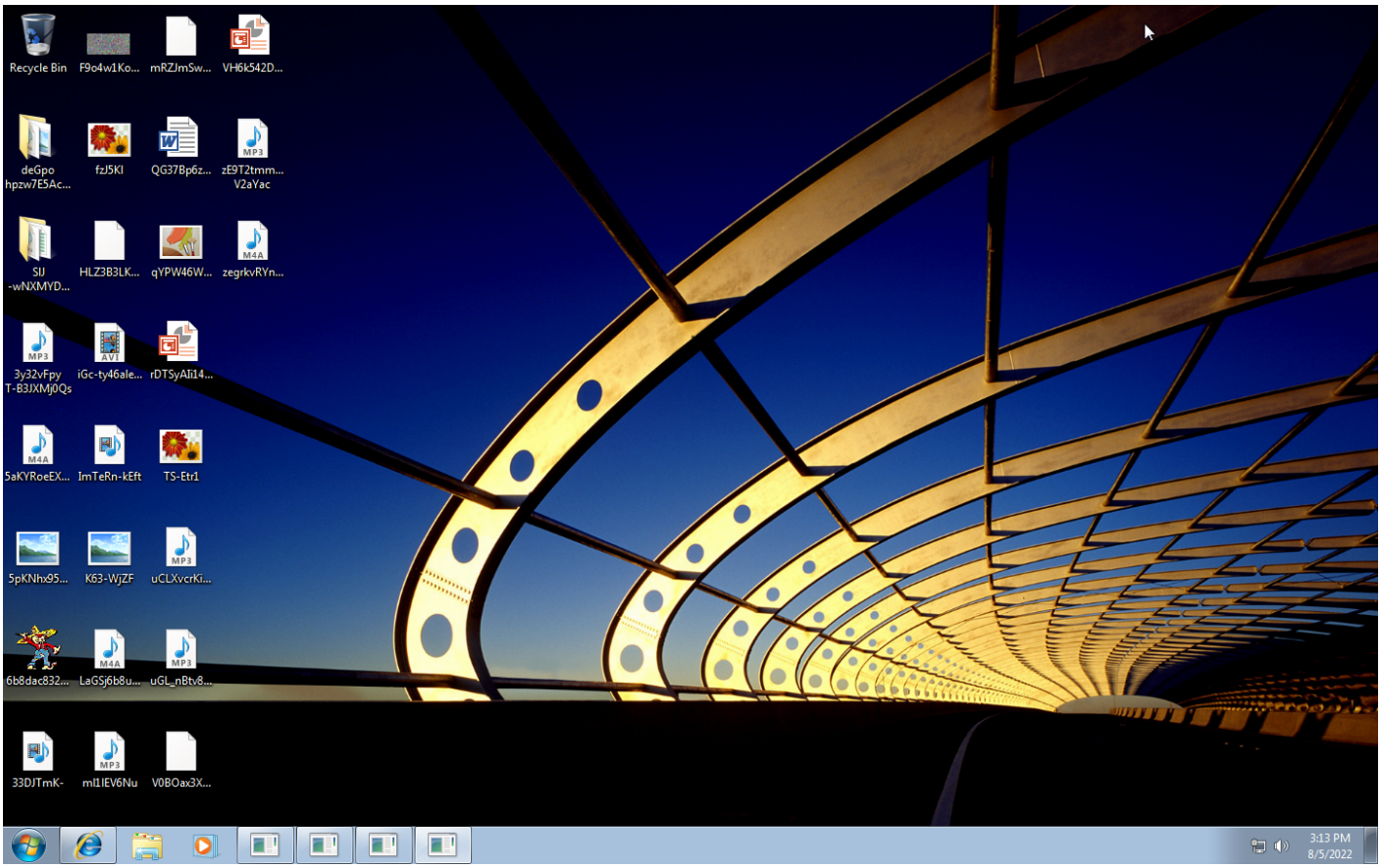
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
				#T1143 Hidden Window	#T1056 Input Capture	#T1082 System Information Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1045 Software Packing		#T1012 Query Registry		#T1113 Screen Capture			
						#T1083 File and Directory Discovery		#T1056 Input Capture			
						#T1124 System Time Discovery					

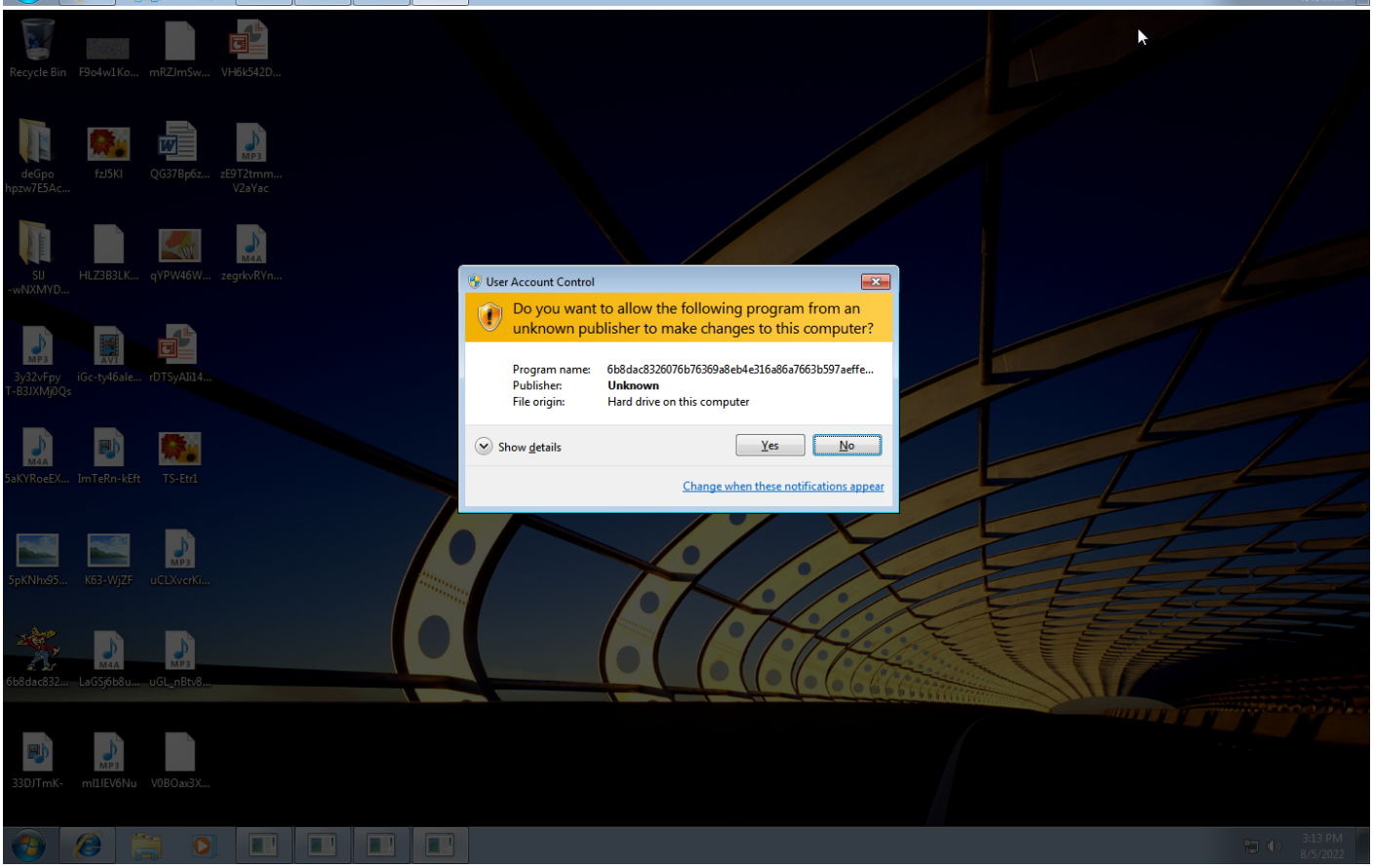
Sample Information

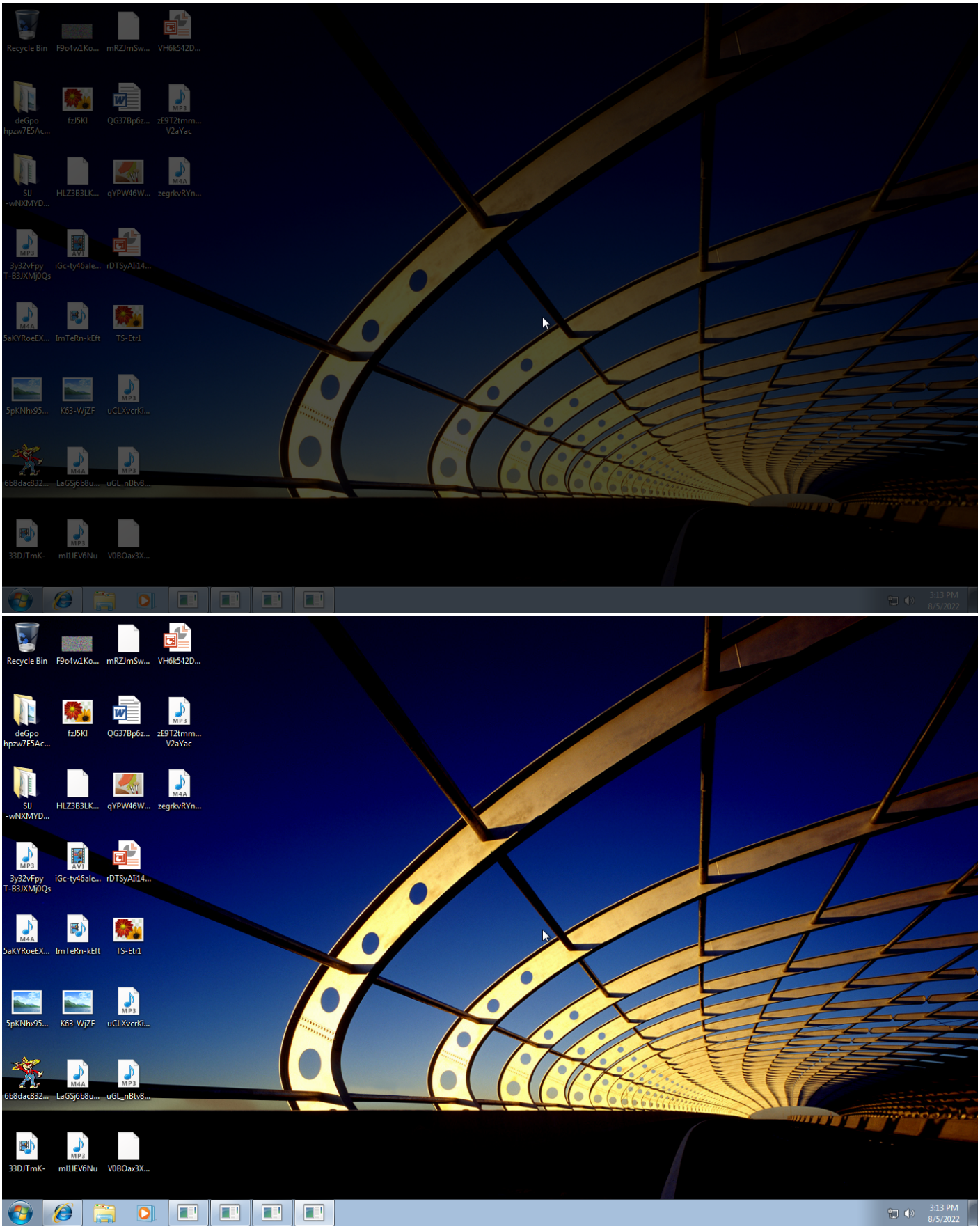
ID	#5068248
MD5	005297e7c0d555822b5a6f31fcdc7661
SHA1	9d5f9d90a1574c333ec68dbc800cb70397a1826d
SHA256	6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0
SSDeep	98304:QxQiz9Gm4H4Ul8zl6CH1OzkcC2lBev7CEObzWxtef1lKhx0vBaU6/yYsXd3VrJSp:QQszlVVOu2l8vJObShhyvBaUeY3+
File Name	6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe
File Size	12674.00 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 17:13 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
F9o4w1Ko...
mRZJmSw...
VH6k542D...
deGpo hpzw7E5Ac...
fzJ5KI
QG37Bp6z...
zE9T2tmm... V2aYac
SU -wNXMYD...
HLZ3B3LK...
qYPW46W...
zegrkvRYn...
3y32vFpy T-B3JXMj0Qs
iGc-ty46ale...
rDTSyAIi14...
5aKYRoeEX...
ImTeRn-kEft
TS-Etr1
5pKNhx95...
K63-WjZF
uCLXvcrKi...
6b8dac832...
LaGSj6b8u...
uGL_nBtv8...
33DJTmK-
mI1IEV6Nu
V0BOax3X...
3:13 PM
8/5/2022


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 6b8dac8326076b76369a8eb4e316a86a7663b597aeffe...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

185.00 KB total sent

5270.19 KB total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

9 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

9 URLs contacted, 1 servers

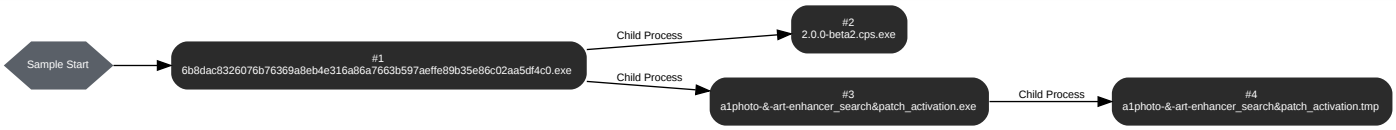
1 sessions, 1849.97 KB sent, 52701.92 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll	-	-		0 bytes	NA
POST	http://51.195.166.178/ecfd0f9298730a5c1fb78c7f49eedff3	-	-		0 bytes	NA
POST	http://51.195.166.178	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll	-	-		0 bytes	NA
GET	http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46289, Reason: Analysis Target
Unmonitor End Time	End Time: 262877, Reason: Terminated
Monitor duration	216.59s
Return Code	0
PID	2640
Parent PID	1916
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe	10240.00 KB	3bc9819912f78fff91eda2cf1d046058a3466c66c4d9f12a6e95532319eeec39	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	579.55 KB	d5b69c60652584a9fe19f3ccbea534ce749df0a86fa30484b0e1d9efd8dd58c7	✖

Host Behavior

Type	Count
Module	5
System	4
Registry	1
File	10
Process	2

Process #2: 2.0.0-beta2.cps.exe

ID	2
File Name	c:\users\keecfmwgj\appdata\local\temp\2.0.0-beta2.cps.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 224974, Reason: Child Process
Unmonitor End Time	End Time: 275482, Reason: Terminated
Monitor duration	50.51s
Return Code	0
PID	2276
Parent PID	2640
Bitness	32 Bit

Dropped Files (9)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\LocalLow\nss3.dll	1994.43 KB	c65b7afb05ee2b2687e6280594019068c3d3829182dfe8604ce4adf2116cc46e	✖
C:\Users\kEecfMwgj\AppData\LocalLow\mozglue.dll	612.43 KB	4191faf7e5eb105a0f4c5c6ed3e9e9c71014e8aa39bbee313bc92d1411e9e862	✖
-	8 bytes	318c5ad51e9b36ff5924ae323dd59031245413a3e0f2aa3e03cc42902e9e7acc	✖
-	5.15 KB	6170285224a1a650e1565d0e9da74d127994a685246f310fb4fbd851461e1e07	✖
C:\Users\kEecfMwgj\AppData\LocalLow\sqlite3.dll	1073.46 KB	47b64311719000fa8c432165a0fdcdfed735d5b54977b052de915b1cbbbf9d68	✖
C:\Users\kEecfMwgj\AppData\LocalLow\freebl3.dll	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\LocalLow\vcruntime140.dll	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\LocalLow\msvcp140.dll	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\LocalLow\softokn3.dll	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	161
Process	2
-	6
-	1
System	54
File	476
Environment	6
Mutex	2
Registry	330
User	1

Network Behavior

Type	Count
HTTP	10

Process #3: a1photo-&-art-enhancer_search&patch_activation.exe

ID	3
File Name	c:\users\keecfmwgj\appdata\local\temp\a1photo-&-art-enhancer_search&patch_activation.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 231148, Reason: Child Process
Unmonitor End Time	End Time: 286543, Reason: Terminated by timeout
Monitor duration	55.40s
Return Code	Unknown
PID	2724
Parent PID	2640
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp	754.50 KB	d12e8487b5941b9552e2ad2f742938cff407cb80825ad4dbb1b54de2c706ce81	✖

Host Behavior

Type	Count
Module	13
System	7
File	205
Environment	1
Window	2
Process	1

Process #4: a1photo-&-art-enhancer_search&patch_activation.tmp

ID	4
File Name	c:\users\keecfmwgj\appdata\local\temp\is-idt09.tmp\a1photo-&-art-enhancer_search&patch_activation.tmp
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp" /SL5="$60182,111616,111616,C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 250440, Reason: Child Process
Unmonitor End Time	End Time: 286543, Reason: Terminated by timeout
Monitor duration	36.10s
Return Code	Unknown
PID	2256
Parent PID	2724
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup_setup64.tmp	6.00 KB	388a796580234efc95f3b1c70ad4cb44bfddc7ba0f9203bf4902b9929b136f95	✖

Host Behavior

Type	Count
Module	154
System	497
Window	144
File	127
Registry	24
Keyboard	133
Environment	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0	C:\Users\kEecfMwgj\Desktop\6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe	Sample File	12674.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3bc9819912f78fff91eda2cf1d046058a3466c66c4d9f12a6e95532319eeec39	C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
c65b7afb05ee2b2687e6280594019068c3d3829182dfe8604ce4adf2116cc46e	C:\Users\kEecfMwgj\AppData\LocalLow\nss3.dll	Downloaded File	1994.43 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	CLEAN
9d02e952396bdff3abfe5654e07b7a713c84268a225e11ed9a3bf338ed1e424c	-	Downloaded File	78.25 KB	application/vnd.microsoft.portable-executable	-	CLEAN
2db7fd3c9c3c4b67f2d50a5a50e8c69154dc859780dd487c28a4e6ed1af90d01	-	Downloaded File	438.75 KB	application/vnd.microsoft.portable-executable	-	CLEAN
4191faf7e5eb105a0f4c5c6ed3e9e9c71014e8aa39bbee313bc92d1411e9e862	C:\Users\kEecfMwgj\AppData\LocalLow\mozglue.dll	Downloaded File	612.43 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN
318c5ad51e9b36ff5924ae323dd59031245413a3e0f2aa3e03cc42902e9e7acc	-	Downloaded File	8 bytes	text/plain	-	CLEAN
9884e9d1b4f8a873ccbd81f8ad0ae257776d2348d027d811a56475e028360d87	-	Extracted File	22.77 KB	application/vnd.microsoft.portable-executable	-	CLEAN
44be3153c15c2d18f49674a092c135d3482fb89b77a1b2063d01d02985555fe0	-	Downloaded File	248.43 KB	application/vnd.microsoft.portable-executable	-	CLEAN
b2ae93d30c8beb0b26f03d4a8325ac89b92a299e8f853e5caa51bb32575b06c6	-	Downloaded File	668.93 KB	application/vnd.microsoft.portable-executable	-	CLEAN
d12e8487b5941b9552e2ad2f742938cff407cb80825ad4dbb1b54de2c706ce81	C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp	Dropped File	754.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
6170285224a1a650e1565d0e9da74d127994a685246f310fb4fbd851461e1e07	-	Downloaded File	5.15 KB	text/plain	-	CLEAN
47b64311719000fa8c432165a0fdcdfed735d5b54977b052de915b1cbbbf9d68	C:\Users\kEecfMwgj\AppData\LocalLow\sqlite3.dll	Downloaded File	1073.46 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete	CLEAN
388a796580234efc95f3b1c70ad4cb44bfddc7ba0f9203bf4902b9929b136f95	C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup_setup64.tmp	Dropped File	6.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
d5b69c60652584a9fe19f3ccbea534ce749df0a86fa30484b0e1d9efd8dd58c7	C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	Dropped File	579.55 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe	Sample File, VM File	-	MALICIOUS
C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup	Accessed File	Access, Create	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\LocalLow\freebl3.dll	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\mm5o9xqs\ecfd0f9298730a5c1fb78c7f49eedff3[1].txt	Downloaded File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\vcruntime140.dll	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\mozglue.dll	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\51_195_166_178[1].txt	Downloaded File, Extracted File	-	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\msvcp140.dll	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\is-Q4RII.tmp_isetup_setup64.tmp	Dropped File, Accessed File, Extracted File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\sqlite3.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Delete	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c\ecfd0f9298730a5c1fb78c7f49eedff3[1].txt	Downloaded File, Extracted File	-	CLEAN
\??\C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\nss3.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\softokn3.dll	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\plg5yM7NbOop	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll	-	51.195.166.178	-	GET	MALICIOUS
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll	-	51.195.166.178	-	GET	CLEAN
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll	-	51.195.166.178	-	GET	CLEAN
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll	-	51.195.166.178	-	GET	CLEAN
http://51.195.166.178/ecfd0f9298730a5c1fb78c7f49eedff3	-	51.195.166.178	-	POST	CLEAN
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll	-	51.195.166.178	-	GET	CLEAN
http://51.195.166.178	-	51.195.166.178	-	POST	CLEAN
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll	-	51.195.166.178	-	GET	CLEAN
http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll	-	51.195.166.178	-	GET	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
51.195.166.178	-	France	TCP, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
CCOYS///hdr	access	2.0.0-beta2.cps.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002A-0000-1000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\A1 Photo & ArtEnhancer_is1	access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002A-0409-1000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion	access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProgramFilesDir	read, access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0116-0409-1000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	2.0.0-beta2.cps.exe, a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002A-0409-1000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\A1 Photo & ArtEnhancer_is1	access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002A-0000-1000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization	read, access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner	read, access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	2.0.0-beta2.cps.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002A-0000-1000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayVersion	read, access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}	access	2.0.0-beta2.cps.exe	CLEAN
HKEY_CURRENT_USER\Software\Mediachance\PhotoArtUpscaler\Settings	access	a1photo-&-art-enhancer_search&patch_activation.tmp	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	2.0.0-beta2.cps.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
2.0.0-beta2.cps.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\2.0.0-beta2.cps.exe"	MALICIOUS
a1photo-&-art-enhancer_search&patch_activation.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"	CLEAN
a1photo-&-art-enhancer_search&patch_activation.tmp	"C:\Users\KEECFM~1\AppData\Local\Temp\is-IDT09.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp" /SL5="$60182,111616,111616,C:\Users\kEecfMwgj\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"	CLEAN
6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe	"C:\Users\kEecfMwgj\Desktop\6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0.exe"	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	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