MALICIOUS

Classifications: Injector, Hacktool

Threat Names: CactusTorch, Cobalt Strike

Verdict Reason: -

Sample Type	**HTML Application**
File Name	**4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta**
ID	#3282649
MD5	c339f9930b7a5d8172acf898f6270632
SHA1	c50a153458e3f8a83ace7f195605bb481d286f6e
SHA256	4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93
File Size	286.62 KB
Report Created	2022-01-15 12:04 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | html_application

OVERVIEW

VMRay Threat Identifiers (7 rules, 10 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Hacktool
	• Rule "CactusTorch" from ruleset "Hacktools" has matched on the sample itself. • Rule "CobaltStrike" from ruleset "Hacktools" has matched on a memory dump for (process #2) notepad.exe. • Rule "CactusTorch" from ruleset "Hacktools" has matched on the function strings for (process #1) mshta.exe.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) mshta.exe modifies memory of (process #2) notepad.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #1) mshta.exe creates thread in (process #2) notepad.exe.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #2) notepad.exe has a thread which sleeps more than 5 minutes.			
3/5	YARA	Suspicious content matched by YARA rules	1	-
	• Rule "ReflectiveLoader" from ruleset "Generic" has matched on a memory dump for (process #2) notepad.exe.			
2/5	Network Connection	Tries to connect using an uncommon port	2	-
	• Tries to connect to TCP port 12342 at 42.193.229.33. • (Process #2) notepad.exe tries to connect to TCP port 12342 at 42.193.229.33.			
1/5	Network Connection	All network connection attempts failed	1	-
	• Host "42.193.229.33" is unavailable.			

Mitre ATT&CK Matrix

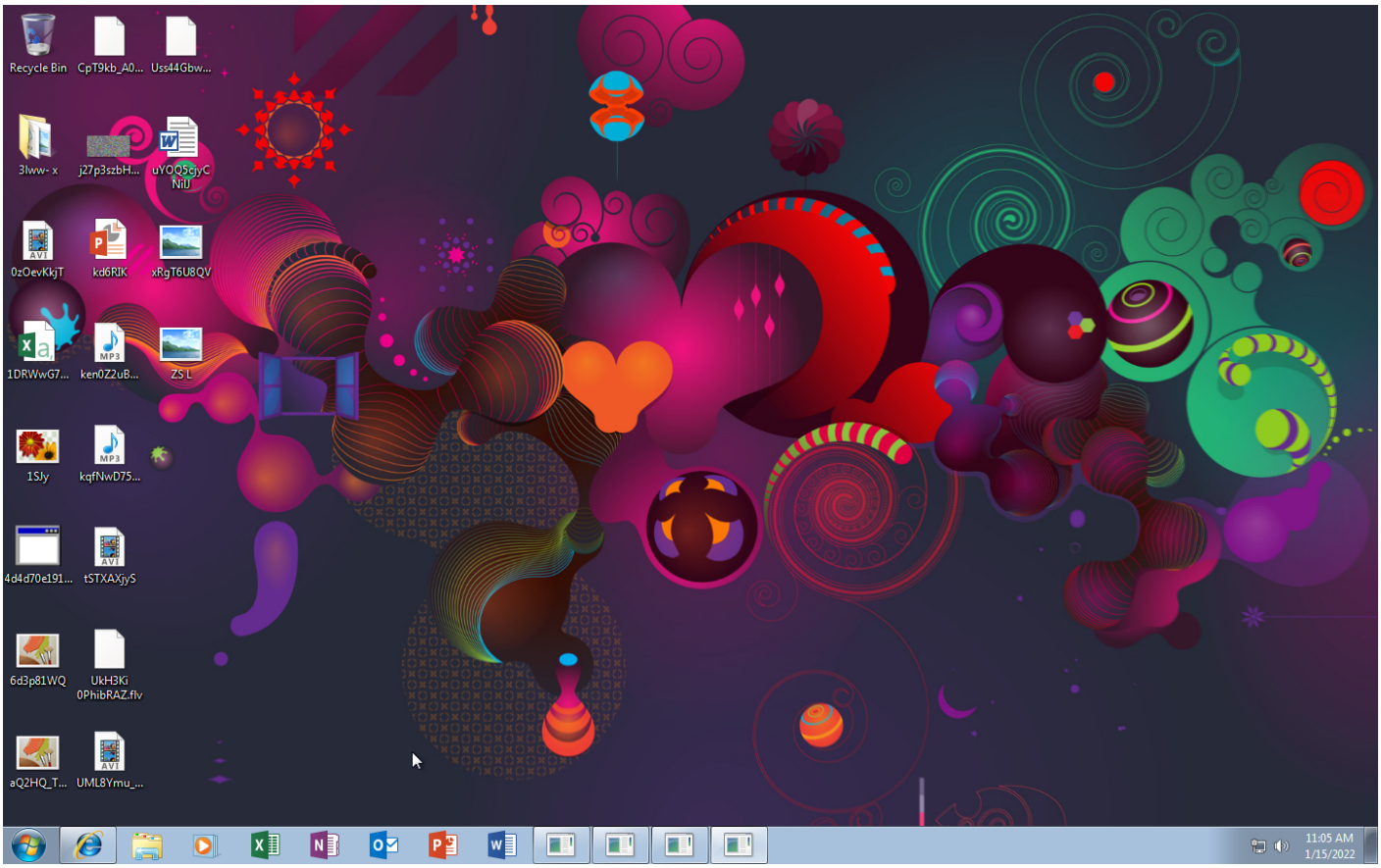
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
									#T1065 Uncommonly Used Port		

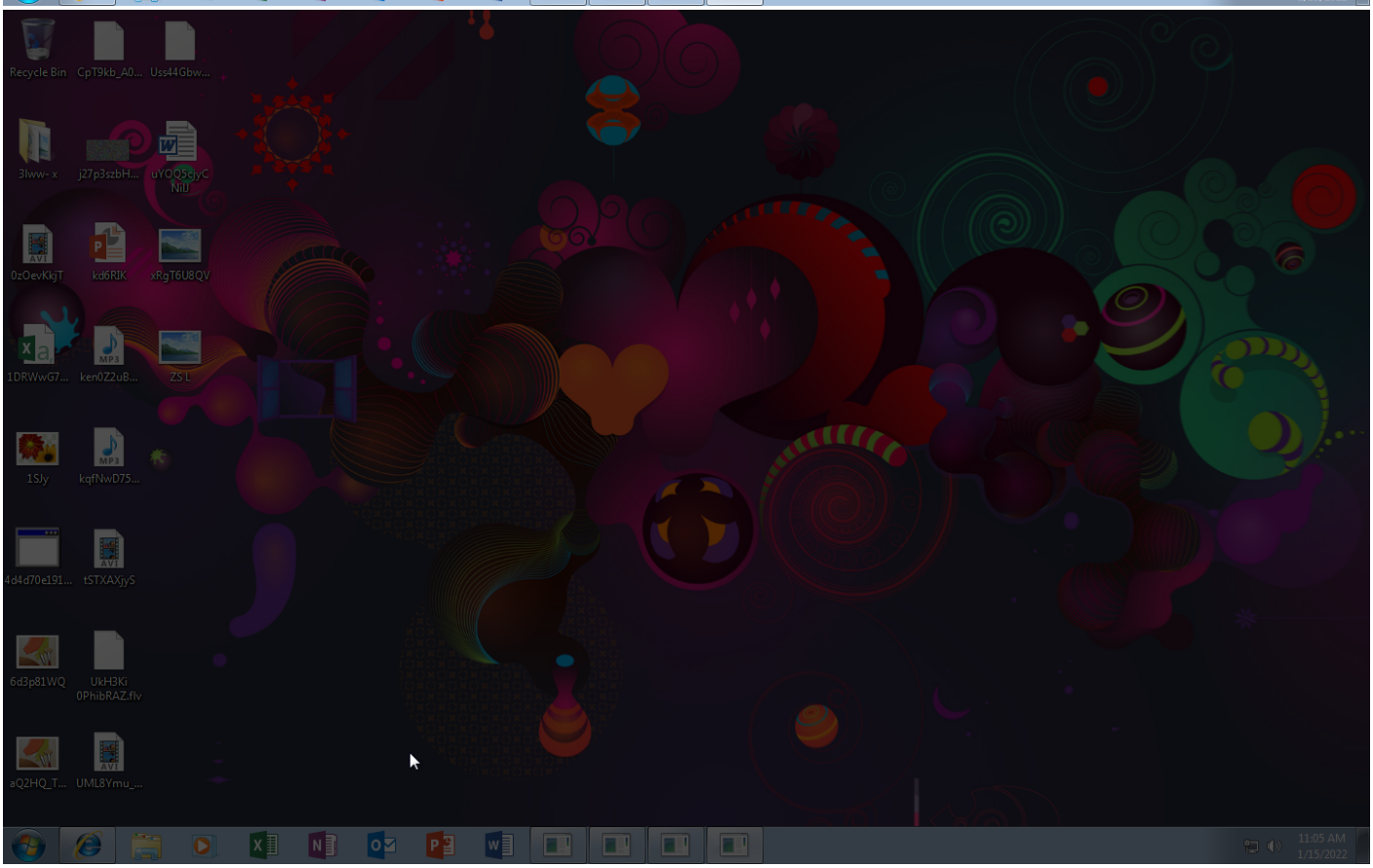
Sample Information

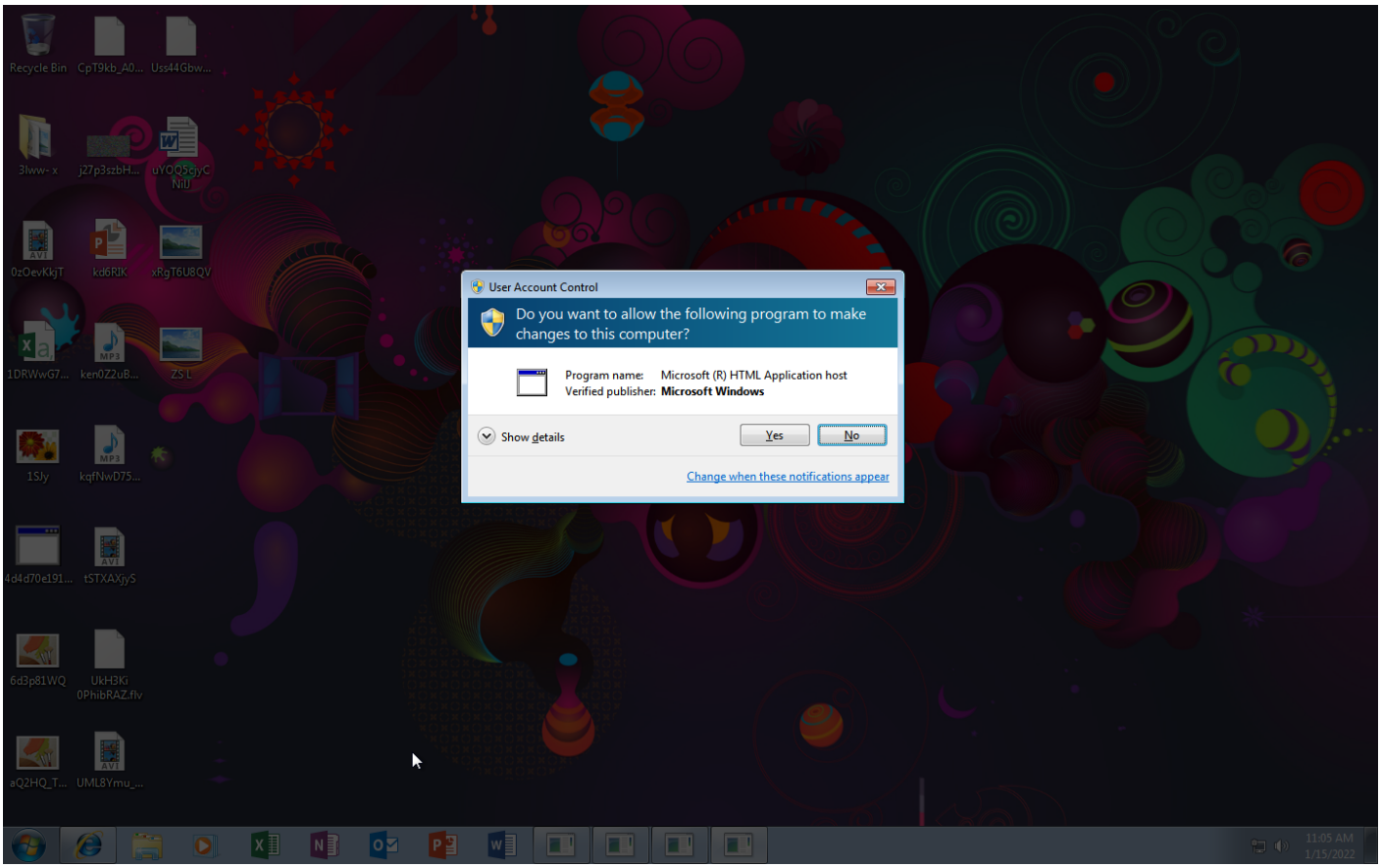
ID	#3282649
MD5	c339f9930b7a5d8172acf898f6270632
SHA1	c50a153458e3f8a83ace7f195605bb481d286f6e
SHA256	4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93
SSDeep	6144:uGser0A9gxLlanBrj5ysuKoAHMVlYSRjlaMMUY726AbpPjj5EZKO/ltwEDHHkqFM:4er9OEUBUBaHMVlDOMUyrSP5O4EzHkmM
File Name	4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta
File Size	286.62 KB
Sample Type	HTML Application
Has Macros	✓

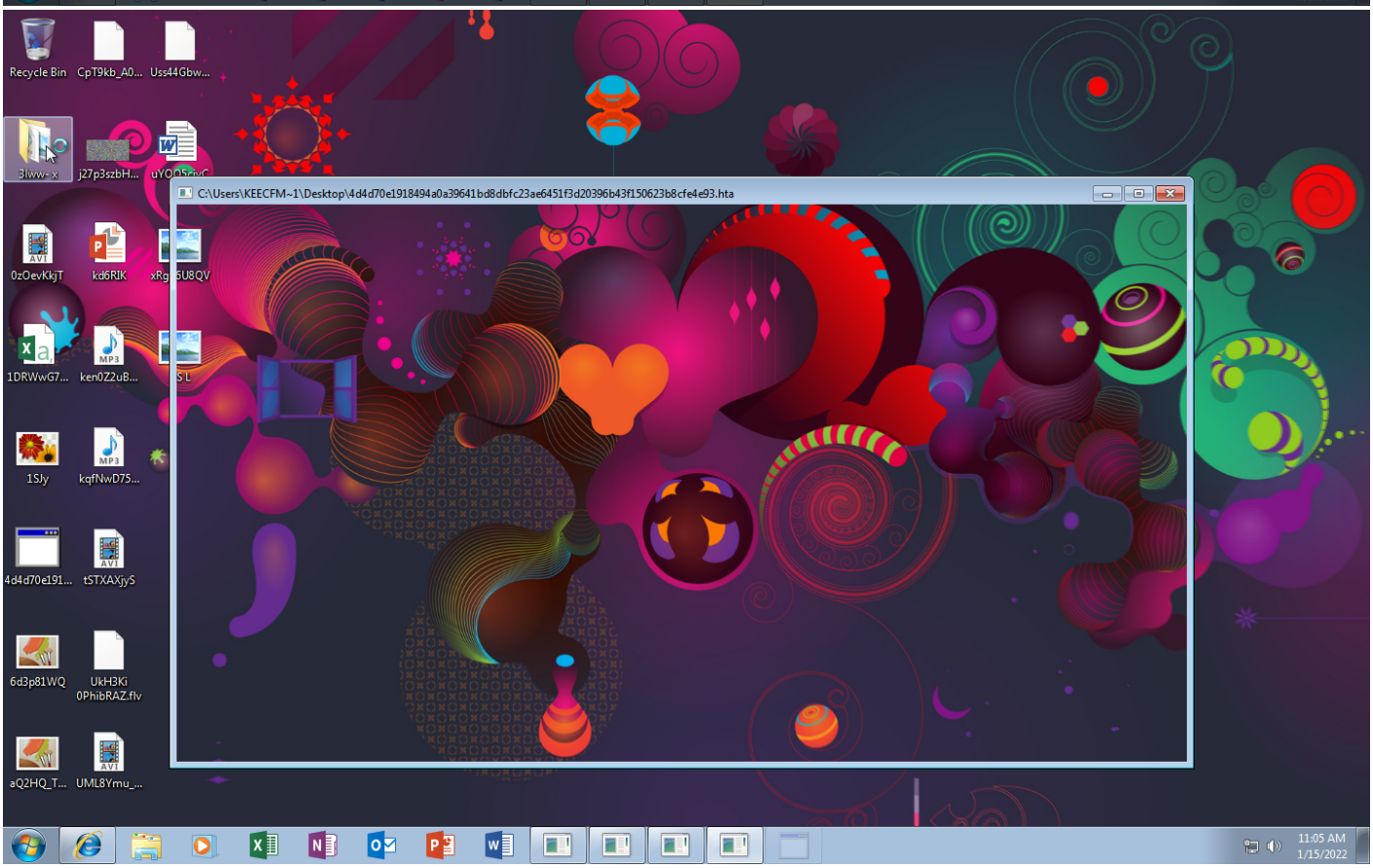
Analysis Information

Creation Time	2022-01-15 12:04 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
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	36


Recycle Bin
CpT9kb_A0...
Uss44Gbw...
3lww- x
j27p3szbH...
uYOQ5cjyC NnJ
0zOevKkjT
kd6RIK
xRgT6U8QV
1DRWwG7...
ken0Z2uB...
ZS L
1SJy
kqfNwD75...
4d4d70e191...
tSTXAXjyS
6d3p81WQ
UkH3Ki 0PhibRAZ.flv
aQ2HQ_T...
UML8Ymu_...
11:05 AM
1/15/2022


Recycle Bin
CpT9kb_A0...
Uss44Gbw...
3lww- x
j27p3szbH...
uYOQ5cjyC NnJ
0zOevKkjT
kd6RIK
xRgT6U8QV
1DRWwG7...
ken0Z2uB...
ZS L
1SJy
kqfNwD75...
4d4d70e191...
tSTXAXjyS
6d3p81WQ
UkH3Ki 0PhibRAZ.flv
aQ2HQ_T...
UML8Ymu_...
11:05 AM
1/15/2022





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 12342

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

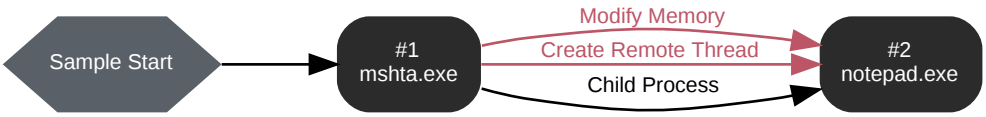
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	42.193.229.33/j.ad	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
-	q9iatrkprh	-	192.168.0.242		NA

BEHAVIOR

Process Graph



Process #1: mshta.exe

ID	1
File Name	c:\windows\system32\mshta.exe
Command Line	"C:\Windows\System32\mshta.exe" "C:\Users\KEECFM~1\Desktop\4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 38426, Reason: Analysis Target
Unmonitor End Time	End Time: 86530, Reason: Terminated
Monitor duration	48.10s
Return Code	0
PID	3856
Parent PID	912
Bitness	64 Bit

Host Behavior

Type	Count
System	30
Module	58
File	5
Environment	3
Registry	103
-	5
Keyboard	2
Mutex	1
Window	7
COM	14
-	1
Process	1
-	2
-	1

Process #2: notepad.exe

ID	2
File Name	c:\windows\syswow64\notepad.exe
Command Line	"C:\Windows\SysWOW64\notepad.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 67510, Reason: Child Process
Unmonitor End Time	End Time: 280358, Reason: Terminated by Timeout
Monitor duration	212.85s
Return Code	Unknown
PID	3912
Parent PID	3856
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\windows\system32\mshta.exe	0xf14	0x70000(458752)	0x33000	✓	1
Create Remote Thread	#1: c:\windows\system32\mshta.exe	0xf14	0x70000(458752)	-	✓	1

Host Behavior

Type	Count
Module	216
System	90
Environment	1
File	3
Keyboard	1
User	1

Network Behavior

Type	Count
HTTP	83
DNS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93	C:\Users\kEecfMwgj\Desktop\4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta	Sample File	286.62 KB	application/hta	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Windows\System32\mshta.exe	Accessed File	Access	CLEAN
Win.ini	Accessed File	Read, Access	CLEAN
C:\Windows\System32\mshtml.dll	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\notepad.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://42.193.229.33/j.ad	-	42.193.229.33	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
q9iatrkprh	192.168.0.242	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
42.193.229.33	-	China	TCP	SUSPICIOUS
192.168.0.1	-	-	DNS, UDP	CLEAN
192.168.0.242	q9iatrkprh	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Local\!PrivacIE!SharedMemory!Mutex	access	mshta.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\InProcServer32	read, access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120	access	mshta.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXTERNAL_STYLE_SHEET_FIX_FOR_SMARTNAVIGATION_KB926131	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXTERNAL_STYLE_SHEET_FIX_FOR_SMARTNAVIGATION_KB926131	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ARIA_SUPPORT	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ARIA_SUPPORT	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_DISPPARAMS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_DISPPARAMS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRIVATE_FONT_SETTING	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRIVATE_FONT_SETTING	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_SHOW_HIDE_EVENTS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_SHOW_HIDE_EVENTS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISPLAY_NODE_ADVISE_KB833311	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISPLAY_NODE_ADVISE_KB833311	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_EXPANDURI_BYPASS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_EXPANDURI_BYPASS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DATABINDING_SUPPORT	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DATABINDING_SUPPORT	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENFORCE_BSTR	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENFORCE_BSTR	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING	access	mshta.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_OM_SCREEN_ORIGIN_DISPLAY_PIXELS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_OM_SCREEN_ORIGIN_DISPLAY_PIXELS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLEANUP_AT_FLS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLEANUP_AT_FLS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFileMenu	read, access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MANAGE_SCRIPT_CIRCULAR_REFS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MANAGE_SCRIPT_CIRCULAR_REFS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DOCUMENT_COMPATIBLE_MODE	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DOCUMENT_COMPATIBLE_MODE	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_DOCUMENT_ZOOM	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_DOCUMENT_ZOOM	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PageSetup	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PageSetup\Print_Background	read, access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XSSFILTER	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XSSFILTER	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SHOW_FAILED_CONNECT_CONTENT_KB942615	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SHOW_FAILED_CONNECT_CONTENT_KB942615	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_TREAT_IMAGE_AS_AUTHORITATIVE	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_TREAT_IMAGE_AS_AUTHORITATIVE	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IEFRAME	access	mshta.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IEFRAME	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDITIONAL_IE8_MEMORY_CLEANUP	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDITIONAL_IE8_MEMORY_CLEANUP	access	mshta.exe	CLEAN

Process

Process Name	Commandline	Verdict
mshta.exe	"C:\Windows\System32\mshta.exe" "C:\Users\KEECFM~1\Desktop\4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta"	SUSPICIOUS
notepad.exe	"C:\Windows\SysWOW64\notepad.exe"	SUSPICIOUS

YARA / AV

YARA (36)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Hacktools	CactusTorch	CactusTorch: payload generator	Sample File	C:\Users\kEecfMwgj\Desktop\4d4d70e1918494a0a39641bd8dbfc23ae6451f3d20396b43f150623b8cfe4e93.hta	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CobaltStrike	Cobalt Strike beacon	Memory Dump	-	Hacktool	5/5
Hacktools	CactusTorch	CactusTorch: payload generator	Function Strings	function_strings_process_1.txt	Hacktool	5/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5
Generic	ReflectiveLoader	Reflective loader usage	Memory Dump	-	-	3/5

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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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