Threat Roundup for February 4 to February 11

blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between Feb. 4 and Feb. 11. As with previous roundups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavioral characteristics, indicators of compromise, and discussing how our customers are automatically protected from these threats.

As a reminder, the information provided for the following threats in this post is non-exhaustive and current as of the date of publication. Additionally, please keep in mind that IOC searching is only one part of threat hunting. Spotting a single IOC does not necessarily indicate maliciousness. Detection and coverage for the following threats is subject to updates, pending additional threat or vulnerability analysis. For the most current information, please refer to your Firepower Management Center, Snort.org, or ClamAV.net.

For each threat described below, this blog post only lists 25 of the associated file hashes and up to 25 IOCs for each category. An accompanying JSON file can be found here that includes the complete list of file hashes, as well as all other IOCs from this post. A visual depiction of the MITRE ATT&CK techniques associated with each threat is also shown. In these images, the brightness of the technique indicates how prevalent it is across all threat files where dynamic analysis was conducted. There are five distinct shades that are used, with the darkest indicating that no files exhibited technique behavior and the brightest indicating that technique behavior was observed from 75 percent or more of the files.

The most prevalent threats highlighted in this roundup are:

Threat Name	Type	Description
Win.Malware.TinyBanker-9938313-1	Malware	TinyBanker, also known as Zusy or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information.
Win.Packed.Tofsee-9938395-0	Packed	Tofsee is multi-purpose malware that features a number of modules used to carry out various activities such as sending spam messages, conducting click fraud, mining cryptocurrency, and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the size of the botnet under the operator's control.
Win.Dropper.Lokibot-9938416-1	Dropper	Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails.
Win.Virus.Xpiro-9938457-1	Virus	Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks.

Threat Name	Type	Description
Win.Dropper.DarkComet-9938488-1	Dropper	DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system.
Win.Worm.Gh0stRAT-9938500-1	Worm	Gh0stRAT is a well-known family of remote access trojans that can provide an attacker with complete control over an infected system. Its capabilities include monitoring keystrokes, collecting video footage from the webcam, and uploading/executing follow-on malware. The source code for Gh0stRAT has been publicly available on the internet for years, significantly lowering the barrier for actors to modify and reuse the code in new attacks.
Win.Malware.Zbot-9938525-0	Malware	Zbot, also known as Zeus, is a trojan that steals information, such as banking credentials, using methods such as key-logging and form-grabbing.

Threat Breakdown

Win.Malware.TinyBanker-9938313-1

Indicators of Compromise

IOCs collected from dynamic analysis of 119 samples

Registry Keys	Occurrences
`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN Value Name: EEFEB657`	107

Mutexes	Occurrences
`EEFEB657`	111
`4A60888F`	4

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`216[.]218[.]185[.]162`	54

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`qytufpscigbb[.]com`	41
`qytufpscigbb[.]net`	41
`qytufpscigbb[.]in`	40
`ghoyvkjbnldc[.]com`	39
`wpad[.]example[.]org`	37
`ghoyvkjbnldc[.]net`	37
`ghoyvkjbnldc[.]in`	37
`mqrvhcolvvnu[.]net`	36
`computer[.]example[.]org`	35
`qytufpscigbb[.]ru`	34
`mqrvhcolvvnu[.]in`	34
`brureservtestot[.]cc`	33
`fettlijyycee[.]com`	33
`fettlijyycee[.]net`	33
`mqrvhcolvvnu[.]com`	31
`fettlijyycee[.]in`	31
`ibyxedcowwot[.]com`	29
`hkleofepnyvv[.]com`	29
`ibyxedcowwot[.]in`	29
`mqrvhcolvvnu[.]ru`	28
`ibyxedcowwot[.]net`	28
`fettlijyycee[.]ru`	28
`hkleofepnyvv[.]in`	27
`dtdqmlwwyekt[.]in`	26
`mmnskehnbbbs[.]in`	26

*See JSON for more IOCs

Files and or directories created	Occurrences
`%HOMEPATH%\AppData\LocalLow\EEFEB657`	107
`%APPDATA%\EEFEB657`	107
`%APPDATA%\EEFEB657\bin.exe`	107
`%APPDATA%\4A60888F\bin.exe`	4
`\Users\user\AppData\Roaming\C085EE96\bin.exe`	1
`\Users\user\AppData\Roaming\F9D340E9\bin.exe`	1
`\Users\user\AppData\Roaming\EFEA19B1\bin.exe`	1
`\Users\user\AppData\Roaming\FCD59BF4\bin.exe`	1
`\Users\user\AppData\Roaming\FE7CEA4A\bin.exe`	1
`\Users\user\AppData\Roaming\29EEFF67\bin.exe`	1
`\Users\user\AppData\Roaming\3B8456CD\bin.exe`	1
`\Users\user\AppData\Roaming\ACF7EE57\bin.exe`	1
`\Users\user\AppData\Roaming\382240CB\bin.exe`	1
`\Users\user\AppData\Roaming\F87C9831\bin.exe`	1
`\Users\user\AppData\Roaming\F21AB61D\bin.exe`	1
`\Users\user\AppData\Roaming\D9419169\bin.exe`	1
`\Users\user\AppData\Roaming\01ACD167\bin.exe`	1
`\Users\user\AppData\Roaming\4DD60A79\bin.exe`	1
`\Users\user\AppData\Roaming\E409BE83\bin.exe`	1
`\Users\user\AppData\Roaming\E607047A\bin.exe`	1
`\Users\user\AppData\Roaming\BF0913D3\bin.exe`	1
`\Users\user\AppData\Roaming\1620527C\bin.exe`	1
`\Users\user\AppData\Roaming\367B3C67\bin.exe`	1
`\Users\user\AppData\Roaming\D515B45E\bin.exe`	1
`\Users\user\AppData\Roaming\2DEACB61\bin.exe`	1

*See JSON for more IOCs

File Hashes

```
0034645eddcb03469720eaadad078584ee871013511e489552b352650dcd1452
00dd160455b6c2a2d378b578405fadf2e9ebf41c3bc0d2d8e8b8c1e93edc4fa3
011e5701074d070f99ac9b9a8992fa24cbe65fa2e4da686e2c4fa3937d9a9132
02b65a12e159d1dd4e18179abc7caf8c5b989883f549ef07c8a12b7d0d6e2b71
03722d9c722f738e87584f9883eca1e109e86a1c87aa164e77ebdaf0697467b8
03d14614eaba728899b58b5cdfc397f30ce9277e78becc3730ab3ed3e86dd44d
05728b20dab685fff4a3f1d7beb42d8fe752b07b36c934653dc6d692f60ca160
0661307f542de2bd0120160bcb7f42fd27575e15669ba7d944d56947eccce4bc
06a8d19314d2f384b3b828db1e7126331797eca14425d377522fc4cebeaeeb65
06e2e8f718f6d8c1b4003d58f50efc68eed8c765f3bfd6db0f312ded0a1815d8
071cb899230183b1eb523e61811e4fb5e6f7dc002b4db4e62384c6c966623c59
07635d904e831a15fc0e2a0faa44891fbce5c53d2da8de9ace8cd13479d7857b
07fa8f9c52147408c3c7ee9b3c04ca2ebbd3cc44f71656d66785f5496c585ae5
08c7d389611e871e4f033af78e2652961a86bcc41ec32226ebc19d7b7b032c9a
09110e30e6b4aeb824c3c3de6b0fc06a98bdab4367e01a7023eb76cd6126b22e
0940189172d8b8e10f64400f57c782d2fad7a76d4993f7c14f0f9010368e8cd3
0a1f8665ed21bd45f0510b4f78f27309e46c0253fbed7961ab70ef7b53fe7487
0a6a500871f751981541692277c1a323945e87e9b2a7b0f4846349979b135a08
0a77fe5654e52c9776a65f639625da92740b334a280a8147dca07e747876197b
0b29cea80ce0bde3c99a5beaa1a472d462a024cb5e8daebf6e8997f878243d12
0bc5badfffd8b74ec1d18307a760af530c7741597ab177c02ec7eb4daf8e6d49
0bd104bc98f4a3b976f49209c5de1094142652a20bab6d914c4622969f57d567
0e003fd1947b3ff94be1f939c060c7d41fec727367d7a56c7ff8c53b6e80532b
0e348a3691c2df9a451c4f1227c04351542a0d9540ff4ad929f8793e77f39078
0e5079d5f217e79fe4fa06fb5181e656f77ac6e939cf006d5321edbcbcaed28b
```

*See JSON for more IOCs

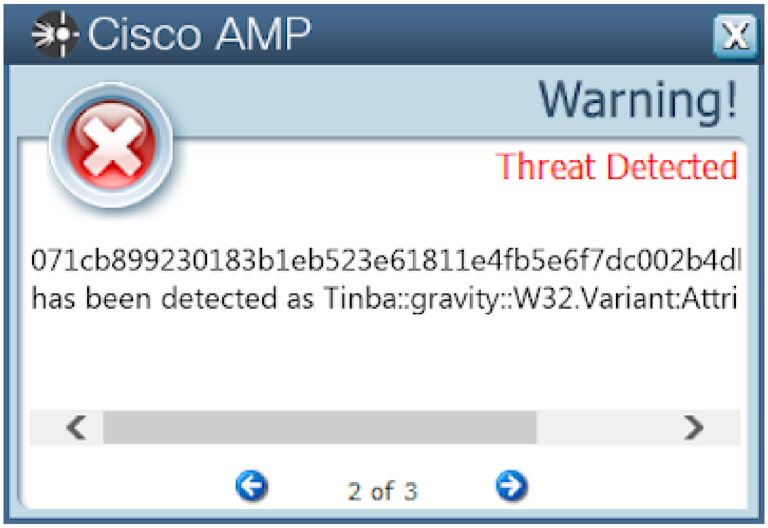
Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	
Email Security	

Product	Protection
Network Security	
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	
WSA	

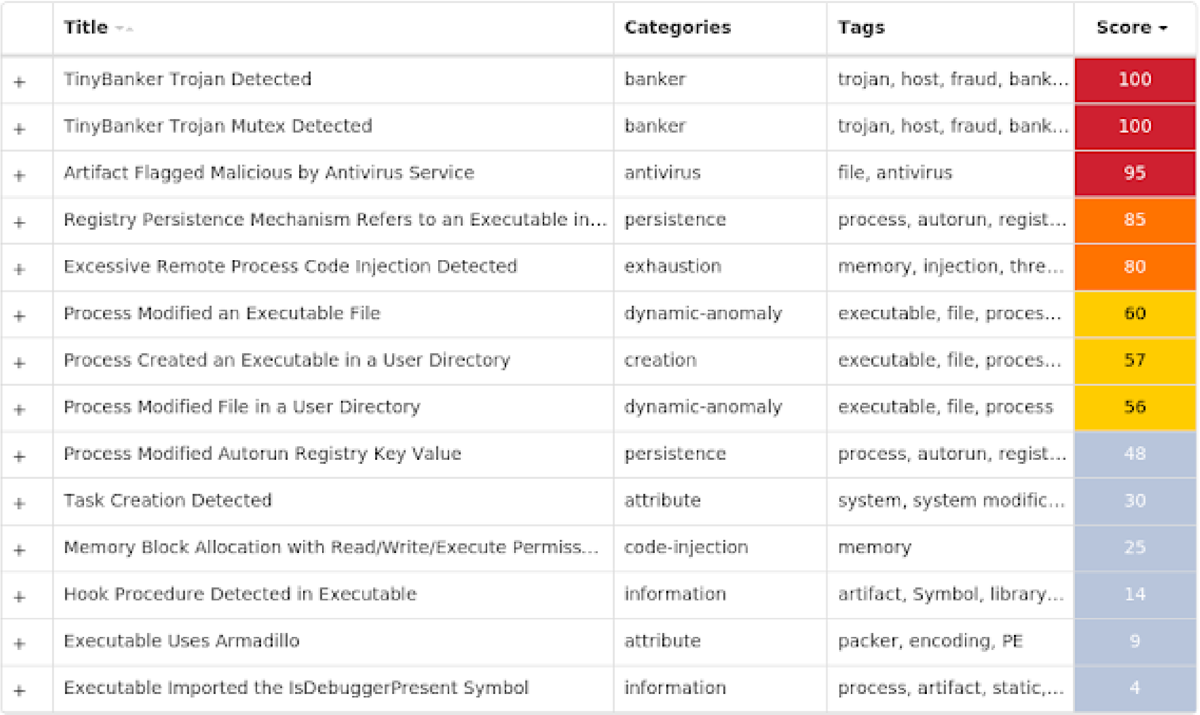
Screenshots of Detection

Secure Endpoint



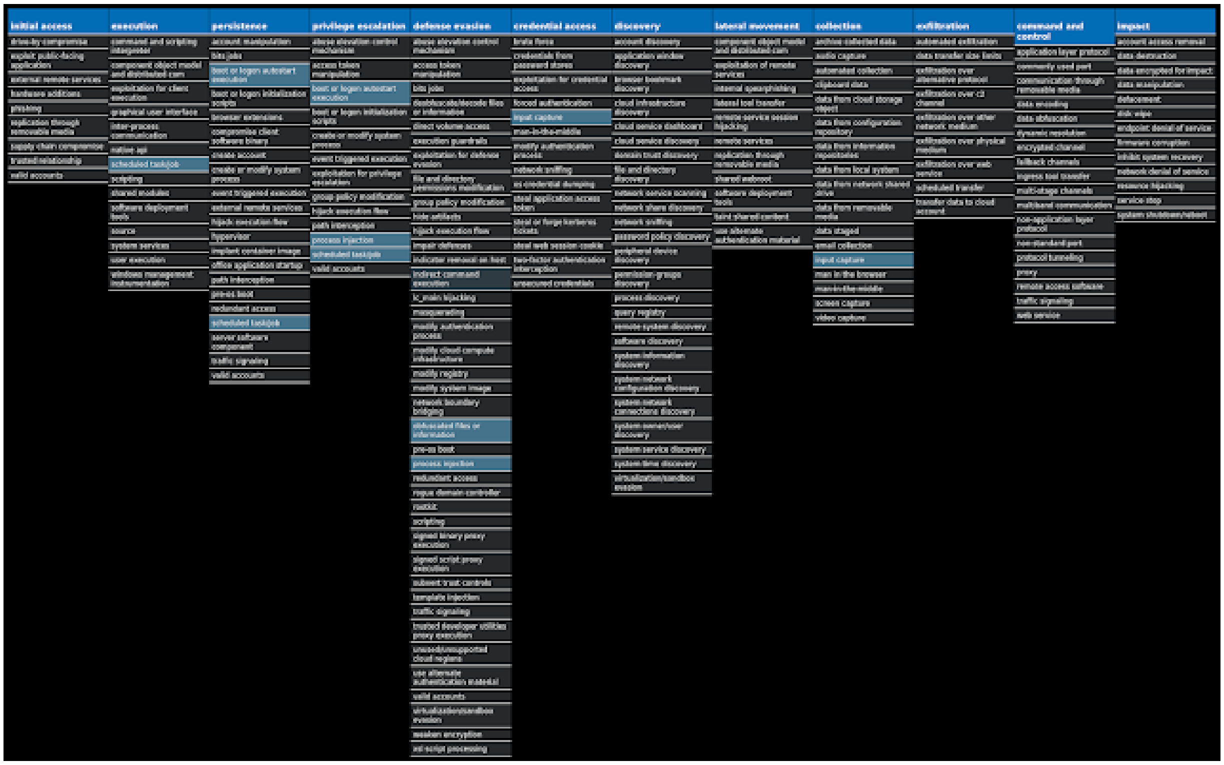
071cb899230183b1eb523e61811e4fb5e6f7dc002b4d
has been detected as Tinba::gravity::W32.Variant:Attri

Secure Malware Analytics



	Title	Categories	Tags	Score
+	TinyBanker Trojan Detected	banker	trojan, host, fraud, bank…	100
+	TinyBanker Trojan Mutex Detected	banker	trojan, host, fraud, bank…	100
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Registry Persistence Mechanism Refers to an Executable in…	persistence	process, autorun, regist…	85
+	Excessive Remote Process Code Injection Detected	exhaustion	memory, injection, thre…	80
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces…	60
+	Process Created an Executable in a User Directory	creation	executable, file, proces…	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56
+	Process Modified Autorun Registry Key Value	persistence	process, autorun, regist…	48
+	Task Creation Detected	attribute	system, system modific…	30
+	Memory Block Allocation with Read/Write/Execute Permiss…	code-injection	memory	25
+	Hook Procedure Detected in Executable	information	artifact, Symbol, library…	14
+	Executable Uses Armadillo	attribute	packer, encoding, PE	9
+	Executable Imported the IsDebuggerPresent Symbol	information	process, artifact, static,…	4

MITRE ATT&CK



initial access	execution	persistence	privilege escalation	defense evasion	credential access	discovery	lateral movement	collection	exfiltration	command and control	impact
drive-by compromise	command and scripting interpreter	account manipulation	abuse elevation control mechanism	abuse elevation control mechanism	brute force	account discovery	component object model and distributed com	archive collected data	automated exfiltration	application layer protocol	account access removal
exploit public-facing application	component object model and distributed com	bits jobs	access token manipulation	access token manipulation	credentials from password stores	application window discovery	exploitation of remote services	audio capture	data transfer size limits	commonly used port	data destruction
external remote services	exploitation for client execution	boot or logon autostart execution	boot or logon autostart execution	bits jobs	exploitation for credential access	browser bookmark discovery	internal spearphishing	automated collection	exfiltration over alternative protocol	communication through removable media	data encrypted for impact
hardware additions	graphical user interface	boot or logon initialization scripts	boot or logon initialization scripts	deobfuscate/decode files or information	forced authentication	cloud infrastructure discovery	lateral tool transfer	clipboard data	exfiltration over c2 channel	data encoding	data manipulation
phishing	inter-process communication	browser extensions	create or modify system process	direct volume access	input capture	cloud service dashboard	remote service session hijacking	data from cloud storage object	exfiltration over other network medium	data obfuscation	defacement
replication through removable media	native api	compromise client software binary	event triggered execution	execution guardrails	man-in-the-middle	cloud service discovery	remote services	data from configuration repository	exfiltration over physical medium	dynamic resolution	disk wipe
supply chain compromise	scheduled task/job	create account	exploitation for privilege escalation	exploitation for defense evasion	modify authentication process	domain trust discovery	replication through removable media	data from information repositories	exfiltration over web service	encrypted channel	endpoint denial of service
trusted relationship	scripting	create or modify system process	group policy modification	file and directory permissions modification	network sniffing	file and directory discovery	shared webroot	data from local system	scheduled transfer	fallback channels	firmware corruption
valid accounts	shared modules	event triggered execution	hijack execution flow	group policy modification	os credential dumping	network service scanning	software deployment tools	data from network shared drive	transfer data to cloud account	ingress tool transfer	inhibit system recovery
	software deployment tools	external remote services	path interception	hide artifacts	steal application access token	network share discovery	taint shared content	data from removable media		multi-stage channels	network denial of service
	source	hijack execution flow	process injection	hijack execution flow	steal or forge kerberos tickets	network sniffing	use alternate authentication material	data staged		multiband communication	resource hijacking
	system services	hypervisor	scheduled task/job	impair defenses	steal web session cookie	password policy discovery		email collection		non-application layer protocol	service stop
	user execution	implant container image	valid accounts	indicator removal on host	two-factor authentication interception	peripheral device discovery		input capture		non-standard port	system shutdown/reboot
	windows management instrumentation	office application startup		indirect command execution	unsecured credentials	permission groups discovery		man in the browser		protocol tunneling	
		path interception		lc_main hijacking		process discovery		man-in-the-middle		proxy	
		pre-os boot		masquerading		query registry		screen capture		remote access software	
		redundant access		modify authentication process		remote system discovery		video capture		traffic signaling	
		scheduled task/job		modify cloud compute infrastructure		software discovery				web service	
		server software component		modify registry		system information discovery					
		traffic signaling		modify system image		system network configuration discovery					
		valid accounts		network boundary bridging		system network connections discovery					
				obfuscated files or information		system owner/user discovery					
				pre-os boot		system service discovery					
				process injection		system time discovery					
				redundant access		virtualization/sandbox evasion					
				rogue domain controller							
				rootkit							
				scripting							
				signed binary proxy execution							
				signed script proxy execution							
				subvert trust controls							
				template injection							
				traffic signaling							
				trusted developer utilities proxy execution							
				unused/unsupported cloud regions							
				use alternate authentication material							
				valid accounts							
				virtualization/sandbox evasion							
				weaken encryption							
				xsl script processing							

Win.Packed.Tofsee-9938395-0

Indicators of Compromise

IOCs collected from dynamic analysis of 12 samples

Registry Keys	Occurrences
<HKCR>\LOCAL SETTINGS\SOFTWARE\MICROSOFT\WINDOWS\SHELL\BAGS\159	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'>	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: Type	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: Start	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: ErrorControl	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: DisplayName	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: WOW64	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: ObjectName	12
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: Description	12
<HKU>\.DEFAULT\CONTROL PANEL\BUSES Value Name: Config4	11
<HKU>\.DEFAULT\CONTROL PANEL\BUSES	11
<HKU>\.DEFAULT\CONTROL PANEL\BUSES Value Name: Config0	11
<HKU>\.DEFAULT\CONTROL PANEL\BUSES Value Name: Config1	11
<HKU>\.DEFAULT\CONTROL PANEL\BUSES Value Name: Config2	11
<HKU>\.DEFAULT\CONTROL PANEL\BUSES Value Name: Config3	11
<HKLM>\SYSTEM\CONTROLSET001\SERVICES\<random, matching '[A-Z0-9]{8}'> Value Name: ImagePath	11
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\nqeybyka	2

Registry Keys	Occurrences
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\jmauxugw	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\knbvyvhx	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\zcqknkwm	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\mpdxaxjz	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\ehvpspbr	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\uxlfifrh	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\ilztwtfv	1
<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS Value Name: C:\Windows\SysWOW64\xaoiliuk	1

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
91[.]243[.]33[.]5	11
35[.]228[.]103[.]145	11
67[.]231[.]149[.]140	10
192[.]0[.]47[.]59	10
211[.]231[.]108[.]46/31	10
157[.]240[.]229[.]174	10
202[.]137[.]234[.]30	9
125[.]209[.]238[.]100	9
212[.]77[.]101[.]4	9
67[.]195[.]204[.]72/30	9
117[.]53[.]116[.]15	9
209[.]222[.]82[.]252/31	9
84[.]2[.]43[.]64/31	9
208[.]76[.]51[.]51	8

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`216[.]146[.]35[.]35`	8
`64[.]98[.]36[.]4`	8
`103[.]224[.]212[.]34`	8
`216[.]163[.]188[.]54`	8
`193[.]222[.]135[.]150`	8
`193[.]0[.]6[.]135`	8
`45[.]33[.]83[.]75`	8
`51[.]81[.]57[.]58`	8
`40[.]93[.]207[.]0/31`	8
`62[.]141[.]42[.]208`	8
`96[.]103[.]145[.]165`	8

*See JSON for more IOCs

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`microsoft-com[.]mail[.]protection[.]outlook[.]com`	12
`microsoft[.]com`	12
`patmushta[.]info`	12
`249[.]5[.]55[.]69[.]bl[.]spamcop[.]net`	11
`249[.]5[.]55[.]69[.]cbl[.]abuseat[.]org`	11
`249[.]5[.]55[.]69[.]dnsbl[.]sorbs[.]net`	11
`249[.]5[.]55[.]69[.]in-addr[.]arpa`	11
`249[.]5[.]55[.]69[.]sbl-xbl[.]spamhaus[.]org`	11
`249[.]5[.]55[.]69[.]zen[.]spamhaus[.]org`	11
`www[.]google[.]com`	11
`whois[.]arin[.]net`	11
`whois[.]iana[.]org`	11
`aspmx[.]l[.]google[.]com`	11

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`mail[.]mailerhost[.]net`	11
`fastpool[.]xyz`	11
`www[.]instagram[.]com`	10
`ianawhois[.]vip[.]icann[.]org`	10
`mx01[.]oxsus-vadesecure[.]net`	10
`mail[.]h-email[.]net`	10
`mx0a-00191d01[.]pphosted[.]com`	10
`smtp[.]yopmail[.]com`	10
`mx1[.]naver[.]com`	9
`mx1[.]seznam[.]cz`	9
`bellsouth[.]com`	9
`naver[.]com`	9

*See JSON for more IOCs

Files and or directories created	Occurrences
`%SystemRoot%\SysWOW64\<random, matching '[a-z]{8}'>`	12
`%SystemRoot%\SysWOW64\config\systemprofile`	11
`%SystemRoot%\SysWOW64\config\systemprofile:.repos`	11
`%System32%\config\systemprofile:.repos`	11
`%TEMP%\<random, matching '[a-z]{8}'>.exe`	11
`%TEMP%\zwqprzv.exe`	1
`\Users\user\AppData\Local\Temp\lkdyrgak.exe`	1
`\Users\user\AppData\Local\Temp\wrnysiik.exe`	1
`\Users\user\AppData\Local\Temp\evrkqnrx.exe`	1
`\Users\user\AppData\Local\Temp\hgrwijsw.exe`	1
`\Users\user\AppData\Local\Temp\tpuuwzks.exe`	1
`\Users\user\AppData\Local\Temp\khbackg.exe`	1

Files and or directories created	Occurrences
`\Users\user\AppData\Local\Temp\wsxxzcnv.exe`	1
`\Users\user\AppData\Local\Temp\ksvvedjb.exe`	1
`\Users\user\AppData\Local\Temp\awbbdgrz.exe`	1
`\Users\user\AppData\Local\Temp\utivytuo.exe`	1
`\Users\user\AppData\Local\Temp\qnhgiqm.exe`	1
`\Users\user\AppData\Local\Temp\ongbujdn.exe`	1

File Hashes

```
15d120755f8a25be6ec7d68e2c055ce49ab1b24a6690016cbb870328f4745adc
232028b9007937cea100813b5caa870924dcf692dfc4368e2ff33771170c08a1
2aeb63ca3ce4ba5832ea9aca3a3bddf658a04e124a8903e97d8ae53eba9c7b98
40c2ad4b954b53a0a134c295428523b08d7e282025c681702b007a462eb6693a
5e8e7b26b5156591b4c29848b94f79f3d9812305de4503addf02355ebeb92894
8acb035dd8d1eaef5053188170e7c6820ad7439eb70e0d32ca1f88e1535af82d
aa4cb6e59d3cbca2cb5b3c0e0e1b1775fba530a0769e3cc105c381f98c1497e8
aa89986881a9c81bba26925326056c5e1c26de85288f3217a956bd2ca466cde2
add6a8419c9332e0e6052b2c60fa6915220f6402f13e478d851b92dc6ca413cd
dfaef1fdf4987beca57098f688530ada6262f481ded1950f6ed7871f5050afe5
f78b5562d7a9acf27d4197eab873648e624bc0d081bf0505ef3d0ad2ea33d415
ff7190ae3095aa0d19caa1843f8a4d36406664872f4026fe34267d84d9f92b7e
```

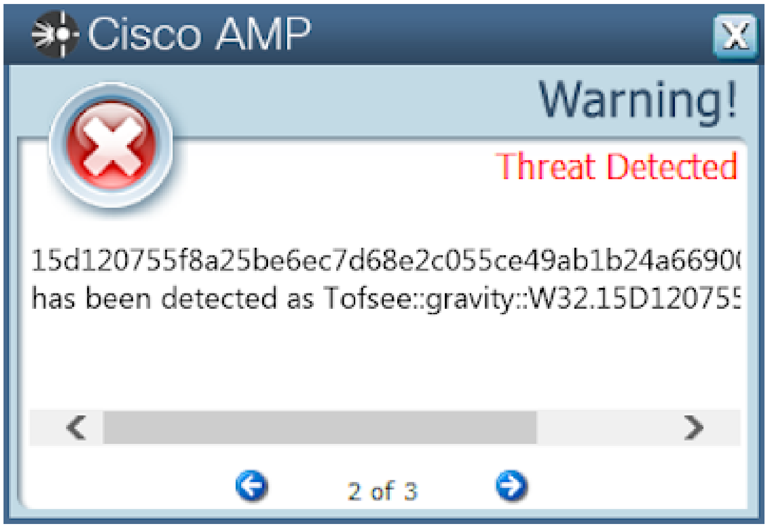
Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	
Email Security	

Product	Protection
Network Security	
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	
WSA	

Screenshots of Detection

Secure Endpoint

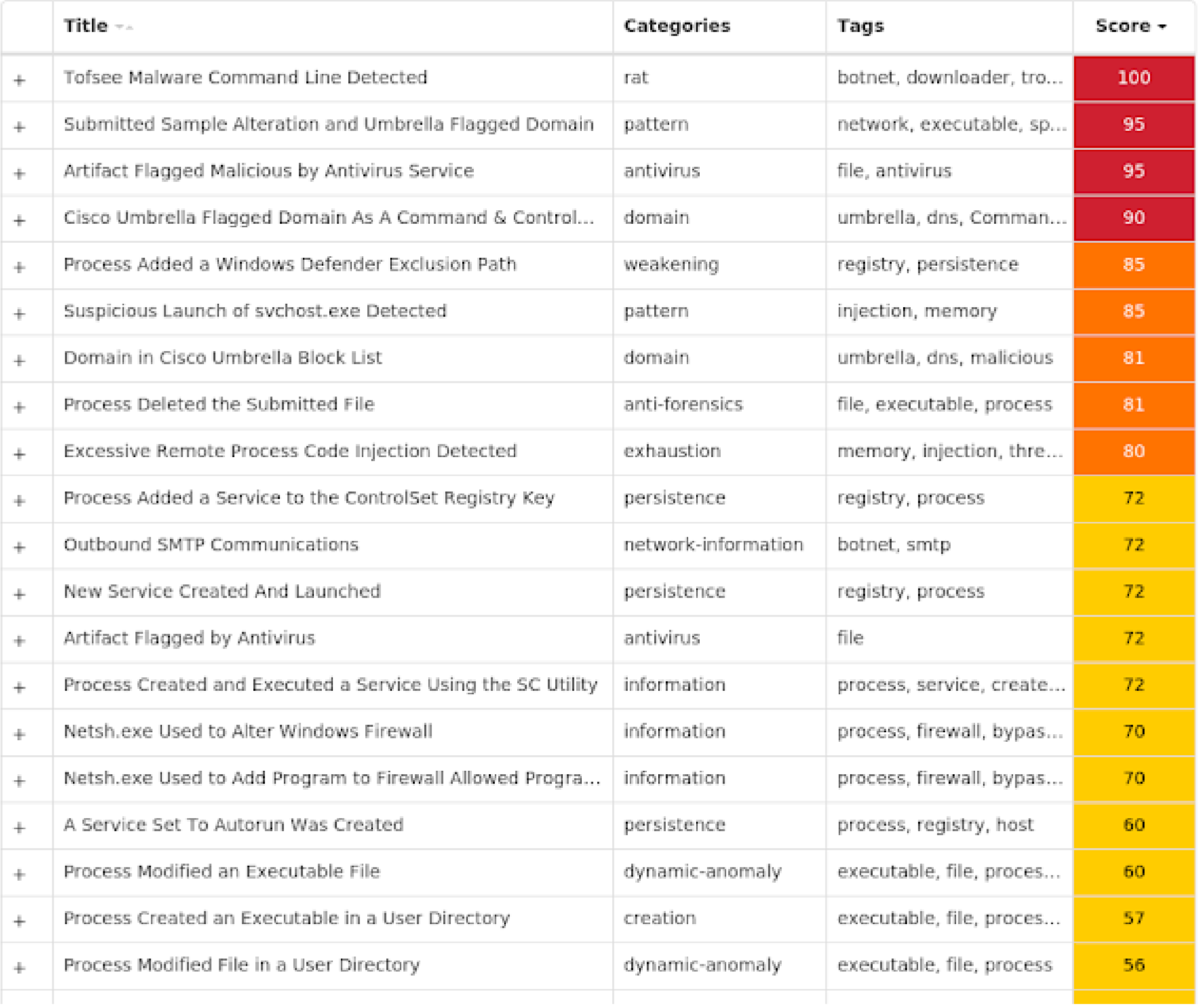


Warning!

Threat Detected

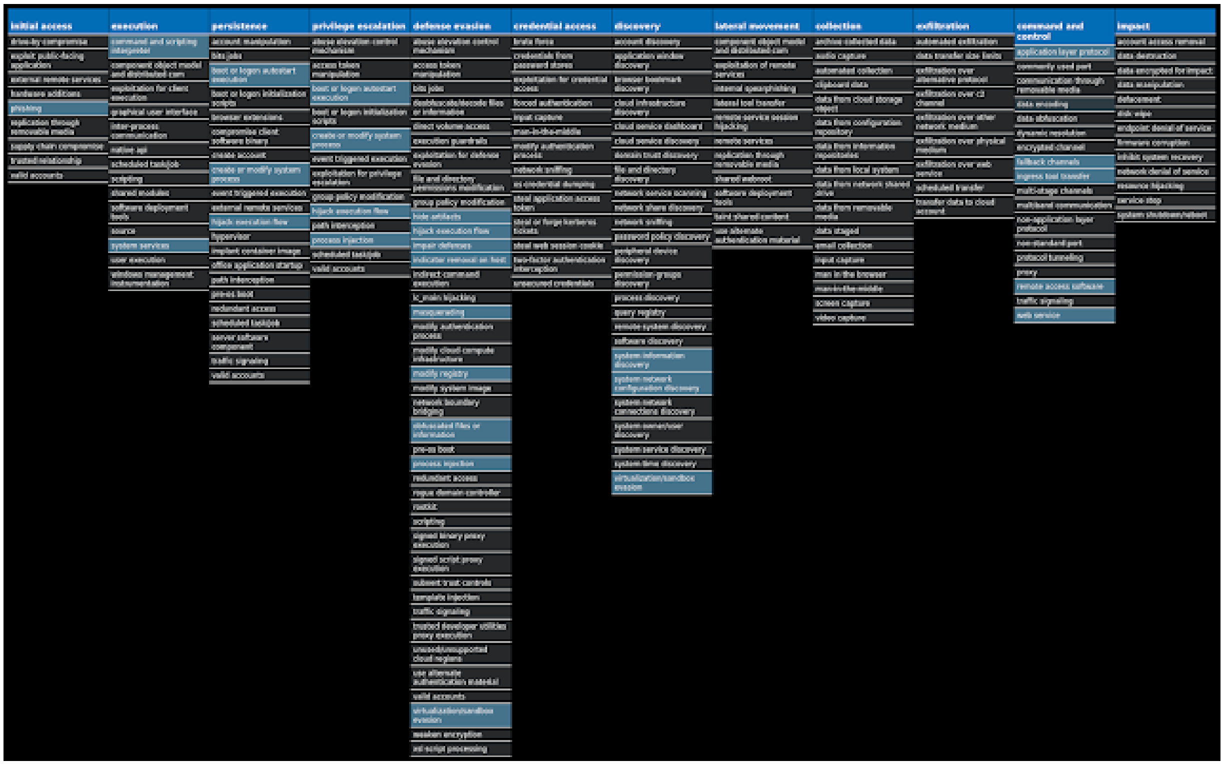
15d120755f8a25be6ec7d68e2c055ce49ab1b24a6690
has been detected as Tofsee::gravity::W32.15D12075

Secure Malware Analytics



	Title	Categories	Tags	Score ▾
+	Tofsee Malware Command Line Detected	rat	botnet, downloader, tro...	100
+	Submitted Sample Alteration and Umbrella Flagged Domain	pattern	network, executable, sp...	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Cisco Umbrella Flagged Domain As A Command & Control...	domain	umbrella, dns, Comman...	90
+	Process Added a Windows Defender Exclusion Path	weakening	registry, persistence	85
+	Suspicious Launch of svchost.exe Detected	pattern	injection, memory	85
+	Domain in Cisco Umbrella Block List	domain	umbrella, dns, malicious	81
+	Process Deleted the Submitted File	anti-forensics	file, executable, process	81
+	Excessive Remote Process Code Injection Detected	exhaustion	memory, injection, thre...	80
+	Process Added a Service to the ControlSet Registry Key	persistence	registry, process	72
+	Outbound SMTP Communications	network-information	botnet, smtp	72
+	New Service Created And Launched	persistence	registry, process	72
+	Artifact Flagged by Antivirus	antivirus	file	72
+	Process Created and Executed a Service Using the SC Utility	information	process, service, create...	72
+	Netsh.exe Used to Alter Windows Firewall	information	process, firewall, bypas...	70
+	Netsh.exe Used to Add Program to Firewall Allowed Progra...	information	process, firewall, bypas...	70
+	A Service Set To Autorun Was Created	persistence	process, registry, host	60
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces...	60
+	Process Created an Executable in a User Directory	creation	executable, file, proces...	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56

MITRE ATT&CK



initial access
- drive-by compromise
- exploit public-facing application
- external remote services
- hardware additions
- phishing
- replication through removable media
- supply chain compromise
- trusted relationship
- valid accounts

execution
- command and scripting interpreter
- component object model and distributed com
- exploitation for client execution
- graphical user interface
- inter-process communication
- native api
- scheduled task/job
- scripting
- shared modules
- software deployment tools
- source
- system services
- user execution
- windows management instrumentation

persistence
- account manipulation
- bits jobs
- boot or logon autostart execution
- boot or logon initialization scripts
- browser extensions
- compromise client software binary
- create account
- create or modify system process
- event triggered execution
- external remote services
- hijack execution flow
- hypervisor
- implant container image
- office application startup
- path interception
- pre-os boot
- redundant access
- scheduled task/job
- server software component
- traffic signaling
- valid accounts

privilege escalation
- abuse elevation control mechanism
- access token manipulation
- boot or logon autostart execution
- boot or logon initialization scripts
- create or modify system process
- event triggered execution
- exploitation for privilege escalation
- group policy modification
- hijack execution flow
- path interception
- process injection
- scheduled task/job
- valid accounts

defense evasion
- abuse elevation control mechanism
- access token manipulation
- bits jobs
- deobfuscate/decode files or information
- direct volume access
- execution guardrails
- exploitation for defense evasion
- file and directory permissions modification
- group policy modification
- hide artifacts
- hijack execution flow
- impair defenses
- indicator removal on host
- indirect command execution
- lc_main hijacking
- masquerading
- modify authentication process
- modify cloud compute infrastructure
- modify registry
- modify system image
- network boundary bridging
- obfuscated files or information
- pre-os boot
- process injection
- redundant access
- rogue domain controller
- rootkit
- scripting
- signed binary proxy execution
- signed script proxy execution
- subvert trust controls
- template injection
- traffic signaling
- trusted developer utilities proxy execution
- unused/unsupported cloud regions
- use alternate authentication material
- valid accounts
- virtualization/sandbox evasion
- weaken encryption
- xsl script processing

credential access
- brute force
- credentials from password stores
- exploitation for credential access
- forced authentication
- input capture
- man-in-the-middle
- modify authentication process
- network sniffing
- os credential dumping
- steal application access token
- steal or forge kerberos tickets
- steal web session cookie
- two-factor authentication interception
- unsecured credentials

discovery
- account discovery
- application window discovery
- browser bookmark discovery
- cloud infrastructure discovery
- cloud service dashboard
- cloud service discovery
- domain trust discovery
- file and directory discovery
- network service scanning
- network share discovery
- network sniffing
- password policy discovery
- peripheral device discovery
- permission groups discovery
- process discovery
- query registry
- remote system discovery
- software discovery
- system information discovery
- system network configuration discovery
- system network connections discovery
- system owner/user discovery
- system service discovery
- system time discovery
- virtualization/sandbox evasion

lateral movement
- component object model and distributed com
- exploitation of remote services
- internal spearphishing
- lateral tool transfer
- remote service session hijacking
- remote services
- replication through removable media
- shared webroot
- software deployment tools
- taint shared content
- use alternate authentication material

collection
- archive collected data
- audio capture
- automated collection
- clipboard data
- data from cloud storage object
- data from configuration repository
- data from information repositories
- data from local system
- data from network shared drive
- data from removable media
- data staged
- email collection
- input capture
- man in the browser
- man-in-the-middle
- screen capture
- video capture

exfiltration
- automated exfiltration
- data transfer size limits
- exfiltration over alternative protocol
- exfiltration over c2 channel
- exfiltration over other network medium
- exfiltration over physical medium
- exfiltration over web service
- scheduled transfer
- transfer data to cloud account

command and control
- application layer protocol
- commonly used port
- communication through removable media
- data encoding
- data obfuscation
- dynamic resolution
- encrypted channel
- fallback channels
- ingress tool transfer
- multi-stage channels
- multiband communication
- non-application layer protocol
- non-standard port
- protocol tunneling
- proxy
- remote access software
- traffic signaling
- web service

impact
- account access removal
- data destruction
- data encrypted for impact
- data manipulation
- defacement
- disk wipe
- endpoint denial of service
- firmware corruption
- inhibit system recovery
- network denial of service
- resource hijacking
- service stop
- system shutdown/reboot

Win.Dropper.Lokibot-9938416-1

Indicators of Compromise

IOCs collected from dynamic analysis of 15 samples

Registry Keys	Occurrences
`<HKCR>\LOCAL SETTINGS\SOFTWARE\MICROSOFT\WINDOWS\SHELL\BAGS\159`	15
`<HKCU>\SOFTWARE\WINRAR`	1

`<HKCU>\SOFTWARE\WINRAR`
`Value Name: HWID`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: 076c8cd6b128aff0be52736591e26777d73497ff0b36a2f5ee9966ca051adf43.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: c02f78ea73a8f86ab721800af6bf9be1ba182a779a2b55fb7b583a1b79a63ce0.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: c081e8dc858925158f65aa758764781f07476edc4641dbbd1d3acdab4a590a87.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: 43fbaf28a8db23ce81f85286b3316b6d3a352af0948bb58f01f7e929631f9740.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: c110ae946c48f8f26287c7163cd1557bc4ad83abb93e26c10b32df856fe5c72e.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: 12cf795390f0849bce4b21f1987e7fbcc92f812accdbb1a297d00638ee3e0004.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: f8448219df30254002bdb8ccf5745b3f2156f25b1b48209d69a451dca03968f2.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: 04f2512b1cbeeab43d96983222b5cfc15031481eed599ed39ecfca0fdf05838f.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: ccdc34aa16b23192f0260b9c21529919f47c3b0e2e59034d512184b94267adc2.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: 52864c84c299b950f3de76f8b8387d6ebda6726ded21d64a8ad565c25d4e4d52.exe`
	1

Registry Keys	Occurrences

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name:`
`17eb09a8fb7eae2aaa740a74234a75b47c072ca93a1b65cda00a175e25720c88.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name:`
`c197343a6c7b1581b2d200e85869d7751b13549ff109b70ae5abd3b838fdea3a.exe`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name:`
`daf3e154beeb32370cf0a5cda571b3a84959a53da4c530a77696ecd1c24ab485.exe`
	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003E9`
`Value Name: F`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name:`
`7d00f5ccb1d443866e2d25a96377ea39787b825cf5dcd099cead7baa630e98a0.exe`
	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000001F5`
`Value Name: F`
	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003EC`
`Value Name: F`
	1

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name:`
`b73f8d8838c450977a85ba646b98db3d556b0e78a33a7b0f5126d8e698d00ba2.exe`
	1

Mutexes	Occurrences
`3749282D282E1E80C56CAE5A`	14
`3BA87BBD1CC40F3583D46680`	8

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`185[.]6[.]242[.]251`	6
`91[.]223[.]82[.]29`	3

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`nextlevlcourier[.]com`	2
`sharonbooks[.]ru`	2
`lidgeys[.]ru`	2
`dunysaki[.]ru`	2
`finelets[.]ru`	2

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`kkeyvenus[.]ru`	1
`joanread[.]ru`	1
`topreadz[.]ru`	1

Files and or directories created	Occurrences
`%APPDATA%\Microsoft\Skype.exe`	15
`%APPDATA%\D282E1`	14
`%APPDATA%\D282E1\1E80C5.lck`	14
`%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2580483871-590521980-3826313501-500\a18ca4003deb042bbee7a40f15e1970b_d19ab989-a35f-4710-83df-7b2db7efe7c5`	14
`%APPDATA%\D1CC40\0F3583.hdb`	8
`%APPDATA%\D1CC40\0F3583.lck`	8
`%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-1258710499-2222286471-4214075941-500\a18ca4003deb042bbee7a40f15e1970b_8f793a96-da80-4751-83f9-b23d8b735fb1`	8
`%APPDATA%\D1CC40\0F3583.exe (copy)`	1
`%TEMP%\105687.bat`	1
`%TEMP%\-1530491364.bat`	1

File Hashes

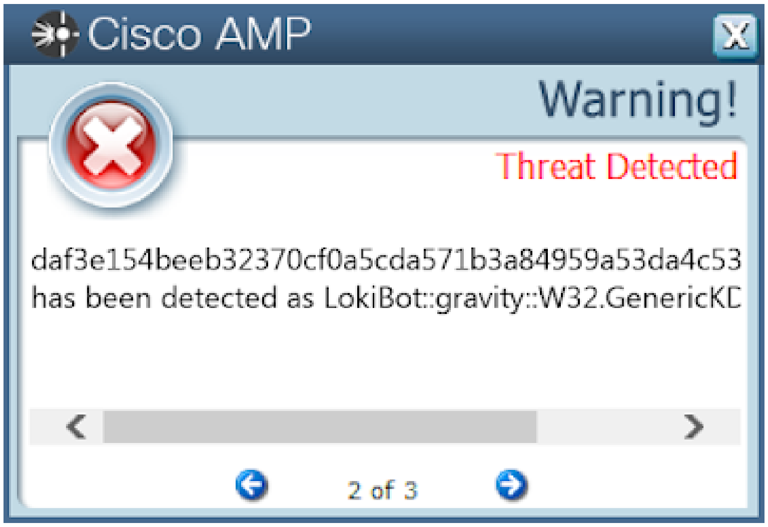
```
04f2512b1cbeeab43d96983222b5cfc15031481eed599ed39ecfca0fdf05838f
076c8cd6b128aff0be52736591e26777d73497ff0b36a2f5ee9966ca051adf43
12cf795390f0849bce4b21f1987e7fbcc92f812accdbb1a297d00638ee3e0004
17eb09a8fb7eae2aaa740a74234a75b47c072ca93a1b65cda00a175e25720c88
43fbaf28a8db23ce81f85286b3316b6d3a352af0948bb58f01f7e929631f9740
52864c84c299b950f3de76f8b8387d6ebda6726ded21d64a8ad565c25d4e4d52
7d00f5ccb1d443866e2d25a96377ea39787b825cf5dcd099cead7baa630e98a0
b73f8d8838c450977a85ba646b98db3d556b0e78a33a7b0f5126d8e698d00ba2
c02f78ea73a8f86ab721800af6bf9be1ba182a779a2b55fb7b583a1b79a63ce0
c081e8dc858925158f65aa758764781f07476edc4641dbbd1d3acdab4a590a87
c110ae946c48f8f26287c7163cd1557bc4ad83abb93e26c10b32df856fe5c72e
c197343a6c7b1581b2d200e85869d7751b13549ff109b70ae5abd3b838fdea3a
ccdc34aa16b23192f0260b9c21529919f47c3b0e2e59034d512184b94267adc2
daf3e154beeb32370cf0a5cda571b3a84959a53da4c530a77696ecd1c24ab485
f8448219df30254002bdb8ccf5745b3f2156f25b1b48209d69a451dca03968f2
```

Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	
Email Security	
Network Security	N/A
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	
WSA	

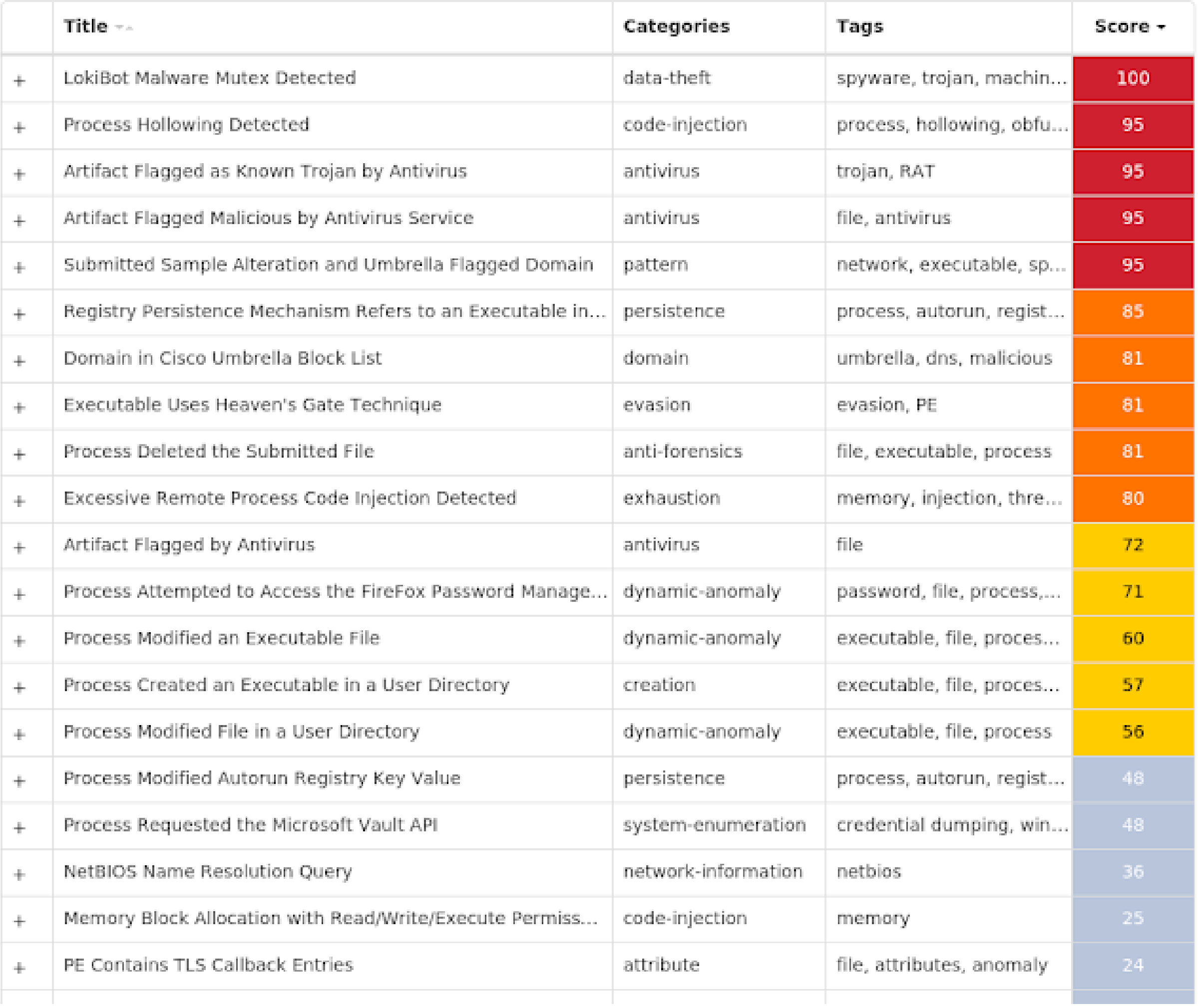
Screenshots of Detection

Secure Endpoint



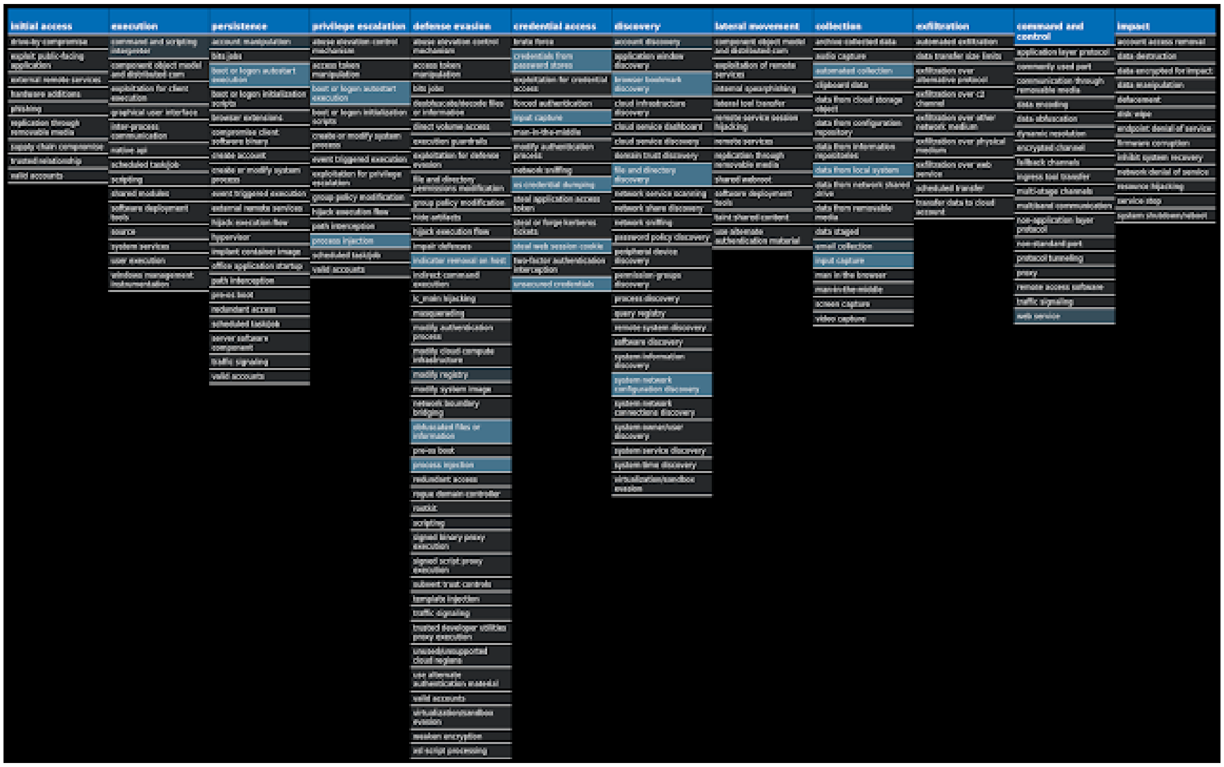
daf3e154beeb32370cf0a5cda571b3a84959a53da4c53
has been detected as LokiBot::gravity::W32.GenericKD

Secure Malware Analytics



	Title	Categories	Tags	Score
+	LokiBot Malware Mutex Detected	data-theft	spyware, trojan, machin...	100
+	Process Hollowing Detected	code-injection	process, hollowing, obfu...	95
+	Artifact Flagged as Known Trojan by Antivirus	antivirus	trojan, RAT	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Submitted Sample Alteration and Umbrella Flagged Domain	pattern	network, executable, sp...	95
+	Registry Persistence Mechanism Refers to an Executable in...	persistence	process, autorun, regist...	85
+	Domain in Cisco Umbrella Block List	domain	umbrella, dns, malicious	81
+	Executable Uses Heaven's Gate Technique	evasion	evasion, PE	81
+	Process Deleted the Submitted File	anti-forensics	file, executable, process	81
+	Excessive Remote Process Code Injection Detected	exhaustion	memory, injection, thre...	80
+	Artifact Flagged by Antivirus	antivirus	file	72
+	Process Attempted to Access the FireFox Password Manage...	dynamic-anomaly	password, file, process,...	71
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces...	60
+	Process Created an Executable in a User Directory	creation	executable, file, proces...	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56
+	Process Modified Autorun Registry Key Value	persistence	process, autorun, regist...	48
+	Process Requested the Microsoft Vault API	system-enumeration	credential dumping, win...	48
+	NetBIOS Name Resolution Query	network-information	netbios	36
+	Memory Block Allocation with Read/Write/Execute Permiss...	code-injection	memory	25
+	PE Contains TLS Callback Entries	attribute	file, attributes, anomaly	24

MITRE ATT&CK



initial access	execution	persistence	privilege escalation	defense evasion	credential access	discovery	lateral movement	collection	exfiltration	command and control	impact
drive-by compromise	command and scripting interpreter	account manipulation	abuse elevation control mechanism	abuse elevation control mechanism	brute force	account discovery	component object model and distributed com	archive collected data	automated exfiltration	application layer protocol	account access removal
exploit public-facing application	component object model and distributed com	bits jobs	access token manipulation	access token manipulation	credentials from password stores	application window discovery	exploitation of remote services	audio capture	data transfer size limits	commonly used port	data destruction
external remote services	exploitation for client execution	boot or logon autostart execution	boot or logon autostart execution	bits jobs	exploitation for credential access	browser bookmark discovery	internal spearphishing	automated collection	exfiltration over alternative protocol	communication through removable media	data encrypted for impact
hardware additions	graphical user interface	boot or logon initialization scripts	boot or logon initialization scripts	deobfuscate/decode files or information	forced authentication	cloud infrastructure discovery	lateral tool transfer	clipboard data	exfiltration over c2 channel	data encoding	data manipulation
phishing	inter-process communication	browser extensions	create or modify system process	direct volume access	input capture	cloud service dashboard	remote service session hijacking	data from cloud storage object	exfiltration over other network medium	data obfuscation	defacement
replication through removable media	native api	compromise client software binary	event triggered execution	execution guardrails	man-in-the-middle	cloud service discovery	remote services	data from configuration repository	exfiltration over physical medium	dynamic resolution	disk wipe
supply chain compromise	scheduled task/job	create account	exploitation for privilege escalation	exploitation for defense evasion	modify authentication process	domain trust discovery	replication through removable media	data from information repositories	exfiltration over web service	encrypted channel	endpoint denial of service
trusted relationship	scripting	create or modify system process	group policy modification	file and directory permissions modification	network sniffing	file and directory discovery	shared webroot	data from local system	scheduled transfer	fallback channels	firmware corruption
valid accounts	shared modules	event triggered execution	hijack execution flow	group policy modification	os credential dumping	network service scanning	software deployment tools	data from network shared drive	transfer data to cloud account	ingress tool transfer	inhibit system recovery
	software deployment tools	external remote services	path interception	hide artifacts	steal application access token	network share discovery	taint shared content	data from removable media		multi-stage channels	network denial of service
	source	hijack execution flow	process injection	hijack execution flow	steal or forge kerberos tickets	network sniffing	use alternate authentication material	data staged		multiband communication	resource hijacking
	system services	hypervisor	scheduled task/job	impair defenses	steal web session cookie	password policy discovery		email collection		non-application layer protocol	service stop
	user execution	implant container image	valid accounts	indicator removal on host	two-factor authentication interception	peripheral device discovery		input capture		non-standard port	system shutdown/reboot
	windows management instrumentation	office application startup		indirect command execution	unsecured credentials	permission groups discovery		man in the browser		protocol tunneling	
		path interception		lc_main hijacking		process discovery		man-in-the-middle		proxy	
		pre-os boot		masquerading		query registry		screen capture		remote access software	
		redundant access		modify authentication process		remote system discovery		video capture		traffic signaling	
		scheduled task/job		modify cloud compute infrastructure		software discovery				web service	
		server software component		modify registry		system information discovery					
		traffic signaling		modify system image		system network configuration discovery					
		valid accounts		network boundary bridging		system network connections discovery					
				obfuscated files or information		system owner/user discovery					
				pre-os boot		system service discovery					
				process injection		system time discovery					
				redundant access		virtualization/sandbox evasion					
				rogue domain controller							
				rootkit							
				scripting							
				signed binary proxy execution							
				signed script proxy execution							
				subvert trust controls							
				template injection							
				traffic signaling							
				trusted developer utilities proxy execution							
				unused/unsupported cloud regions							
				use alternate authentication material							
				valid accounts							
				virtualization/sandbox evasion							
				weaken encryption							
				xsl script processing							

Win.Virus.Xpiro-9938457-1

Indicators of Compromise

IOCs collected from dynamic analysis of 29 samples

Registry Keys	Occurrences

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V2.0.50727_32`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V2.0.50727_64`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V4.0.30319_32`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V4.0.30319_32`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V4.0.30319_64`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V4.0.30319_64`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\COMSYSAPP`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\COMSYSAPP`
`Value Name: Start`
	28

Registry Keys	Occurrences

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\IEETWCOLLECTORSERVICE`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\IEETWCOLLECTORSERVICE`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\MSISERVER`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\MSISERVER`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\OSE`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\OSE`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\UI0DETECT`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\UI0DETECT`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\VDS`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\VDS`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\VSS`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\VSS`
`Value Name: Start`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\WMIAPSRV`
`Value Name: Type`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\WMIAPSRV`
`Value Name: Start`
	28

`<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\SECURITY CENTER\SVC\S-1-5-21-2580483871-590521980-3826313501-500`	28

`<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\SECURITY CENTER\SVC\S-1-5-21-2580483871-590521980-3826313501-500`
`Value Name: EnableNotifications`
	28

`<HKLM>\SYSTEM\CONTROLSET001\SERVICES\CLR_OPTIMIZATION_V2.0.50727_32`
`Value Name: Start`
	28

Mutexes	Occurrences
`kkq-vx_mtx63`	28

Mutexes	Occurrences
`kkq-vx_mtx64`	28
`kkq-vx_mtx65`	28
`kkq-vx_mtx66`	28
`kkq-vx_mtx67`	28
`kkq-vx_mtx68`	28
`kkq-vx_mtx69`	28
`kkq-vx_mtx70`	28
`kkq-vx_mtx71`	28
`kkq-vx_mtx72`	28
`kkq-vx_mtx73`	28
`kkq-vx_mtx74`	28
`kkq-vx_mtx75`	28
`kkq-vx_mtx76`	28
`kkq-vx_mtx77`	28
`kkq-vx_mtx78`	28
`kkq-vx_mtx79`	28
`kkq-vx_mtx80`	28
`kkq-vx_mtx81`	28
`kkq-vx_mtx82`	28
`kkq-vx_mtx83`	28
`kkq-vx_mtx84`	28
`kkq-vx_mtx85`	28
`kkq-vx_mtx86`	28
`kkq-vx_mtx87`	28

*See JSON for more IOCs

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`69[.]16[.]231[.]59`	16
`64[.]70[.]19[.]203`	14
`35[.]205[.]61[.]67`	11
`208[.]100[.]26[.]245`	10
`20[.]189[.]173[.]20/31`	9
`52[.]182[.]143[.]212`	5
`45[.]79[.]19[.]196`	4
`20[.]42[.]73[.]29`	4
`95[.]213[.]137[.]98`	4
`147[.]75[.]63[.]87`	4
`72[.]14[.]185[.]43`	2
`20[.]189[.]173[.]22`	2
`104[.]208[.]16[.]94`	2
`96[.]126[.]123[.]244`	1
`45[.]56[.]79[.]23`	1
`52[.]168[.]117[.]173`	1
`147[.]75[.]61[.]38`	1

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`wpad[.]example[.]org`	27
`computer[.]example[.]org`	26
`kgbrelaxxlub[.]ru`	18
`clientconfig[.]passport[.]net`	17
`grewz-platker[.]ru`	16
`vmss-prod-weu[.]westeurope[.]cloudapp[.]azure[.]com`	12
`kasperskygay-formula[.]in`	12
`www[.]microavrc-usb33bit[.]com`	12
`fmyjo-boneb[.]com`	12

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`fkegy-bikav[.]com`	12
`angar-promarenda[.]ru`	12
`fdecub-ydyg[.]ru`	12
`fgefa-bugin[.]com`	12
`silcroadseevers[.]net`	11
`fethardanabiozdoviplat[.]com`	11
`bobamajopa2018[.]org`	11
`fpykyb-aquh[.]ru`	10
`vmss-prod-seas[.]southeastasia[.]cloudapp[.]azure[.]com`	8
`vmss-prod-eus[.]eastus[.]cloudapp[.]azure[.]com`	8
`zxspectrum4ever[.]in`	8
`directconnectionx[.]ws`	8
`www[.]indirs-lockit[.]ws`	8
`indir-connectx[.]ws`	8
`mpykyb-aquh[.]ru`	8
`mmyjo-boneb[.]com`	8

*See JSON for more IOCs

Files and or directories created	Occurrences
`%CommonProgramFiles(x86)%\microsoft shared\Source Engine\OSE.EXE`	28
`%ProgramFiles(x86)%\Microsoft Office\Office14\GROOVE.EXE`	28
`%ProgramFiles(x86)%\Mozilla Maintenance Service\maintenanceservice.exe`	28
`%SystemRoot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe`	28
`%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe`	28
`%SystemRoot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe`	28
`%SystemRoot%\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe`	28
`%System32%\FXSSVC.exe`	28

Files and or directories created	Occurrences
`%System32%\UI0Detect.exe`	28
`%System32%\VSSVC.exe`	28
`%System32%\alg.exe`	28
`%System32%\dllhost.exe`	28
`%System32%\ieetwcollector.exe`	28
`%System32%\msdtc.exe`	28
`%System32%\msiexec.exe`	28
`%System32%\snmptrap.exe`	28
`%System32%\sppsvc.exe`	28
`%System32%\vds.exe`	28
`%System32%\wbem\WmiApSrv.exe`	28
`%System32%\wbengine.exe`	28
`%SystemRoot%\ehome\ehsched.exe`	28
`%SystemRoot%\SysWOW64\dllhost.exe`	28
`%SystemRoot%\SysWOW64\msiexec.exe`	28
`%SystemRoot%\SysWOW64\svchost.exe`	28
`%SystemRoot%\SysWOW64\dllhost.vir`	28

*See JSON for more IOCs

File Hashes

```
12d9d3d438f8cf5e2cf8d3918f8228cf05830cc126376a4e411a4f58b1fdb78b
13f7d41bfa85d9698a3a85b02bd92c9d5454af74e6a8670e0df326ccf501f7e5
1c088ac2b3618e0230cabc4771104fb618b7842fc77b8380dedf8d7b40f29f92
1e657d63949d28e86fcc7ae0e0a963404b1c14a707ed2fdcd6f26ac568e2c4fd
1f43ff07475d63d7a1bc21eae9e75a64585af55168ade456fc19e7f2cc1f61b2
20c378d521841f48c964d61f192c2272663f5fe2fb8424f4461dc44a44b906c4
2d5209d8e4bd155ea3b5c7a4ff65847817a77744751513ce0f0d61c726eb5a84
3a9c31454e584355f07269a3a8ed226a6ad392e0f43076713d00200f2fa24d65
3ebeba1ea83a3db1d0c57811a65e5e8d1214559f595909aa898c749b84e42630
423a0c1bc0630bd11ff3f38d7be6735f097437dbbd51f68c9929f89ace4bb2fc
45eada2a2a4a0d8d1d4a74f3704cae34e8d326693fdd4c387253da469129ef25
5a2b08102a57e63e82ee86a871456ffc429e603b4231f4d2569857b046545503
5ebbb9527c740f5186a58a56f1c304d8fa0ff313695a06f24bcd637a9f23c762
```

```
6c06078490cf24f68ddbb898453048dadf2add5ff15fa24c5fa19ca6b265bfe7
70bdbe1fda1f0fca2f422ae4e2a447ea6278db99435492852b37f2b55f3ff849
7455f299568d3eb6ce4cb8a37b2d9665641fb30f64e9d4df64d820f0d0e26eb3
77fa98a5b5d5f448898538250ba65b65b4e486d95ad98bfdf7154a1e745d741e
7c7b0e39df9ba26a1701ee93ec84523cae5a997a039d5a1d99eab4774c8dc9a3
84f928d52e0fb045c4911a1ea54e445ceff8af7971b0d8f71b0f359cec962584
871b2e111a6193a265821d9223cf8820ae7cefada1d3d6f75cb8474c2a8a5820
9bbc214cc19a49956aed36c43cbecd454fc6d881d47937f2f4fb18679ec58c5e
b4639640121a2cc1b0b51f93fe0acf23a43f89862d5e5fffd847c97a6d147a56
b4aea243d08387872f981607899ae4dbfde9fed1c597ee5cc07f068c0b098688
b9ea1073ecae7096f10f296898fb02ba7e8b4cc1dbed70548d76c4ff028a55ac
c2e0b6a1839889b4277a0e20da80d858b33fe94e8af49975b2c0da7abc84c48e
```

*See JSON for more IOCs

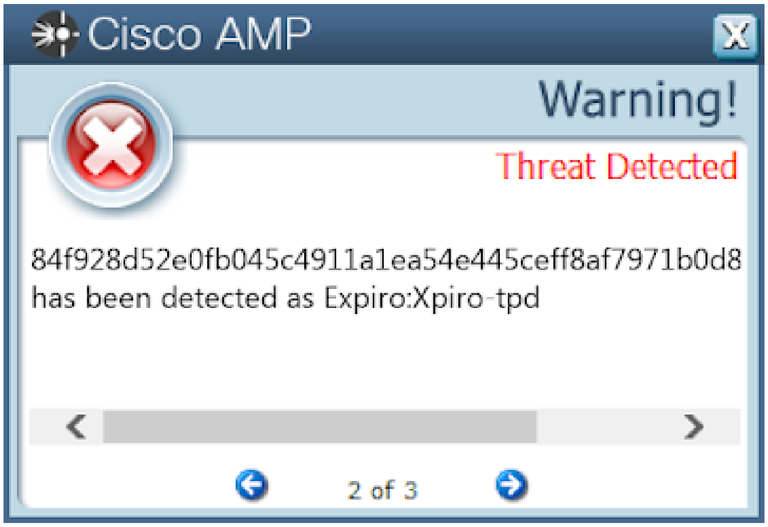
Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	
Email Security	
Network Security	N/A
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	

Product	Protection
WSA	

Screenshots of Detection

Secure Endpoint



Cisco AMP

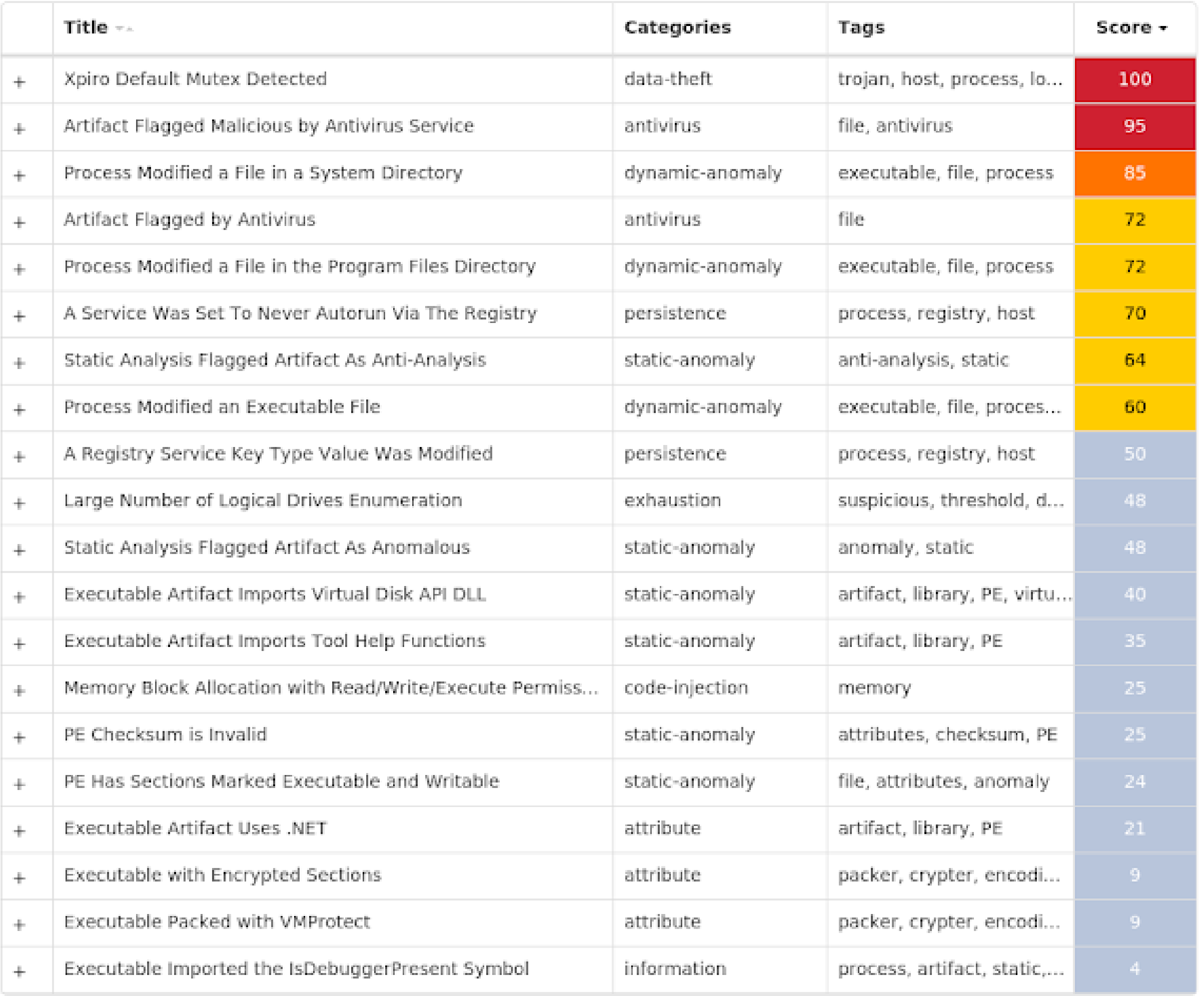
Warning!

Threat Detected

84f928d52e0fb045c4911a1ea54e445ceff8af7971b0d8
has been detected as Expiro:Xpiro-tpd

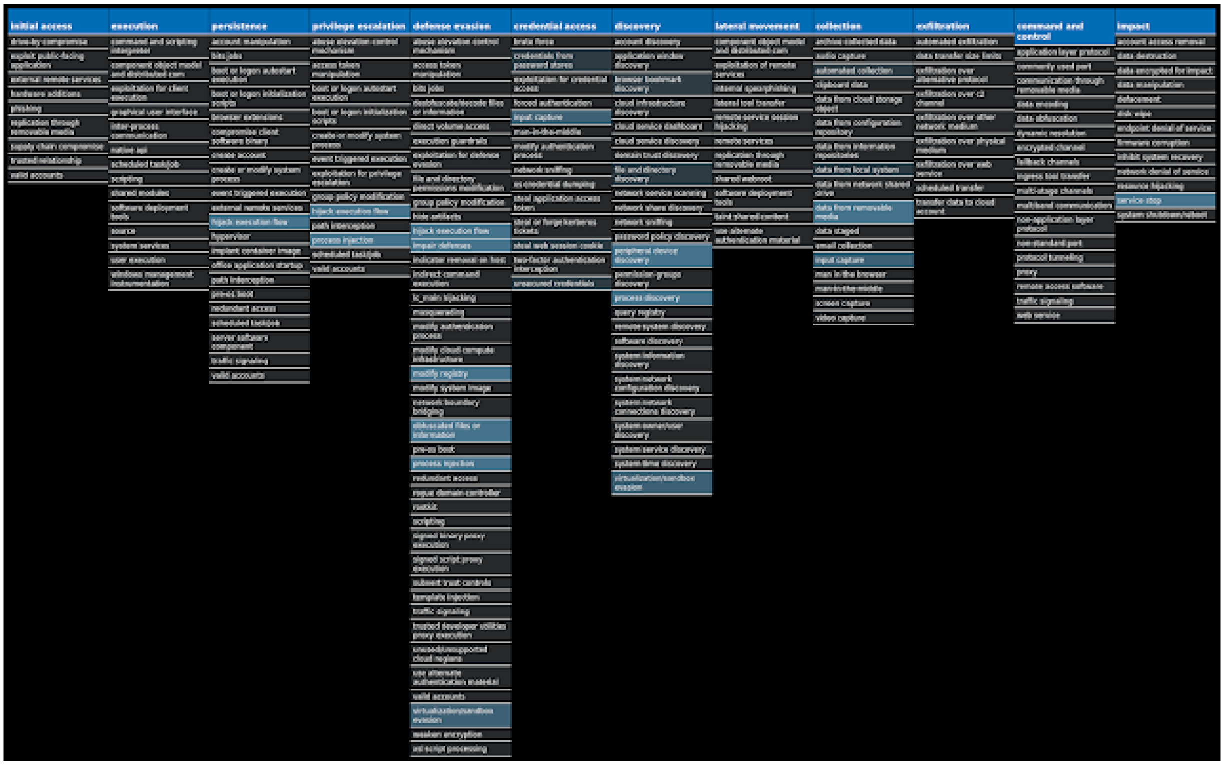
2 of 3

Secure Malware Analytics



	Title	Categories	Tags	Score
+	Xpiro Default Mutex Detected	data-theft	trojan, host, process, lo...	100
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Process Modified a File in a System Directory	dynamic-anomaly	executable, file, process	85
+	Artifact Flagged by Antivirus	antivirus	file	72
+	Process Modified a File in the Program Files Directory	dynamic-anomaly	executable, file, process	72
+	A Service Was Set To Never Autorun Via The Registry	persistence	process, registry, host	70
+	Static Analysis Flagged Artifact As Anti-Analysis	static-anomaly	anti-analysis, static	64
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces...	60
+	A Registry Service Key Type Value Was Modified	persistence	process, registry, host	50
+	Large Number of Logical Drives Enumeration	exhaustion	suspicious, threshold, d...	48
+	Static Analysis Flagged Artifact As Anomalous	static-anomaly	anomaly, static	48
+	Executable Artifact Imports Virtual Disk API DLL	static-anomaly	artifact, library, PE, virtu...	40
+	Executable Artifact Imports Tool Help Functions	static-anomaly	artifact, library, PE	35
+	Memory Block Allocation with Read/Write/Execute Permiss...	code-injection	memory	25
+	PE Checksum is Invalid	static-anomaly	attributes, checksum, PE	25
+	PE Has Sections Marked Executable and Writable	static-anomaly	file, attributes, anomaly	24
+	Executable Artifact Uses .NET	attribute	artifact, library, PE	21
+	Executable with Encrypted Sections	attribute	packer, crypter, encodi...	9
+	Executable Packed with VMProtect	attribute	packer, crypter, encodi...	9
+	Executable Imported the IsDebuggerPresent Symbol	information	process, artifact, static,...	4

MITRE ATT&CK



initial access	execution	persistence	privilege escalation	defense evasion	credential access	discovery	lateral movement	collection	exfiltration	command and control	impact
drive-by compromise	command and scripting interpreter	account manipulation	abuse elevation control mechanism	abuse elevation control mechanism	brute force	account discovery	component object model and distributed com	archive collected data	automated exfiltration	application layer protocol	account access removal
exploit public-facing application	component object model and distributed com	bits jobs	access token manipulation	access token manipulation	credentials from password stores	application window discovery	exploitation of remote services	audio capture	data transfer size limits	commonly used port	data destruction
external remote services	exploitation for client execution	boot or logon autostart execution	boot or logon autostart execution	bits jobs	exploitation for credential access	browser bookmark discovery	internal spearphishing	automated collection	exfiltration over alternative protocol	communication through removable media	data encrypted for impact
hardware additions	graphical user interface	boot or logon initialization scripts	boot or logon initialization scripts	deobfuscate/decode files or information	forced authentication	cloud infrastructure discovery	lateral tool transfer	clipboard data	exfiltration over c2 channel	data encoding	data manipulation
phishing	inter-process communication	browser extensions	create or modify system process	direct volume access	input capture	cloud service dashboard	remote service session hijacking	data from cloud storage object	exfiltration over other network medium	data obfuscation	defacement
replication through removable media	native api	compromise client software binary	event triggered execution	execution guardrails	man-in-the-middle	cloud service discovery	remote services	data from configuration repository	exfiltration over physical medium	dynamic resolution	disk wipe
supply chain compromise	scheduled task/job	create account	exploitation for privilege escalation	exploitation for defense evasion	modify authentication process	domain trust discovery	replication through removable media	data from information repositories	exfiltration over web service	encrypted channel	endpoint denial of service
trusted relationship	scripting	create or modify system process	group policy modification	file and directory permissions modification	network sniffing	file and directory discovery	shared webroot	data from local system	scheduled transfer	fallback channels	firmware corruption
valid accounts	shared modules	event triggered execution	hijack execution flow	group policy modification	os credential dumping	network service scanning	software deployment tools	data from network shared drive	transfer data to cloud account	ingress tool transfer	inhibit system recovery
	software deployment tools	external remote services	path interception	hide artifacts	steal application access token	network share discovery	taint shared content	data from removable media		multi-stage channels	network denial of service
	source	hijack execution flow	process injection	hijack execution flow	steal or forge kerberos tickets	network sniffing	use alternate authentication material	data staged		multiband communication	resource hijacking
	system services	hypervisor	scheduled task/job	impair defenses	steal web session cookie	password policy discovery		email collection		non-application layer protocol	service stop
	user execution	implant container image	valid accounts	indicator removal on host	two-factor authentication interception	peripheral device discovery		input capture		non-standard port	system shutdown/reboot
	windows management instrumentation	office application startup		indirect command execution	unsecured credentials	permission groups discovery		man in the browser		protocol tunneling	
		path interception		lc_main hijacking		process discovery		man-in-the-middle		proxy	
		pre-os boot		masquerading		query registry		screen capture		remote access software	
		redundant access		modify authentication process		remote system discovery		video capture		traffic signaling	
		scheduled task/job		modify cloud compute infrastructure		software discovery				web service	
		server software component		modify registry		system information discovery					
		traffic signaling		modify system image		system network configuration discovery					
		valid accounts		network boundary bridging		system network connections discovery					
				obfuscated files or information		system owner/user discovery					
				pre-os boot		system service discovery					
				process injection		system time discovery					
				redundant access		virtualization/sandbox evasion					
				rogue domain controller							
				rootkit							
				scripting							
				signed binary proxy execution							
				signed script proxy execution							
				subvert trust controls							
				template injection							
				traffic signaling							
				trusted developer utilities proxy execution							
				unused/unsupported cloud regions							
				use alternate authentication material							
				valid accounts							
				virtualization/sandbox evasion							
				weaken encryption							
				xsl script processing							

Win.Dropper.DarkComet-9938488-1

Indicators of Compromise

IOCs collected from dynamic analysis of 25 samples

Registry Keys	Occurrences
`<HKCU>\SOFTWARE\DC3_FEXEC`	25

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: MicroUpdate`
	25

`<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON`
`Value Name: UserInit`
	25

`<HKCR>\LOCAL SETTINGS\SOFTWARE\MICROSOFT\WINDOWS\SHELL\BAGS\159`	24

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 7:01:02 AM`
	14

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 7:02:02 AM`
	9

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:04:02 AM`
	4

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:03:02 AM`
	4

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 7:01:03 AM`
	4

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 7:02:01 AM`
	3

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:05:01 AM`
	2

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:04:01 AM`
	2

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:05:02 AM`
	1

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:04:09 AM`
	1

`<HKCU>\SOFTWARE\DC3_FEXEC`
`Value Name: 2/5/2022 at 1:04:03 AM`
	1

Mutexes	Occurrences
`DC_MUTEX-HMNSNR1`	25

Mutexes	Occurrences
RtkNGUI64	25

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
moneybag123[.]myftp[.]biz	25

Files and or directories created	Occurrences
%APPDATA%\dclogs	25
%TEMP%\MSDCSC	25
%TEMP%\MSDCSC\msdcsc.exe	25
%HOMEPATH%\Gfxv2_0	25
%HOMEPATH%\Gfxv2_0\WindowsUpdateElevatedInstaller.exe	25
%TEMP%\MSDCSC\zVtZSjWSmT8T	25
%TEMP%\MSDCSC\zVtZSjWSmT8T\msdcsc.exe	25
%System32%\Tasks\BitLockerWizardElev	25
%TEMP%\MSDCSC\zVtZSjWSmT8T\zVtZSjWSmT8T	19
%TEMP%\MSDCSC\zVtZSjWSmT8T\zVtZSjWSmT8T\msdcsc.exe	19

File Hashes

```
00c4d334768f563cced2a243cf640c592149cec38044bb8792e49945a23ee61b
04b793b2cf5441a512f49044f12199110fbc24abd5300f6de5da21c95a1b118a
0523cf6dcd6a1b89943cbd432e01e572f03c0abab43dcb055e95a301e9b1f957
126954e3d7bb42e1757598481610e6c229d3cfca43bca9ebaf2b788f58a3a2c9
13bae0fb3015efd0a27e6ea77fb9c5dfb885321c809d9668c34899ce9472c157
1642b09633ce8e3f79bcdad20242a3989645d3a60d6f686235b018c8914b8660
19a57c2208ef58387cb38412b0db3060b1ddcaf4f02929213f5355c40776a98d
21454d9e2f5e0c502b423ffadbbe802ae69f81a99fbc7c50817b1f80a083cf1a
293f0baa32b35d17e90cd03980a58d2fe1cff22efb4c09b8b2bbe210f4054856
2db522042954becd5b940edc0afbfc93f0039d3f4f775d4cfa45b7012587574e
33302b6dfc2b669df38aab7a4a7e74c512ce31ba3a5a9151aea435a86c36b738
37edc65fde51628d1604ddbf0c14f06035e8c6819b7d0bfac7fee8dd4bf30bc7
41d6765ff915ef589039b311d958c052d32d13bb03ce8b5af005161da952885a
461031f7db840c45b1c0b6644d2f8772105d57785b94fda069a5fbf921879da5
4ffc3229a0db6972c70c80db3be8c93017a4163f2724c6edf300ce87ba49041b
611196f2e7768773cd724ec0f5b6bf602187e6bb5fc1ec59fe379b47c78e4fcc
6b4a4161813a01e51ecca9b68e6d8b852ede2cfe6ff6f634f709493930f4b32b
8545cb2dea3b9d2948143182235218226146 1e5d91d441109eb562c818d3ceff
96c821c14f746271a3a89587cd25fbd47686e143bd53750c0416673df9e58a12
```

```
9a1056d1898a71f3b88c875ff08b5d465b549d03206cbe02efcb19c144582ee8
9c641719e876dc8b3f7ce206a59c3228b2d7abda81adecc2279a68186ce1a2d1
aec82f9487cdd2b727aa619b21b070b77db0572a98637212d3514f1868032828
b17c1f8063ba70ecef31071a6c51117953dddf37d4b54c1a92b01525cb44c38f
b40e00192ed4d4cf0c90e3c03c11124dae8fc7f2182be609b2c3efcc585a00be
b5201f282c7e067e5dca7de945ed48805af74c9dae94ec3f83ff93c151f83c39
```

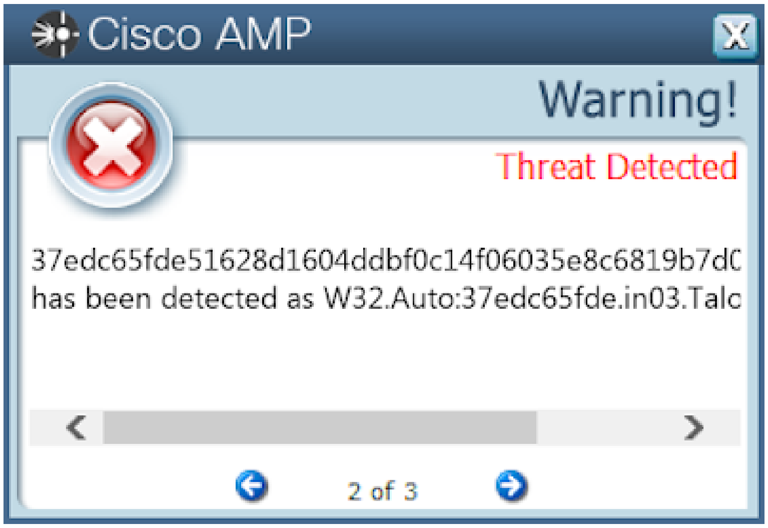
*See JSON for more IOCs

Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	
Email Security	
Network Security	N/A
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	N/A
WSA	N/A

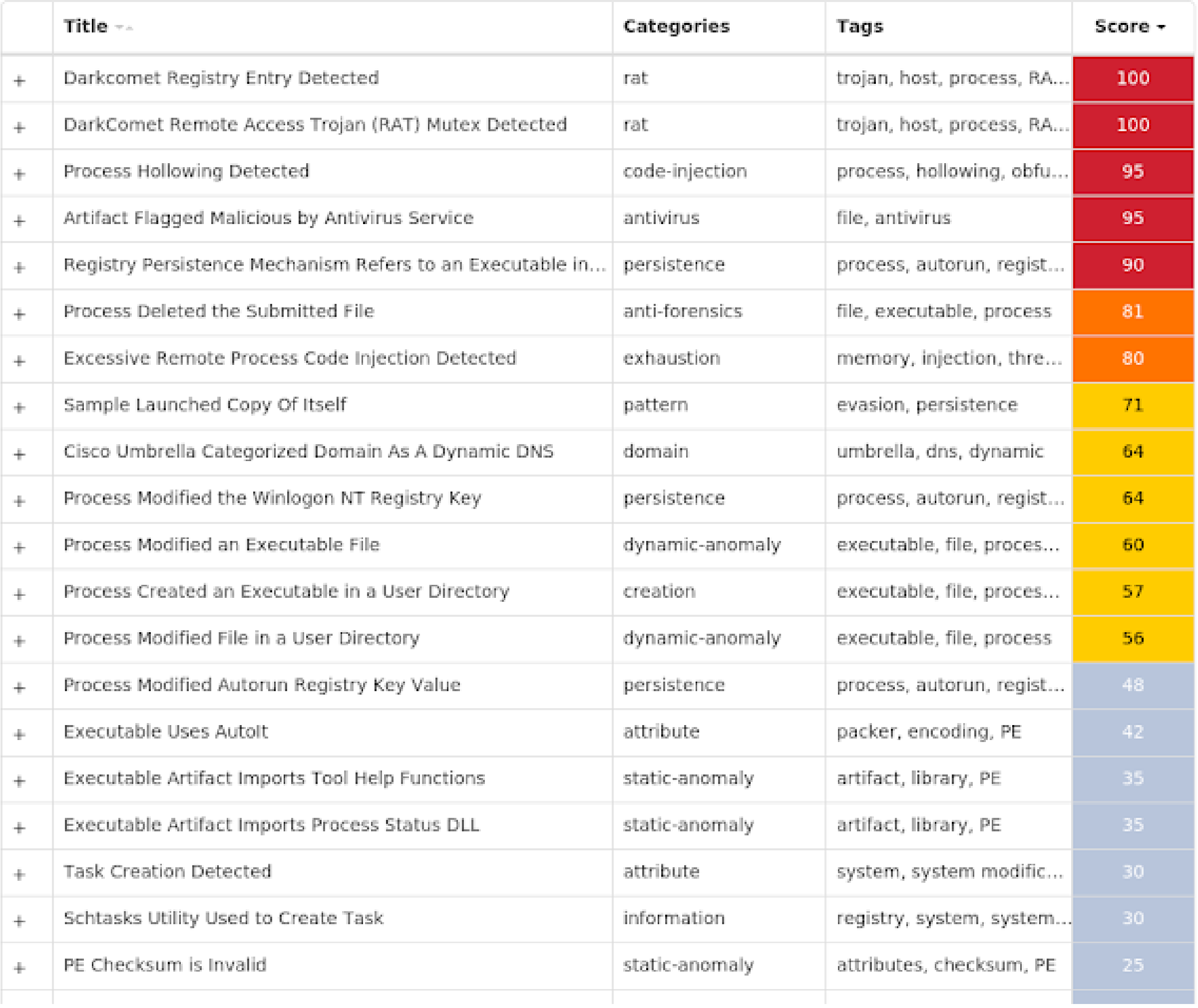
Screenshots of Detection

Secure Endpoint



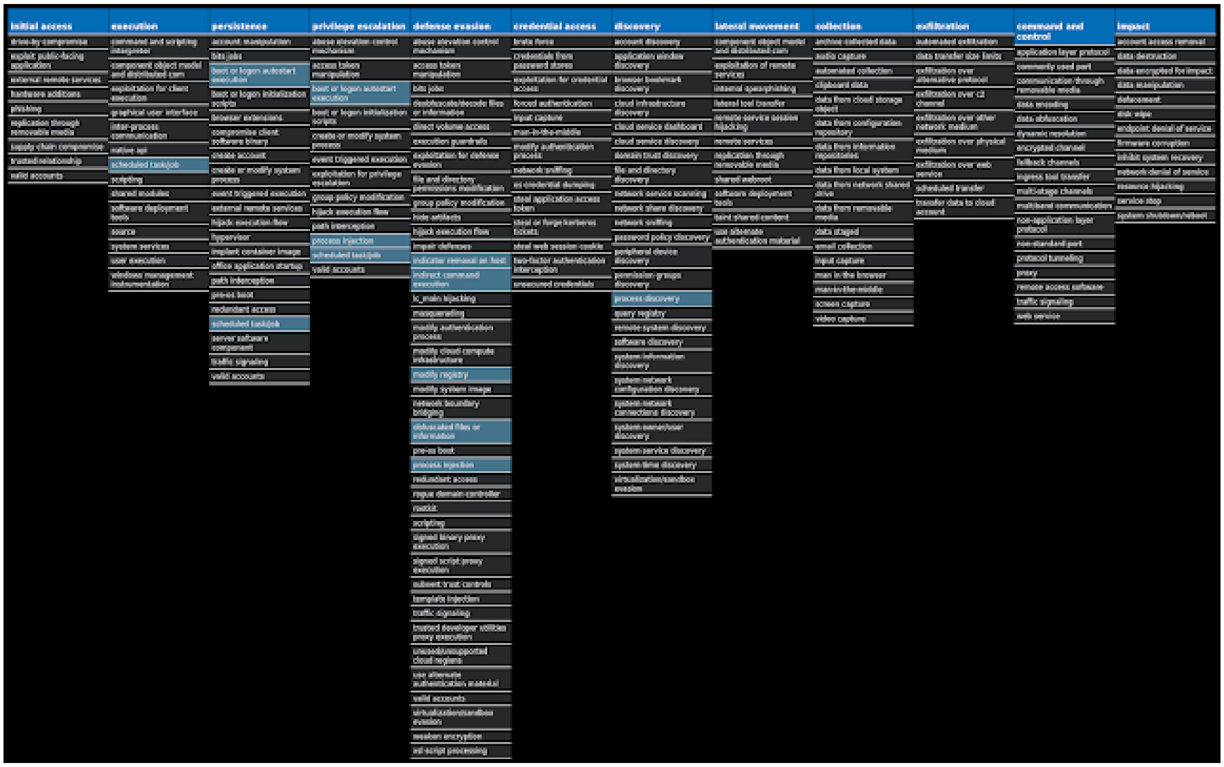
37edc65fde51628d1604ddbf0c14f06035e8c6819b7d0
has been detected as W32.Auto:37edc65fde.in03.Talc

Secure Malware Analytics



	Title	Categories	Tags	Score
+	Darkcomet Registry Entry Detected	rat	trojan, host, process, RA...	100
+	DarkComet Remote Access Trojan (RAT) Mutex Detected	rat	trojan, host, process, RA...	100
+	Process Hollowing Detected	code-injection	process, hollowing, obfu...	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Registry Persistence Mechanism Refers to an Executable in...	persistence	process, autorun, regist...	90
+	Process Deleted the Submitted File	anti-forensics	file, executable, process	81
+	Excessive Remote Process Code Injection Detected	exhaustion	memory, injection, thre...	80
+	Sample Launched Copy Of Itself	pattern	evasion, persistence	71
+	Cisco Umbrella Categorized Domain As A Dynamic DNS	domain	umbrella, dns, dynamic	64
+	Process Modified the Winlogon NT Registry Key	persistence	process, autorun, regist...	64
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces...	60
+	Process Created an Executable in a User Directory	creation	executable, file, proces...	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56
+	Process Modified Autorun Registry Key Value	persistence	process, autorun, regist...	48
+	Executable Uses AutoIt	attribute	packer, encoding, PE	42
+	Executable Artifact Imports Tool Help Functions	static-anomaly	artifact, library, PE	35
+	Executable Artifact Imports Process Status DLL	static-anomaly	artifact, library, PE	35
+	Task Creation Detected	attribute	system, system modific...	30
+	Schtasks Utility Used to Create Task	information	registry, system, system...	30
+	PE Checksum is Invalid	static-anomaly	attributes, checksum, PE	25

MITRE ATT&CK



initial access
- drive-by compromise
- exploit public-facing application
- external remote services
- hardware additions
- phishing
- replication through removable media
- supply chain compromise
- trusted relationship
- valid accounts

execution
- command and scripting interpreter
- component object model and distributed com
- exploitation for client execution
- graphical user interface
- inter-process communication
- native api
- scheduled task/job
- scripting
- shared modules
- software deployment tools
- source
- system services
- user execution
- windows management instrumentation

persistence
- account manipulation
- bits jobs
- boot or logon autostart execution
- boot or logon initialization scripts
- browser extensions
- compromise client software binary
- create account
- create or modify system process
- event triggered execution
- external remote services
- hijack execution flow
- hypervisor
- implant container image
- office application startup
- path interception
- pre-os boot
- redundant access
- scheduled task/job
- server software component
- traffic signaling
- valid accounts

privilege escalation
- abuse elevation control mechanism
- access token manipulation
- boot or logon autostart execution
- boot or logon initialization scripts
- create or modify system process
- event triggered execution
- exploitation for privilege escalation
- group policy modification
- hijack execution flow
- path interception
- process injection
- scheduled task/job
- valid accounts

defense evasion
- abuse elevation control mechanism
- access token manipulation
- bits jobs
- deobfuscate/decode files or information
- direct volume access
- execution guardrails
- exploitation for defense evasion
- file and directory permissions modification
- group policy modification
- hide artifacts
- hijack execution flow
- impair defenses
- indicator removal on host
- indirect command execution
- lc_main hijacking
- masquerading
- modify authentication process
- modify cloud compute infrastructure
- modify registry
- modify system image
- network boundary bridging
- obfuscated files or information
- pre-os boot
- process injection
- redundant access
- rogue domain controller
- rootkit
- scripting
- signed binary proxy execution
- signed script proxy execution
- subvert trust controls
- template injection
- traffic signaling
- trusted developer utilities proxy execution
- unused/unsupported cloud regions
- use alternate authentication material
- valid accounts
- virtualization/sandbox evasion
- weaken encryption
- xsl script processing

credential access
- brute force
- credentials from password stores
- exploitation for credential access
- forced authentication
- input capture
- man-in-the-middle
- modify authentication process
- network sniffing
- os credential dumping
- steal application access token
- steal or forge kerberos tickets
- steal web session cookie
- two-factor authentication interception
- unsecured credentials

discovery
- account discovery
- application window discovery
- browser bookmark discovery
- cloud infrastructure discovery
- cloud service dashboard
- cloud service discovery
- domain trust discovery
- file and directory discovery
- network service scanning
- network share discovery
- network sniffing
- password policy discovery
- peripheral device discovery
- permission groups discovery
- process discovery
- query registry
- remote system discovery
- software discovery
- system information discovery
- system network configuration discovery
- system network connections discovery
- system owner/user discovery
- system service discovery
- system time discovery
- virtualization/sandbox evasion

lateral movement
- component object model and distributed com
- exploitation of remote services
- internal spearphishing
- lateral tool transfer
- remote service session hijacking
- remote services
- replication through removable media
- software deployment tools
- taint shared content
- use alternate authentication material

collection
- archive collected data
- audio capture
- automated collection
- clipboard data
- data from cloud storage object
- data from configuration repository
- data from information repositories
- data from local system
- data from network shared drive
- data from removable media
- data staged
- email collection
- input capture
- man in the browser
- man-in-the-middle
- screen capture
- video capture

exfiltration
- automated exfiltration
- data transfer size limits
- exfiltration over alternative protocol
- exfiltration over c2 channel
- exfiltration over other network medium
- exfiltration over physical medium
- exfiltration over web service
- scheduled transfer
- transfer data to cloud account

command and control
- application layer protocol
- commonly used port
- communication through removable media
- data encoding
- data obfuscation
- dynamic resolution
- encrypted channel
- fallback channels
- ingress tool transfer
- multi-stage channels
- multiband communication
- non-application layer protocol
- non-standard port
- protocol tunneling
- proxy
- remote access software
- traffic signaling
- web service

impact
- account access removal
- data destruction
- data encrypted for impact
- data manipulation
- defacement
- disk wipe
- endpoint denial of service
- firmware corruption
- inhibit system recovery
- network denial of service
- resource hijacking
- service stop
- system shutdown/reboot

Win.Worm.Gh0stRAT-9938500-1

Indicators of Compromise

IOCs collected from dynamic analysis of 26 samples

Registry Keys	Occurrences
`<HKCR>\LOCAL SETTINGS\SOFTWARE\MICROSOFT\WINDOWS\SHELL\BAGS\159`	26

`<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
`Value Name: dtfd`
	26

Mutexes	Occurrences
`Mhost123.zz.am:6658`	26
`host123.zz.am:6658`	26

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`107[.]163[.]56[.]110`	26
`107[.]160[.]131[.]253`	26
`107[.]160[.]131[.]254`	26

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
`host123[.]zz[.]am`	26

Files and or directories created	Occurrences
`\1.txt`	26
`%TEMP%\<random, matching '[a-z]{4,9}'>.exe`	26
`%ProgramFiles%\<random, matching '[a-z]{5,9}\[a-z]{3,9}'>.exe`	26
`%ProgramFiles%\<random, matching '[a-z]{5,9}\[a-z]{3,9}'>.dll`	26
`%ProgramFiles%\<random, matching '[a-z]{5,8}'>`	24
`%ProgramFiles%\axofwxn\12010043`	2
`%ProgramFiles%\uqvba\12010043`	1
`%ProgramFiles%\mvbii\12010043`	1
`%ProgramFiles%\cjzls\12010043`	1
`%ProgramFiles%\pdvzn\12010043`	1
`%ProgramFiles%\yhfes\12010043`	1
`%ProgramFiles%\mqbaqfto\12010043`	1
`%ProgramFiles%\fycasauyy`	1
`%ProgramFiles%\mtotuwc\12010043`	1
`%ProgramFiles%\jaafc\12010043`	1
`%ProgramFiles%\tkxvwyhl\12010043`	1
`%ProgramFiles%\mqdug\12010043`	1
`%ProgramFiles%\fycasauyy\12010043`	1
`%ProgramFiles%\axddl\12010043`	1
`%ProgramFiles%\tufcwnkzd`	1
`%ProgramFiles%\cidhqek\12010043`	1
`%ProgramFiles%\qytxj\12010043`	1
`%ProgramFiles%\bghvo\12010043`	1
`%ProgramFiles%\qhpobisc\12010043`	1
`%ProgramFiles%\tufcwnkzd\12010043`	1

*See JSON for more IOCs

File Hashes

```
01b1fcc6a12cc903fe0dbc560d5a4ef1a1c97338c3250f4b95ded8bffb9a5334
0281fe6b45250edb67ea958b6f40117352c4ef5a508ad250694ed6367d702fcd
0391037f82b2bc2738e54552d764d706643cadaf405de682bfe64ca911a34bc5
08d01b5a2cf7371fb2929a43e3de40d3a7ebde7abd2a30016db5721fdc9f493a
09ec933e44eda616bc5dd6b1b9defd4cd2c247e01eda3a1e02fa4a81708e49a3
123782513add1750a253e0acc93cba7424610a8112745431928fc0c21d00e844
300ba8c9e61fc6fd9223bd981681ca6ee9d79e7e03703bda9f14159eaf4e2c5f
34e0e3d43abcc0eefc3b70ef4b5e8889d61d4ea4571d928501341822de881f3a
35a84a43a11e09b7d5e19656f834034b171bc4c8cd258cbcad7f7ffb8934d5fa
3645fd55b8c92764181907e22fba8c4e55af5bcda1fb030cb1cfa02a3a283ac4
42a9e037df7faa5ce3262c06523129982ac77337f2384af75324e1e8902a294c
500c35cf8e2d231c5e8151d090c3d8aafb276b442ddc91dec24cc44715b3e4d7
5667d97bd3b84c1abd779edfc9593e0f8837941af9aa9ef5c9711a136da85420
5a1a2b62d56065bf4b5c08e8c8bd0bdb90f50d6552b5b8955df1aa82f1ecd720
5e3623e2ab92a23b3eb853c1da9b1b6ce4b22a7c608d3f42f72b38c91a3220dc
657b475c7fd898e000c2da73a2803ebe69e4b51f569ff705b3371c5a5605202f
6d2e67f375c0638bd38a53f89d9495feba1cb20e88d3a4ed92dd3b0a47743fe5
6e11e5de537441490eda85e5813011c587bb862859069003c6e30f8ea65e2bf9
72f1acb9e0dd790b7435f3f108e23336c23804a36cef06ba16cb768d32fcbba6
7a1df46ccca8f3c04c6a811ed718d77eba4054302570c7bba71059e9d562d0df
7d35e4715ea04cb3065c77feff47867fea87c1825ce61550b8ed4860c8aa48a5
7f6124b007c97f56551e57a9a43155d5a52df2ab485248256df0b08f817cc96a
8820066073cfbf71f70b3fcc64191aab651f718542a0582e5675a538e4427201
8a5100f5b8bbd1d332ec35c489bb8fa69230dde67db7a73e6a29a4c7bb448ae7
9421107200ff0bdb97cc027179bd3c3ca9a5448c32a7d60a38e080a35c7f8ca2
```

*See JSON for more IOCs

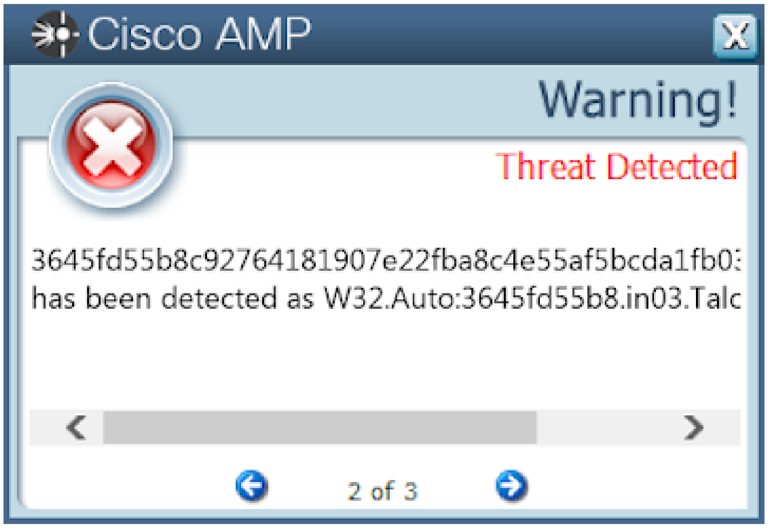
Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	

Product	Protection
Email Security	
Network Security	N/A
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	N/A
WSA	N/A

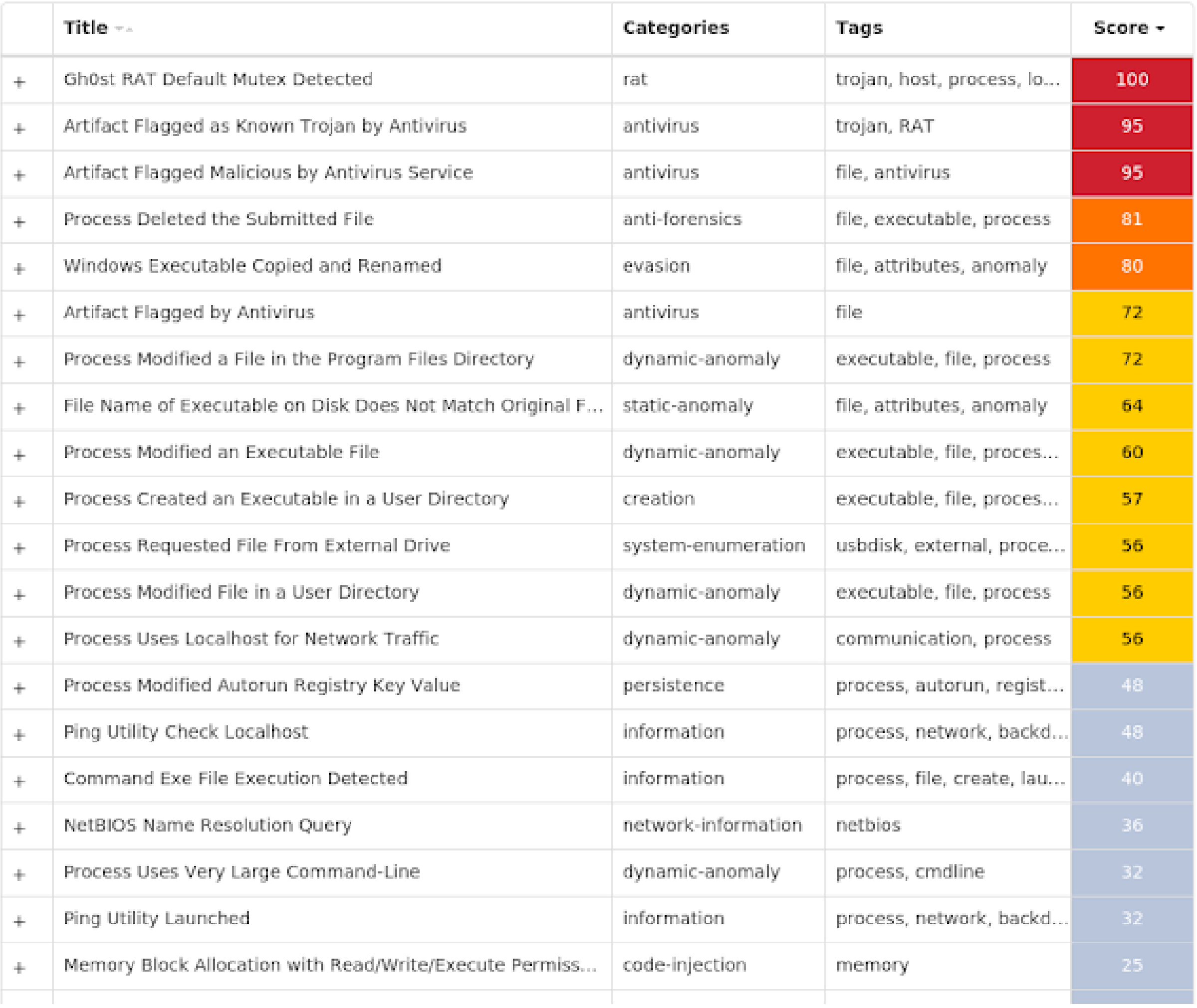
Screenshots of Detection

Secure Endpoint



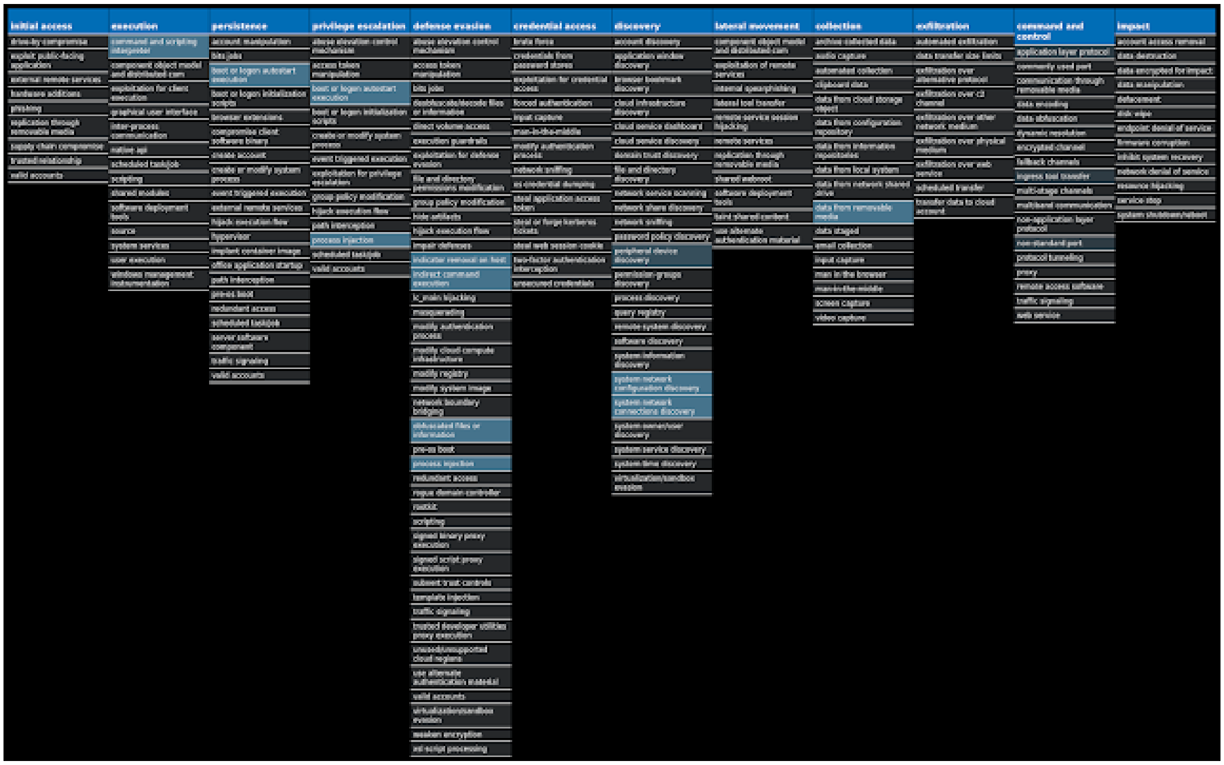
3645fd55b8c92764181907e22fba8c4e55af5bcda1fb0
has been detected as W32.Auto:3645fd55b8.in03.Talc

Secure Malware Analytics



	Title	Categories	Tags	Score
+	Gh0st RAT Default Mutex Detected	rat	trojan, host, process, lo...	100
+	Artifact Flagged as Known Trojan by Antivirus	antivirus	trojan, RAT	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Process Deleted the Submitted File	anti-forensics	file, executable, process	81
+	Windows Executable Copied and Renamed	evasion	file, attributes, anomaly	80
+	Artifact Flagged by Antivirus	antivirus	file	72
+	Process Modified a File in the Program Files Directory	dynamic-anomaly	executable, file, process	72
+	File Name of Executable on Disk Does Not Match Original F...	static-anomaly	file, attributes, anomaly	64
+	Process Modified an Executable File	dynamic-anomaly	executable, file, proces...	60
+	Process Created an Executable in a User Directory	creation	executable, file, proces...	57
+	Process Requested File From External Drive	system-enumeration	usbdisk, external, proce...	56
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56
+	Process Uses Localhost for Network Traffic	dynamic-anomaly	communication, process	56
+	Process Modified Autorun Registry Key Value	persistence	process, autorun, regist...	48
+	Ping Utility Check Localhost	information	process, network, backd...	48
+	Command Exe File Execution Detected	information	process, file, create, lau...	40
+	NetBIOS Name Resolution Query	network-information	netbios	36
+	Process Uses Very Large Command-Line	dynamic-anomaly	process, cmdline	32
+	Ping Utility Launched	information	process, network, backd...	32
+	Memory Block Allocation with Read/Write/Execute Permiss...	code-injection	memory	25

MITRE ATT&CK



initial access
- drive-by compromise
- exploit public-facing application
- external remote services
- hardware additions
- phishing
- replication through removable media
- supply chain compromise
- trusted relationship
- valid accounts

execution
- command and scripting interpreter
- component object model and distributed com
- exploitation for client execution
- graphical user interface
- inter-process communication
- native api
- scheduled task/job
- scripting
- shared modules
- software deployment tools
- source
- system services
- user execution
- windows management instrumentation

persistence
- account manipulation
- bits jobs
- boot or logon autostart execution
- boot or logon initialization scripts
- browser extensions
- compromise client software binary
- create account
- create or modify system process
- event triggered execution
- external remote services
- hijack execution flow
- hypervisor
- implant container image
- office application startup
- path interception
- pre-os boot
- redundant access
- scheduled task/job
- server software component
- traffic signaling
- valid accounts

privilege escalation
- abuse elevation control mechanism
- access token manipulation
- boot or logon autostart execution
- boot or logon initialization scripts
- create or modify system process
- event triggered execution
- exploitation for privilege escalation
- group policy modification
- hijack execution flow
- path interception
- process injection
- scheduled task/job
- valid accounts

defense evasion
- abuse elevation control mechanism
- access token manipulation
- bits jobs
- deobfuscate/decode files or information
- direct volume access
- execution guardrails
- exploitation for defense evasion
- file and directory permissions modification
- group policy modification
- hide artifacts
- hijack execution flow
- impair defenses
- indicator removal on host
- indirect command execution
- lc_main hijacking
- masquerading
- modify authentication process
- modify cloud compute infrastructure
- modify registry
- modify system image
- network boundary bridging
- obfuscated files or information
- pre-os boot
- process injection
- redundant access
- rogue domain controller
- rootkit
- scripting
- signed binary proxy execution
- signed script proxy execution
- subvert trust controls
- template injection
- traffic signaling
- trusted developer utilities proxy execution
- unused/unsupported cloud regions
- use alternate authentication material
- valid accounts
- virtualization/sandbox evasion
- weaken encryption
- xsl script processing

credential access
- brute force
- credentials from password stores
- exploitation for credential access
- forced authentication
- input capture
- man-in-the-middle
- modify authentication process
- network sniffing
- os credential dumping
- steal application access token
- steal or forge kerberos tickets
- steal web session cookie
- two-factor authentication interception
- unsecured credentials

discovery
- account discovery
- application window discovery
- browser bookmark discovery
- cloud infrastructure discovery
- cloud service dashboard
- cloud service discovery
- domain trust discovery
- file and directory discovery
- network service scanning
- network share discovery
- network sniffing
- password policy discovery
- peripheral device discovery
- permission groups discovery
- process discovery
- query registry
- remote system discovery
- software discovery
- system information discovery
- system network configuration discovery
- system network connections discovery
- system owner/user discovery
- system service discovery
- system time discovery
- virtualization/sandbox evasion

lateral movement
- component object model and distributed com
- exploitation of remote services
- internal spearphishing
- lateral tool transfer
- remote service session hijacking
- remote services
- replication through removable media
- shared webroot
- software deployment tools
- taint shared content
- use alternate authentication material

collection
- archive collected data
- audio capture
- automated collection
- clipboard data
- data from cloud storage object
- data from configuration repository
- data from information repositories
- data from local system
- data from network shared drive
- data from removable media
- data staged
- email collection
- input capture
- man in the browser
- man-in-the-middle
- screen capture
- video capture

exfiltration
- automated exfiltration
- data transfer size limits
- exfiltration over alternative protocol
- exfiltration over c2 channel
- exfiltration over other network medium
- exfiltration over physical medium
- exfiltration over web service
- scheduled transfer
- transfer data to cloud account

command and control
- application layer protocol
- commonly used port
- communication through removable media
- data encoding
- data obfuscation
- dynamic resolution
- encrypted channel
- fallback channels
- ingress tool transfer
- multi-stage channels
- multiband communication
- non-application layer protocol
- non-standard port
- protocol tunneling
- proxy
- remote access software
- traffic signaling
- web service

impact
- account access removal
- data destruction
- data encrypted for impact
- data manipulation
- defacement
- disk wipe
- endpoint denial of service
- firmware corruption
- inhibit system recovery
- network denial of service
- resource hijacking
- service stop
- system shutdown/reboot

Win.Malware.Zbot-9938525-0

Indicators of Compromise

IOCs collected from dynamic analysis of 15 samples

Registry Keys	Occurrences
`<HKCR>\LOCAL SETTINGS\SOFTWARE\MICROSOFT\WINDOWS\SHELL\BAGS\159`	11

`<HKCU>\SOFTWARE\PWRKXXZKWU`
`Value Name: License`
	5

`<HKLM>\SOFTWARE\WOW6432NODE\PWRKXXZKWU`
`Value Name: License`
	5

`<HKLM>\SOFTWARE\WOW6432NODE\PWRKXXZKWU`	5
`<HKCU>\SOFTWARE\PWRKXXZKWU`	5
`<HKCU>\SOFTWARE\WINRAR`	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003E9`
`Value Name: F`
	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000001F5`
`Value Name: F`
	1

`<HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003EC`
`Value Name: F`
	1

`<HKCU>\SOFTWARE\WINRAR`
`Value Name: HWID`
	1

Mutexes	Occurrences
`85485515`	11
`Global\8e4d9ae1-86e8-11ec-b5f8-00501e3ae7b6`	1
`Global\844108c1-86e8-11ec-b5f8-00501e3ae7b6`	1
`Global\7ad43141-86e8-11ec-b5f8-00501e3ae7b6`	1
`Global\7e601721-86e8-11ec-b5f8-00501e3ae7b6`	1

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
`104[.]208[.]16[.]94`	3
`20[.]189[.]173[.]22`	2
`20[.]189[.]173[.]20`	2

IP Addresses contacted by malware. Does not indicate maliciousness	Occurrences
46[.]165[.]243[.]51	1
50[.]7[.]252[.]125	1
95[.]211[.]222[.]156	1
52[.]182[.]143[.]212	1
52[.]168[.]117[.]173	1
62[.]76[.]185[.]233	1
62[.]76[.]178[.]192	1
62[.]76[.]188[.]38	1
62[.]76[.]47[.]5	1

Domain Names contacted by malware. Does not indicate maliciousness	Occurrences
computer[.]example[.]org	15
wpad[.]example[.]org	15
clientconfig[.]passport[.]net	9
vmss-prod-weu[.]westeurope[.]cloudapp[.]azure[.]com	7
net-forwarding[.]com	5
vmss-prod-eus[.]eastus[.]cloudapp[.]azure[.]com	5
t14qb[.]mrbasic[.]com	4
discover-lang[.]com	3
vmss-prod-seas[.]southeastasia[.]cloudapp[.]azure[.]com	3
onedsblobprdcus16[.]centralus[.]cloudapp[.]azure[.]com	3
geio-pricing[.]com	2
onedsblobprdwus17[.]westus[.]cloudapp[.]azure[.]com	2
onedsblobprdwus15[.]westus[.]cloudapp[.]azure[.]com	2
windowsupdate[.]s[.]llnwi[.]net	1
onedsblobprdcus15[.]centralus[.]cloudapp[.]azure[.]com	1
onedsblobprdeus16[.]eastus[.]cloudapp[.]azure[.]com	1

Files and or directories created	Occurrences
`%TEMP%\st1m.bat`	4
`\Users\user\AppData\Local\Temp\st1m.bat`	2
`%TEMP%\-1399634684.bat`	1
`\Users\user\AppData\Local\Temp\tmp72f12c56.bat`	1
`\Users\user\AppData\Local\Temp\tmp9263c976.bat`	1
`\Users\user\AppData\Local\Temp\tmp83b27453.bat`	1
`\Users\user\AppData\Local\Temp\tmp791b5ee5.bat`	1

File Hashes

```
 0359b8913493b41b7c0209a133d3492c6893c420ecd97af7a9a997fa1efbf7ad
1023e8030a884209b44b046ee3fd47996c6e3a356a0022b2184335623192d0e8
3465f83eb61a1c4b32242e1ee52deddb8e507f155f8ac9b476b54de8a0ab19be
41085ad88d42f4fff9cc0375a934b775607821538381 80aa84725750081db662
48dd72cfc8802b263921c471e1bc87d36667996971cc522d2904950d4e3708cd
4fc174ba2eb3848639ead3bbc2b88136b53e3a04af1bcd5dd1616afb18715af2
58dc89acadbd0377dbdf5fb442238c387ddff2033ac3d9b00031a32931307b39
7112aa176e6098a97c984d8cff643733655467a9deedf6df3850833412032d64
89869a26121998e8c994ccf0725a3fadcf803ff8922219519c663db67b42a1e2
8b213a839cfa60bbb405f91504b86cb305d5ad19374895f3c37700ca6f943e32
c5ebaa812220fbbb09996ef31827546c128873b891968b96f12d4e827ab23dd1
d2c296a48c4dcb1f1c6254c55e6d97702d570119cda1d5bf509898e253662a81
db341e594d1ca60c33fe7688f3422053df2be10a8a9de4a00227147ad23559e3
ed601fa3467259be08db4756f41979d6528b7f8a630bb2a74b6240da0c5b7ef0
f4c630b94e4f13cc3a53f86f2b7c076e5096e83b0640c237644101b8ca3d9607
```

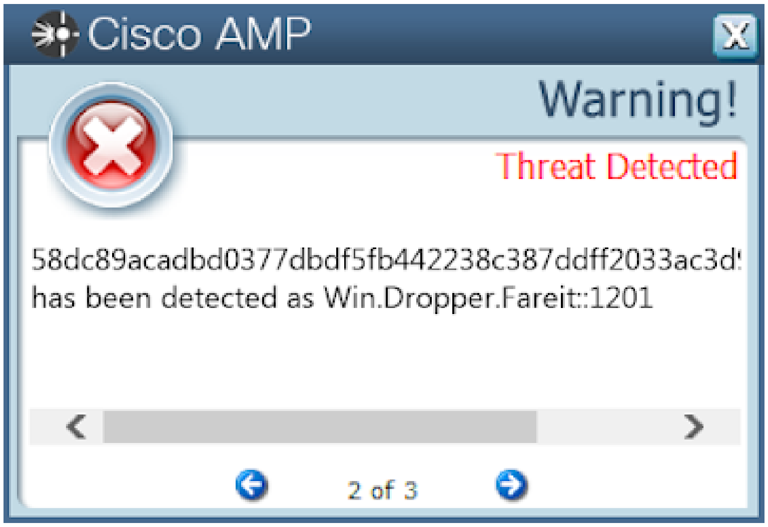
Coverage

Product	Protection
Secure Endpoint	
Cloudlock	N/A
CWS	

Product	Protection
Email Security	
Network Security	
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Secure Malware Analytics	
Umbrella	N/A
WSA	N/A

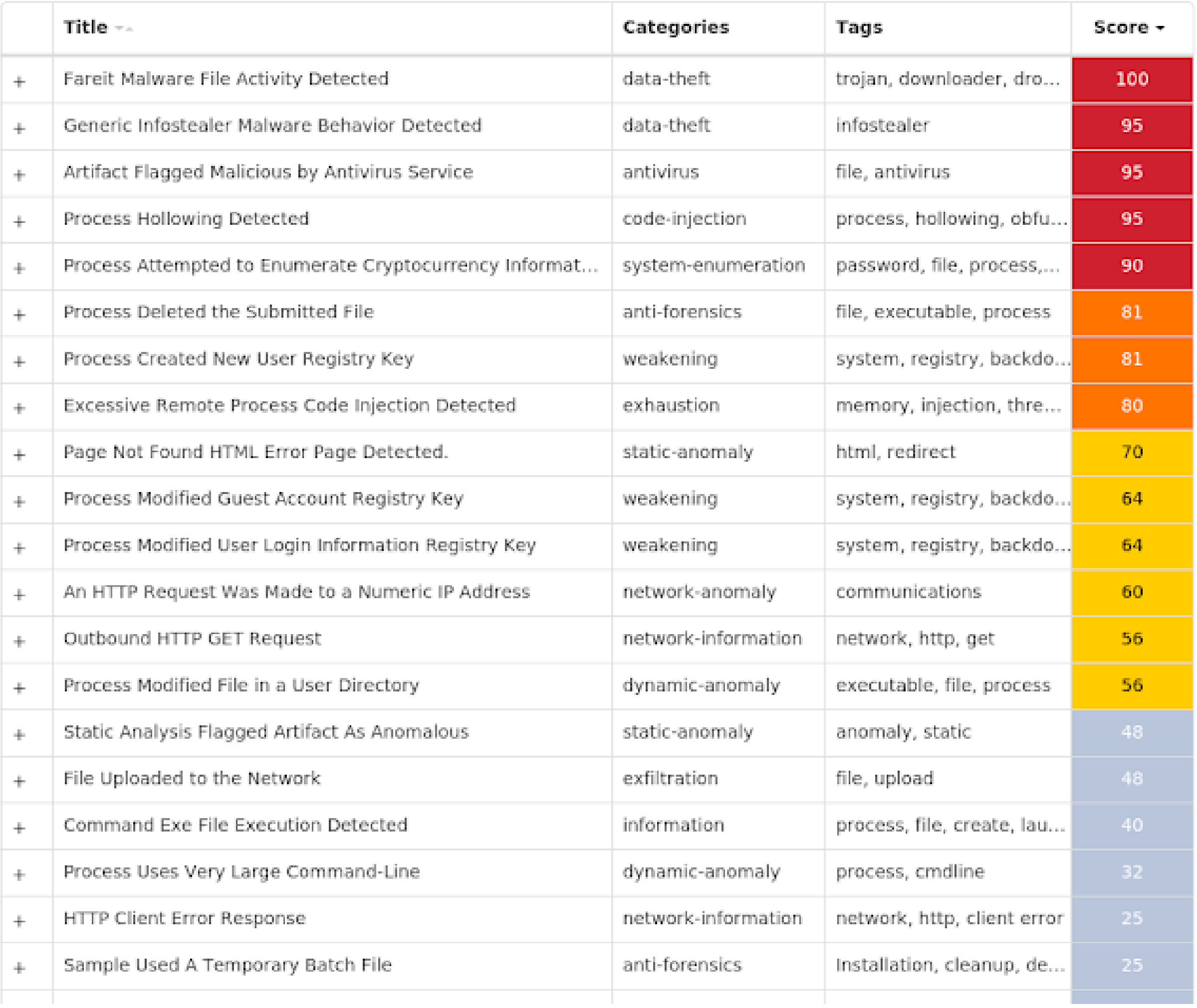
Screenshots of Detection

Secure Endpoint



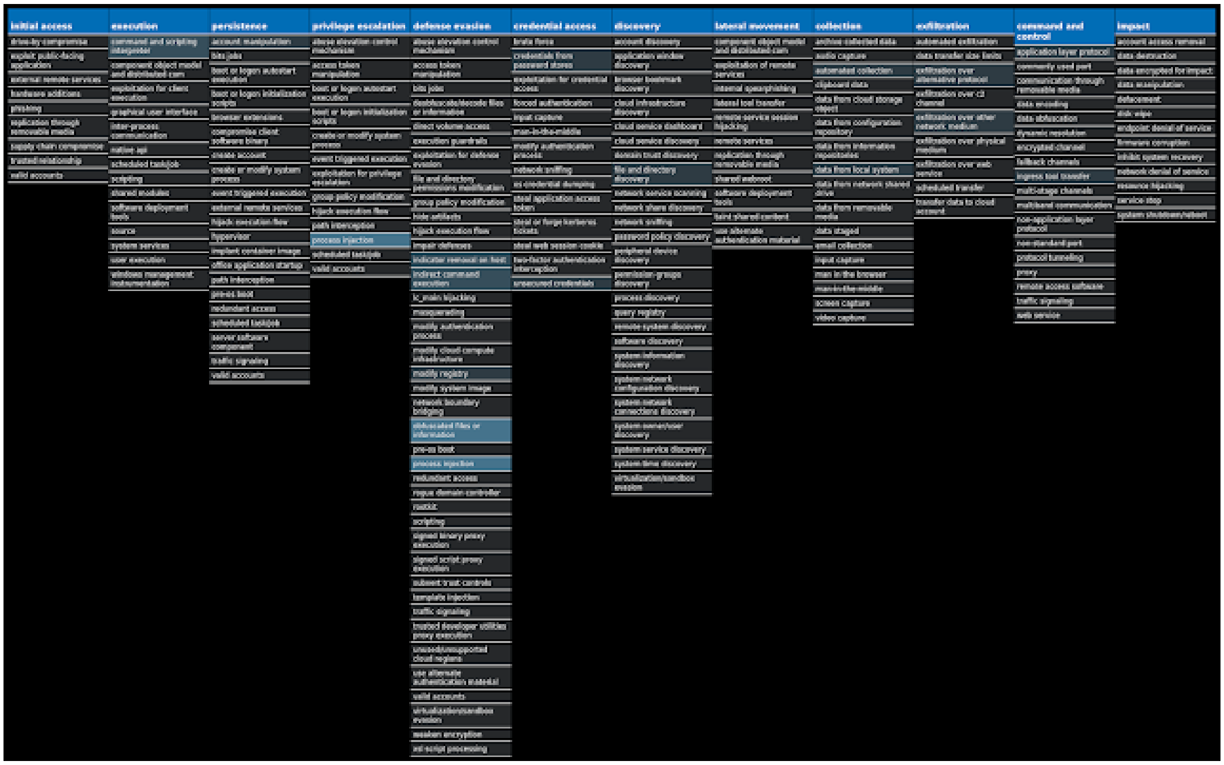
58dc89acadbd0377dbdf5fb442238c387ddff2033ac3d
has been detected as Win.Dropper.Fareit::1201

Secure Malware Analytics



	Title	Categories	Tags	Score
+	Fareit Malware File Activity Detected	data-theft	trojan, downloader, dro...	100
+	Generic Infostealer Malware Behavior Detected	data-theft	infostealer	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	95
+	Process Hollowing Detected	code-injection	process, hollowing, obfu...	95
+	Process Attempted to Enumerate Cryptocurrency Informat...	system-enumeration	password, file, process,...	90
+	Process Deleted the Submitted File	anti-forensics	file, executable, process	81
+	Process Created New User Registry Key	weakening	system, registry, backdo...	81
+	Excessive Remote Process Code Injection Detected	exhaustion	memory, injection, thre...	80
+	Page Not Found HTML Error Page Detected.	static-anomaly	html, redirect	70
+	Process Modified Guest Account Registry Key	weakening	system, registry, backdo...	64
+	Process Modified User Login Information Registry Key	weakening	system, registry, backdo...	64
+	An HTTP Request Was Made to a Numeric IP Address	network-anomaly	communications	60
+	Outbound HTTP GET Request	network-information	network, http, get	56
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	56
+	Static Analysis Flagged Artifact As Anomalous	static-anomaly	anomaly, static	48
+	File Uploaded to the Network	exfiltration	file, upload	48
+	Command Exe File Execution Detected	information	process, file, create, lau...	40
+	Process Uses Very Large Command-Line	dynamic-anomaly	process, cmdline	32
+	HTTP Client Error Response	network-information	network, http, client error	25
+	Sample Used A Temporary Batch File	anti-forensics	Installation, cleanup, de...	25

MITRE ATT&CK



initial access	execution	persistence	privilege escalation	defense evasion	credential access	discovery	lateral movement	collection	exfiltration	command and control	impact
drive-by compromise	command and scripting interpreter	account manipulation	abuse elevation control mechanism	abuse elevation control mechanism	brute force	account discovery	component object model and distributed com	archive collected data	automated exfiltration	application layer protocol	account access removal
exploit public-facing application	component object model and distributed com	bits jobs	access token manipulation	access token manipulation	credentials from password stores	application window discovery	exploitation of remote services	audio capture	data transfer size limits	commonly used port	data destruction
external remote services	exploitation for client execution	boot or logon autostart execution	boot or logon autostart execution	bits jobs	exploitation for credential access	browser bookmark discovery	internal spearphishing	automated collection	exfiltration over alternative protocol	communication through removable media	data encrypted for impact
hardware additions	graphical user interface	boot or logon initialization scripts	boot or logon initialization scripts	deobfuscate/decode files or information	forced authentication	cloud infrastructure discovery	lateral tool transfer	clipboard data	exfiltration over c2 channel	data encoding	data manipulation
phishing	inter-process communication	browser extensions	create or modify system process	direct volume access	input capture	cloud service dashboard	remote service session hijacking	data from cloud storage object	exfiltration over other network medium	data obfuscation	defacement
replication through removable media	native api	compromise client software binary	event triggered execution	execution guardrails	man-in-the-middle	cloud service discovery	remote services	data from configuration repository	exfiltration over physical medium	dynamic resolution	disk wipe
supply chain compromise	scheduled task/job	create account	exploitation for privilege escalation	exploitation for defense evasion	modify authentication process	domain trust discovery	replication through removable media	data from information repositories	exfiltration over web service	encrypted channel	endpoint denial of service
trusted relationship	scripting	create or modify system process	group policy modification	file and directory permissions modification	network sniffing	file and directory discovery	shared webroot	data from local system	scheduled transfer	fallback channels	firmware corruption
valid accounts	shared modules	event triggered execution	hijack execution flow	group policy modification	os credential dumping	network service scanning	software deployment tools	data from network shared drive	transfer data to cloud account	ingress tool transfer	inhibit system recovery
	software deployment tools	external remote services	path interception	hide artifacts	steal application access token	network share discovery	taint shared content	data from removable media		multi-stage channels	network denial of service
	source	hijack execution flow	process injection	hijack execution flow	steal or forge kerberos tickets	network sniffing	use alternate authentication material	data staged		multiband communication	resource hijacking
	system services	hypervisor	scheduled task/job	impair defenses	steal web session cookie	password policy discovery		email collection		non-application layer protocol	service stop
	user execution	implant container image	valid accounts	indicator removal on host	two-factor authentication interception	peripheral device discovery		input capture		non-standard port	system shutdown/reboot
	windows management instrumentation	office application startup		indirect command execution	unsecured credentials	permission groups discovery		man in the browser		protocol tunneling	
		path interception		lc_main hijacking		process discovery		man-in-the-middle		proxy	
		pre-os boot		masquerading		query registry		screen capture		remote access software	
		redundant access		modify authentication process		remote system discovery		video capture		traffic signaling	
		scheduled task/job		modify cloud compute infrastructure		software discovery				web service	
		server software component		modify registry		system information discovery					
		traffic signaling		modify system image		system network configuration discovery					
		valid accounts		network boundary bridging		system network connections discovery					
				obfuscated files or information		system owner/user discovery					
				pre-os boot		system service discovery					
				process injection		system time discovery					
				redundant access		virtualization/sandbox evasion					
				rogue domain controller							
				rootkit							
				scripting							
				signed binary proxy execution							
				signed script proxy execution							
				subvert trust controls							
				template injection							
				traffic signaling							
				trusted developer utilities proxy execution							
				unused/unsupported cloud regions							
				use alternate authentication material							
				valid accounts							
				virtualization/sandbox evasion							
				weaken encryption							
				xsl script processing							