MVISION Insights: Vicious Panda: The COVID-19 campaign

Technical Articles ID: KB92636
Last Modified: 8/28/2020

Environment

IMPORTANT: This Knowledge Base article discusses a specific threat that is being automatically tracked by MVISION Insights technology. The co
for use by MVISION Insights users, but is provided for general knowledge to all customers. Contact us for more information about MVISION Insig

Summary

Description of Campaign
Vicious Panda targeted the Mongolian public sector, using RTF attachments disguised as documents sent from the Mongolian Ministry of Foreign
The threat actor behind the attack used the COVID-19 pandemic as a lure and infected victims with a remote access trojan. This trojan can exfiltra
and delete files and folders. The Royal Road RTF Weaponizer tool was used to create the malicious documents. These documents contained em
that exploited the Equation Editor flaws in Microsoft Word. Persistence, defense evasion, and execution were achieved using rundll32.exe, the W
folder, and obfuscation.

How to use this article:

1. If a Threat Hunting table has been created, use the rules contained to search for malware related to this campaign.
2. Review the product detection table and confirm that your environment is at least on the specified content version.
   To download the latest content versions, go to the Security Updates page.
3. Scroll down and review the "Product Countermeasures" section of this article. Consider implementing them if they are not already in place.
4. Review KB91836 - Countermeasures for entry vector threats.
5. Review KB87843 - Dynamic Application Containment rules and best practices.
6. Review KB82925 - Identify what rule corresponds to an Adaptive Threat Protection and Threat Intelligence Exchange event.

Campaign IOC

Type	Value
Ip-dst	95.179.242.6
Ip-dst	95.179.242.27
Ip-dst	199.247.25.102
Ip-dst	95.179.210.61
Ip-dst	95.179.156.97
Host name	dw.adyboh.com
Host name	wy.adyboh.com
Host name	feb.kkooppt.com
Host name	compdate.my03.com
Host name	jocoly.esvnpe.com
Host name	bmy.hqoohoa.com
Host name	bur.vueleslie.com
Host name	wind.windmilldrops.com
SHA256	2A42F500D019A64970E1C63D48EEFA27727F80FE0A5B13625E0E72A6EC98B968
SHA256	C51658ED15A09E9D8759C9FBF24665D6F0101A19A2A147E06D58571D05266D0A
SHA256	5187C9A84F5E69BA4B08538C3F5E7432E7B45AC84DEC456EA07325FF5E94319A
SHA256	E9766B6129D9E1D59B92C4313D704E8CDC1A9B38905021EFCAC334CDD451E617
SHA256	C322D10EF3AA532D4625F1C2589EAE0F723208DB37A7C7E81E4F07E36C3A537E
SHA256	1C98A36229B878BAE15985C1AE0FF96E42F36FA06359323F205E18431D780A3B
SHA256	80392BEBE21245128E3353EEC7F499BDC5550E67501ECEEBF21985644D146768

SHA256	9E12094C15F59D68AD17E5ED42EBB85E5B41F4258823B7B5C7472BDFF21E6CEE
SHA256	679A8519587909F655BACEA438168CBB4C03434AEDE9913D9A3A637C55A0EAE7
SHA256	DDB24E0A38BA9194FE299E351E54FACB2CCA9E6011DB2F5242210284DF91F900
SHA256	215C72DF44FE8E564D24F4D9930C27409E7F76E2045C67940CDCECDBDBD3B04F
SHA256	3C756D761E89A0EA1216E2B7E57250AC76A80D5FE4F072E3B4B372E609ECE74E
SHA256	238FA49ED966CB746BFFEE3E7CA95B4A9DB3BB0F897B8FD8AE560F9080749A82
SHA256	D7F15F750CCEEB9E28E412F278949F183F98AEB65FE99731B2340C8F1C008465
SHA256	E9621840E1BFAF16EAEE37E2D1E9D1F0032158A09E638EAEBFF6D8626D47C95A
SHA256	69724A9BD8033BD16647BC9AEA41D5FE9FB7F7A83C5D6FBFB439D21B7B9F53F6
SHA256	A5AB358D5AB14B81DF2D37AEDF52716B5020AB45DA472DEDC8B8330D129D70BF

Minimum Content Versions:

Content Type	Version
V2 DAT (VirusScan Enterprise)	9568
V3 DAT (Endpoint Security)	4019

Detection Summary

IOC	Scanner	Detection
2A42F500D019A64970E1C63D48EEFA27727F80FE0A5B13625E0E72A6EC98B968	AVEngine V2	Generic trojan.jw
AVEngine V3	Generic trojan.jw	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
C51658ED15A09E9D8759C9FBF24665D6F0101A19A2A147E06D58571D05266D0A	AVEngine V2	RTFObfustream.a
AVEngine V3	RTFObfustream.a!0D28743F8CBA	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
5187C9A84F5E69BA4B08538C3F5E7432E7B45AC84DEC456EA07325FF5E94319A	AVEngine V2	RTFObfustream.a
AVEngine V3	RTFObfustream.a!23DAD71A3A55	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection

E9766B6129D9E1D59B92C4313D704E8CDC1A9B38905021EFCAC334CDD451E617	AVEngine V2	Generic trojan.jv
AVEngine V3	Generic trojan.jw	
JTI (ATP Rules)	JTI/Suspect.196612!3009db32ca88	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
C322D10EF3AA532D4625F1C2589EAE0F723208DB37A7C7E81E4F07E36C3A537E	AVEngine V2	Generic trojan.jw
AVEngine V3	Generic trojan.jw	
JTI (ATP Rules)	JTI/Suspect.196612!4a13d87f18af	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
1C98A36229B878BAE15985C1AE0FF96E42F36FA06359323F205E18431D780A3B	AVEngine V2	Trojan-FSAN!4F0428160
AVEngine V3	Trojan-FSAN!4F0428160556	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
80392BEBE21245128E3353EEC7F499BDC5550E67501ECEEBF21985644D146768	AVEngine V2	Trojan-FSAO!70AB82E
AVEngine V3	Trojan-FSAO!70AB82BFDC09	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
9E12094C15F59D68AD17E5ED42EBB85E5B41F4258823B7B5C7472BDFF21E6CEE	AVEngine V2	Generic trojan.jw
AVEngine V3	Generic trojan.jw	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
679A8519587909F655BACEA438168CBB4C03434AEDE9913D9A3A637C55A0EAE7	AVEngine V2	Trojan-FSAO!76ACD
AVEngine V3	Trojan-FSAO!76ACDA3C0DC6	
JTI (ATP Rules)	-	

RP Static	-
RP Dynamic	-

IOC	Scanner	Detection
DDB24E0A38BA9194FE299E351E54FACB2CCA9E6011DB2F5242210284DF91F900	AVEngine V2	RTFObfustream.a
AVEngine V3	RTFObfustream.a!7C986CFDF3FA	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
215C72DF44FE8E564D24F4D9930C27409E7F76E2045C67940CDCECDBDBD3B04F	AVEngine V2	Trojan-FSAO!8B
AVEngine V3	Trojan-FSAO!8B75BB1D547C	
JTI (ATP Rules)	JTI/Suspect.196612!8b75bb1d547c	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
3C756D761E89A0EA1216E2B7E57250AC76A80D5FE4F072E3B4B372E609ECE74E	AVEngine V2	Generic trojan.jw
AVEngine V3	Generic trojan.jw	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
238FA49ED966CB746BFFEE3E7CA95B4A9DB3BB0F897B8FD8AE560F9080749A82	AVEngine V2	Trojan-FSAO!A4F695
AVEngine V3	Trojan-FSAO!A4F695D4F912	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
D7F15F750CCEEB9E28E412F278949F183F98AEB65FE99731B2340C8F1C008465	AVEngine V2	RTFObfustream.a
AVEngine V3	RTFObfustream.a!A6CCE77325E4	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
E9621840E1BFAF16EAEE37E2D1E9D1F0032158A09E638EAEBFF6D8626D47C95A	AVEngine V2	Trojan-FSAN!C91268
AVEngine V3	Trojan-FSAN!C91268989EDE	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
69724A9BD8033BD16647BC9AEA41D5FE9FB7F7A83C5D6FBFB439D21B7B9F53F6	AVEngine V2	Trojan-FSAO!D744B1
AVEngine V3	Trojan-FSAO!D744B176835C	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
A5AB358D5AB14B81DF2D37AEDF52716B5020AB45DA472DEDC8B8330D129D70BF	AVEngine V2	Trojan-FSAN!F820FE
AVEngine V3	Trojan-FSAN!F820FE427295	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

Minimum set of Manual Rules to improve protection to block this campaign

IMPORTANT: Always follow best practices when you enable new rules and signatures.

When you implement new rules or signatures, always set them to **Report** mode first and check the alerts generated. Resolve any issues that aris rules to **Block**. This step mitigates against triggering false positives and allows you to refine your configuration.

For more information, see KB87843 - List of and best practices for Endpoint Security Dynamic Application Containment rules.

Endpoint Security - Advanced Threat Protection:

Rule ID: 4 Use GTI file reputation to identify trusted or malicious files

Endpoint Security - Exploit Prevention:
Rule ID: 428 Generic Buffer Overflow

Endpoint Security - Access Protection Custom Rules:

Rule: 1
Executables (Include): *
Subrules: Subrule Type: Files
Operations: Create
Targets (Include):?:\users\public\documents*.cab

Rule: 2
Executables (Include): C:\Program Files\Common Files\Microsoft Shared\EQUATION*.EXE
Subrules: Subrule Type: Files
Operations: Delete
Targets (Include): C:\Users\Administrator\AppData\Local\Temp*.t

Rule: 3
Executables (Include): eqnedt32.exe
Subrules: Subrule Type: Files
Operations: Create
Targets (Include): ?:\users*\appdata*.dll

Rule: 4
Executables (Include): winword.exe
Subrules: Subrule Type: Files
Operations: Create
Targets (Include): ?:\users*\appdata\local\temp*.t

Rule: 5
Executables (Include): eqnedt32.exe
Subrules: Subrule Type: Files
Operations: Create
Targets (Include): ?:\users*\appdata\roaming\microsoft***.wll

VirusScan Enterprise - Access Protection Custom Rules:

Rule: 1
Rule Type: File
Process to include: *
File or folder name to block: *\users\public\documents*.cab
File actions to prevent: Create

Rule: 2
Rule Type: File
Process to include: C:\Program Files\Common Files\Microsoft Shared\EQUATION*.EXE
File or folder name to block: C:\Users\Administrator\AppData\Local\Temp*.t
File actions to prevent: Delete

Rule: 3
Rule Type: File
Process to include: eqnedt32.exe
File or folder name to block: *\users*\appdata*.dll
File actions to prevent: Create

Rule: 4
Rule Type: File
Process to include: winword.exe
File or folder name to block: *\users*\appdata\local\temp*.t
File actions to prevent: Create

Rule: 5
Rule Type: File
Process to include: eqnedt32.exe
File or folder name to block: *\users*\appdata\roaming\microsoft***.wll
File actions to prevent: Create

Aggressive set of Manual Rules to improve protection to block this campaign

IMPORTANT: Always follow best practices when you enable new rules and signatures.

When you implement new rules or signatures, always set them to **Report** mode first and check the alerts generated. Resolve any issues that aris rules to **Block**. This step mitigates against triggering false positives and allows you to refine your configuration.

For more information, see KB87843 - List of and best practices for Endpoint Security Dynamic Application Containment rules.

Host Intrusion Prevention:
Rule ID: 1148 CMD Tool Access by a Network Aware Application
Rule ID: 6011 Generic Application Invocation Protection
Rule ID: 6010 Generic Application Hooking Protection
Rule ID: 1020 Windows Agent Shielding - File Access
Rule ID: 2806 Attempt to create a hardlink to a file
Rule ID: 344 New Startup Program Creation

Endpoint Security - Dynamic Application Containment:

Modifying the Services registry location