COVID-19

Threat Landscape Summary

April 2020

Cyberint

TABLE OF CONTENTS

Cyberint Copyright © All Rights Reserved 2020

OVERVIEW

Cyberint research team is actively tracking the surge in COVID-19 related attacks since January 2020.

Threat actors have been capitalizing on the global attention surrounding COVID-19 global pandemic to launch phishing campaigns designed to spread malware to unsuspected users and organizations. Cyberint research team published numerous reports and blog-posts describing those campaigns distributing various malware families.

Both eCrime and nation state threat actors are taking part in leveraging COVID-19 to launch their campaigns primarily focusing on email phishing as a primary attack vector.

Out of those malware families we have mapped their TTP's to more than 90 MITRE ATT&CK tactics and techniques. some of the most prevalent malware families used by threat actors during their campaigns include AgentTesla, AZORult, Remcos, Ryuk, CoronaVirus Ransomware, Emotet, NanoCore, AsyncRAT, LokiBot, GuLoader, and more. Additionally, some of the most targeted countries include USA, UK, Germany, Italy, South Korea, and France.

DETAILS

The first observation of a COVID-19 related phishing campaign we observed was some weeks after China's public announcement of the previously unknown COVID-19 outbreak out of the city of Wuhan, since then we observed a massive uptake in COVID-19 related attacks from both eCrime and nation-state threat actors.

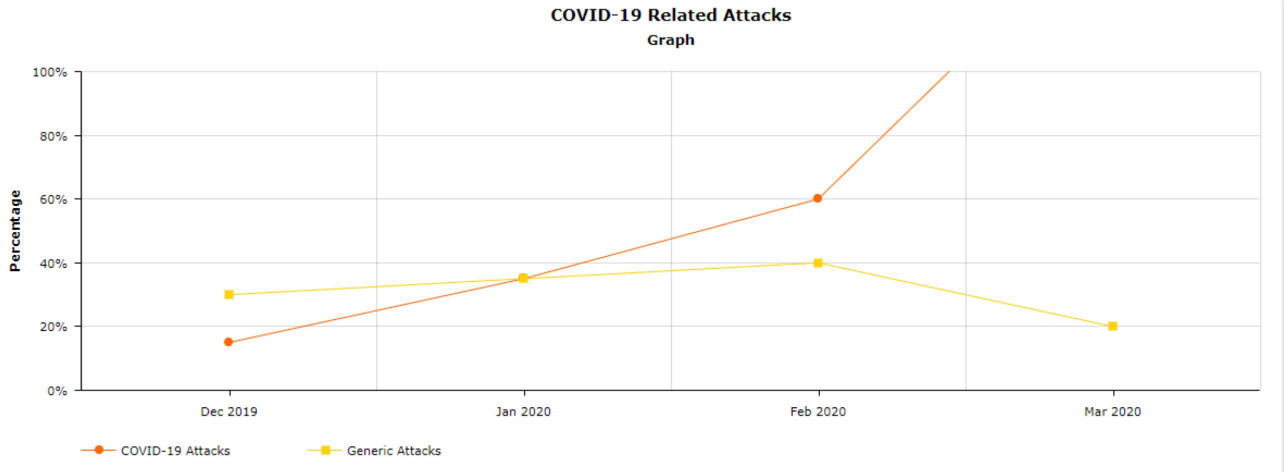


Figure 1 - COVID-19 Attacks Graph Trend

The chart above shows the increasing trend in COVID-19 related attacks observed since December 2019, and the following uptake in following months.

MOST PREVALENT MALWARE USING DURING COVID-19 RELATED ATTACKS

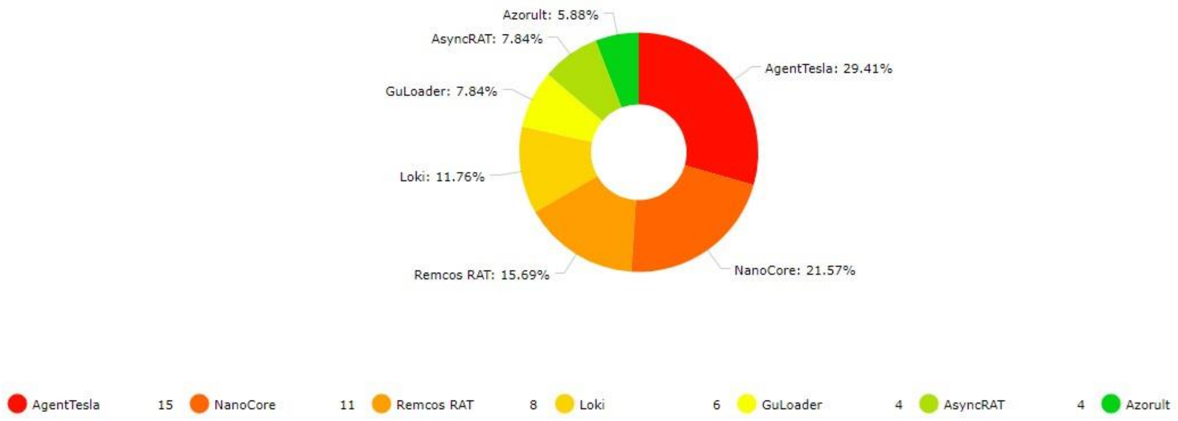
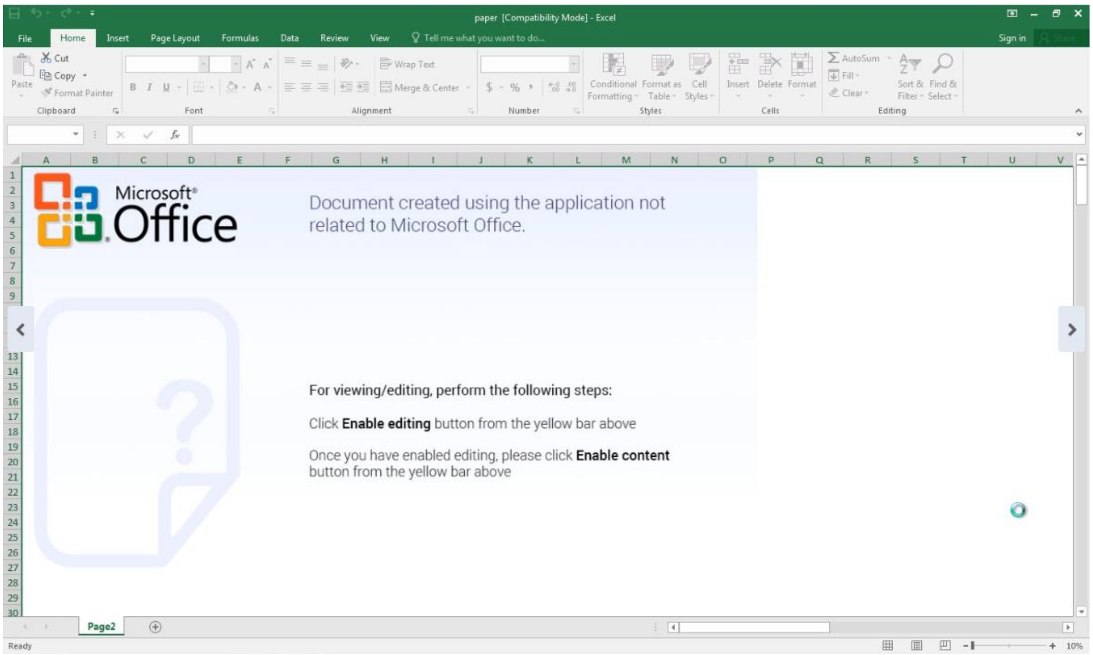


Figure 2 - Most Prevalent Malware Related to COVID-19

COVID-19 CAMPAIGNS OBSERVED DURING JANUARY 2020

During the early January 2020, we observed a phishing campaign leveraging COVID-19 macro-enabled excel attachments, the campaign is attributed to TA505 one of the most active eCrime groups today targeting primarily the financial and retail sectors.



Document created using the application not related to Microsoft Office.

For viewing/editing, perform the following steps:

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Figure 3 - malicious excel sheet sent as an attachment by TA505

The macro enabled excel sheet contains an embedded executable that is dropped to disk and loaded to memory, the embedded executable is CobaltStrike beacon DLL loader, and once loaded it enumerate running processes and beacon to its C2 in the following URL [https://[dysoool[.].com/casemd](http://dysoool.com/casemd)] this example shows how TA505 immediately shifted focus from their normal operations using generic financial lures and started to leverage COVID-19 global focus to launch their campaigns

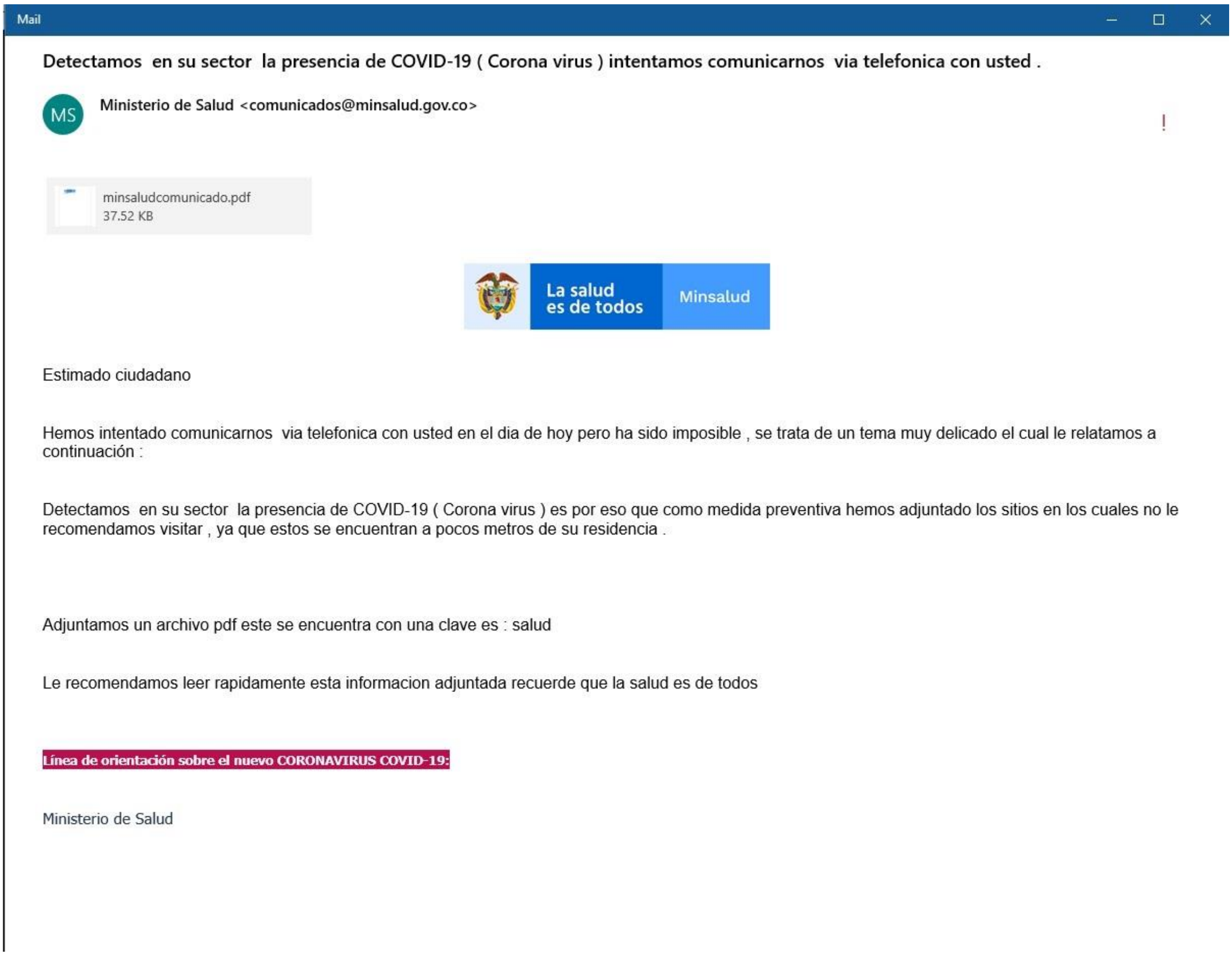
MITRE ATT&CK TECHNIQUES MAPPING

Techniques	Tactics
Spear phishing Attachment - T1193	Initial Access
Scripting - T1064	Defense Evasion, Execution
Process Discovery - T1057	Discovery
File and Directory Discovery - T1083	Discovery
Standard Application Layer Protocol - T1071	Command and Control
Standard Cryptographic Protocol - T1032	Command and Control

COVID-19 CAMPAIGNS OBSERVED DURING FEBRUARY 2020

Cyberint researchers started to see an increase in COVID-19 related campaigns during Feb 2020.

One campaign Targeting Colombia using a phishing email with a PDF containing a malicious shorten URL.



Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted .

Ministerio de Salud <comunicados@minsalud.gov.co>

minsaludcomunicado.pdf
37.52 KB

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación :

Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar , ya que estos se encuentran a pocos metros de su residencia .

Adjuntamos un archivo pdf este se encuentra con una clave es : salud

Le recomendamos leer rapidamente esta informacion adjuntada recuerde que la salud es de todos

Línea de orientación sobre el nuevo CORONAVIRUS COVID-19:

Ministerio de Salud

Figure 4 - fake Colombia Ministry of health phishing email

The text translates to the following:

Dear citizen

We have tried to communicate with you by telephone today but it has been impossible, it is a very delicate subject which we will tell you below: We detect the presence of COVID-19 (Corona virus) in your sector, which is why, as a preventive measure, we have attached the sites in which we do not recommend visiting, since they are located a few meters from your residence. We attach a pdf file this is found with a key is: health We recommend you read this attached information quickly, remember that health belongs to everyone Orientation line on the new CORONAVIRUS COVID-19: In Bogotá: +57 (1) 330 5041 Rest of the country: 018000955590

Ministry of Health

Cyberint Copyright © All Rights Reserved 2020

The email contains a PDF file with a shortened URL as seen below

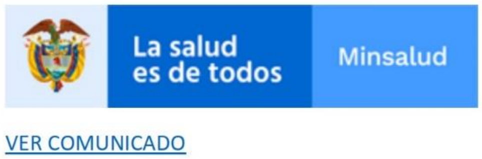


Figure 5 - Attached PDF with an embedded link

The PDF name minsaludcomunicado.pdf translated to minsaludstatement.pdf contains a link to a Shortened URL [https://acortaurl[.]com/minsaludprevencioncomunicadosoficiales_--ampquotquotpdf] once clicked the URL downloads an executable masked as PDF the executable is a variant of the known Remcos RAT used by the threat actors to steal information from infected victims.

This campaign shows how threat actors tap into the fear and uncertainty that is widespread in the public and leverage that to conduct their malicious activities.

MITRE ATT&CK TECHNIQUES MAPPING

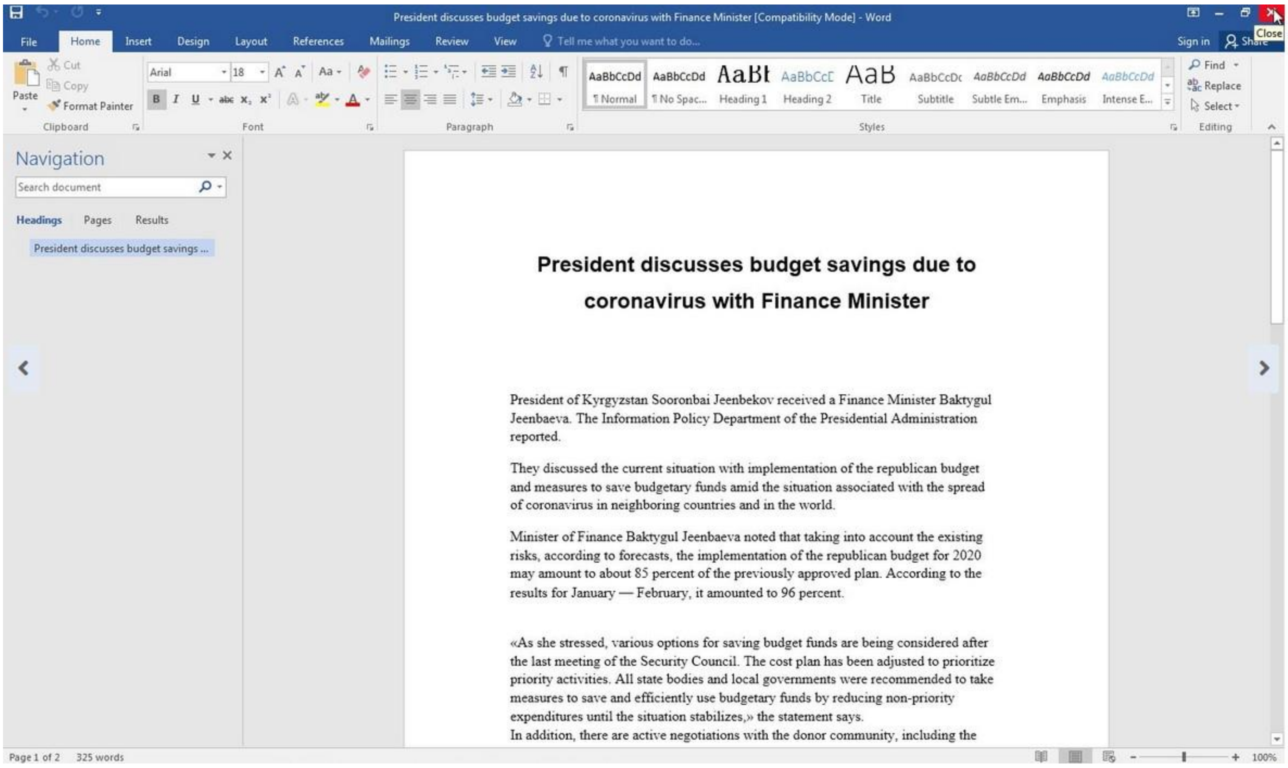
Techniques	Tactics
Hooking - T1179	Credential Access, Persistence, Privilege Escalation
Registry Run Keys / Startup Folder - T1060	Persistence
Software Packing - T1045	Defense Evasion
Hidden Window - T1143	Defense Evasion
Modify Registry - T1112	Defense Evasion
Input Capture - T1056	Collection, Credential Access
Network Share Discovery - T1135	Discovery
System Network Connections Discovery - T1049	Discovery
System Network Configuration Discovery - T1016	Discovery
Clipboard Data - T1115	Collection
Input Capture - T1056	Collection, Credential Access

COVID-19 CAMPAIGNS OBSERVED DURING MARCH 2020

During March 2020 indicates the peak of the global COVID-19 crisis, this fact also holds true to the amount of COVID-19 related malicious campaigns.

During March 2020 Cyberint researchers discovered a campaign we attribute to APT17 a Chinese state sponsored threat actor.

During The Campaign targeting Kyrgyzstan APT17 used a malicious RTF document called President discusses budget savings due to coronavirus with Finance Minister.rtf exploiting a vulnerability in Microsoft Office (CVE-2017-11882) to drop a malicious DLL to disk together with a legitimate executable used in what is known DLL Search Order Hijacking to load the DLL to memory.


President discusses budget savings due to coronavirus with Finance Minister [Compatibility Mode] - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Navigation
Search document
Headings
Pages
Results
President discusses budget savings ...
Page 1 of 2
325 words
100%

President discusses budget savings due to coronavirus with Finance Minister

President of Kyrgyzstan Sooronbai Jeenbekov received a Finance Minister Baktygul Jeenbaeva. The Information Policy Department of the Presidential Administration reported.

They discussed the current situation with implementation of the republican budget and measures to save budgetary funds amid the situation associated with the spread of coronavirus in neighboring countries and in the world.

Minister of Finance Baktygul Jeenbaeva noted that taking into account the existing risks, according to forecasts, the implementation of the republican budget for 2020 may amount to about 85 percent of the previously approved plan. According to the results for January — February, it amounted to 96 percent.

«As she stressed, various options for saving budget funds are being considered after the last meeting of the Security Council. The cost plan has been adjusted to prioritize priority activities. All state bodies and local governments were recommended to take measures to save and efficiently use budgetary funds by reducing non-priority expenditures until the situation stabilizes,» the statement says.
In addition, there are active negotiations with the donor community, including the

Figure 6 - The Content of the malicious RTF file used in the phishing campaign

Once the document is executed it exploits a vulnerability in the Microsoft Word (CVE-2017-11882) and drops two files in the %temp% directory

- LBTServ.dll - backdoor
- confax.exe - legitimate signed executable part of the logitech Bluetooth package

The exploit code loads confax.exe which then calls LBTServ.dll. LBTServ.dll is a legitimate DLL also part of the Logitech Bluetooth services, during this campaign APT17 used DLL Search Order Hijacking technique to load a malicious DLL with the same name to memory by executing confax.exe which then loads LBTServ.dll residing in the current directory.

Once in memory confax.exe beacons to its C2 servers in the following domains

- [brands[.]newst[.]dnsabr[.]com](http://brands.newst.dnsabr.com/)
- [ru[.]mst[.]dns-cloud[.]net](http://ru.mst.dns-cloud.net/)

MITRE ATT&CK TECHNIQUES MAPPING

Techniques	Tactics
Execution through Module Load - T1129	Execution
Exploitation for Client Execution - T1203	Execution
Registry Run Keys / Startup Folder - T1060	Persistence
Query Registry - T1012	Discovery
Software Packing - T1045	Defense Evasion
Virtualization/Sandbox Evasion - T1497	Defense Evasion, Discovery

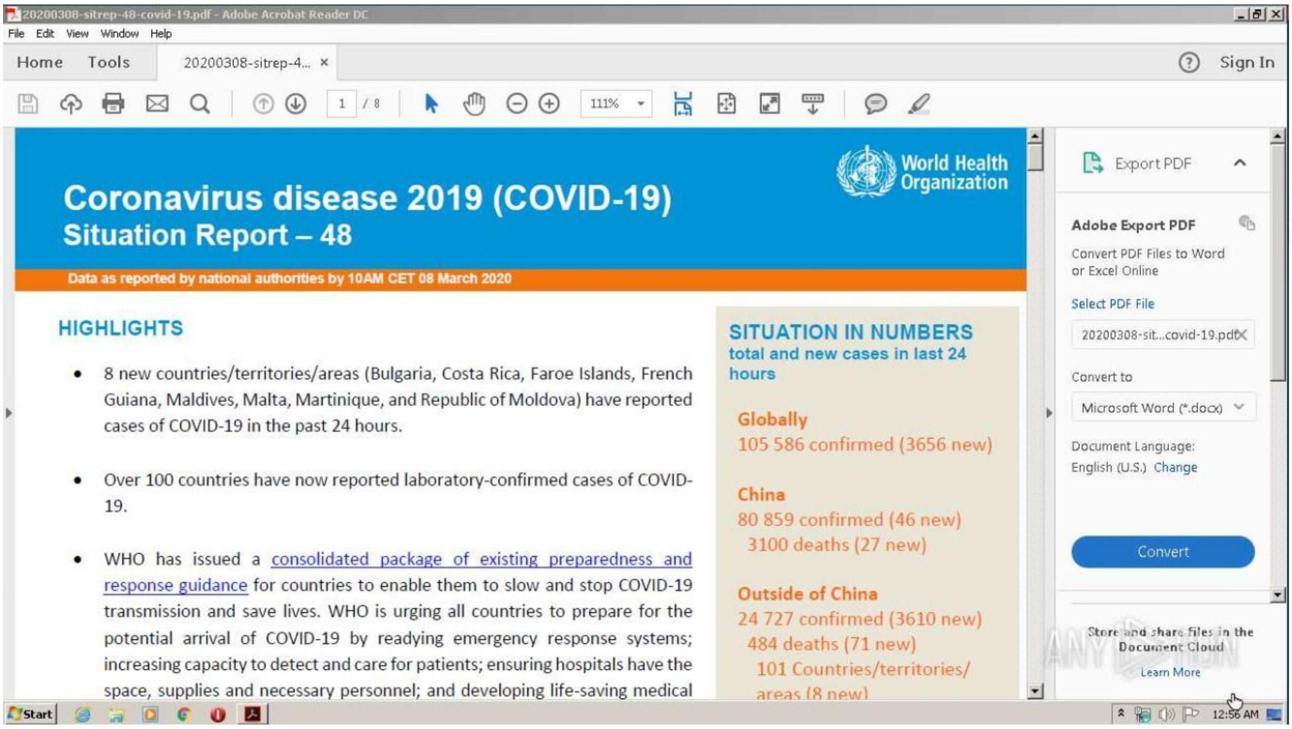
On another Campaign discovered during March 2020 attributed to Emissary Panda a Chinese sponsored nation-state threat actor, during the campaign Emissary Panda used a specially crafted link file with an embedded base64 encoded code. the link file covid.pdf.lnk masks as PDF drops several files to disk once executed.

A trusted legitimate copy of certutil.exe renamed as msoia.exe and two temp file one is a copy of the original link file and the second temp file is an XML COM script with an embedded VBS code.

The link file looks for the following string "TVNDRgAAAA" which is the base64 encoded of the MSCF file format or a CAB header (Microsoft Compressed Archive), it then executes msoia.exe to decode the CAB file and extract the files in the %TEMP% directory.

- 20200308-sitrep-48-covid-19.pdf - Decoy file
- 486AULMsOPmf6W.tmp - legitimate signed file part of the old office 2010 package
- 3UDBUTNY7YstRc.tmp - KorPlug backdoor
- 9sOXN6Ltf0afe7.js - Java Script loader
- cSi1r0uywDNvDu.tmp - KorPlug Loader

Cyberint Copyright © All Rights Reserved 2020


20200308-sitrep-48-covid-19.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools 20200308-sitrep-4... ×
Sign In
1 / 8
111%
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
20200308-sit...covid-19.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert
Store and share files in the Document Cloud
Learn More
Start
12:56 AM

World Health Organization

Coronavirus disease 2019 (COVID-19)
Situation Report – 48

Data as reported by national authorities by 10AM CET 08 March 2020

HIGHLIGHTS

- 8 new countries/territories/areas (Bulgaria, Costa Rica, Faroe Islands, French Guiana, Maldives, Malta, Martinique, and Republic of Moldova) have reported cases of COVID-19 in the past 24 hours.
- Over 100 countries have now reported laboratory-confirmed cases of COVID-19.
- WHO has issued a consolidated package of existing preparedness and response guidance for countries to enable them to slow and stop COVID-19 transmission and save lives. WHO is urging all countries to prepare for the potential arrival of COVID-19 by readying emergency response systems; increasing capacity to detect and care for patients; ensuring hospitals have the space, supplies and necessary personnel; and developing life-saving medical

SITUATION IN NUMBERS
total and new cases in last 24 hours

Globally
105 586 confirmed (3656 new)

China
80 859 confirmed (46 new)
3100 deaths (27 new)

Outside of China
24 727 confirmed (3610 new)
484 deaths (71 new)
101 Countries/territories/
areas (8 new)

Figure 7 - Legitimate PDF Decoy from the WHO (World Health Organization)

The first file is the legitimate PDF from the World Health Organization (WHO) discussing the COVID-19 global pandemic to deflect any suspicion from the victim, in the background the loader calls wscript.exe to execute the 9sOXN6Ltf0afe7.js.

The js loader creates a folder called cscript.exe under the %tmp% directory and copy script from the %systemroot%\System32 to the newly created directory and saves it as msproof.exe.

It then moves cSi1r0uywDNvDu.tmp from the %temp$ directory and saves it as WsmPty.xsl

WsmPty.xsl is an encoded COM XML with VBS code which is XOR encoded

The decoded VBS code the script generates a persistence mechanism using an lnk file called Accessories.lnk under the startup directory which launchers rundell32.exe that loads MSOSTYLE.EXE which is an old Microsoft Office WBEM component using search order hijacking it loads OINFO12.OCX which is the KorePlug DLL component. It then launches winrm.vbs a legitimate vbs script responsible for interacting with Windows Remote Management using the following command.

If Windows Remote Management is running on the local machine the command will return an XML schema of the basic machine information like the operating system version and more.

The loader then deletes C:\Users\admin\OFFICE12\Wordcnvpxy.exe and execute ping.exe with one ICMP packet to 127.0.0.1, the loader then moves 486AULMsOPmf6W.tmp and 3UDBUTNY7YstRc.tmp from the %temp% directory to OFFICE12\.

Cyberint Copyright © All Rights Reserved 2020

MSOSTYLE.EXE is a legitimate file part of the Microsoft office package, OINFO12.OCX is the KorPlug DLL.

The loader then copies 2m7EBxdH3wHwBO.tmp and MiZl5xsDRylf0W.tmp.The loader then sets a persistence mechanism by dropping a lnk file called Accessories.lnk under the Startup directory that points to MSOSTYLE.EXE, the loader then launches the decoy PDF.

The Korplug payload executes on a system reboots and the user logins to the system by running the Acceptable.lnk described earlier, KorePlug then communicated with his C2 hxxp://motivation[.]neighboring[.]site/01/index.php which was down at the time of analysis.

MITRE ATT&CK TECHNIQUES MAPPING

Techniques	Tactics
T1059 - Command-Line Interface	Execution
T1106 - Execution through API	Execution
T1129 - Execution through Module Load	Execution
T1064 - Scripting	Defense Evasion, Execution
T1060 - Registry Run Keys / Startup Folder	Persistence
T1012 - Query Registry	Discovery

DEFENDING COVID-19 RELATED ATTACKS

Cyberint research team estimate with high certainty that COVID-19 related attacks conducted by both eCrime and nation state actors will continue as long as the COVID-19 global pandemic continues to cause uncertainty.

While most attacks leverage various phishing campaigns with malicious attachments or links threat actors will also look into other attack vectors such as exposed RDP interfaces or water hole attacks to gain access to their victims.

Due to the increased volume of COVID-19 related attacks. we believe this elevated risk posed to organizations we provide recommendations to prevent falling victim to such attacks.

- Watch out for unrecognized COVID-19 related emails or text messages impersonating legitimate government or health organizations attempting to lure the recipients to take immediate action.
- Do not open any email attachments or clicking any links especially when the sender requests the receiver to visit a suspicious-looking site requesting personally identifiable information or other sensitive and confidential information
- Make sure your Operating System and applications are updated to their latest versions as soon as they become available
- Use an antivirus and firewall solution and make sure they are always up-to-date with the latest patches and antivirus signatures.
- Organizations should employ frequent user security awareness training to ensure their employees know how to pay attention and promptly report suspicious activity
- Consider staying updated to the latest developments around related COVID-19 threats by subscribing to our weekly Cyber feed newsletter

Cyberint Copyright © All Rights Reserved 2020

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City

Cyberint Copyright © All Rights Reserved 2020