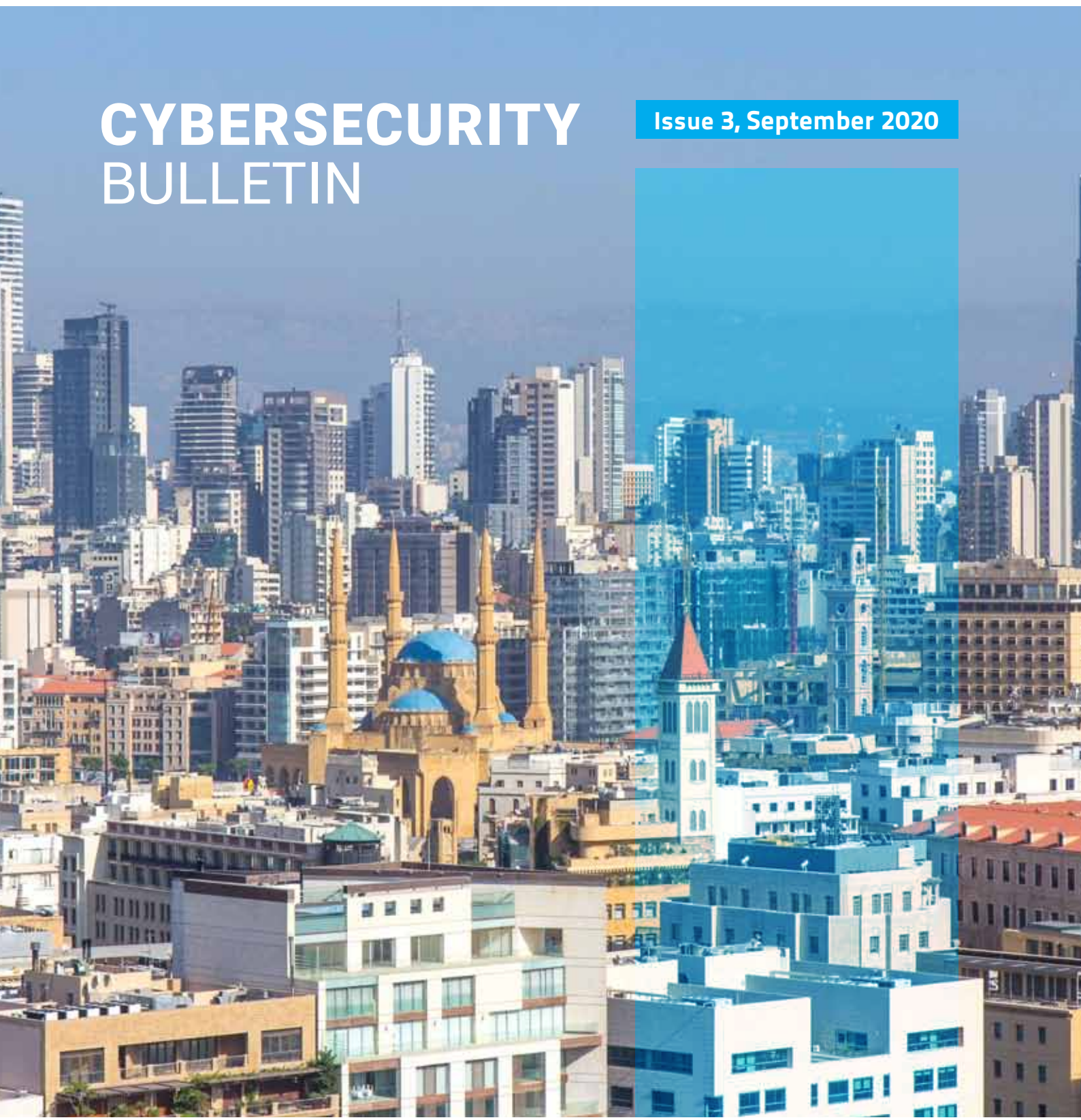
CYBERSECURITY BULLETIN

Issue 3, September 2020



GLOBALCOM DATA SERVICES

WELCOME

Welcome to the third edition of GDS Cybersecurity bulletin.

With cyber-attacks, data breaches and leakage of confidential data on the rise, GDS SOC team, consisting of cybersecurity professionals, is continuously developing and implementing the right procedures and policies in combination with the security tools to help you fight those threats. The main roles of those measures are to:

- Ensure that systems are compliant with the security standards and fix problems in case those systems are breached.
- Deploy advanced techniques to detect threats based on anomalous data correlated with security events using machine learning capabilities.
- Perform code checks using advanced techniques and methodologies for reverse engineering and provide recommended protection steps.

GDS will continuously put all efforts to lead its customers to the best way of protecting and monitoring its network.

TABLE OF CONTENTS

SUMMARY

Insights collected by GDS SOC show the most prevalent sources, types, and vectors of threats that happened during last month.
Hackers are trying to benefit from human weaknesses to be able to penetrate the company fortress. This type of technique should be faced by user awareness trainings, enforcing security polices and updating security devices.


INNOVATION
DATA

GDS
SIEM AND MACHINE LEARNING

After the Beirut port explosion on the 4th of August 2020, GDS AEGIS, our fully managed SIEM solution, detected several VPN access failures due to immediate remote work intervention using VPN to connect from home.

Based on our SIEM alerts correlated with our machine learning dashboard that confirmed this behaviour, we were able to identify the cause of this anomaly.

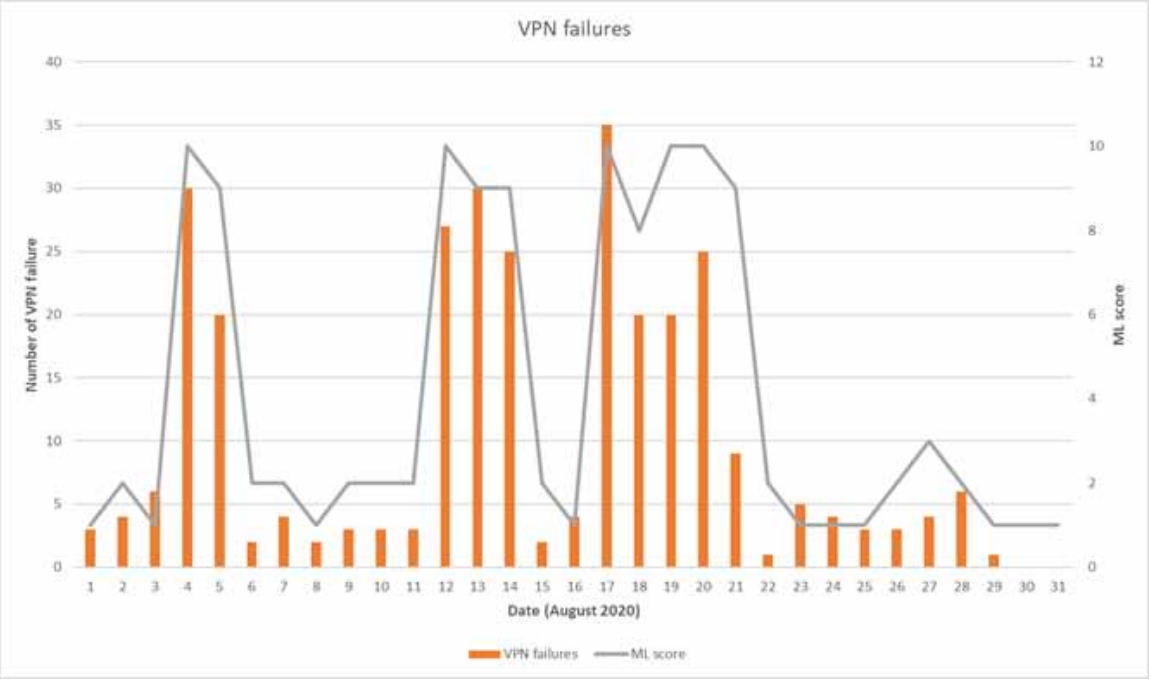


Figure 1: VPN failures diagram

Day 4: The day of the explosion
Peak of VPN failures due to immediate start-up of the remote work

Day 5,6,7,8,9,10,11: Work at offices is suspended
Drop in the peak of VPN failures due to less users working remotely and busy to fix damages.

Day 12,13,14: Employees working remotely from home
Work back to normal causing the second peak.

Day 15,16: Weekend
Normal days VPN failure attempts.

Day 17,18,19,20,21,22: Employees working remotely from home
Third peak of VPN failures due to our intervention with the users to help them with the proper way of using the VPN and solve all possible issues.

Monitoring anomalous data can be critical in detecting a rare data pattern or potential problem in any malfunctioning service or security fraud. In this real-life case it was possible to tie the abnormal rate of VPN access failure to known events and malicious activities were confirmed to be missing.

GDS HONEYPOT SPAM DETECTION RATE

Cyber security has become lately a key priority for organizations in the Middle East following rising geopolitical tensions and a series of recent attacks against regional financial institutions. This is driving the growth of the regional cyber security market.

Earlier this month, researchers at US cyber security company FireEye identified a “wave of emails containing malicious attachments being sent to multiple banks in the Middle East”. The researchers assert that hackers are probing the defenses of banks and ISPs in the Middle East, using malware-infected emails sent to bank and ISPs employees to collect information about their networks and accounts.

GDS honeypot solution detected several malicious IP addresses trying to search for open relays and to send spam emails that are linked to the wave of spam emails reported by FireEye

You can find in Figure 2 some of the IP addresses related to this attack.

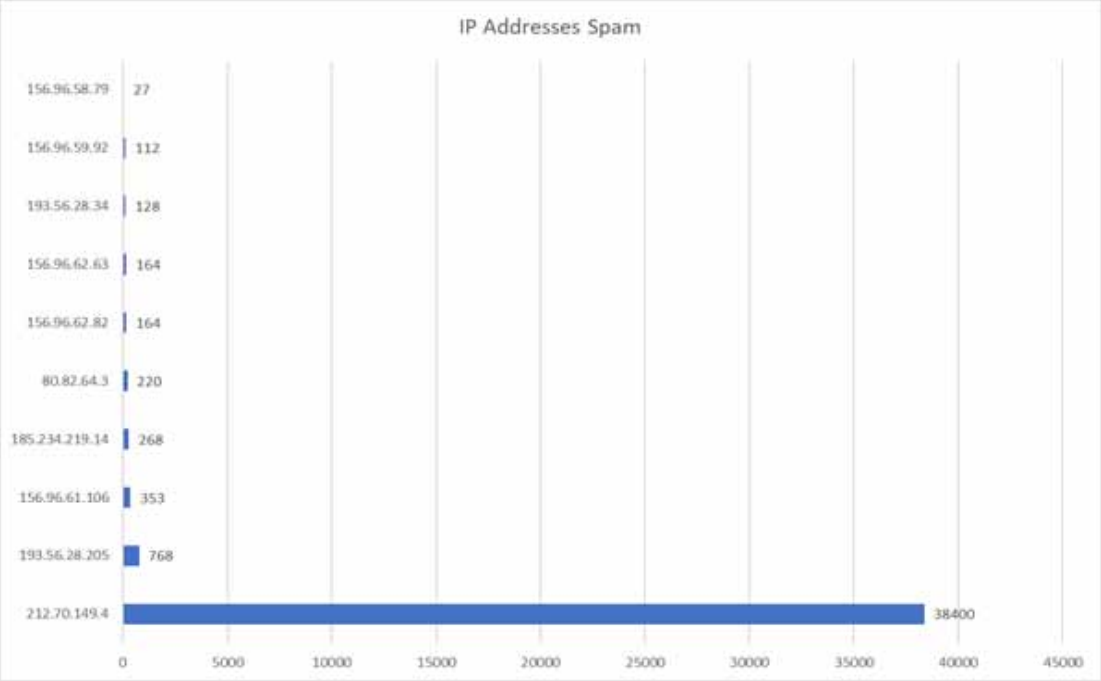


Figure 2: Spam IP addresses attempts

GDS SOC recommends that you mark those IP addresses below on your watch list:

- 212.70.149.4
- 193.56.28.205
- 156.96.61.106
- 185.234.219.14
- 80.82.64.3
- 156.96.62.82
- 156.96.62.63
- 193.56.28.34
- 156.96.59.92
- 156.96.58.79

A super-secret company developed a "supersecretprogram" that grants access to top secret information if executed properly. What follows is a description of how a poorly developed software leads to an adversary gaining access to this information.

The exploit attempt starts by exploring the type of the file being dealt with. In this case, it is an executable file.

Below is the output showing the results of the execution: "Access Denied".

```
home@ubuntu:~/Desktop$ file supersecretprogram
supersecretprogram: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamic
ally linked, interpreter /lib64/l, for GNU/Linux 2.6.24, BuildID[sha1]=e06e0b022
9279a69506925702a7f79e36bdc3eb2, not stripped
home@ubuntu:~/Desktop$ ./supersecretprogram
Access Denied
```

Figure 3: supersecretprogram

One can see that by looking at Figure 3, using the command "file" shows that the program is not stripped, meaning it includes debugging information that is usually important for developers to understand how the program is working.

Next is the use of "ltrace" which is a software tool that runs a specified command until it exits. It intercepts and records the dynamic libraries called by the running process and the signals during the execution of the program. Figure-4 show the output of the command.

```
home@ubuntu:~/Desktop$ ltrace ./supersecretprogram
__libc_start_main(0x40087d, 1, 0x7fffb38137f8, 0x400a70 <unfinished ...>
strncmp("CLUTTER_IM_MODULE=xim", "Passw0rd=", 9)                    = -13
strncmp("LS_COLORS=rs=0:di=01;34:ln=01;36"..., "Passw0rd=", 9)      = -4
strncmp("LESSCLOSE=/usr/bin/lesspipe %s %"..., "Passw0rd=", 9)      = -4
strncmp("XDG_MENU_PREFIX=gnome-", "Passw0rd=", 9)                   = 8
strncmp("LANG=en_US.UTF-8", "Passw0rd=", 9)                         = -4
strncmp("DISPLAY=:0", "Passw0rd=", 9)                               = -12
strncmp("GNOME_SHELL_SESSION_MODE=ubuntu", "Passw0rd=", 9)          = -9
```

Figure 4: run using ltrace

```
home@ubuntu:~/Desktop$ export Passw0rd=hey
home@ubuntu:~/Desktop$ ltrace ./supersecretprogram
__libc_start_main(0x40087d, 1, 0x7ffe7db0c648, 0x400a70 <unfinished ...>
strncmp("CLUTTER_IM_MODULE=xim", "Passw0rd=", 9)                    = -13
strncmp("LS_COLORS=rs=0:di=01;34:ln=01;36"..., "Passw0rd=", 9)      = -4
strncmp("Passw0rd=hey", "Passw0rd=", 9)                             = 0
MD5_Init(0x7ffe7db0c4b0, 0x400b06, 9, 6)                            = 1
strlen("hey")                                                       = 3
MD5_Update(0x7ffe7db0c4b0, 0x7ffe7db0e9f1, 3, 0x7ffe7db0e9f1)       = 1
MD5_Final(0x7ffe7db0c510, 0x7ffe7db0c4b0, 0x7ffe7db0c4b0, 0x7965)   = 1
sprintf("60", "%02x", 0x60)                                         = 2
sprintf("57", "%02x", 0x57)                                         = 2
sprintf("f1", "%02x", 0xf1)                                         = 2
sprintf("3c", "%02x", 0x3c)                                         = 2
sprintf("49", "%02x", 0x49)                                         = 2
sprintf("6e", "%02x", 0x6e)                                         = 2
sprintf("cf", "%02x", 0xcf)                                         = 2
sprintf("7f", "%02x", 0x7f)                                         = 2
sprintf("d7", "%02x", 0xd7)                                         = 2
sprintf("77", "%02x", 0x77)                                         = 2
sprintf("ce", "%02x", 0xce)                                         = 2
sprintf("b9", "%02x", 0xb9)                                         = 2
sprintf("e7", "%02x", 0xe7)                                         = 2
sprintf("9a", "%02x", 0x9a)                                         = 2
sprintf("e2", "%02x", 0xe2)                                         = 2
sprintf("85", "%02x", 0x85)                                         = 2
strcmp("d8578edf8458ce06fbc5bb76a58c5ca4"..., "6057f13c496ecf7fd777ceb9e79ae285"...) = 46
puts("Access Denied"Access Denied
)                                                                   = 14
+++ exited (status 1) +++
home@ubuntu:~/Desktop$ printf "hey" | md5sum | cut -d' ' -f1
6057f13c496ecf7fd777ceb9e79ae285
```

Figure 5: Export password

From the first look, this program is accessing all environmental variables of the operating system and trying to compare using "strncmp" function the first 9 characters with field "Passw0rd". The "Passw0rd" field is then set to a random value "hey" before running "ltrace" again as shown in Figure 5.

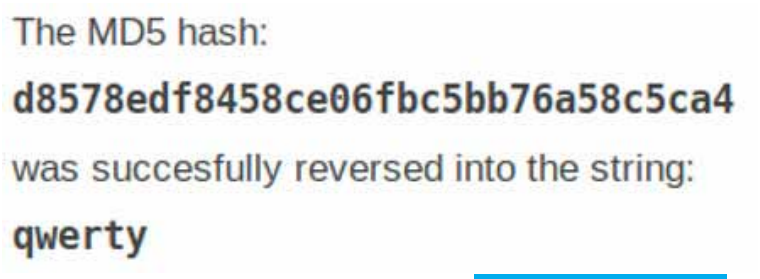


Figure 6: MD5 Hash

The program "supersecretprogram" is comparing two MD5 hashes when running it using the password "hey". Taking the first MD5 hash that is being compared to the MD5 of the random input password, a google search results with a reversed password "qwerty" as shown in Figure 6.

"Passw0rd" is now set to "qwerty" and the program is run again as shown in Figure 7.

```
home@ubuntu:~/Desktop$ export Passw0rd=qwerty
home@ubuntu:~/Desktop$ ./supersecretprogram
Access Granted
```

Figure 7: Gaining Access

Success: access has been granted and password was bypassed successfully.

So it is advisable to always follow the below recommendations:

- Never use weak passwords even if they are being hashed and stored. In the above example, the password used is "qwerty" and the hashing algorithm used is "MD5". If the password was more complex, the reversing of the hash will not be straightforward.
- Never keep the debugging information of a developed software since it can be used as a vector to attack the application.
- While developing an application that requires some sort of authentication to access, use cloaking techniques to the values needed to authenticate with.
- Never use field names that point to the usage of the field (in our example the field name that is used to store the password value is "Passw0rd").

A successful approach to protecting code is a multi-layered one. No single measure can guarantee full protection by itself but missing a single measure can lead to a breach of the program defences.

Executive Summary

Security experts from NVISO Labs recently spotted the activity of a new malware gang, tracked as Epic Manchego, that is actively targeting companies across the world with phishing emails since June 2020. The phishing messages carry weaponized Excel documents that can bypass security checks and have low detection rates.

The trick used by the Epic Manchego gang consists of compiling the documents with a .NET library called EPPlus, instead of the standard Microsoft Office software.

Attack Analysis

Upon opening the Excel files, the embedded malicious script is executed after the victims clicked the "Enable editing" button. Then the script (a macro) would download and install the malicious code, a data stealer, on the victims' systems. Experts observed the attackers delivering well-known infostealer trojans, like Azorult, AgentTesla, Formbook, Matiex, and njRat.

According to the researchers, the first attack dates to June 22, 2020. Since that first attack, experts detected more than 200 malicious documents over a period of 2 months. The cybercrime gang has increased its activity in the last weeks. The researchers recently spotted more than 10 new malicious documents on some days.

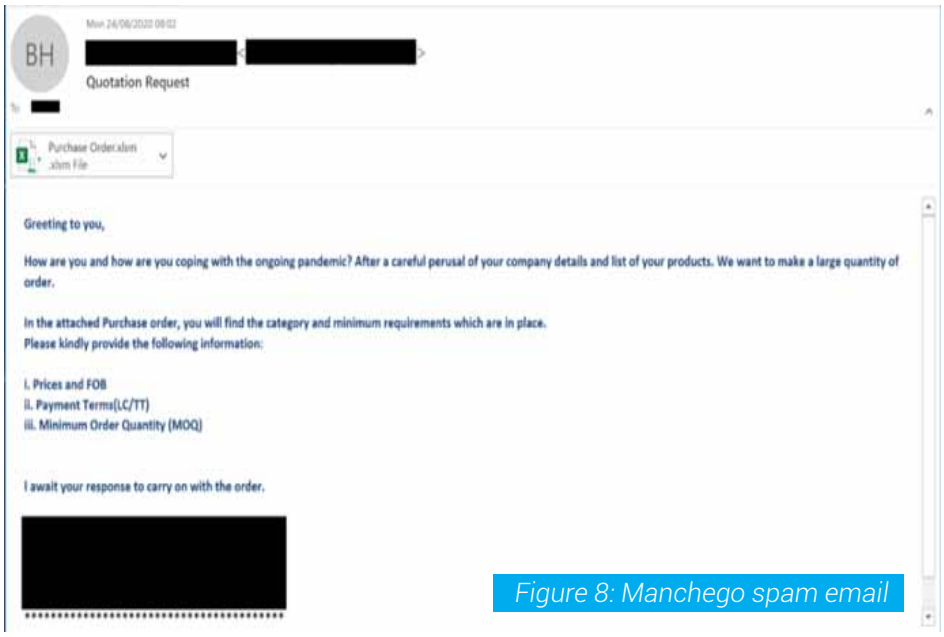


Figure 8: Manchego spam email

Recommendation and mitigation

- Filter email attachments and emails sent from outside your organization.
- Implement robust endpoint detect and respond defenses.
- Create phishing awareness trainings and perform a phishing exercise.

Indicators of Compromise

Hashes (SHA256)

1a000b08359d94eda05df64622b24c451ceffc772ad6473f3cce6fe95dc889c9
2ba660e566a7bbaf32c1141d72009736e3772adcbb6d497ec56b32beaddc56a8
307bf15bfb598feb5fa1fb506db3cc89219e4a2bff75f69dea3821bd 6240446

Email Subject

Re: Quotation required/
Quote volume and weight for preferred
*****SPAM****
FW:Offer_10044885_[companyname]_2_09_2020.xlsx
[SUSPECTED SPAM] Alternatives for Request
Purchase Order Details
Quotation Request

MIDDLE EAST THREAT
THANOS RANSOMWARE

Executive Summary

On July 6 and July 9, 2020, Palo Alto cybersecurity team observed file associated with an attack on two state-run organizations in the Middle East and North Africa that ultimately installed and ran a variant of the Thanos ransomware. The Thanos variant created a text file that displayed a ransom message requesting the victim transfers "20,000$" into a specified Bitcoin wallet to restore the files on the system. Palo Alto do not have visibility into the overall impacts of these attacks or whether the threat actors were successful in receiving a payment from the victims.

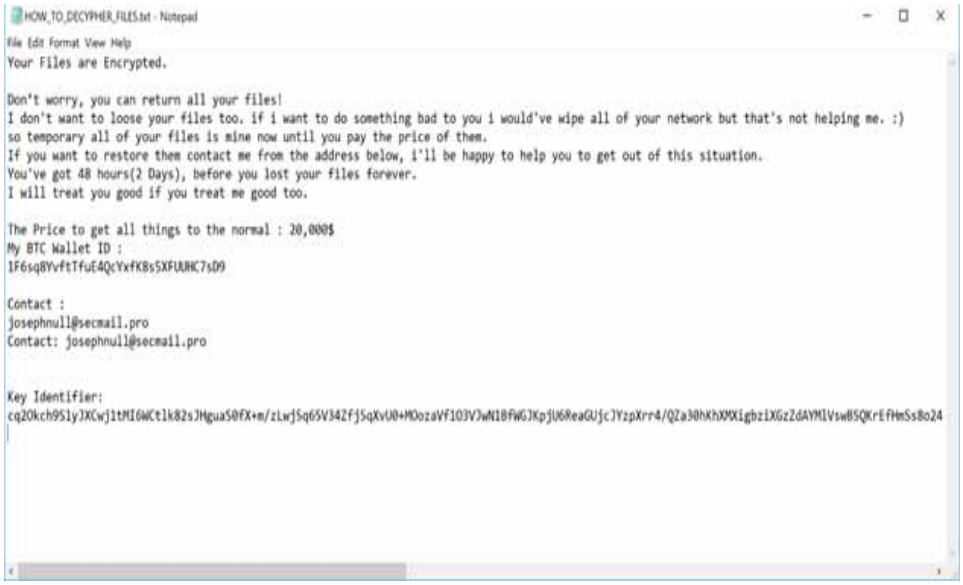


Figure 9: Thanos' ransom note displayed after encrypting files.

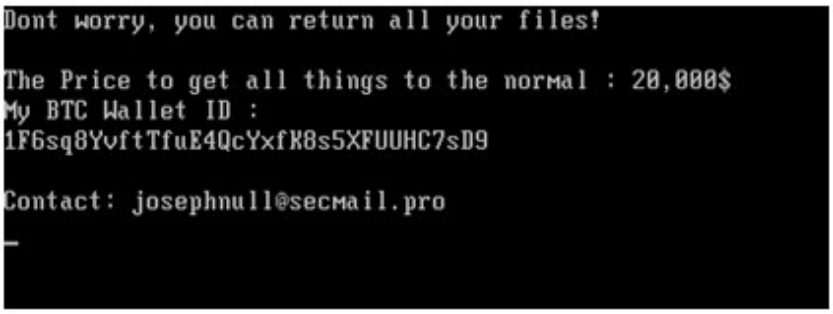
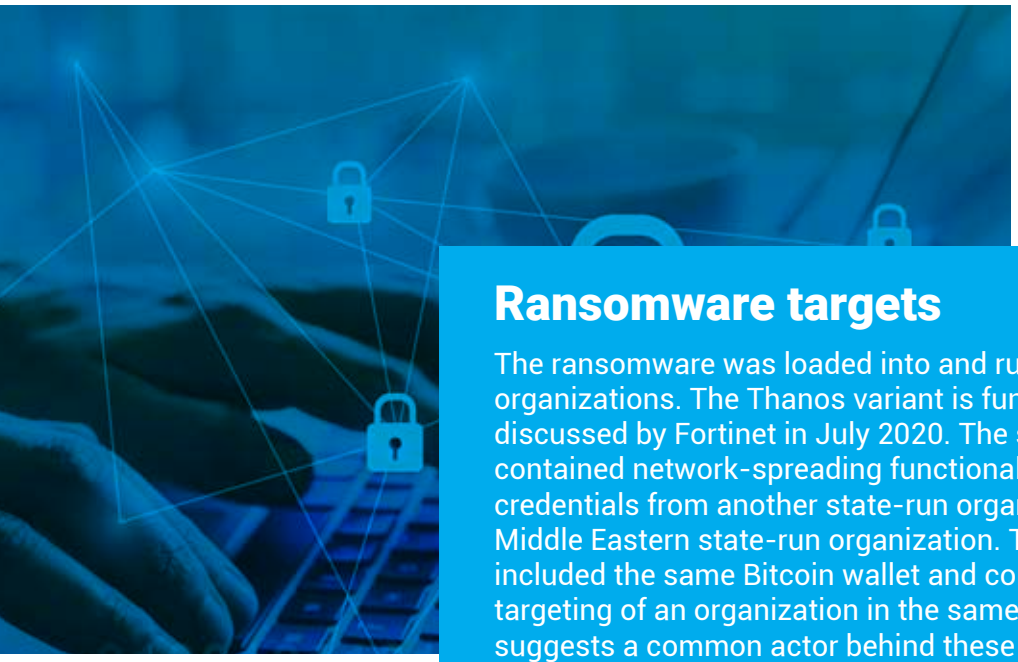


Figure 10: Thano's ransom MBR exception message that prevents booting



Ransomware targets

The ransomware was loaded into and run from within memory at the targeted organizations. The Thanos variant is functionally very similar to the variant discussed by Fortinet in July 2020. The sample analysed by Fortinet also contained network-spreading functionality enabled, which included network credentials from another state-run organization in the same region as the Middle Eastern state-run organization. The sample analysed by Fortinet included the same Bitcoin wallet and contact email. When combined with the targeting of an organization in the same region in a similar time frame, this suggests a common actor behind these attacks.

Advanced analysis

The actors deploying the Thanos ransomware at the Middle Eastern state-run organization also used a downloader that is called PowGoop. The actors would use the PowGoop downloader to reach out to a remote server to download and execute additional PowerShell scripts.

Conclusion and mitigation

While the Thanos ransomware is not new, it appears that it is still under active development as the variant used in these attacks contained new functionality. The new functionality included the ability to detect and evade more analysis tools, the enumeration of local storage volumes via a technique used by the Ragnar Locker ransomware and a new capability to monitor for newly attached storage devices.

Most importantly, this variant of Thanos also included the new ability to overwrite the MBR and display the same ransom message. Overwriting the MBR is a much more destructive approach to ransomware than previously used by Thanos and would require more effort for victims to recover their files even if they paid the ransom.

Indicators of Compromise

Hashes (SHA256)

40890a1ce7c5bf8fda7bd84b49c577e76e0431e4ce9104cc152694fc0029ccbf
06d5967a6b90b5b5f6a24b5f1e6bfc0fc5c82e7674817644d9c3de61008236dc
c460fc0d4fdaf5c68623e18de106f1c3601d7bd6ba80ddad86c10fd6ea123850
ae66e009e16f0fad3b70ad20801f48f2edb904fa5341a89e126a26fd3fc80f75

PowGoop Samples

legitimate Google installer, GoogleUpdate.exe
legitimate Google DLL, goopdate86.dll)
PowGoop Loader, goopdate.dll
PowGoop Downloader, config.dat

Palo Alto Networks

THREAT SUMMARY
CYBERSQUATTING

Executive Summary

Users on the internet rely on domain names to find brands, services, professionals, and personal websites. Cybercriminals take advantage of the essential role that domain names play on the internet by registering names that appear related to existing domains or brands, with the intent of profiting from user mistakes. This is known as cybersquatting. The purpose of squatting domains is to confuse users into believing that the targeted brands (such as Netflix) own these domain names (such as netflix-payments[.]com) or to profit from users' typing mistakes (such as whatsalpp[.]com for WhatsApp). While cybersquatting is not always malicious toward users, it is illegal in the U.S.,[1] and squatting domains are often used or repurposed for attacks.

Launch date, objectives & targets

Launch Date: December 2019 to date.

Objectives: Phishing, malware distribution, command and control (C2C), re-bill scam, potential unwanted program (PUP), technical support scam, reward scam and domain parking.

Target: Mainstream search engines, social media, financial, shopping and banking websites.

Recommended Actions /mitigation techniques

- Type the URL — and make sure it is totally accurate
- Do not open suspicious emails — or click links within them
- Eliminate vulnerabilities in your OS and applications
- Install Internet security software — and keep it update

Indicators of Compromise

Malware/Phishing Squatting Hostname

- apple.com.recover[.]support
- Facebook.com-account-loginmanage.yourfiresale[.]com
- icloud.com-iphone[.]support
- microsoft-alert[.]club
- microsoft-sback-server[.]com
- microsoft-store-drm-server[.]com
- microsoft[.]comxn--microsof-wyb[.]com)
- netflix-payments[.]com
- netflixbrazilcovid[.]com
- Samsungeblyaiphone[.]com
- samsungpr0mo[.]online
- www.icloud.com-secure-login[.]info

Grayware Hostname

- facebookwinners2020[.]com
- micposoft[.]com
- walrmart44[.]com
- whatsalpp[.]com

URL

- samsungeblyaiphone[.]com/dolce.exe
- samsungeblyaiphone[.]com/index.php

Palo Alto Networks

CYBERSECURITY LESSON
BE PREPARED AND LEAD THE EFFORT

Since the potential effects of a cyberattack can be severe, leaders must understand their role when it comes to prevention and protection. Senior managers and executives should be the ones to spearhead cybersecurity campaigns and best practices within their organizations. In fact, after surveying executives from over 200 organizations, the statistics shows that attention from senior management was the biggest factor in the strength of a business's ability to manage cybersecurity risks.

The best proactive approach when it comes to the threat of hacking includes tactics similar to the ones below:

- **Continuously updating company software:** WannaCry mostly affected computers using older versions of Windows XP, Windows 7 and Windows Server 2008. Executives, especially Chief Information Officers, should make sure their information technology departments routinely check for and install software updates.
- **Communicating responsibilities:** according to a Clearswift survey of over 500 IT personnel and 4,000 employees, 22 %of respondents do not feel they are obligated to safeguard their employer's data. Executives should ensure every employee feels responsible for cybersecurity. They can relay this information through company-wide meetings or incorporate the importance of cybersecurity into their new hire onboarding programs.
- **Educating employees on how to spot fraudulent emails and links:** executives must take the lead in establishing training programs to help employees spot possible hacking attempts. Phishing campaigns, for example, try to imitate legitimate senders, but there are almost always subtle differences that a trained eye can identify.
- **Limiting communication between work and personal devices:** an employee can accidentally forward an infected email from his phone to his work address. Executives should instruct their staff not to mix work and personal communications if possible. If employees must use their personal devices for work, executives should instruct them to adopt security best practices at home, so they do not accidentally spread malware to work.
- **Consistently testing internal security measures:** executives should instruct their IT departments to routinely test and provide reports of their security efforts. If a weak point is found, executives should research and approve methods to fix it. Hacker techniques are constantly improving, and routine testing helps businesses remain up to date.

Executives also have greater control over the company budget. They can invest in measures like firewalls, encryption services, SIEM solutions and top-tier information security teams, all of which provide a stronger defense against cyberattacks.

VULNERABILITIES

The following vulnerabilities have high score which means they have high impact if discovered on the premises thus leaving the network vulnerable for attacks either local or external.

It is highly recommended to use the links provided in the "Source & Patch Info" to patch these vulnerabilities. Read the info about the update carefully before applying to make sure that no services will be affected.

Primary Vendor -- Product	Description	Published	CVSS Score	Source & patch info
Internet Explorer and Windows 10	A remote code execution vulnerability exists in internet explorer 11 and windows 10 build 18363. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode	2020-08-12	7.8	CVE-2020-0986
Cisco Jabber for Windows	A vulnerability in the application protocol handling features of Cisco Jabber for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands on a targeted system with the privileges of the user account that is running the Cisco Jabber client software.	2020-09-03	8.8	CVE-2020-3430
OS4Ed openSIS 7.3	An exploitable SQL injection vulnerability exists in the login functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	2020-09-01	9.8	CVE-2020-6141
LG mobile	An issue was discovered on LG mobile devices with Android OS 9 and 10 software. LGTelephonyProvider allows a bypass of intended privilege restrictions.	2020-08-31	9.8	CVE-2020-25062

Source,Nist: https://nvd.nist.gov/vuln/full-listing

To learn more about GDS and our security portfolio, visit https://www.gds.com.lb/security.php

GLOBALCOM DATA SERVICES

Globalcom Data Services sal
Holcom Bldg., 4th floor
Corniche Al Nahr - Beirut - LEBANON
Tel: +961 - 1 - 59 52 59
info@gds.com.lb

About Globalcom Data Services sal

Operating since 1996, GDS is widely regarded as being one of the first Data Service Providers in Lebanon to bring modern and fast connectivity to the country. Always leading the way to the future for individuals and businesses, GDS has been continuously supporting new technologies for more than 20 years.

Building on its extensive network and security expertise, GDS provides a comprehensive security services portfolio. A team of security experts is available to assist customers with facing the complex security threats and cyber-attacks that might affect their business