CYBERSECURITY BULLETIN

Issue ١, July ٢٠٢٠

GLOBALCOM
DATA SERVICES

WELCOME

Welcome to the first edition of GDS Cybersecurity bulletin.

While GDS has been in the security business for more than a decade, only recently have we started to put our extensive knowledge at the service of the ICT community. GDS' own sister companies have relied on its state-of-the-art security services, platforms and intelligence for years, allowing them to thwart threats that are becoming more and more complex. It is no secret, and a bit of a cliché, that Lebanon is a proxy battleground for regional forces all intent on mutual destruction. This struggle is eminently reflected in the threats and attacks that are causing red lights to flash with persistence in our SOC. Some of the most proficient states in cybersecurity attacks roam around our networks. Not many security service providers, whatever the commercial backing behind them, are honed to face nation-state threats.The human experience factor remains critical to ensuring protection.Our belief is that through this monthly bulletin we can share with our customers part of our knowledge and human experience to the benefit of everyone. After all we are part of the same network, and a network is as strong as its weakest link.

TABLE OF CONTENT

WELCOME

TABLE OF CONTENT

GDS THREAT INTELLIGENCE

GDS HONEYPOTS

GDS IRON WALL

GDS SIEM 5

COVID-19, CYBERTHREATS

THREAT SUMMARY
BANKING MALWARE

THREAT SUMMARY
–VALAK MALWARE

THREAT SUMMARY
-WASTED LOCKER RANSOMWARE

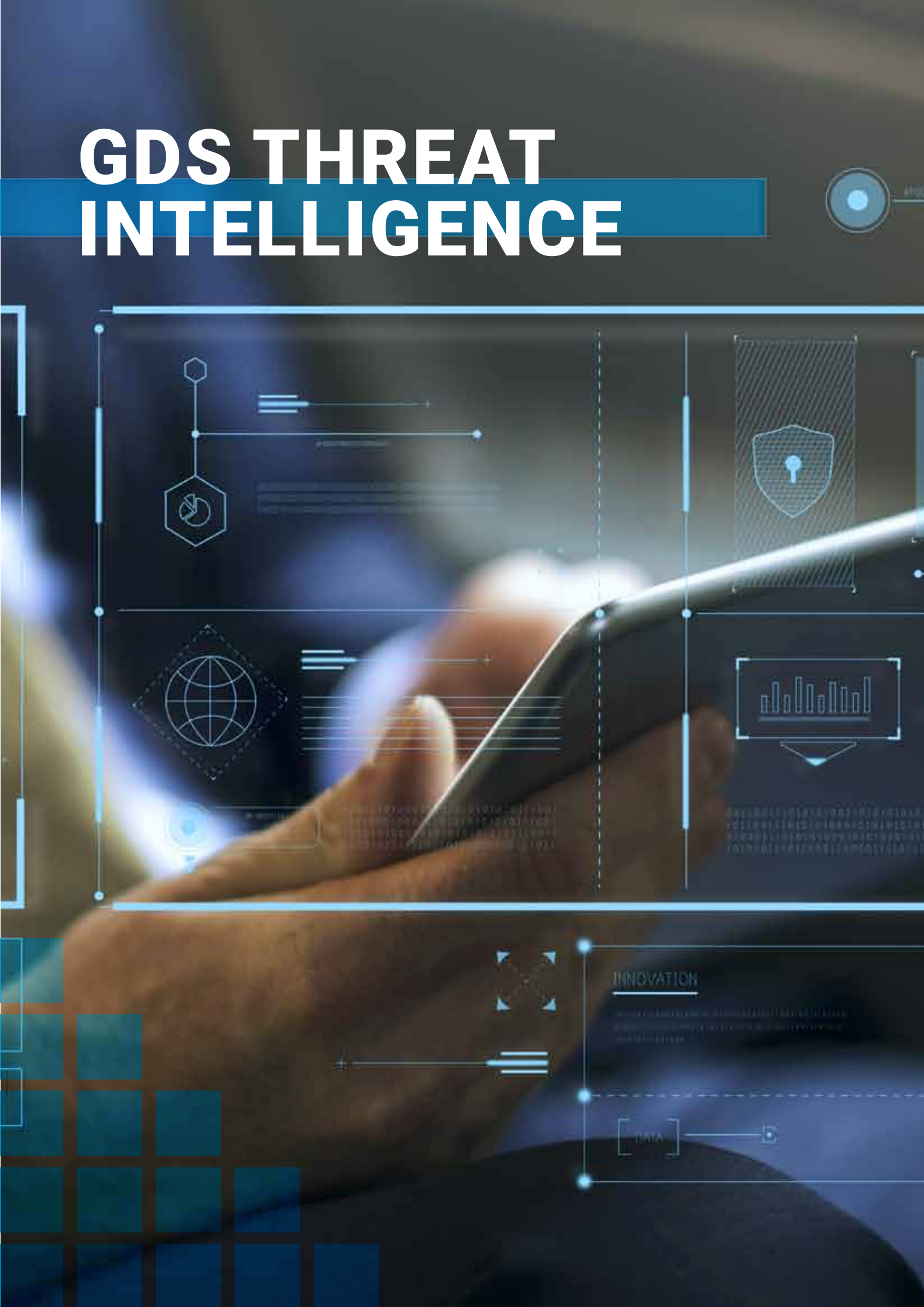
VULNERABILITIES

SUMMARY

Insights collected by GDS SOC show the most prevalent sources, types and vectors of threats.

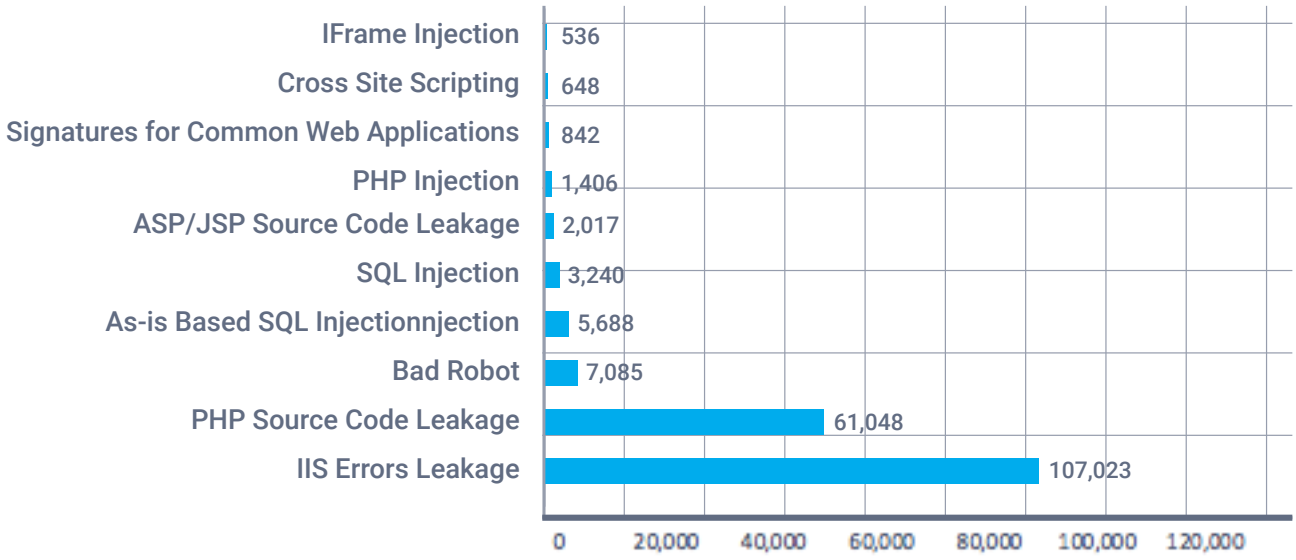
The COVID-19 pandemic and the legitimate health concerns that it rises created the perfect opportunity for cyber criminals to conduct their malicious activities with ease. Social distancing measures, enforced all over the world and in Lebanon, accelerated the shift in work habits from office based to home based. The resulting increased reliance on software tools was a godsend for the ever opportunistic cyber criminals. Multiple threat intelligence sources raised the alarm. We present a few such cases of COVID-19 related threats in the next pages.

GDS THREAT INTELLIGENCE

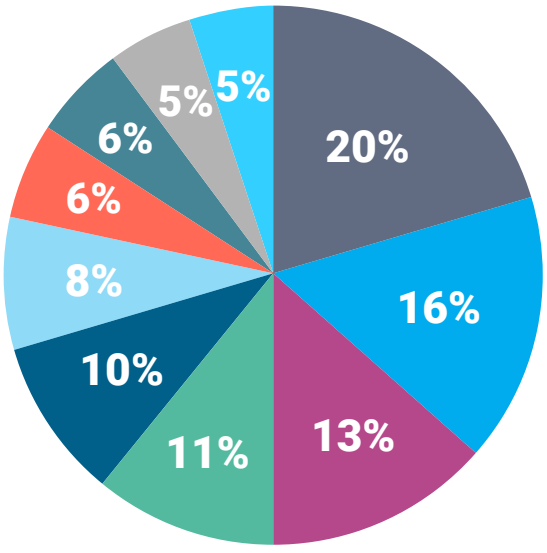


GDS Threat Intelligence has detected attacks being launched against web applications and trojans being used. We recommend you look at the signatures and make sure your antivirus is up to date to detect such signatures.

Top 10 Attacks By Name



Top 10 Malwares By Name

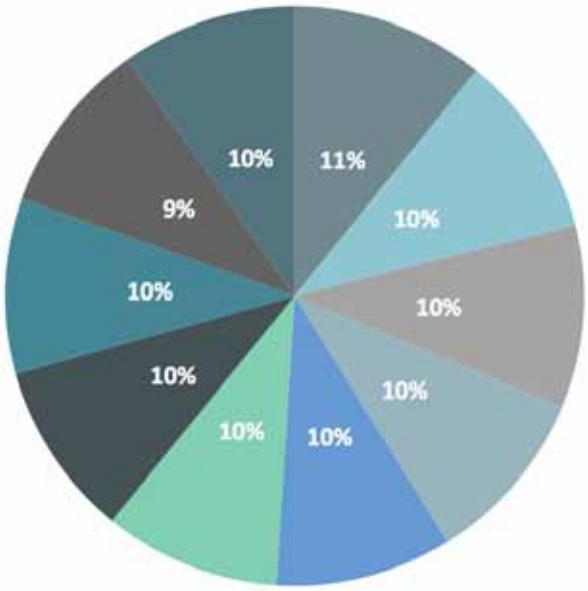


GDS HONEYPOTS

GDS SOC has detected on its network of honeypots the below IP addresses originating from different countries. The activities were scan attempts on a server running Remote Desktop Protocol, login with credentials or exploit deployment to gain access to the system. GDS SOC recommends that you mark the IP addresses shown in figure 3 as malicious and add them to your watchlist especially if you have a server running Remote Desktop Protocol and exposed to the internet.

Source IP	Country	CNT
67.207.81.177	United Stated	7,921
195.133.3.140	Russia	6,611
67.207.81.177	Vietnam	7,921
195.133.3.140	United Kingdom	6,611
67.207.81.177	France	7,921
195.133.3.140	United Arab Emirates	6,611
67.207.81.177	Republic of Korea	7,921
195.133.3.140	Mongolia	6,611
67.207.81.177	Mongolia	7,921
47.52.103.56	Hong Kong	6,611

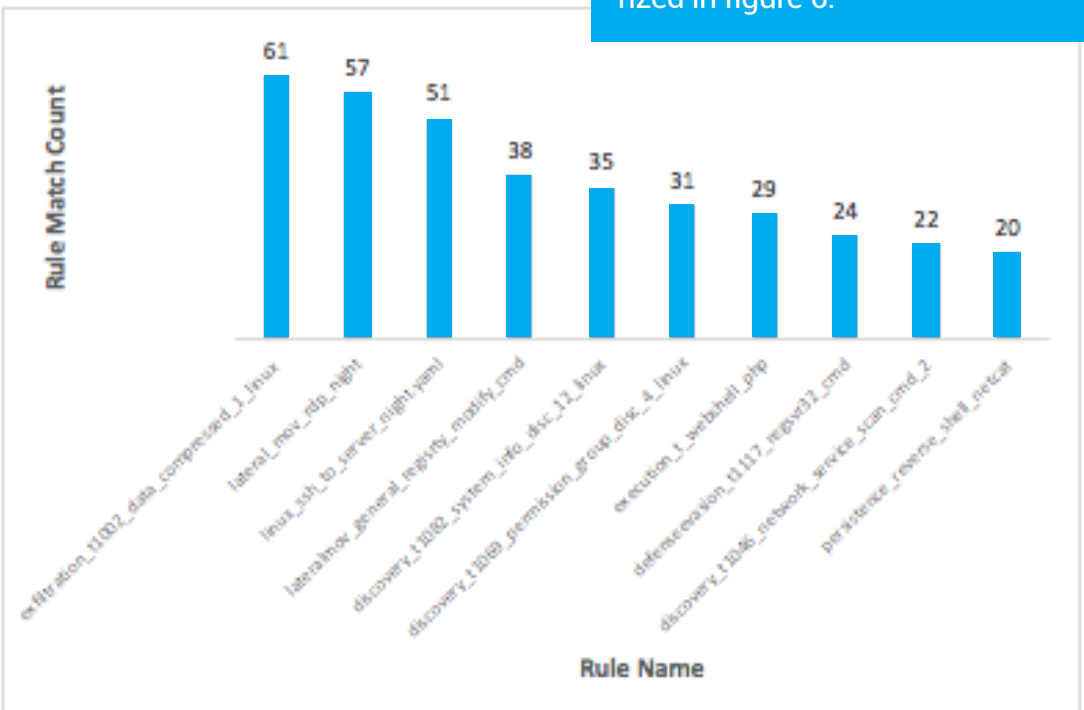
GDS IRONWALL



Malicious activities were observed on GDS Iron Wall. The IP addresses in figure 5 were the cause of activities such as generating invalid packets and sending malformed DNS traffic. We encourage you to closely monitor those addresses as they are continuously repeating the same behaviour.

GDS SIEM

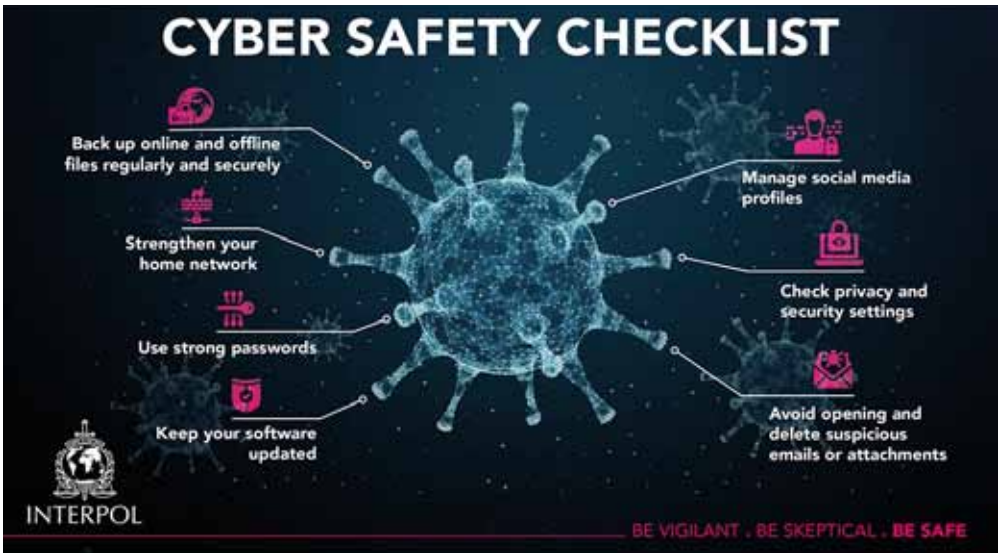
GDS AEGIS, our fully managed SIEM solution, is continuously solicited due to non-stop malicious activities on those networks where it is deployed. The resulting activity is summarized in figure 6.



COVID-19 CYBERTHREATS

"There are a considerable number of registered domains on the Internet that contain the terms: "coronavirus", "corona-virus", "covid19" and "covid-19".
While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware."

This phenomenon, described by Interpol, is not a new approach but rather a typical opportunistic one previously adopted on a smaller scope with other topics. Given the fact that COVID-19 is a pandemic, meaning that its reach and thus related interest is global, the difference now is that the scale of this criminal behaviour is larger than usual.



Keep your information safe

•Back up all your important files and store them independently from your system (e.g. in the cloud, on an external drive).

•Always verify you are on a company's legitimate website before entering login details or sensitive information.

Check your software and systems

•Ensure you have the latest anti-virus software installed on your computer and mobile devices.

•Secure email gateways to thwart threats via spam.

•Strengthen your home network.

•Secure system administrations vulnerabilities that attackers could abuse.

•Disable third-party or outdated components that could be used as entry points.

•Download mobile applications or any other software from trusted platforms only.

•Perform regular health scans on your computers or mobile devices.

Be vigilant

•Talk to your family, including children, about how to stay safe online.

•Regularly check and update the privacy settings on your social media accounts.

•Update your passwords and ensure they strong (a mix of uppercase, lowercase, numbers and special characters).

•Do not click on links or open attachments in emails which you were not expecting to receive or come from an unknown sender.

Source, Interpol: https://www.interpol.int/en/Crimes/Cybercrime/C

THREAT SUMMARY
BANKING MALWARE

During the first half of 2020, particularly during Q2 as the Coronavirus crisis increased and came to the forefront of global concerns, BT Security Threat Intelligence has observed a significant and sustained increase in the development and use of banking trojans. Threat actors have not only spread the malware to new sectors using previously observed tools, but have also reworked tools, with new modules added to increase the potency and stealth of the malware, as well as take advantage of new attack vectors. Alongside this, completely new banking trojans have been observed.

OUTLOOK

It is difficult in the current climate to gauge if the use of banking trojans has peaked given the dependency on the discovery of exploits and the continued COVID-19 pandemic, yet it is assessed that the increased use of banking trojans is set to continue. The current global crisis has pushed many inexperienced technology users towards online banking services which they would never have used before. As reluctance to go into physical bank branches continues, online banking has been a key tool in allowing business to operate as close to normal as possible. It is highly likely that it will continue to gain more of a market share with regards to banking services, even after the COVID-19 pandemic.

The abuse of the Android Accessibility Service has been a key factor in the increase of banking malware, and until this issue is solved by Google, it will present a very attractive attack vector for threat actors. It has also highlighted again the continuing weaknesses on the Play Store, as while applications go through a Virus Total-like selection of engines to establish the presence of malicious content, threat actors are still able to customize malware to appear non-malicious, rendering all Play Store security generally ineffective.

Indicators of Compromise (Top 3)

IP adresses	Domains	Hashes (MD5)
45.147.231.107	http://dcgljuzrb.pw/wp-config.php	69815835866E5D828C9855FCA44512C374342955
23.95.227.159	http://finuclier.com/sound.php	B0DA26512179F6B64C8429D6B509AE29B8F1746E
107.172.221.106	http://penaz.info/gate.php	52A55134B4470830DD07D233D2DCD385A0F300CD

THREAT SUMMARY
VALAK MALWARE

The Valak Malware is a sophisticated malware previously classified as a malware loader. It is a modular information-stealer that attackers have deployed to various countries. The research shows that Valak is more than just a loader for other malware and can also be used independently as an information stealer to target individuals and enterprises. This malware is typically delivered via malicious spam email campaigns that leverage password-protected ZIP archives to evade detection by email security solutions that may inspect the contents of emails entering corporate networks. The email campaigns distributing downloaders associated with Valak also appear to be leveraging existing email threads to lend credibility to the emails and increase the likelihood that victims will open file attachments and initiate the Valak infection process. The overwhelming majority of campaigns occurred over the last couple of months and targeted organizations in the financial, manufacturing, health care and insurance verticals.

Recommended action /mitigation techniques

- Consider social engineering awareness and training, which are key in preventing such attacks.
- Disable macros and install an endpoint protection solution to help mitigate similar attacks.
- Be cautious with emails and files received from unknown senders.
- Do not open unknown attachments or click on links within the emails.
- Beware of lookalike domains, spelling errors in emails and websites, and unfamiliar email senders.
- Search for existing signs of the indicated IOCs in your environment.
- Block all harmful hashes in the NGAV / EDR approach.
- Block all malicious IP's at firewall/ gateway Router.
- Malicious URL's/Domains should be blocked at Proxy level.

Note: recommendations are not limited to above only, more can be applied as per your organization environment. Check the business justification before blocking IOC's in your environment.

Indicators of Compromise (Top 3)

IP adresses	Domains	Hashes (MD5)
103[.]224[.]212[.]222	360yunkang[.]com	00201c81ddac90753e561427e62f3a4d7149bcb39437c6d6a2da7ccf6a832004
104[.]216[.]124[.]121	5continentsproperty[.]com	01d8f8fb10433b00f61afc855a14907ee8854e2a93655e54a396e6fd26c0d8fb
107[.]180[.]51[.]12	7ayatok[.]com	02307b4f5c037ea0d566788ab43834c225c1c7dc1c334f0983756932120e1176

THREAT SUMMARY
WASTED LOCKER RANSOMWARE

The Russian cybercrime group known as Evil Corp has added a new ransomware to its arsenal called Wasted Locker. This ransomware is used in targeted attacks against the enterprise. The Evil Corp gang, also known by CrowdStrike as Indrik Spider, started as affiliates for the ZeuS botnet. Over time, they formed into a group that focused on distributing the banking Trojan and downloader called Dridex via phishing emails. As attacks evolved, the group created a ransomware called BitPaymer which was delivered via the Dridex malware in targeted attacks against corporate networks. The end goal of these attacks is to cripple the victim's IT infrastructure by encrypting most of their computers and servers to demand a multimillion-dollar ransom.

Launch date, geo-location & industries impacted

Launch Date: Discovered in May 2020 and latest seen in June 2020.

Geo-location Impacted:
Primarily, United States of America.

Industries Impacted:
Industries and Organizations in a diverse range of sectors were attacked.

Recommended actions /mitigation techniques

To protect your organisation from malware, it is important that you use good computing habits and security software. A good security software solution that incorporates behavioural detections to combat malware and not just use signature detections or heuristics is important as well.

Indicators of Compromise (Top 3)

IP adresses	Domains	Hashes (MD5)
185.189.151.38	szn[.]services	2f72550c99a297558235caa97d025054f70a276283998d9686c282612ebdbea0
185.162.235.167	dns[.]proactiveads[.]be I	389f2000a22e839ddafb28d9cf522b0b71e303e0ae89e5fc2cd5b53ae9256848
185.82.127.38	grarcosbann[.]club	3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3

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
adobe -- flash_player	Adobe Flash Player versions 32.0.0.371 and earlier, 32.0.0.371 and earlier, and 32.0.0.330 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-12	10	CVE-2020-9633 CONFIRM GENTOO
lansweeper -- lansweeper	Lansweeper 6.0.x through 7.2.x has a default installation in which the admin password is configured for the admin account, unless "Built-in admin" is manually unchecked. This allows command execution via the Add New Package and Scheduled Deployments features.	2020-06-15	7.5	CVE-2020-14011 MISC MISC
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	2020-06-18	7.7	CVE-2020-14434 CONFIRM

Disclaimer

To enquire about the content of this bulletin, contact us through soc@gds.com.lb
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