GLOBALCOM
DATA SERVICES

CYBERSECURITY BULLETIN

ISSUE 2

August 2020

WELCOME

Welcome to this new edition of GDS Cybersecurity bulletin.

Scientia potentia est: nowhere is the fact that "knowledge means power" more applicable than in the cybersecurity sphere. Improved awareness is the first stage of a successful security strategy. Armed with pertinent information, it becomes possible to pre-empt attacks and avoid security breaches.

In this edition, GDS provides five complementary approaches for reaching its target of increasing the security awareness among its customers by means of knowledge:

- Live statistics from the security tools' dashboards to show the real trend of cyberthreats in Lebanon.
- Brief information about the techniques used to detect, analyze, and take conclusive actions.
- Examples of attack types including link analysis showing the path and steps done by the intruder.
- Information about the latest threats based on worldwide international threat intelligence that have targeted some customers in Lebanon.
- Advice to share any possible attack that happened at the customer level and to assess periodically its security posture

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

CONTENTS

SUMMARY

Insights collected by GDS SOC show the most prevalent sources, types, and vectors of threats that happened during the past 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, enforcement of security polices and security devices updates.

GDS Security Gateways

GDS Security Gateways are the front-end protection walls that receive all the malicious traffic. Their advanced capabilities filter Internet-bound traffic by inspecting web requests against updated policies and signatures. It may come as a surprise that the end-user within the organisation is often the weakest link in the cyber defence chain and the first to compromise security. All the more reason to implement anti-spam gateways to filter received email since most of the new attacks are delivered through email attachments.

GDS SOC recommends that you add those domains shown in figure 2 to your watch list.

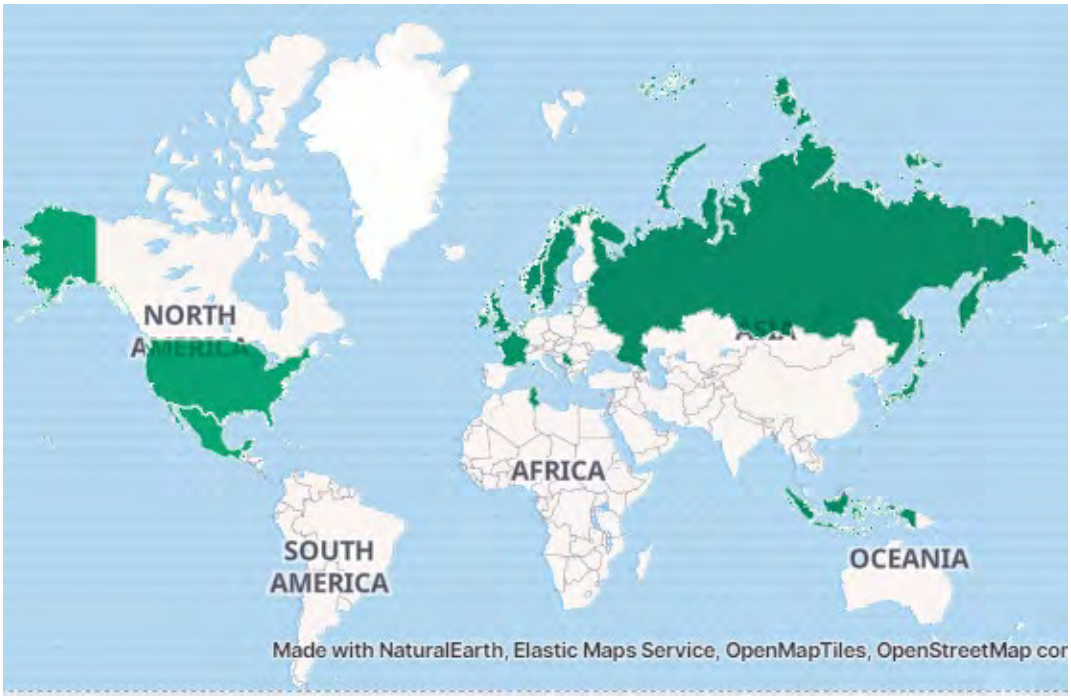

Figure 1 WAF attack distribution map

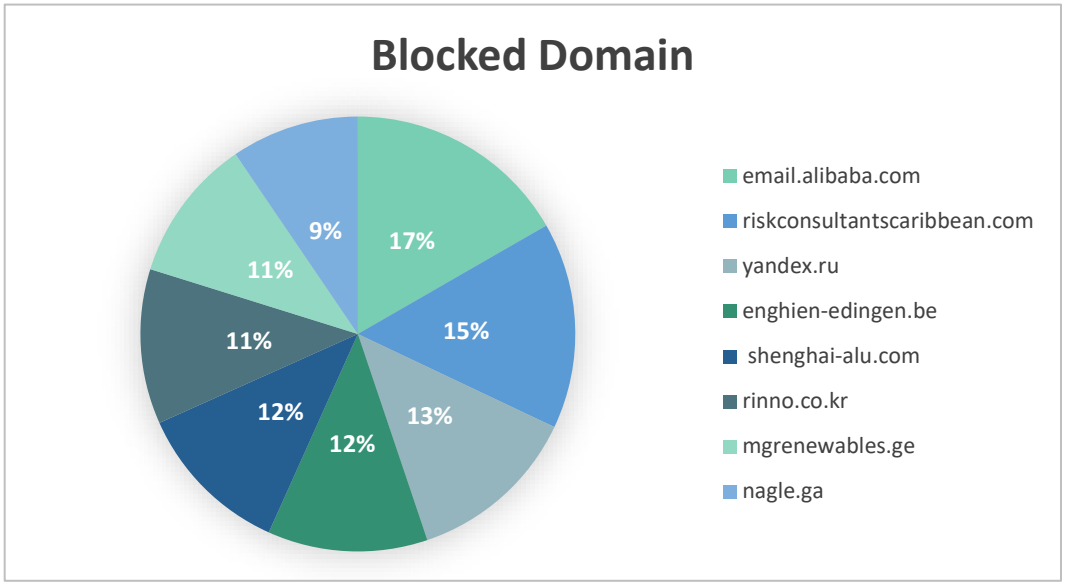

Figure 2 Anti-spam blocked domains

GDS Machine learning

Malicious attacks are getting more sophisticated for traditional security tools to effectively detect them. GDS SOC is continuously building Machine Learning (ML) capabilities to be able to prevent and block those evolved malicious threats. ML algorithms can analyse and learn from patterns to help prevent similar attacks and respond to changing behaviour.

An example of an ML algorithm is one that finds anomalies in process creation, process path and failed authentication. Figure 3 shows an example of anomaly detection.

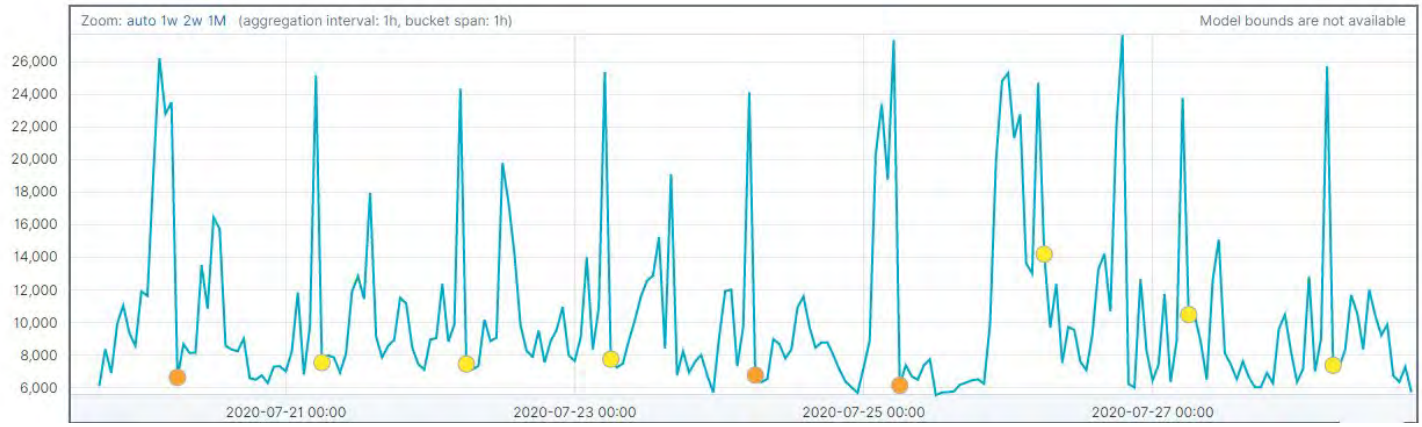

Figure 3 – Anomaly monitoring for endpoint log spikes

The ML algorithm helps to detect any uncommon and rare link between parent process and child process creation (figure 4) such as "bitsadmin.exe" process under "w3wp.exe" web service process flagged with a high anomaly score for abnormal process creation (same for the rest).

We recommend that you monitor the processes creation and their occurrences in correlation with parent-child links.

Anomaly Score	Parent Process name	Process name
90	w3wp.exe	bitsadmin.exe
75	apache	wget
85	excel.exe	ipconfig.exe

Figure 4 – Score for process anomaly detection

GDS IRON WALL

Malicious activities were observed on GDS Iron Wall. The IP addresses in figure 5 were the cause of abnormal 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.

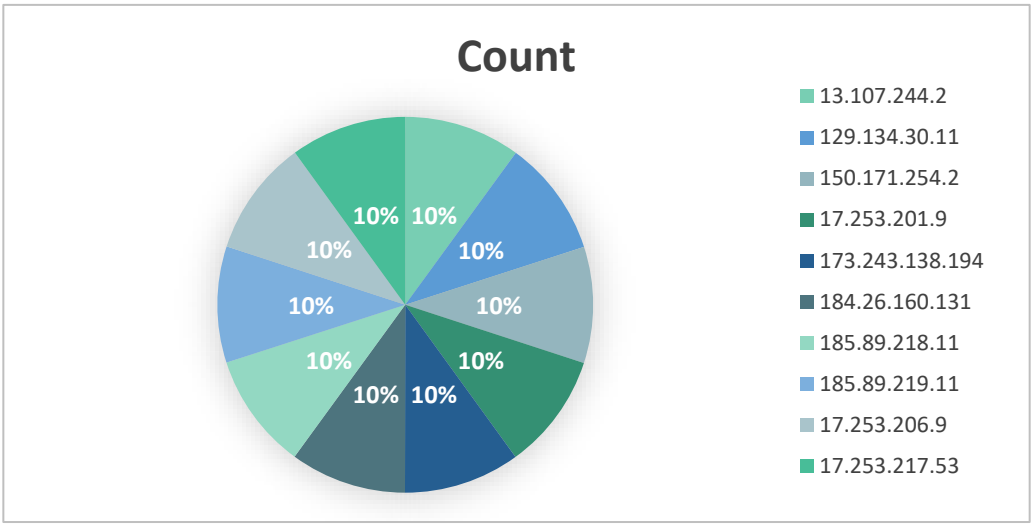

Figure 5 - Top 10 IP addresses blocked due to malicious activities

GDS SIEM

GDS AEGIS, our fully managed SIEM solution is mapped with the MITRE ATT&CK framework for end-point behavioural tactics and techniques. Top tactics during July 2020 are shown in figure 6.

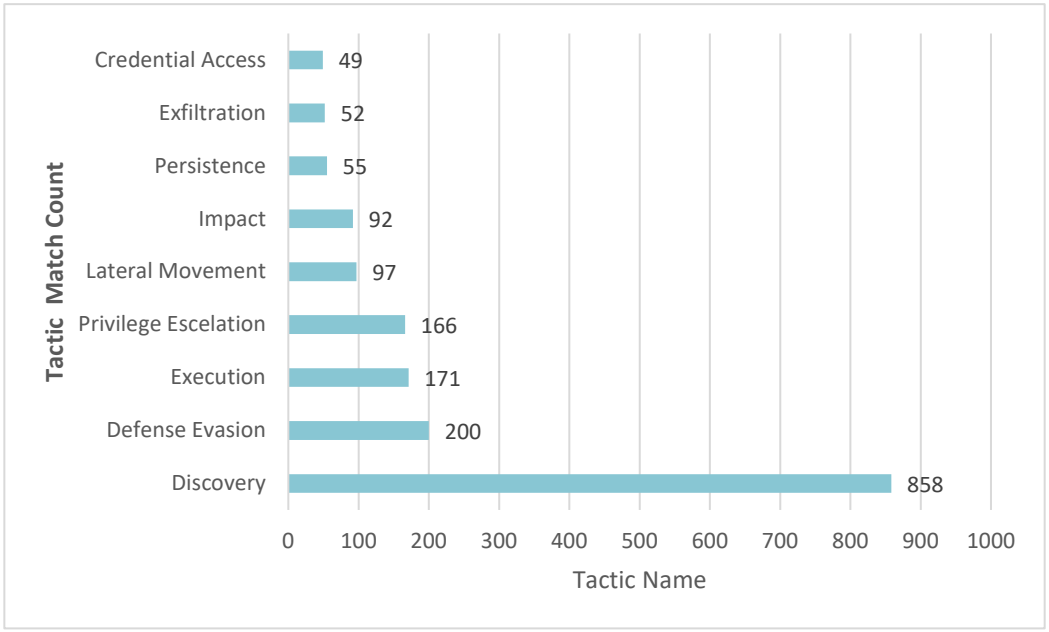

Figure 6 -Top 10 endpoint attacks mapped to MITRE ATT&CK matrix

Business Email Compromise Fraud

"Don't let scammers trick you into making payments to their accounts".

Criminals hack into email systems or use social engineering tactics to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account.

Protect your corporate systems

- Use anti-virus, firewall and scan computers and devices regularly.
- Keep your personal and business computers up to date: pay attention to security alerts, update security patches, conduct periodic systems checks.

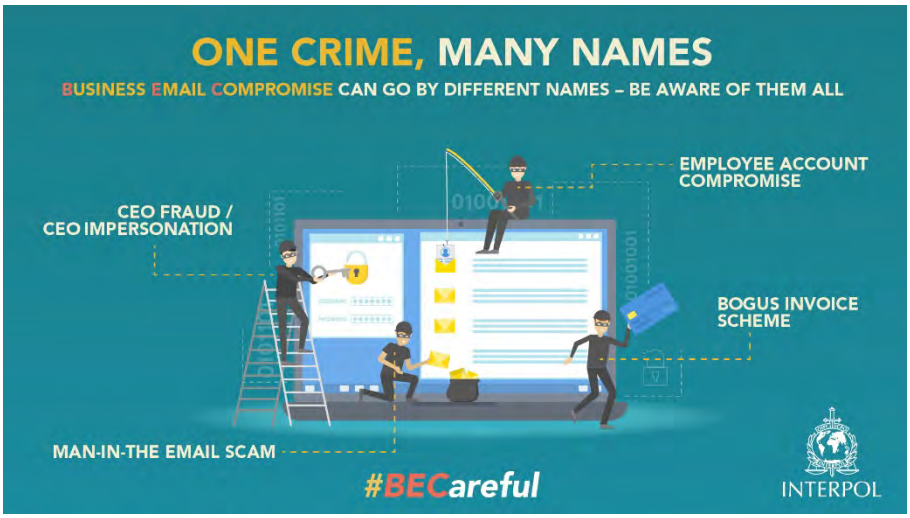

Figure 7 -Email compromise

Avoid becoming a target

- Do not post sensitive or personal information on social media. This can be used by fraudsters to target you.
- Shred all confidential documents and dispose of them properly.
- Use different passwords for every account, change them regularly and enable two-factor authentication on all your accounts whenever possible.

Be vigilant

- Look carefully at the sender's email address. Criminals often create an account with a very similar email address to your business partners so keep your eyes peeled!
- Spread the word so any colleagues dealing with bank accounts are aware of the scam.
- If you receive an email concerning a change of payment method or bank account, DO contact the payment recipient through another channel (phone) to verify this claim. DON'T reply directly to the email.
- Verify the authenticity of websites before providing any personal or sensitive information.

Source, Interpol: https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud

THREAT SUMMARY – Tetrade 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.

Launch date, geo-location & industries impacted

Geo-location Impacted: North America Latin America, Europe (Not limited to these locations – some customers in Lebanon were also targeted).
Launch date: First seen in 2015, and spike seen in July 2020
Industries impacted: financial institutions.

Attack Vector

Tetrade includes four banking Trojan families: Guildma, Javali, Melcoz and Grandoreiro uses different techniques to compromise hosts.

The initial attack vector is more likely to be gained through email shots containing a malicious file in compressed format attached to the email body. File types vary from Visual Basic Script to LNK and emails include an MSI (Microsoft Installer) file with an embedded Visual Basic Script that downloads the final malicious payload from a remote C2; it also uses DLL side loading and several layers of obfuscation to hide its malicious activities from analysts and security solutions. Experts noticed that the malware uses the BITS Admin tool to download the additional modules. Attackers used the tool to avoid detection since it is whitelisted from the Windows operating system.

Most of the phishing messages emulate business requests, packages sent over courier services or any other regular corporate subjects, including the COVID-19 pandemic, but always with a corporate appearance.

Indicators of Compromise (Top 3)

	Hashes (MD5)	
	0219ef20ab2df29b9b29f8407cf74f1c 5ce1eb8065acad5b59288b5662936f5d 1b50b1e375244ce5d4e690cf0dbc96d8	

Source, British Telecom

THREAT SUMMARY – Conti RANSOMEWARE

Conti is a newly observed ransomware that uses a unique encryption routine to identify and encrypt files incredibly quickly and used in human-operated attacks against several targets. It allows a threat actor to control how Conti iterates over files to encrypt, such as local files, SMB shares, IPs inputted by an actor. It uses a large number of independent threads to perform encryption, allowing up to 32 simultaneous encryption efforts, resulting in faster encryption compared to many other families, according to Carbon Black blog post that the ransomware and some of the features that set it apart from others in terms of performance and a focus on network-based targets. It too abuses the Windows Restart Manager to close applications that lock certain files, thus ensures all files can be encrypted. It will encrypt all files except those with the extensions of exe, dll, lnk, and sys and represents another human-operated ransomware variant.

Launch date, geo-location & industries impacted

Launch date: December 2019, and spike seen in July 2020.
Geo-location North America and Europe (Not limited to these locations – some customers in Lebanon were also targeted).
Industries impacted: large corporations or government networks.

Recommended actions/mitigation techniques

- Search for existing signs of the indicated IOCs in your environment.
- Secure configurations are applied to all devices.
- Security updates are applied at the earliest opportunity.
- Multi-factor authentication (MFA) and lockout policies are used where practicable.
- Administrative accounts are only used for necessary purposes.
- Remote administration services use strongly encrypted protocols
- 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

File name	Emails	Hashes (MD5)
CONTI_README[.]txt	xersami[@]protonmail[.]com flapalinta1950[@]protonmail[.]com	b7b5e1253710d8927cbe07d52d2d2e10

Source, British Telecom

How to Spot Fake News

Fake news is nothing new, the phenomenon has been around since humans have been able to relay information – from spoken word to the first newspapers and now, to social media. Fake news, in 1898, helped start a war between the United States and Spain over the sinking of a US Navy cruiser in Havana.

While not as dramatic as an armed conflict, the effects of fake news on organisations can still be far reaching. But it is also nothing to be afraid of. When armed with the right tools and information, anyone can spot fake news from a mile away.

What to look for

- First, start by checking the "URL": if the news is located in a web page, look at the top of the page and check what is the website. Use your logic to find out what is the website, is it a local news agency, belongs to a political party? Have you seen news from this website before?
- Check out the grammatical outline of the news. News outlets usually watch out for grammatical mistakes in their posts and often review their content to make sure it is well formatted, they concentrate on the proper spelling of Names, Places, Countries and other important information they want their news to focus on. Search for grammatical mistakes, weak construction of sentences and other signs that shows the lack of a review before the news were posted.
- Check for references. News agencies, if relaying a headline from another agency, often mention the original link that contains the original content as a reference and a proof. Fake news do not do that. They tend to mention a headline that they say another agency wrote without focusing on the original link because it simply does not exist.
- If the news is posted on a social media account (Twitter, Facebook etc..), take a look at their profile. Lots of clues might be hiding in plain sight. Check the account's date of creation, usually you will see the date of creation is near your current date, maybe 2-3 months earlier. Check their content, is it original? Do they only retweet (in case of Twitter)? Do they spam threads with the same comment? Do they have followers, and have they been interacting with their followers or friends?

- Check other sources. Is the same news posted on other legitimate news outlets? If so, does it have the same content? You can often see fake news manipulating words to make you think that the same subject is posted elsewhere: when the headline seems to be same, the content is often not.
- Use Google. Look at the content in question, take important words like places, names, words in quotations (this usually means it is mentioned as it is), search the keywords all together on Google, find out where those specific keywords are mentioned altogether and if they are found in a legitimate website.

You are now equipped with some basic knowledge to detect fake news, when all else fails it is better to contact officials if the issue is dangerous. Fake news is used to spread propaganda whether its goal is to cause fear and disfunction or to populate a political agenda. Be careful out there and stay vigilant.

Figure 8 shows how "spam" or "automated" accounts identified by twitter are increasing with time. This is due to both an increase in their numbers and to ever more sophisticated techniques used by Twitter to identify them.

Figure 8 - number of Twitter accounts that has been identified to being either "spam" or "bot"

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
Microsoft 365_apps	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	2020-07-14	9.3	CVE-2020-1240 MISC
Juniper_networks srx_series_devices	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, processing a malformed HTTP message can lead to a Denial of Service (DoS) or Remote Code Execution (RCE)	2020-07-17	7.5	CVE-2020-1654 CONFIRM
Cisco ASA	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system.	2020-07-22	7.5	CVE-2020-3452
google -- chrome	Use after free in tab strip in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-07-22	9.3	CVE-2020-6515 SUSE MISC MISC GENTOO

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 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.

GLOBALCOM DATA SERVICES