GDS

GLOBALCOM
DATA SERVICES

CYBERSECURITY BULLETIN
ISSUE 5
November 2020

WELCOME

Welcome to the fifth edition of GDS cybersecurity bulletin.

As social engineering attacks continue to evolve in sophistication and frequency, individuals should heed data protection advice and take the appropriate measures to keep sensitive personal information safe and secure.

The success of social engineering techniques depends mainly on the ability of the attacker to manipulate the victim into performing certain actions or providing confidential information. In this edition, GDS SOC team provides tips for countering social engineering techniques such as monitoring activity on mobile devices and protecting data from threats.

Looking forward to your valuable feedback!

CONTENTS

SUMMARY

What are the latest attacks discovered by GDS security endpoints? How to remove a hacker from your smartphone? How to respond to the shortage of skills in the cybersecurity field?

The next few pages answer these questions in addition to focusing on other topics relevant to social accounts protection and data breach.

GDS IRON WALL

DDoS attacks seek to overwhelm a targeted web application or server with fake traffic, deplete network bandwidth and make it unavailable to legitimate users. DDoS attacks happen in several different ways including amplification, flooding, protocol-based, and reflection.

Malicious activities were observed on GDS Iron Wall. The IP addresses in **Error! Reference source not found.**were the cause of DDoS attacks. We encourage you to closely monitor those addresses as they are continuously repeating the same behaviour.

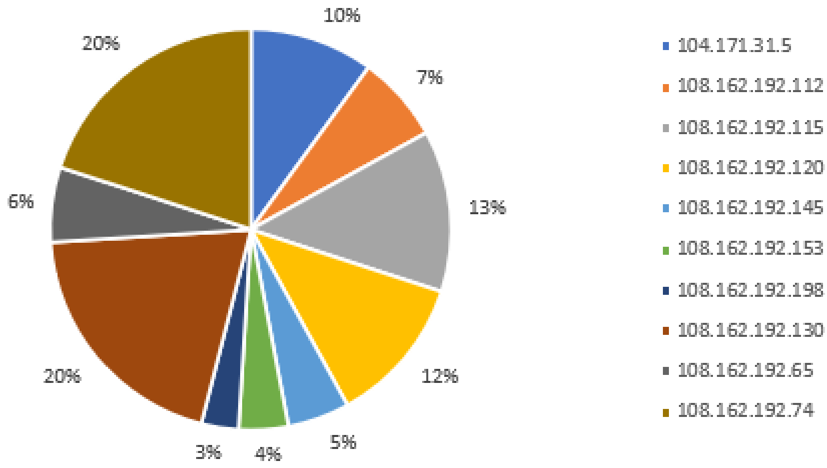


Figure 1: top 10 IP addresses launching DDOS attacks

GDS NEXT GENERATION ANTIVIRUS

GDS next generation antivirus protects against all type of threats, known and unknown, through the combination of artificial intelligence, behavioral detection, and machine learning algorithms. Malicious malwares were detected and blocked by our Next Generation Antivirus. A closer look at the list of malware shows that some exploits are still used although they are dated to 2017 like "CVE-2017-11882.Gen". This means that a patch management policy that could assist in avoiding such risk is not well implemented.

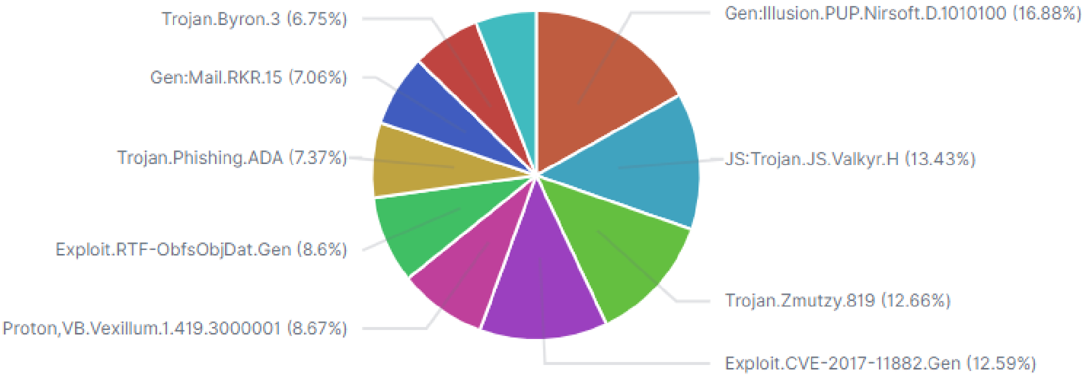


Figure 2: top detected malwares

As new malwares are rising every hour, make sure you implement a next generation antivirus updated with the latest signatures.

GDS WEB APPLICATION FIREWALL

Web Application Firewall (WAF) is the first line of defense between a web application and the internet traffic and shields the web application from being accessed by malicious actors, botnets, and bad traffic. It monitors all the traffic and requests made to the application and filters out the malicious ones.

GDS WAF is an essential part of a layered defense-in-depth strategy for protecting applications.

Figure 3 shows the top ten attacks detected and blocked by GDS WAF. The highest number of attacks matching the blocking rule on the WAF, is the one denying the techniques of the attackers used to discover sensitive information related to the files of the websites. So, it is important not to leave any file disclosing critical information such as db. backup or password text files under any directory for the website.

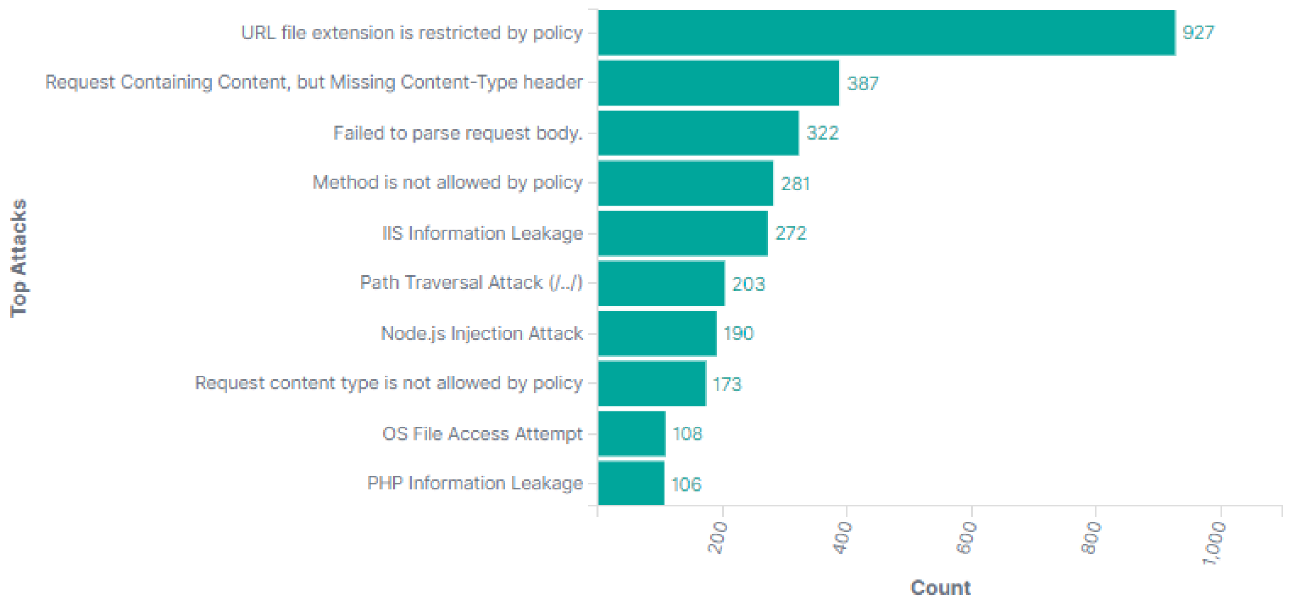


Figure 3: top attacks detected by WAF

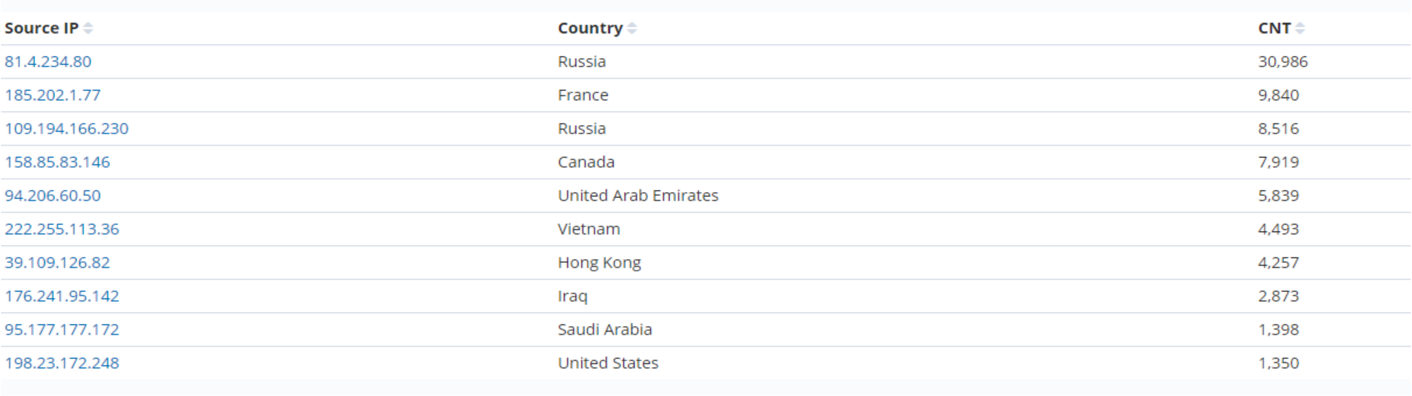
GDS HONEYPOT RDP SCANS

With the spread of COVID-19, organizations worldwide have introduced remote working, which is having a direct impact on cybersecurity and the threat landscape.

Alongside the higher volume of corporate traffic, the use of third-party services for data exchange and employees working on home computers, another headache for infosec teams is the increased number of people using remote-access tools.

One of the most popular application-level protocols for accessing Windows workstations or servers is Microsoft's proprietary protocol RDP. The lockdown has led to the exposure of a great number of computers and servers to the internet using this protocol.
GDS honeypot solution detected several malicious IP addresses trying to search for workstations and servers having remote desktop protocol enabled on them.

Figure 4 depicts some of the IP addresses related to attacks on RDP which should be blocked on the external gateway of the network.



Source IP	Country	CNT
81.4.234.80	Russia	30,986
185.202.1.77	France	9,840
109.194.166.230	Russia	8,516
158.85.83.146	Canada	7,919
94.206.60.50	United Arab Emirates	5,839
222.255.113.36	Vietnam	4,493
39.109.126.82	Hong Kong	4,257
176.241.95.142	Iraq	2,873
95.177.177.172	Saudi Arabia	1,398
198.23.172.248	United States	1,350

Figure 4: top 10 IP addresses launching RDP attacks

HOW TO REMOVE A HACKER FROM YOUR SMARTPHONE

How to know if someone is hacking your phone

One or more of these could be a red flag that someone has breached your phone:

Figure 5: hacker inside your phone

1. **Your phone loses charge quickly.** Malware and fraudulent apps sometimes use malicious code that tends to drain a lot of power.

2. **Your phone runs abnormally slowly.** A breached phone might be giving all its processing power over to the hacker's shady applications. This can cause your phone to slow to a crawl. Unexpected freezing, crashes, and unexpected restarts can sometimes be symptoms.

3. **You notice strange activity on your other online accounts.** When a hacker gets into your phone, they will try to steal access to your valuable accounts. Check your social media and email for password reset prompts, unusual login locations or new account signup verifications.

4. **You notice unfamiliar calls or texts in your logs.** Hackers may be tapping your phone with an SMS trojan. Alternatively, they could be impersonating you to steal personal info from your loved ones. Keep an eye out since either method leaves breadcrumbs like outgoing messages.

How to protect your phone from being hacked

1. **Do not download sketchy or unreputable apps**. Look at reviews and research before installing if you are unsure. If you are not confident in safety of app, do not install it.

2. **Do not jailbreak your phone.** While it allows you to download from unofficial app stores, jailbreaking ups your risk of unknowingly getting hacked. Aside from malware or spyware, this means you will miss security patches in the latest OS updates. Jailbreakers skip updates to keep the jailbreak functional. This makes your risks of being hacked even higher than normal.

3. **Always keep your phone with you.** Physical access is the easiest way for a hacker to corrupt your phone. Theft and a single day of effort could result in your phone being breached. If you can keep your phone with you, a hacker will have to work much harder to get into it.

4. **Always use a passcode lock and use complex passwords.** Do not use easily guessable PINs, like birthdays, graduation dates, or basic defaults like "0000" or "1234." Use an extended passcode if available, like those with 6 characters. Do not ever reuse a password in more than one place.

5. **Do not store passwords on your device.** Remembering unique passwords for every account can be difficult. So use a secure password manager instead. These services allow you to store all your secure credentials in a digital vault — giving you easy access and the security you need.

6. **Frequently clear your internet history.** It can be simple to profile trends about your life from all the breadcrumbs of your browser history. So, clear everything, including cookies and cache.

7. **Enable a lost device tracking service.** If you lose track of your device out in public, you can use a lost device finder to trace its current location. Some phones have a native application for this, while others may need a third-party app to add this feature.

8. **Keep all apps up to date.** Even trusted apps can have programming bugs that hackers exploit. App updates come with bug fixes to protect you from known risks. The same applies to your OS, so update your phone itself when you can.

9. **Always enable two-factor authentication (2FA).** This is a second verification method that follows an attempt to use your password. 2FA uses another private account or something you physically have. Apple ID and Google accounts offer 2FA in case your device is used by unsavory actors, so always activate it for more security. Biometrics like fingerprints and face ID are becoming popular options. Physical USB keys are also a great choice when available.

10. **Be cautious about using text or email for your 2FA.** Text message and email 2FA are better than no protection but might be intercepted through hacks like SIM swapping.

11. **Do not use public Wi-Fi without a virtual private network (VPN).** VPN products encrypt and anonymize your data so unwanted viewers cannot see it.

Source : https://www.kaspersky.com/resource-center/threats/how-to-stop-phone-hacking

HACKING THE SKILLS SHORTAGE

Every day we read of another company being hacked. Attacks outpace defense, and one reason for this is the lack of an adequate cybersecurity workforce. The cybersecurity workforce shortfall remains a critical vulnerability for companies and nations. Conventional education and policies cannot meet demand. New solutions are needed to build the cybersecurity workforce necessary in a networked world.

The deficit of cybersecurity talent is a challenge for every industry sector. The lack of trained personnel exacerbates the already difficult task of managing cybersecurity risks. McAfee's study quantifies the global cybersecurity workforce shortage and analyzes how companies and governments should approach cybersecurity workforce development to build a robust and sustainable pipeline of skills.

The continued skills shortage creates tangible risks to organizations, and companies say they have already incurred damages because of this workforce gap. Respondents say their organizations, unable to maintain adequate cybersecurity staff, have been targeted by hackers who suspect a shortage of cybersecurity skills at their organization. One in four respondents say their organizations have lost proprietary data because of their cybersecurity skills gap.

Has a shortage of cybersecurity skills had a negative effect on your organization?

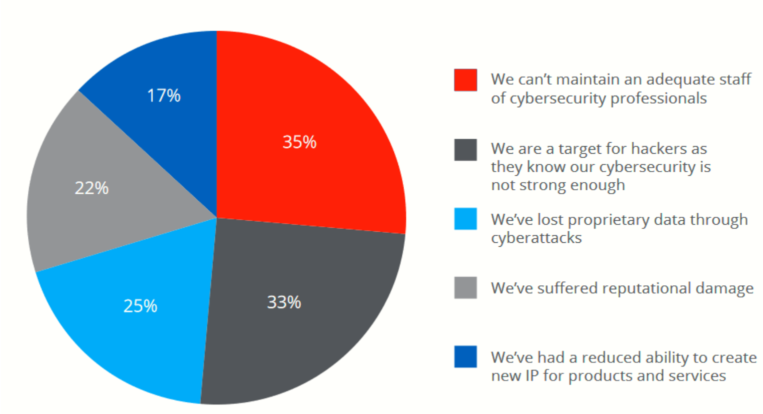


Figure 6: impact of cybersecurity workforce shortage.

Recommendations

Closing the gap in cybersecurity skills requires countries to develop critical technical skills, cultivate a larger and more diverse workforce, and reform education and training programs to include more hands-on learning. McAfee's study revealed that Australia, France, Germany, Israel, Japan, Mexico, UK, and the US face similar roadblocks to closing the skills gap, but each country also has distinct challenges.

Conclusion

A secure cybersecurity environment requires a robust workforce, yet currently there are not enough cybersecurity professionals to adequately defend computer networks. Countries and companies must act quickly to fix this problem by facilitating the entry of more people into this profession through improvements in education, workforce diversity, training opportunities, security technology, and data collection. These concurrent efforts are vital to defeating cybersecurity threats and creating a more secure network environment.

Source : https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

PROTECTING YOUR ACCOUNTS

A breached site is not always the cause for identity theft and account fraud. Sometimes the loss of information can also be attributed to individuals. Despite increased awareness and savviness of users, many still fall prey to classic phishing scams, done using different methods that range from email to malicious websites. Users are not entirely to blame; attackers are growing more sophisticated. Phishing scams are much more advanced, with scammers often impersonating legitimate companies and asking for login details or account credentials. There are also fake websites that ask for login details before allowing users to see certain content - something legitimate sites also do frequently. As users catch on to old tricks, scammers just make new ones.

Protecting your accounts:

1. Think before you click. Before you click on an email from an unknown source, before you link any social media account to a new game or app, or even before you sign in to any new site, make sure that it is legitimate. Cybercriminals often use clickbait to lure in users into giving up their credentials. Sporting events and other big events are a popular lure used to ask people to "sign-up" for free tickets or merchandise.

2. Keep updated. Update your OS and make sure you have the latest security patches. Weak or non-existent defence make it easier for malicious actors to steal vital information from your device.

3. Use 2FA. What have we learned from the breaches on sites such as Yahoo, LinkedIn, and Dropbox? That cybercriminals have proven to be successful at grabbing millions of usernames and passwords from popular sites. One way to protect your accounts is to enable the two-factor authentication option, a feature offered by a lot of popular sites and services. This feature requires two types of authentication for your online account, such as a password and a code sent via mobile, to make it hard for unauthorized parties to log on using stolen credentials.

4. Monitor your finances. Regularly check your billing statements to find out if your credit or debit card has been compromised. Keep an eye on your accounts and notify your bank quickly if you notice any suspicious activity.

5. Use unique passwords on different sites. This practice eliminates the danger of having stolen credentials from one account compromising your other accounts. Earlier this year, an online backup firm was targeted by attackers using credentials stolen from another site. Attackers assume users reuse passwords across multiple sites, so make sure you use strong and unique passwords for different accounts.

6. Keep separate emails for different purposes. Use separate emails for personal communication, work, and online entertainment. This way, if one email is compromised, attackers will have limited access to sensitive information and other accounts.

7. Get comprehensive protection. Effective and comprehensive security solutions can help you enjoy your digital life safely.

Source :https://www.trendmicro.com/vinfo/pl/security/news/online-privacy/ncsam-protecting-your-online-accounts

ANIMAL JAM – DATA BREACH

Figure 7: Animal Jam

The company behind the wildly popular kids' game Animal Jam has announced that hackers stole a menagerie of account records during a breach of a third-party vendor's server in October 2020 — more than 46 million of them, in fact.

The company, WildWorks, said that it was unaware that the data had been compromised, until 7 million records turned up on an underground forum used by malicious actors to distribute lifted data, on November 11, 2020.

The Animal Jam compromise

Hackers were able to obtain a key to a server database maintained by a third-party vendor that WildWorks uses for intra-company communication, according to the company. It did not name the vendor.

"We believe our vendor's server was compromised sometime between Oct. 10 and 12," the company said in a statement announcing the breach. "It was not apparent at the time that a database of account names was accessed because of the break-in, and all relevant systems were altered and secured against further intrusion. WildWorks learned of the database theft in Nov. 11, 2020, when security researchers monitoring a public hacker forum saw the data posted there and alerted us."

According to its own reporting, the company said that cybercriminals were able to steal 7 million parent account email addresses, and 32 million usernames associated with the parent accounts, containing encrypted passwords, players' birthdays, gender, and more.

"No real names of children were part of this breach," the company's site explained. "Billing name and billing address were included in 0.02 percent of the stolen records; otherwise no billing information was stolen, nor information that could potentially identify parents of players. All Animal Jam usernames are human-moderated to ensure they do not include a child's real name or other personally identifying information."

One way the cybercriminals may abuse this data is to carry out a phishing attack. Therefore, users, or their parents, need to watch out for any emails asking for personal information. It is important that the account password is changed immediately as well to avoid an account takeover. Passwords should also be changed across any other service where it might have been reused. The attackers might cross-reference your account information on other services to find other exploitable services.

Keeping connected toys and games safe

It raises the question as to how deeply embedded technology has become in all aspects of our lives, where even children's toys and games need accounts to be setup which potentially can hold sensitive information and make an attractive target to attackers. He suggested that a closer partnership between manufacturing and technology could help mitigate risks to kids and their data.

Not just in products but create to a culture of security that pushes good security practices to the forefront. While no one approach will be able to prevent all breaches, it is important that data is not collected unless necessary, and the data that is collected, is done for legitimate purposes, and secured properly.

Gaming, under fire from cybercriminals

The gaming industry overall has become an increasingly attractive target for attacks. In late October the game "Among Us" was hacked and rendered nearly unplayable for many, by what appeared to be a single malicious actor who got a thrill out of ruining the game for others.
Just a week earlier, a ransomware gang claimed to have accessed the source code for Watch Dogs: Legion, ahead of its release. Another title called Albion was similarly compromised and game databases released on underground forums.

The Ragnar Locker ransomware gang was able to gain access to 1 terabyte of sensitive data on the network of gaming giant Capcom, the company behind titles including Resident Evil, Street Fighter and others.

The gaming industry is a common target for attacks, be it data theft or ransomware attacks.
An interesting observation within the gaming industry is that player accounts are often high-value assets due to in-app purchases, or rewards from leveling up. In other words, gaming accounts are often seen as items for sale — at least accounts owned by adults spending money. However, we now have proof that even educational games for children are no longer safe and are valuable resources for bad actors.

Source : https://threatpost.com/animal-jam-hack-data-breach/161177/

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
Oracle - Solaris	Vulnerability in the Oracle Solaris product of Oracle Systems. Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris.	10/21/2020	10	CVE-2020-14871
Google - Chrome	Heap buffer overflow in UI in Google Chrome on Windows prior to 86.0.4240.183 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. 2	11/2/2020	10	CVE-2020-16011
IOS - WhatsApp	A use-after-free in a logging library in WhatsApp for iOS prior to v2.20.111 and WhatsApp Business for iOS prior to v2.20.111 could have resulted in memory corruption, crashes and potentially code execution	11/3/2020	10	CVE-2020-1909
Samsung - Mobile	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. Attackers can bypass Factory Reset Protection (FRP) via Secure Folder.	11/8/2020	9.8	CVE-2020-28340

Source, US-CERT: https://us-cert.cisa.gov/ncas/bulletins/sb20-272

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.

GDS
GLOBALCOM
DATA SERVICES