GDS
GLOBALCOM
DATA SERVICES

CYBERSECURITY BULLETIN

ISSUE 4

October 2020

WELCOME

Welcome to the fourth edition of GDS Cybersecurity bulletin.

One of the current US military doctrines addresses how to systematically evaluate the effects of significant characteristics of the operational environment for specific missions. Part of this doctrine is the Intelligence Preparation of the Battlefield (IPB). IPB is a critical component of the military decision-making process. It relies on threat intelligence sources (SIGINT, CYBINT, COMINT, ELINT) to build an understanding of the cyberthreats and counter them effectively.

Cybersecurity in the Enterprise is akin to that in the military: it is a battle scene in all senses of the word. Cyber Threat Intelligence is the basis of any solid cyber defence. Integrating Cyber Threat Intelligence into the security decision and platform at the level of the enterprise and using it to face future threats is basically conducting an IPB, just like the US military.

Ignoring Cyber Threat Intelligence, cybersecurity developments, news and risks lead you to missing important updates that could affect your business. So how do you stay up to date?

- Read blogs and online news on the topic of cyber security. Sign up for newsletters, threat bulletins and follow experts' Twitter accounts.
- Hire professional security engineers to keep you informed and protect your company.
- Get continuous updates from trusted network security providers. The security provider is an expert in developing highly effective defences for your network; you can trust them to offer solid advice and recommendations on potential and imminent threats.

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

CONTENTS

SUMMARY

What are the key components of a reliable Threat Intelligence source? What is the most prevalent threat seen during the last month? How to produce more secure code?

The next few pages answer these questions in addition to focusing on the increased threat trying to exploit the schools changing landscape with the massive reliance on remote classes as well as other topics relevant to students and the general public.

In today's cyber landscape, decision makers constantly question the value of their security investments, asking whether each dollar is helping secure the business. Meanwhile, cyber attackers are growing smarter and more capable every day. Today's security teams often find themselves falling behind, left to analyse artifacts from the past to try to determine the future. As organizations work to bridge this gap, threat intelligence (TI) is growing in popularity, usefulness and applicability.

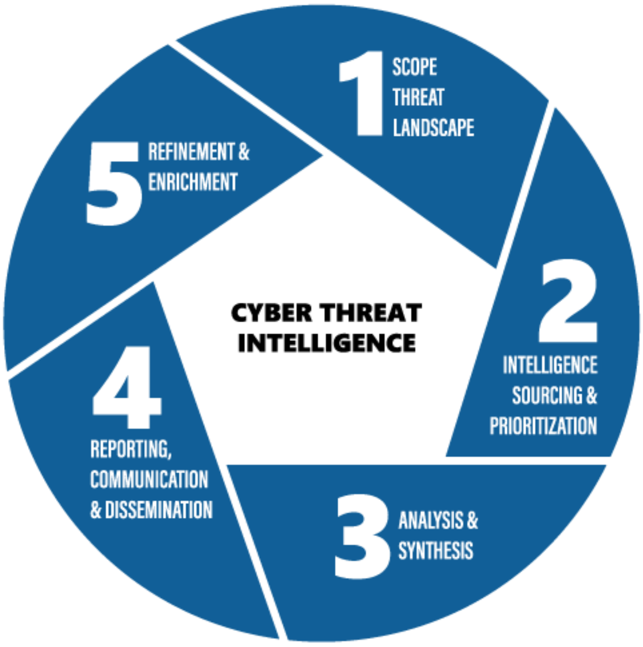

CYBER THREAT INTELLIGENCE
1 SCOPE THREAT LANDSCAPE
2 INTELLIGENCE SOURCING & PRIORITIZATION
3 ANALYSIS & SYNTHESIS
4 REPORTING, COMMUNICATION & DISSEMINATION
5 REFINEMENT & ENRICHMENT

Figure 1: Revolutionary Security 5 key components of Cyber Threat Intelligence

Components of Cyber Threat Intelligence

1. Threat landscape scoping – Define priority intelligence requirements, threat categories and integrate a framework for industry-specific threats.
2. Intelligence sourcing & prioritization – Identify and prioritize intelligence sources, establish intelligence intake and processing approach, and establish operational processes.
3. Data analysis & synthesis – Include intelligence analysis and value extraction, integration into the security technology stack, proactive network hunting, and a proactive mitigation model. Here comes the value of a well-trained & experienced dedicated team to assist in the process of data analysis to minimize the false positives & ensure the data sent to customers is actionable.
4. Reporting, communication and dissemination – Establish an enterprise-wide communication campaign, intelligence reporting for awareness and response, and intelligence dissemination according to the organization's functional needs.
5. Refinement & enrichment – Establish a continuous improvement program with a focus on enriching operational capabilities, improving business value and justifying the value of the CTI.

Naming of the components can be different, but it all comes down to the fact that the CTI organization you subscribe to has an adequate and well-experienced team to refine and correlate data on your behalf for better detection.

GDS HONEYPOT RDP SCANS

For connecting to remote systems, Remote Desktop Protocol (RDP) is one of the most ubiquitous technologies used today. There are millions of systems with RDP ports exposed online, which makes RDP a massive attack vector among ransomware operators.

- At first, attackers use open source port-scanning tools to scan for exposed RDP ports online and then try gaining access to a system using brute-force tools or stolen credentials purchased from black markets.
- Once the attackers gain access to the target system, they make the network vulnerable by deleting backups, disabling antivirus software, or changing configuration settings.
- After disabling the security systems and making the network vulnerable, attackers deliver malware payloads. The process involves installing ransomware, using infected machines to distribute spam, deploying keyloggers, or installing backdoors to be used for future attacks.

GDS honeypot solution detected several malicious IP addresses trying to search for workstations/servers having remote desktop protocol enabled on them.
You can find in Figure 2 some of the IP addresses related to this attack.

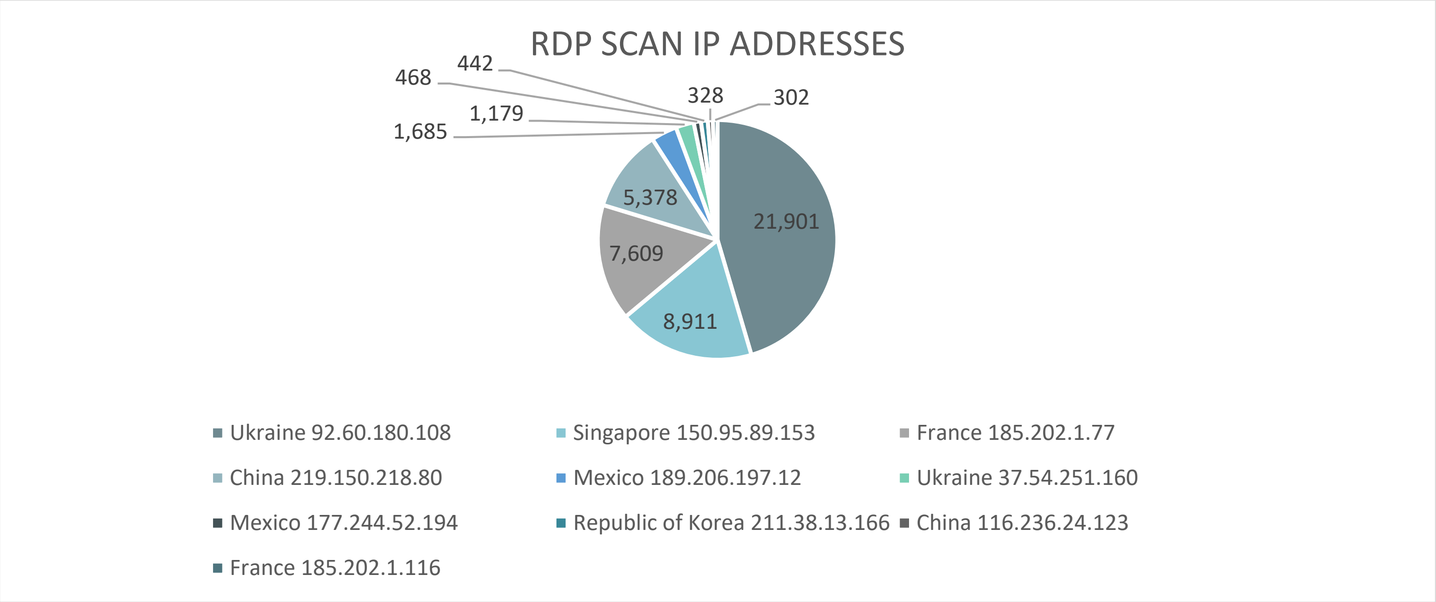


Figure 1: RDP Scan IP addresses attempts

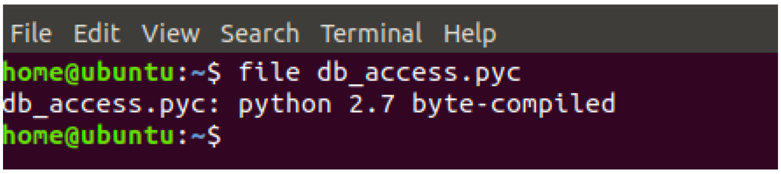
GDS SOC recommends that you mark those IP addresses below on your watch list:

IP Address	Count
92.60.180.108	21,901
150.95.89.153	8,911
185.202.1.77	7,609
219.150.218.80	5,378
189.206.197.12	1,685
37.54.251.160	1,179
177.244.52.194	468
211.38.13.166	442
116.236.24.123	328
185.202.1.116	302

GDS DevSecOps

GDS SOC team discovered a new file belonging to the super-secret company that developed a “supersecretprogram” analysed in the “Cybersecurity Bulletin Issue 3”. This time the file is called “db_access.pyc”; we will venture into further discovering the company’s assets.

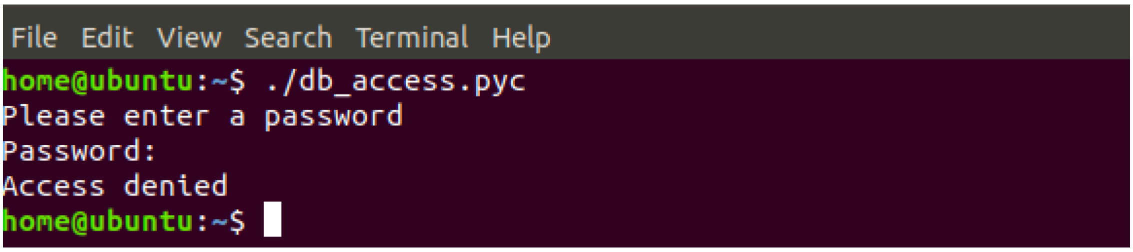
The exploit attempt starts by exploring the type of the file being dealt with. In this case, it is a python-compiled code. Below is the output showing the results of the execution: “Access Denied”.



```
home@ubuntu:~$ file db_access.pyc
db_access.pyc: python 2.7 byte-compiled
home@ubuntu:~$
```

Figure 2: db_access.pyc

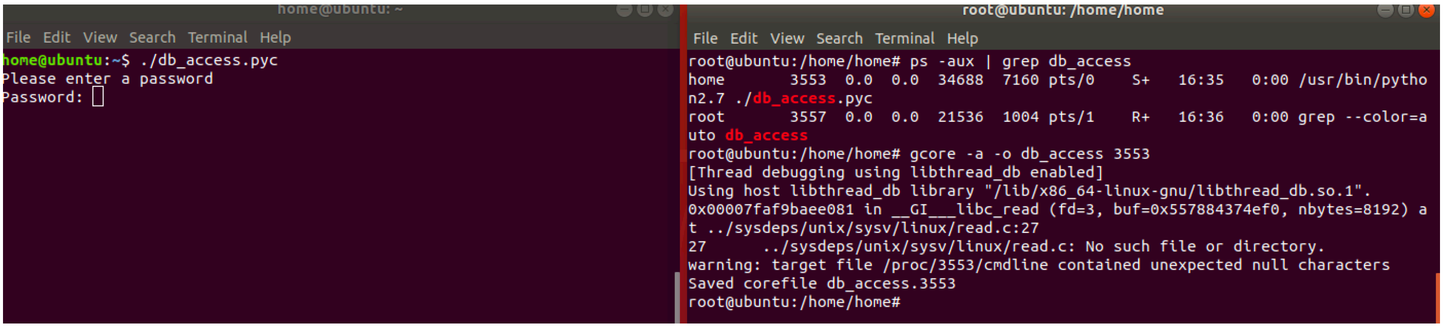
Given that the file can be easily decompiled and brought back to its source code, we will trust that “super-secret company” have made de-compilation hard by obfuscating the source code.
Next step is to try executing the program and see what that does.



```
home@ubuntu:~$ ./db_access.pyc
Please enter a password
Password:
Access denied
home@ubuntu:~$
```

Figure 3: Run db_access.pyc

The program asked for a password and we entered a random one which gave us an “access denied” error.
Next is to try to dump the process’ memory; this technique is used to physically extract whatever there is in memory for the process including all the strings, variables and other important data used in memory to speed execution. We first get the PID of the process then use “gcore” command that will dump the whole memory block of the identified process.

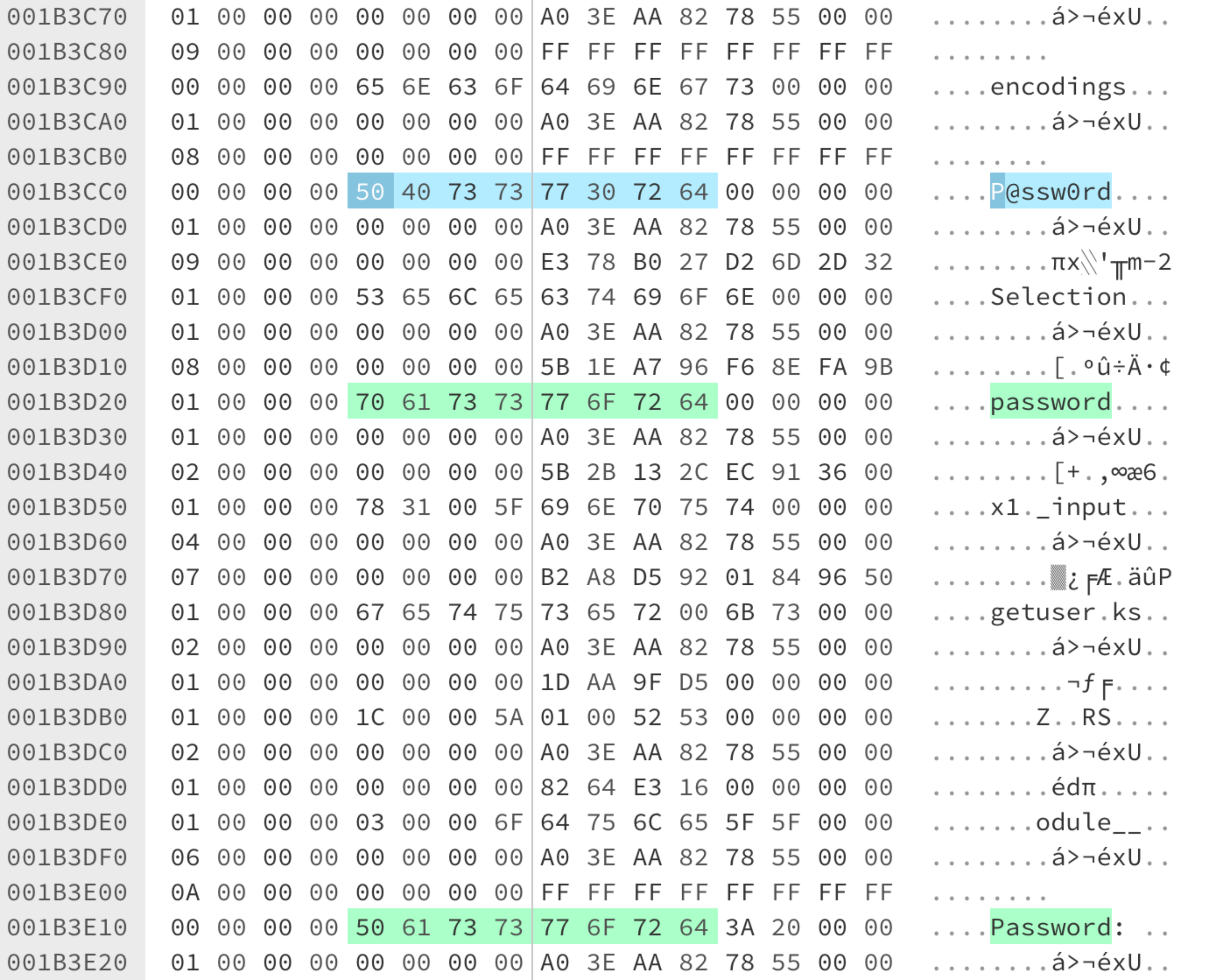

home@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu: /home/home
File Edit View Search Terminal Help

```
home@ubuntu:~$ ./db_access.pyc
Please enter a password
Password:
```

```
root@ubuntu:/home/home# ps -aux | grep db_access
home        3553  0.0  0.0  34688  7160 pts/0    S+   16:35   0:00 /usr/bin/pytho
n2.7 ./db_access.pyc
root        3557  0.0  0.0  21536  1004 pts/1    R+   16:36   0:00 grep --color=a
uto db_access
root@ubuntu:/home/home# gcore -a -o db_access 3553
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
0x00007faf9baee081 in __GI___libc_read (fd=3, buf=0x557884374ef0, nbytes=8192) a
t ../sysdeps/unix/sysv/linux/read.c:27
27      ../sysdeps/unix/sysv/linux/read.c: No such file or directory.
warning: target file /proc/3553/cmdline contained unexpected null characters
Saved corefile db_access.3553
root@ubuntu:/home/home#
```

Figure 4: Dump process memory

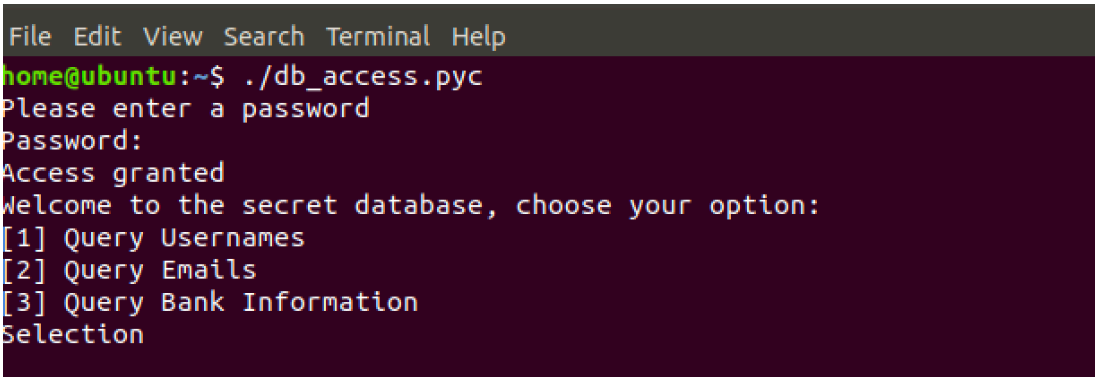
“gcore” command give us an output “db_access.3553” which is a raw memory dump of the process. Opening this file with a simple HEX editor allows us to find important strings and variables that are being used in memory.



```
001B3C70  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3C80  09 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ........
001B3C90  00 00 00 00 65 6E 63 6F 64 69 6E 67 73 00 00 00  ....encodings...
001B3CA0  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3CB0  08 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ........
001B3CC0  00 00 00 00 50 40 73 73 77 30 72 64 00 00 00 00  ....P@ssw0rd....
001B3CD0  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3CE0  09 00 00 00 00 00 00 00 E3 78 B0 27 D2 6D 2D 32  ........πx▒'╥m-2
001B3CF0  01 00 00 00 53 65 6C 65 63 74 69 6F 6E 00 00 00  ....Selection...
001B3D00  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3D10  08 00 00 00 00 00 00 00 5B 1E A7 96 F6 8E FA 9B  ........[.ºû÷Ä·¢
001B3D20  01 00 00 00 70 61 73 73 77 6F 72 64 00 00 00 00  ....password....
001B3D30  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3D40  02 00 00 00 00 00 00 00 5B 2B 13 2C EC 91 36 00  ........[+.,∞æ6.
001B3D50  01 00 00 00 78 31 00 5F 69 6E 70 75 74 00 00 00  ....x1._input...
001B3D60  04 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3D70  07 00 00 00 00 00 00 00 B2 A8 D5 92 01 84 96 50  ........▒¿╒Æ.äûP
001B3D80  01 00 00 00 67 65 74 75 73 65 72 00 6B 73 00 00  ....getuser.ks..
001B3D90  02 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3DA0  01 00 00 00 00 00 00 00 1D AA 9F D5 00 00 00 00  .........¬ƒ╒....
001B3DB0  01 00 00 00 1C 00 00 5A 01 00 52 53 00 00 00 00  .......Z..RS....
001B3DC0  02 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3DD0  01 00 00 00 00 00 00 00 82 64 E3 16 00 00 00 00  ........édπ.....
001B3DE0  01 00 00 00 03 00 00 6F 64 75 6C 65 5F 5F 00 00  .......odule__..
001B3DF0  06 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
001B3E00  0A 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ........
001B3E10  00 00 00 00 50 61 73 73 77 6F 72 64 3A 20 00 00  ....Password: ..
001B3E20  01 00 00 00 00 00 00 00 A0 3E AA 82 78 55 00 00  ........á>¬éxU..
```

Figure 5: Open raw memory dump in HEX editor

We start by searching for "password" strings: many are found. Going through them one by one leads to the value "password" written with character substitution (P@ssw0rd) that might be the actual password of the program. Trying it results in the following output.



```
home@ubuntu:~$ ./db_access.pyc
Please enter a password
Password:
Access granted
Welcome to the secret database, choose your option:
[1] Query Usernames
[2] Query Emails
[3] Query Bank Information
Selection
```

Figure 6: Gaining Access

Success, access has been granted and password was found successfully. We now have access to internal company information.

"super-secret company" has clearly failed to develop its programs securely. What security advice can be gleaned from this use case?

- Choice of the development language in the first stages of the process is essential. The end product always justifies the choice. If, for example, the target is to develop a small and fast program to get a simple task done without including security risks, most organisations would go to Python as it provides simple ways to get things done. On the other hand, Python code doesn’t have access to memory so attackers can leverage this weakness to find and exploit vulnerabilities left behind by the code in memory. That doesn’t mean that choosing other programming languages like “C” is secure by default, but a language with low-level access to memory gives control over what is happening in memory.
- Again, like with the use case of “supersecretprogram”, using a variable named “password” to point to passwords makes life easier for hackers to guess the location of the variable itself. Non-descript variable names, while they may not stop serious hackers, could stop or slow scipt-kiddies.
- The programmer did not encrypt the passwords, and this is a fatal error that lots of experienced and non-experienced developers do. Encrypting the password and chunking it into parts adds another, strong, security layer.
- Letter substitution is a viable strategy for getting stronger passwords if carefully implemented. ”P@ssw0rd” instead of “password” is not an example to follow as the initial word is still recognisable. The rationale behind letter substitution in passwords is to make them a little more difficult for brute-force/dictionary attacks while keeping it possible for users to remember them. However, a better level of security can be reached by combining letter substitution with sentences instead of words followed by condensing such sentences. The value of the password would become unrecognisable in memory if stored in clear and would not be vulnerable to dictionary attacks and its variants.

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

GDS 0-DAY ATTACK ANALYSIS

GDS SOC has lately encountered a sophisticated piece of malware executed by a customer that was a social engineering attack text-book example. GDS SOC team went through the steps and measures taken from the initial file download till the detection, monitoring and remediation.

Attack Path Analysis

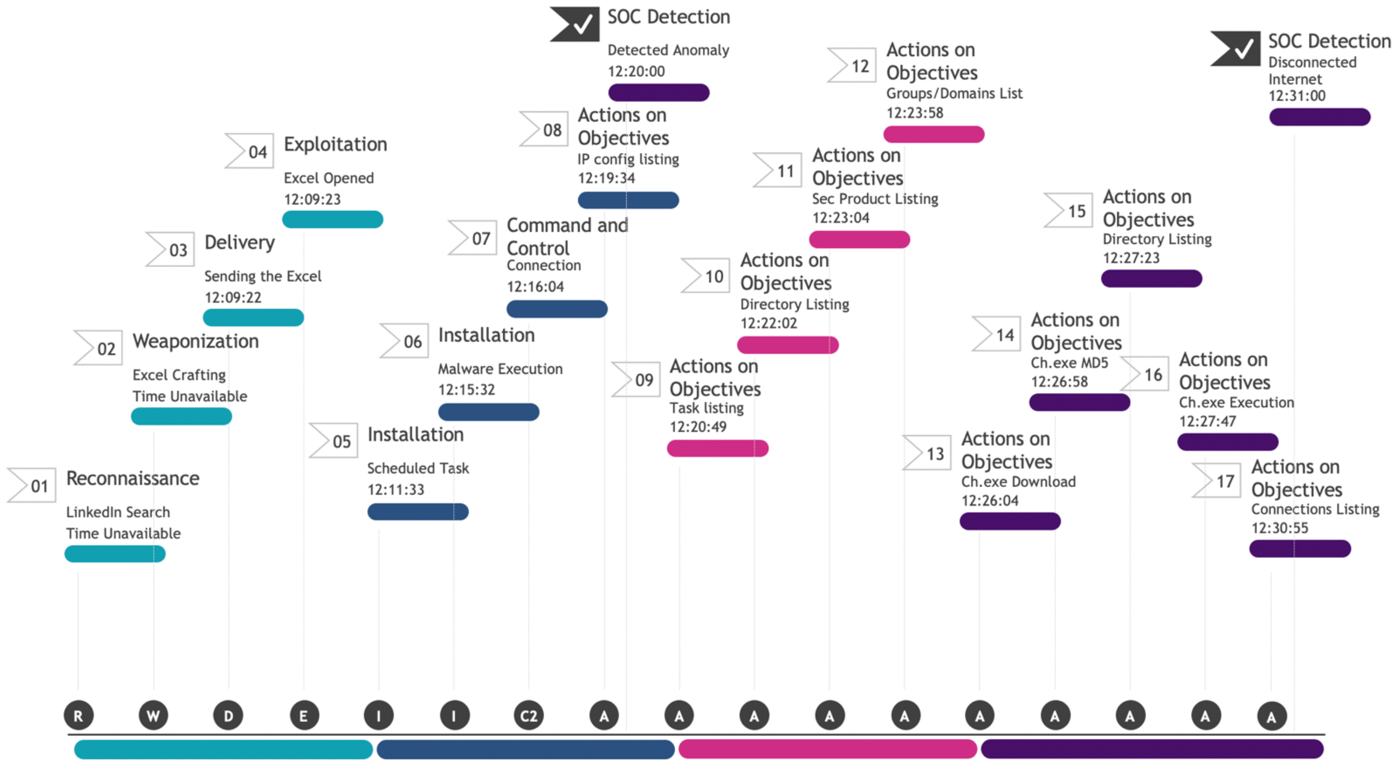


Figure 7: Attack Path Timeline

Timeline Analysis

- The first 3 steps of the attack path were identified as a discovery time at first; then GDS SOC identified the Delivery time after the analysis of the whole incident.
- The SOC system autonomously detected an anomaly based on the steps done in 5,6,7 & 8. GDS' AV and IP-based threat intelligence were not able to detect the file nor the IP at that time because they were 0-days.
- After detecting an anomaly, the SOC team isolated the PC and let the attacker continue working on the compromised PC. This decision was taken to leave the flow of the attack ongoing and capture more data.
- After the attacker downloaded the executable and executed a local reconnaissance, GDS SOC decided to shut down the internet from the PC as enough information had already been collected to start the analysis.

It was identified that the attack belonged to an APT that was targeting the Middle East. The SOC team immediately identified the malicious activity and started the mitigation process. It is important correlate the malicious events with stages of attacks to better understand where the weaknesses are and apply proper fixes to further empower the detection/mitigation speed of the SOC team.

EDUCATION SYSTEM - RANSOMWARE

A slew of ransomware attacks and other cyberthreats have plagued back-to-school plans adding to the stress already facing administrators due to the pandemic. Security researchers point to this increase in incidents as a sign that this year, cyberattacks may likely become the new "snow day" – particularly with the advent of pandemic-driven online learning. As students prepare to return to school, whether in-person or virtually, school districts are battling a slew of ransomware, phishing and virtual classroom hijacking attacks.

A cyberattack, earlier in July, on the Athens school district in Texas USA led to schools being delayed by a week (and the district paying attackers a $50,000 ransom in exchange for a decryption key).

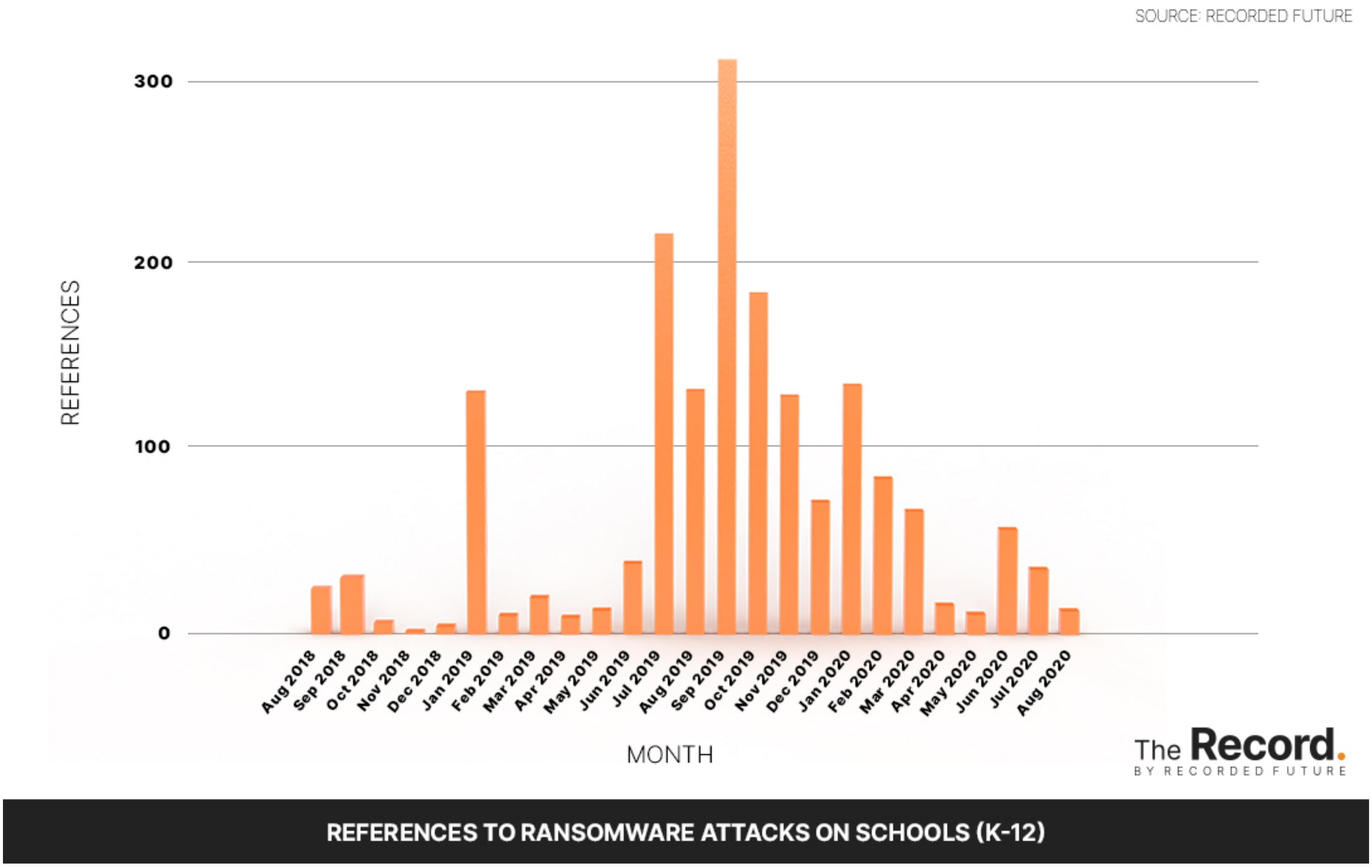


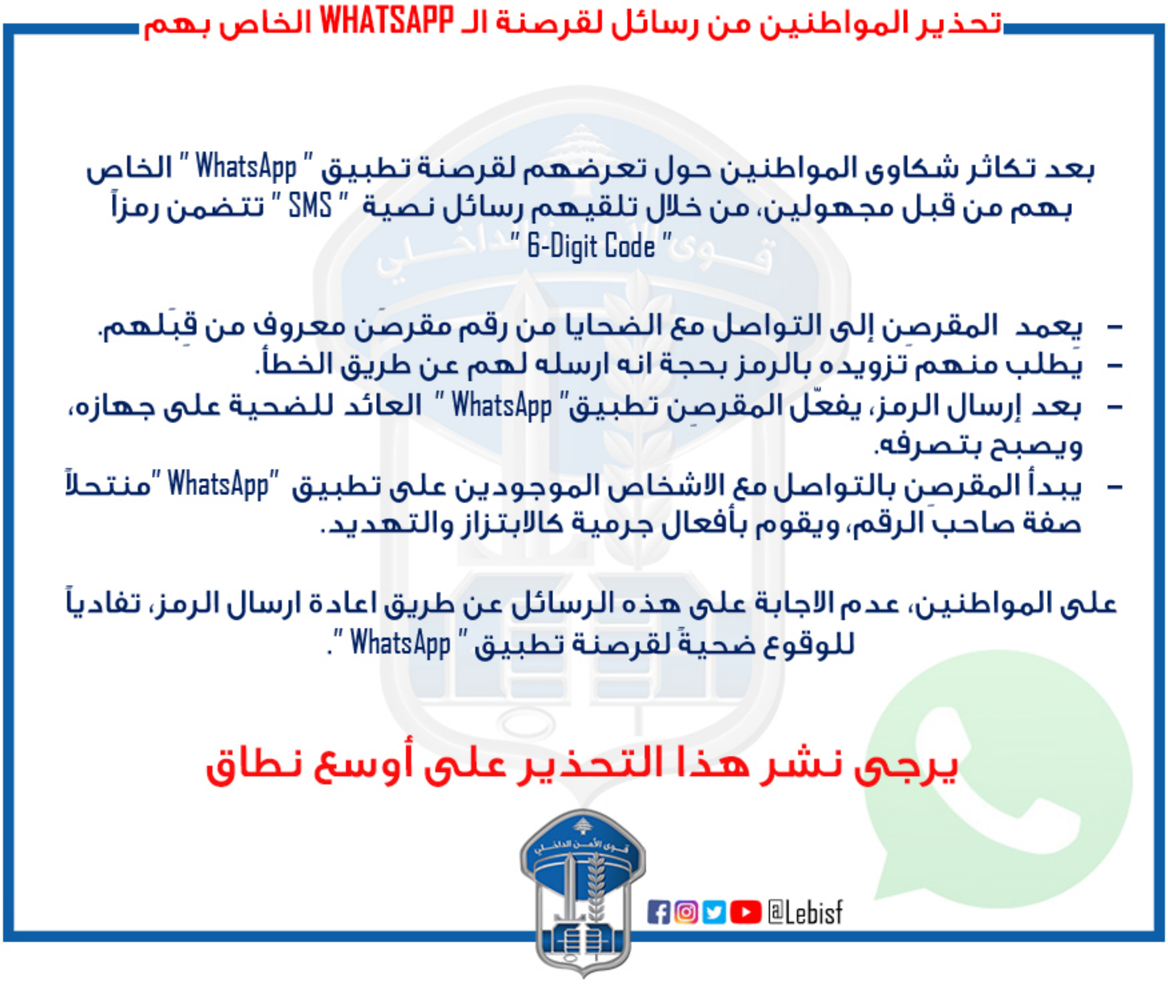
Figure 8: Recorded Future statistics on ransomware from 2018-2020

Figure 9 depicts the spike in attacks on education systems between September & October which is the usual opening date for schools worldwide. During that period, the education system is at its most vulnerable as attackers exploit the fact that schools need to open, and they might see paying for a ransomware as being a lesser evil than a delay and disruption to the school year.

There were no pandemics in 2019, yet there was a spike in ransomware attacks. This gives an insight of what will come in the next few months given the fact that new technologies are being integrated in the schooling system to support remote learning and other processes.

THREAT SUMMARY – WhatsApp Hijacking

Usage of messaging applications has soared through isolation and the information overload that has accompanied the coronavirus pandemic. And no platform has seen a greater surge in messaging than market leader WhatsApp – usage is up by more than 40% across the world, and in some markets even more than that. It is now clear that the unprecedented public health emergency the world is going through has also seen a surge in cybercrime. Every imaginable scam, from phishing to malware, and from delivery hijacks to counterfeits, has grown exponentially in recent weeks. It's a trend that shows no signs of abating. So it doesn't come as a little surprise that an alarming WhatsApp hack that has been going around for a year is now back and experiencing a new surge. The bad news is that this hack is simple for a cybercriminal to execute, and people are falling for it in their droves. The good news is that the fix is guaranteed to remediate the vulnerability and will take a few minutes to implement.



تحذير المواطنين من رسائل لقرصنة الـ WHATSAPP الخاص بهم

بعد تكاثر شكاوى المواطنين حول تعرضهم لقرصنة تطبيق " WhatsApp " الخاص بهم من قبل مجهولين، من خلال تلقيهم رسائل نصية " SMS " تتضمن رمزاً " 6-Digit Code "

- يعمد المقرصِن إلى التواصل مع الضحايا من رقم مقرصَن معروف من قِبَلهم.
- يطلب منهم تزويده بالرمز بحجة انه ارسله لهم عن طريق الخطأ.
- بعد إرسال الرمز، يفعّل المقرصِن تطبيق" WhatsApp " العائد للضحية على جهازه، ويصبح بتصرفه.
- يبدأ المقرصِن بالتواصل مع الاشخاص الموجودين على تطبيق "WhatsApp" منتحلاً صفة صاحب الرقم، ويقوم بأفعال جرمية كالابتزاز والتهديد.

على المواطنين، عدم الاجابة على هذه الرسائل عن طريق اعادة ارسال الرمز، تفادياً للوقوع ضحيةً لقرصنة تطبيق " WhatsApp ".

يرجى نشر هذا التحذير على أوسع نطاق

@Lebisf

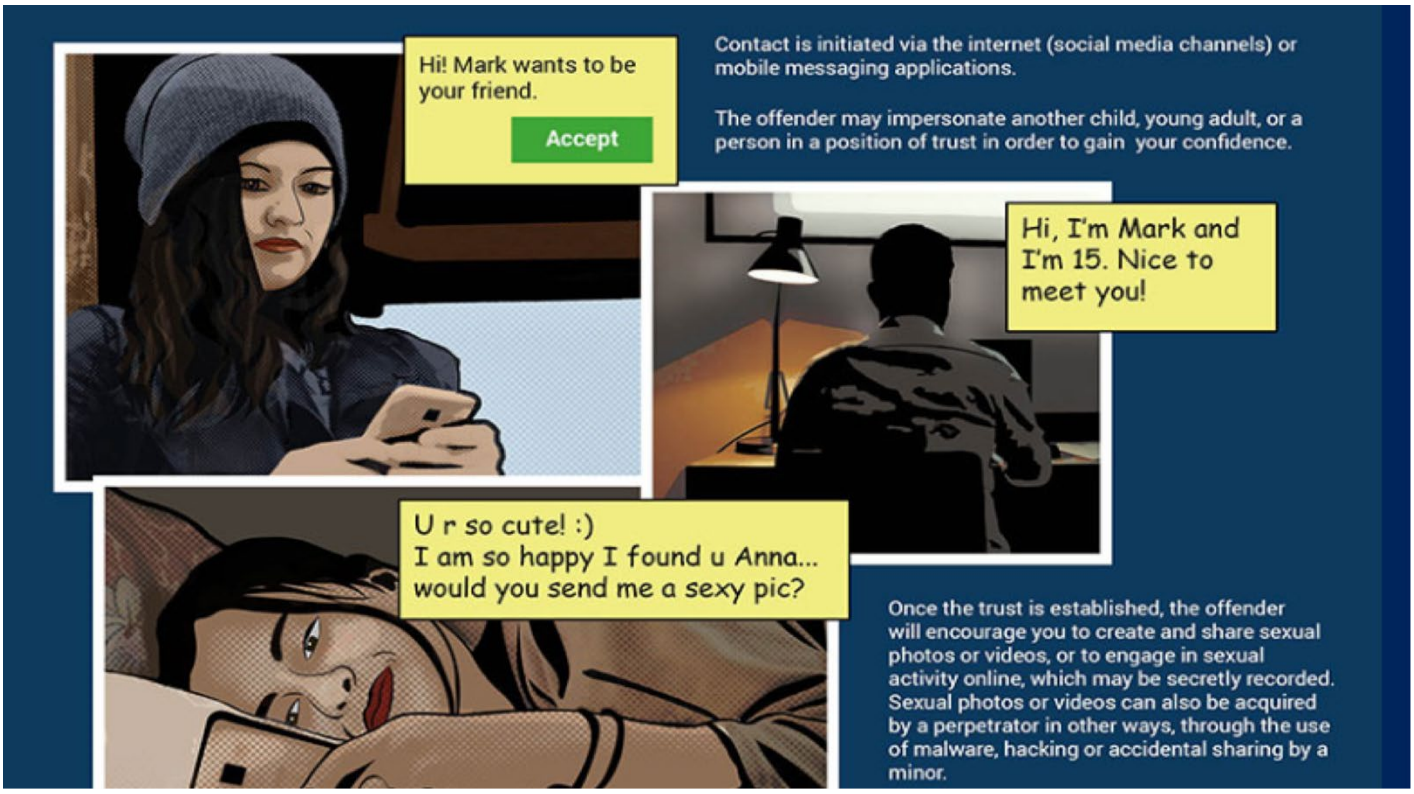
Figure 10: Internal Security Forces warning people not to fall to the scam

Mitigation

Enable two-step verification by following the steps mentioned on
https://faq.whatsapp.com/general/verification/using-two-step-verification/?lang=en

THREAT SUMMARY: Rise in sexual abuse crimes

The offence of sextortion consists of blackmailing and extorting sexual or monetary favours via the Internet from people whose compromising images or videos fall in the wrong hands. Sextortion is often called webcam blackmail. Sextortion is the main cause of complaints to police cybercrime units in most West African countries. Cyber-investigation makes it possible to combat this new form of crime. Crimes such as online fraud, extortion and online sexual abuse of children that target individuals, and the use of ransom software to compromise systems - including hospitals, are on the rise, especially since the beginning of the COVID-19 pandemic.


Hi! Mark wants to be your friend.
Accept
Hi, I'm Mark and I'm 15. Nice to meet you!
U r so cute! :) I am so happy I found u Anna... would you send me a sexy pic?

Contact is initiated via the internet (social media channels) or mobile messaging applications.

The offender may impersonate another child, young adult, or a person in a position of trust in order to gain your confidence.

Once the trust is established, the offender will encourage you to create and share sexual photos or videos, or to engage in sexual activity online, which may be secretly recorded. Sexual photos or videos can also be acquired by a perpetrator in other ways, through the use of malware, hacking or accidental sharing by a minor.

Figure 11: UNODC Sextortion Cyber Crime

What should you do if you are a victim of sextortion?

- Contact your local police and Internet Service Provider immediately. Stop communicating with criminals. Take screenshots of all your communications. "The Internal Security Forces will always maintain complete confidentiality in dealing with cybercrime investigations and will make every effort to help you solve the problem you are facing" (www.isf.gov.lb/en/cybersecurity).
- Prevention is the best way to avoid sextortion altogether. Never take, store or send explicit images or videos because there is no way of knowing where these might end up. Educating people about Internet safety is essential to prevent them from becoming victims.

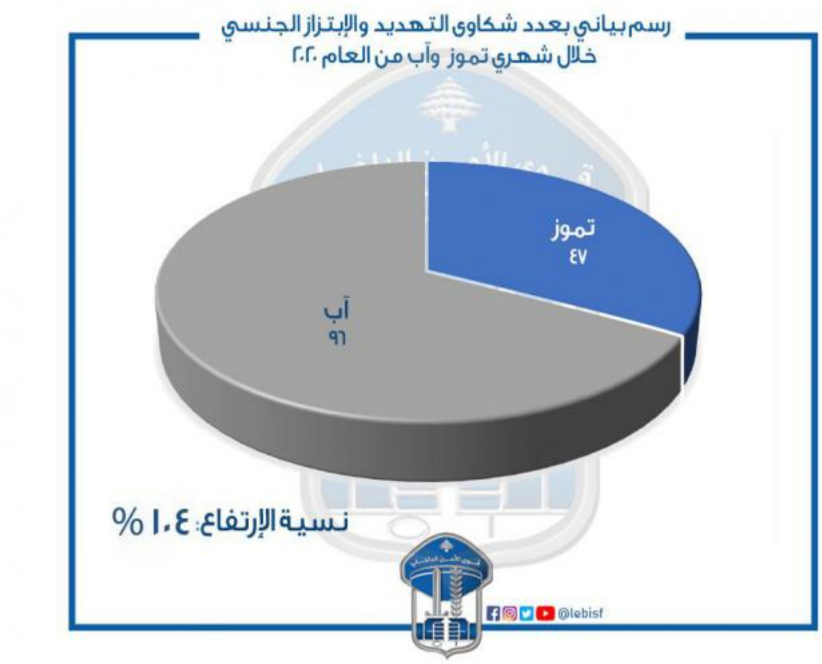


Figure 12: Internal Security Forces rise in Sextortion cases

How to protect children online

- Use parental controls.
- Do not let children use unprotected devices when they are alone.
- Monitor their online activity.
- Don't give them their own appliances, or if you do, don't let them lock you out of the appliances.
- Familiarize yourself with the applications or social networks your children use and be friends with them on social networks.

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
Google - Android	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-143604331	2020-09-18	7.5	CVE-2020-0354 PATCH
Google - Chrome	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-09-21	9.3	CVE-2020-6549 PATCH
Google - Chrome	Use after free in IndexedDB in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-09-21	9.3	CVE-2020-6550 PATCH
Google - Chrome	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2020-09-21	9.3	CVE-2020-6548 PATCH

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