GLOBALCOM
DATA SERVICES

# CYBERSECURITY BULLETIN
# ISSUE 8
# February 2021

## WELCOME

Welcome to the eighth edition of GDS Cybersecurity bulletin.

A poll conducted in 2021 amongst C-suite executives showed that they strongly intend to invest in advanced technologies driven by regulations and increased awareness. Several cybersecurity prediction reports concur in outlining the most prevalent cyberthreats that will play out in 2021.

So, what are these latest threats that targeted our customers during the last month and will continue to appear in 2021? And what should be our main security focus to reduce the damages and impact on the organizations in the coming year?

GDS will provide few insights regarding actionable security plan to fight against the rise of critical threats.

## CONTENTS




**SUMMARY**

"Cybercrime is constantly evolving. The COVID-19 pandemic has accelerated digital transformation, which has opened new opportunities for cybercriminals," said Craig Jones, INTERPOL's Director of Cybercrime.

In this report, we will provide overview about few threats that are expected to grow in 2021 along with actionable solutions.

# CYBERSECURITY TRENDS IN 2021

The latest changes around the world such as remote working, online education and 5G deployment increased the vulnerabilities and methods for malicious intruders to illegitimately access network.

So, what are the expected cyber security problems that would result from those changes and what would be the right responses to them? On which security risks should one focus in 2021?

## Fileless malware

It is a type of malicious software different from conventional threat malwares and is difficult to detect because it is memory-based instead of being file-based. Traditional malwares are usually executed through malicious files installed on the target computer and saved on the disk. Fileless malware, on the other hand, can infiltrate a device by executing malicious activity using legitimate software or tools and is written in RAM, making it difficult to detect using traditional antiviruses.

There are three types of fileless malware attacks:

- **Windows registry manipulation:** uses Windows processes to write and execute fileless code into the registry. Example: Kovter and Powelike which transform a system to a click-bot connecting with websites and click through-ads.
- **Memory code injection:** hides malicious code in the memory of legitimate applications like PowerShell. The commands executed by these programs are usually assumed to be safe.
- **Script-based techniques:** based on scripts that use the above techniques and is not completely fileless. Example: SamSam ransomware and Operation Cobalt Kitty.

To protect the organizations against fileless malware, it is important to deploy an Endpoint Detection and Response (EDR) solution which relies on continuous real time monitoring of emails, incoming and outgoing network traffic and unwanted tasks in operations like PowerShell.

In addition, the integration of EDR with an advanced SIEM solution that includes behaviour analysis, will give the security teams visibility on what triggered the chain of malicious events from the beginning. The flexibility of integrating GDS SIEM with any EDR solutions for correlation with other events is of high demand to fight against the rise of these type of threats.

## DDOS Attacks

The deployment of faster internet connections through 5G or fibre technologies makes it possible to easily perform DDOS attacks leading to high impact on the targeted organizations.
GDS Arbor solution, implemented in GDS data centre to protect customers from volumetric and slow and low attacks, shows the number and size of attacks along any given month, as depicted in figure 1.

GDS recommends the deployment of a DDOS solution to protect your network . A good DDOS solution should mainly include the below features:

- Ability to optimize the filtering rules that clean bad traffic on the scrubbing devices.
- Full visibility about the type of traffic flow and DDOS attacks targeting your subnets.
- Support for slow and low attacks mitigation.
- Duration of the detection time for DDOS attacks should be less than 1 minute.

- Automatic trigger for the attack mitigation process to reduce the impact of complete failure during attack occurrence.

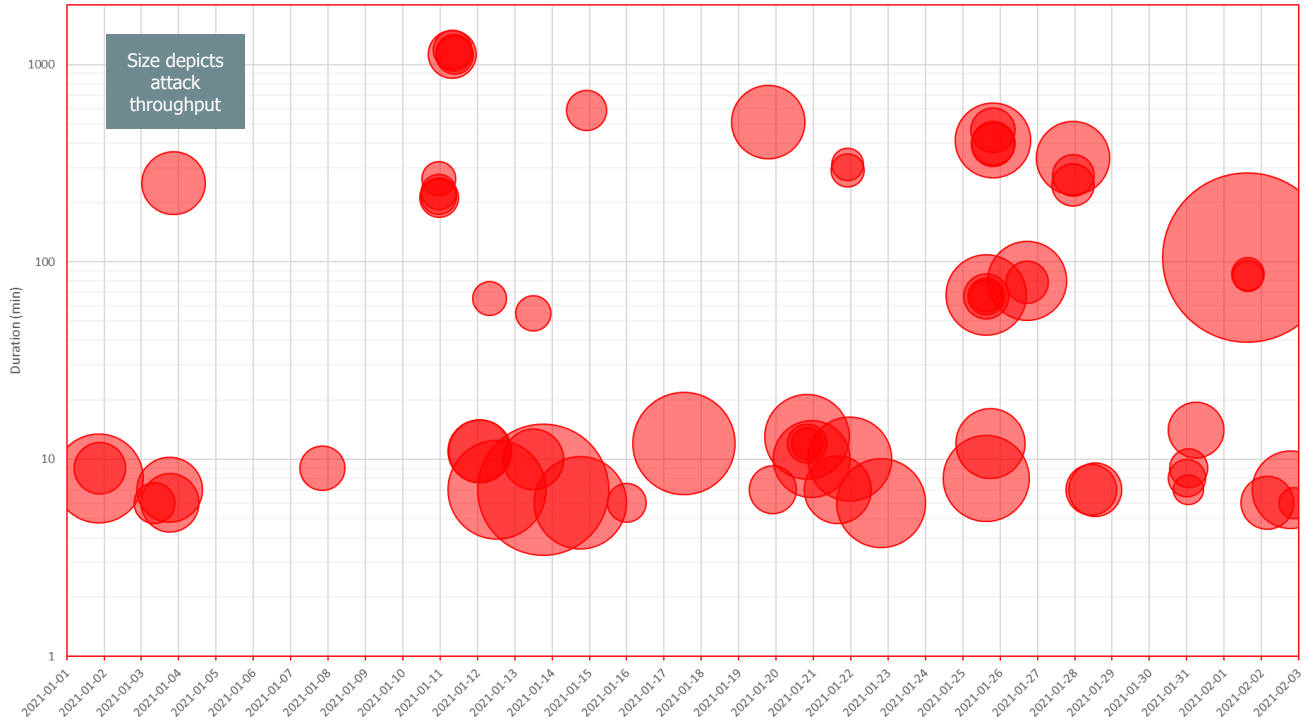


*Figure 1 - DDoS attacks detected by GDS*

## Data Breach

Due to the change in work locations and the transition to a work from home model, the number of vulnerabilities exploitable by attackers has drastically increased and will continue to do so in 2021, allowing the attackers to benefit from this situation to target sensitive data.

According to Forrester, *remote work will lead to an increase of insider threats, that were at around 25% in 2020 of the total security incidents affecting an organisation, to reach 33% in 2021.*

In addition, based on the latest reports of Risk Based Security, *unauthorized access to systems and networks (shown in Figure 2 as "Hack" in the chart) is responsible for 64% of all reported breaches.*

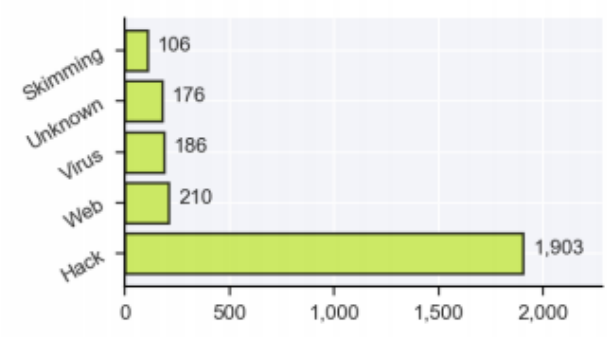


*Figure 2: Number of breaches by breach type reported in Q3,2020.*

The most suitable solution for protecting critical data is Privileged Access Management. Authorized accounts accessing digital assets should be controlled.

GDS can provide professional services and guidance for implementing the proper solution based on an organisation's specific needs and supporting the below features:

- Session management to control the relevant sessions.
- Password management and control which verifies authorized access and controls the access.
- Multi-factor authentication to verify the user privileges and corelate with other parameters like time.
- Session and access recording.

Reference: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf

## Ransomware Attacks

According to the latest security reports, ransomware attacks increased sevenfold in 2020 compared to the previous year and it will continue increasing in 2021.
These attacks use tailored pretexts to trick targets, enabling the infection and encryption of endpoints, and spread across the network costing organizations millions of dollars in damages.

So how can these attacks be prevented?

- Increase user awareness since ransomware attacks are usually spread through phishing emails and social engineering.
- Perform automated backup. Usually, the ransomware forces the targets to pay a ransom in order regain access to the encrypted files. If the files were saved to another location, the risk will be reduced.
- Enforce patch management and keep the operating system, vulnerabilities, antivirus, and applications patched.
- Set a proper incident response plan whenever a ransomware attack is detected including the following actions:
  1- Quarantine the affected systems to avoid spreading the threats over the network.
  2- Notify the incident response team to perform malware analysis.
  3- Do not restart the computer since some ransomwares encrypt critical file systems. So, the systems may not power back.
  4- Make a copy of the infected drive since during the decryption process, the files could be damaged.
  5- Restore the systems from clean version and clean backup files because in some cases the ransomware may have persistent mechanisms that are difficult to remove without a full format.

GDS SOC team is ready to assist in performing a full data recovery of the infected system through the digital forensics service.

# LATEST THREATS

GDS SOC team is performing continuous research about the latest threats and IOCs to be able to integrate with our monitoring tools and inform the impacted customers.

During the last months, the IOCs of the below attacks were monitored:

- **SolarWinds attacks** – detailed in our previous releases.

- **Emotet-101**
  It is a computer malware program that was originally developed in the form of a banking trojan. The goal was to access foreign devices and spy on sensitive private data. It is known to deceive

basic antivirus programs and hide from them. Once infected, the malware spreads like a computer worm and attempts to infiltrate other computers in the network.
It sends phishing emails to stored contacts like, friends, family members, and work colleagues. Most of the time, the emails contain an infected Word document that the recipient is supposed to download, or a dangerous link. The correct name is always displayed as the sender so that the recipients think the email is safe: everything looks like a legitimate email. Recipients then (in most cases) click on the dangerous link or download the infected attachment.

Europol announced end of January 2021 that, as part of an operation dubbed Ladybird, European authorities seized control of the EMOTET malware. As part of the information collected after seizing the malware infrastructure, Europol grabbed millions of email addresses that are affected by it.

To assess if you are impacted by this malware use the email checker in the below website: https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html

- **Lebanese Cedar APT**
  The group's main attack vector is through an intrusion into Oracle and Atlassian Web servers. In early 2020, suspicious network activities and hacking tools were found in a range of companies. Comprehensive forensic research of the infected systems revealed a strong connection to Lebanese Cedar and a new version of the "Explosive" V4 RAT (Remote Access Tool) or "Caterpillar" V2 WebShell was found within the victims' networks.

Our monitoring tools on the border router during the last 2 months showed that 25 corporate customers are affected by Cedar APT, 24 by SolarWinds and 12 by Emotet.

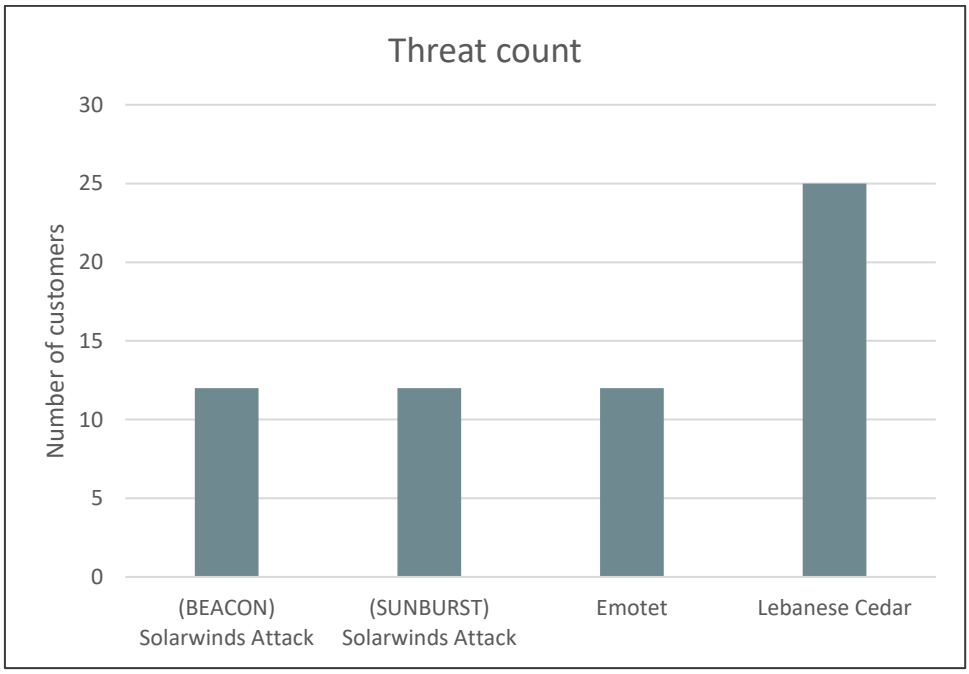


*Figure 3: Corporate customer count per threats.*

GDS is ready to assist you in performing investigations in your network and implementing of the required protection rules.

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.