GLOBALCOM
DATA SERVICES

CYBERSECURITY BULLETIN

ISSUE 9

March 2021

WELCOME

Welcome to the ninth edition of GDS Cybersecurity bulletin.

A cyber security strategy that puts proactiveness at the forefront of security measures is fundamental to anticipating and fending-off threats instead of reacting to them after the damage is done, which can be expensive and time consuming.

In this newsletter, we will tackle three security aspects that often require strengthening.

CONTENTS

SUMMARY

An increasing number of cybersecurity threats start with a phishing email, which allows access to a target infrastructure by exploiting weak systems with non-patched vulnerabilities or through key theft.

In this report, we will provide recommendations to defend against these threats, including possible mitigation measures.

CYBERSECUTITY TIPS TO KEEP YOUR BUSINESS SECURE

Following the latest Cybersecurity awareness months, it became mandatory to look at ways to keep your organization safe from hackers, identify weaknesses within your network and implement the right protection, detection and monitoring controls.

Some tips are listed hereunder that helps you to avoid becoming victims of cybersecurity threats.

1- Patch management process.

Nowadays, most of the data breaches are attributed directly to attackers exploiting a known vulnerability that was not patched on the targeted systems.

Several well-known organizations around the world are having difficulties in performing patch management due to lengthy and complicated processes that lead to service disruption for the end users in some cases. In addition, the increasing number of CVEs published per year is considered a main challenge for most of organizations to keep up to date in their patches.
So, what is an effective process for the patch management?

Five fundamental points should be considered in the patch management process while taking into consideration that a clear role and ownership should be established for each step and communicated to the stakeholders.

Step1: Discovery
IT team must ensure that they have an updated comprehensive inventory of the network, system, and applications including the release version and installed patches. They must utilize tools that perform automated scan about their environments and get comprehensive view of everything on the network. Automating the process will decrease the chance of intrusion on forgotten systems.

Step2: Categorization
This step will add the flexibility in segregating the patch management policy per category based on the risks and criticality of each system. For example, critical systems should be treated with high priority and always remain up to date.

Step3: Patch management policy creation
The policy depends on each system and should address aspects such as schedule, frequency, backup and regression testing. It is recommended to automate the patching as much as possible by setting the right policies so as to gain time and reduce vulnerabilities.

Step4: Monitor for new patches and vulnerabilities.
It is important to rely on efficient solutions capable to automatically scan the network and provide timely vulnerability disclosures. Based on the scan results, the adopted policies shall be implemented.

Step5: Patch implementation
This step includes patch testing, auditing, and deployment then generation of compliance patch report including risks about exclusive actions.

GDS experience in patch management highlights two additional capabilities that should be present in any patch management solution or process:

- Ability to integrate with the general risk register database of the organization to be able to show the impact of the patch process on the overall business.
- API support to integrate with other solutions like SIEM for monitoring and correlation with other alerts.

2- Email security strategy.

Nowadays, the humble email is becoming a valuable and viable attack vectors for threat actors. The numbers in 2020 demonstrate that most of the cyberattacks that took place that year started with phishing emails such as espionage, fraud, credential thefts, data breaches and island hopping, due to the below reasons:

- Provide direct access to an individual employee.
- Allow access to internal infrastructure.
- Can get information about security checks.
- Can lead to easy success without requiring high skills from the threat actor.

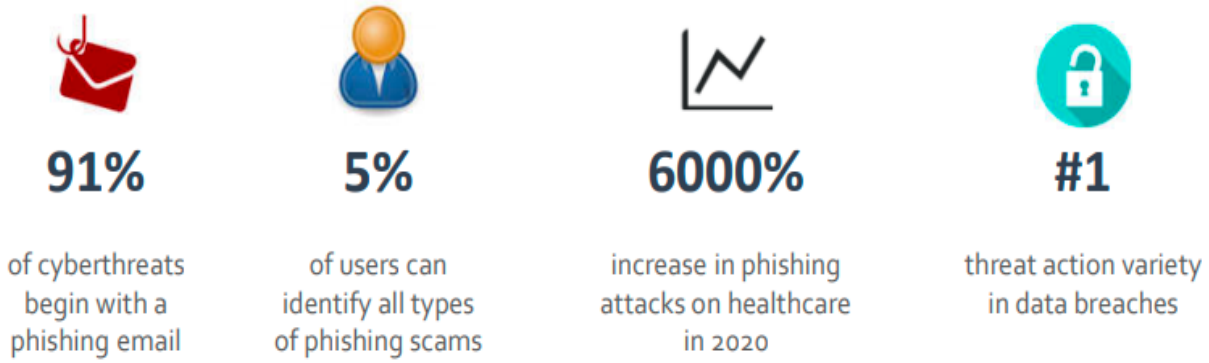

Figure 1: Statistics numbers in 2020

These numbers should act as a trigger to build up an email defence strategy. This starts by understanding how attacks through emails are implemented and deployed by criminals. The MITRE ATT&CK framework includes many relevant attack tactics and techniques as well as examples and mitigation steps that could help build such strategy.

Ten techniques that are directly related to the email's attacks will be highlighted:

- **Reconnaissance phase**, where the attacker starts gathering information using phishing emails to get data about the target, check whether the email is viable, if the receiver is alive, responsive…
- **Resource development,** using compromised accounts which helps in the validity of the sender to get immediate response.
- **Initial access, many** techniques can be corelated with email attacks such as:
- Phishing technique including malicious malware, links, and attachment to download a payload on the targeted systems and link it to C2C controls.
- Trusted relationship techniques between two companies that could lead to fraud, espionage.
- Valid accounts that are the result of malware attacks after interacting with phishing emails.

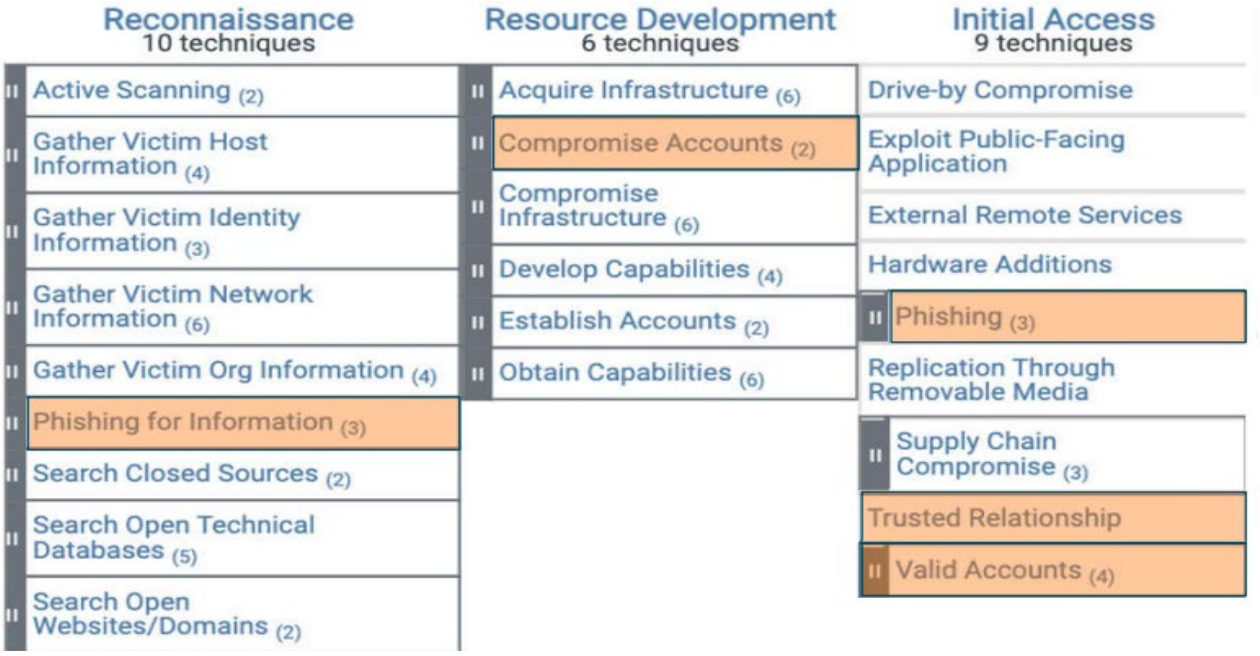

Figure 2: MITRE ATT&CK Techniques (1)

- **Execution,** where the attacker runs a code on the endpoint that is going to be the initial foothold with the aim of gaining persistence on the machine. This could be done using the exploitation of vulnerabilities on the client's side and sending a malicious macro through emails that leads to the user performing execution.
- **Privilege escalations**, of which the main intent is to gain privilege escalation on the vulnerable system through the malicious files sent through emails.
- **Persistence**, when after gaining access to a system via email, the attacker will try to perform some account manipulation, change permissions… to keep a backdoor open into the system.

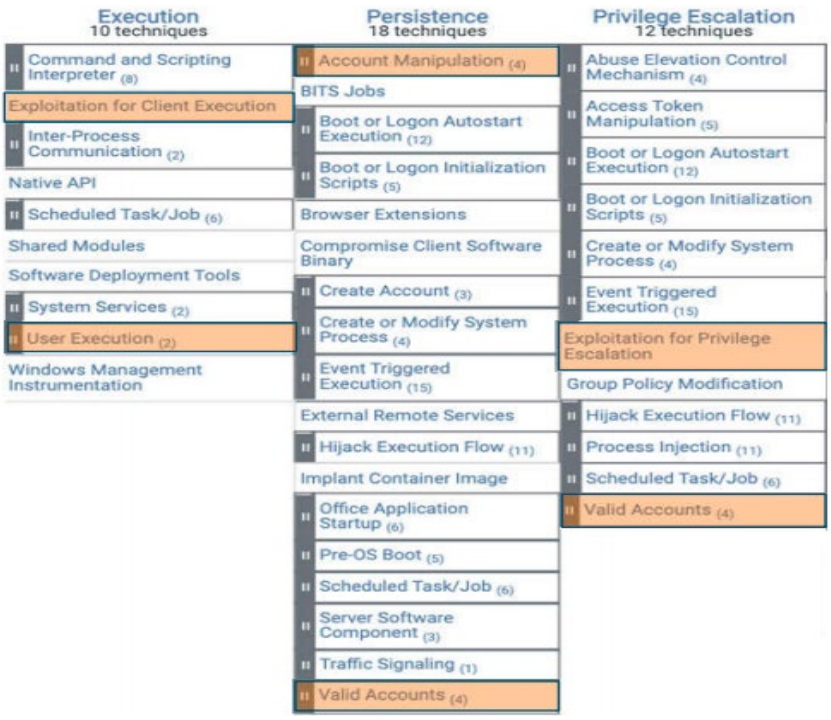

Figure 3: MITTRE ATT&CK Techniques (2)

So, what are possible mitigation strategies against email-based attacks?

- At the network side, the use of efficient DPI and IPS solutions to detect and prevent activities on the network that looks anomalous based on threat intelligence, behaviour, heuristics is a must.
- Implementing an intelligent email security solution that checks the context of the inbox to block malicious links, detects credential theft sites that impersonate well-known solutions like Microsoft Office 365 or performs email analysis about the profiles of the senders is another effective line of defence.
- At the endpoint levels, use of sandboxing for application isolation and watching activities, endpoint protection, vulnerability management, antivirus, and antimalware is a third valuable measure.
- At the user level, continuous awareness training is a must.

GDS SOC team's approach is similar to that when working on a defence strategy, for any email-based attack vector.

3- Cryptography: Key management and risks

Cryptography is a critical science for modern communication and computing systems. Every such system used in practice has its risks and potential weaknesses, including most often risk of compromise of the cryptographic algorithms due to a weak implementation done by software developers that are not cryptologists at their core. Without proper knowledge, a programmer can take shortcuts that eventually lead to a compromise of the encryption keys. Weaknesses in implementation can affect the keys themselves (low entropy of key generators resulting in easy guess of keys) or how they are stored and exchanged (why would a hacker bother with a computationally intensive attack that tries to "guess" an encryption key when such key could simply be recovered from the system where it is stored, if not enough protection is deployed around it?)
A case in point is the latest SolarWinds supply chain attacks directly featured key-misuse in SUNSPOT code. Then, in post exploit attacks against selected targets from the pool of SolarWinds customers compromised by SUNSPOT, key theft through Golden SAML attacks were detected.

Major encryption challenges are summarized below:

- Algorithms' inherent risks mitigated by frequent updates of the software using these algorithms with the latest development and enhancements done in cryptography.
- Implementation of key generation, key re-use and non-key specific aspects.
- Protection of the keys from theft or misuse.
-

So what could be a reliable strategy to protect your keys?

"The starting point in any certificate and private key management strategy is to create a comprehensive inventory of all certificates, their locations and responsible parties."
https://en.wikipedia.org/wiki/Key_management#

It is important to think of the location of your encrypted keys, that could be located on:

- Your internal PKI certification authority
- Federated authentication servers
- Code signing
- Cloud resources like storage account keys
- Database encryption
- VM encryption
- Document and transaction signing

- SSL and TLS certificates for secure web browsing
- SSH certificates for secure machine access
- PII and credit card tokenization
- Kerberos TGT key
- BitLocker

The next step is to protect your key storage from theft using any or a combination of the below technologies:

Figure 3: Hardware key storage

- **Hardware** (HSMs, Smartcards, TPMs, etc.): the keys stay inside the hardware and all the processing is done on it. In this case a strong physical protection is needed to prevent key access. No other code should run on the hardware and it must be certified to ensure compliance.
  Some disadvantages should be taken into consideration such as the management and high maintenance needed specifically in virtualized world as well as the vulnerability of hardware cryptographic modules to side channel attacks such as DPA.

Figure 4: Software key storage

- **Software** (whitebox crypto, hardening): this solution is easy to scale, suitable for a virtualized environment, easy to update and fix vulnerabilities. It can be deployed on any hardware and not bound to any vendor. But the problem here, is the security since obfuscation and white-box crypto techniques are easily broken.

- **Trusted execution environment**: is becoming an emerging ubiquitous solution. The keys are protected in secure enclaves. TEE provides data protection within the trusted execution enviroment :
  - Memory encrytpion
  - Code running in the encalve cannot be viewed
  - Can be used for protection keys and general data.
  - Attestation methods to make sure correct code is running.

  Although TEEs have a reduced attack surface compared to non-secure code execution environments due to a reduced codebase and restricted interface, they are not failproof as has been proven in multiple real-world hacks.

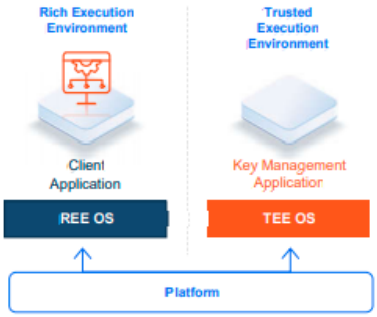

Figure 5: TEE

- **Secure multiparty computation (MPC).** The process of building MPC key store falls under the below conditions:

Figure 6: Building MPC Key Store

The keys are split between completely different environment like on-premises, AWS and Azure, making it very hard to detect and decrypt those keys.

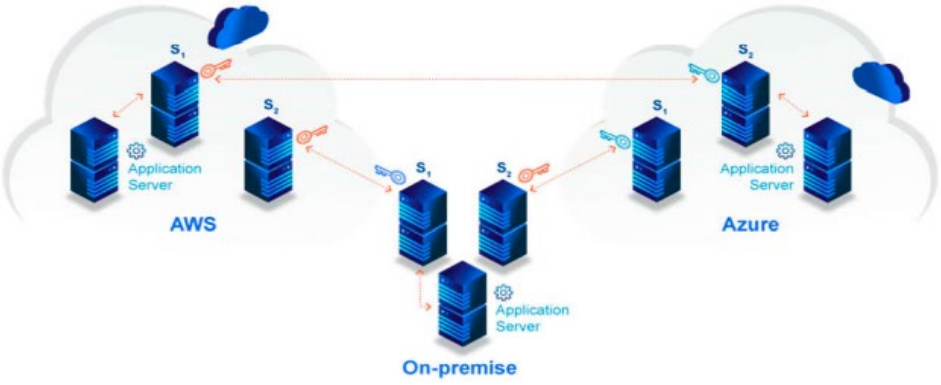

Figure 7: MPC Key design

This solution is scalable, fully virtualized, with no single point of failure providing high availability and disaster recovery at low cost.

Different solutions can be combined depending on functional and security environments: for example you can run MPC inside TEE environment or you can use HSMs in some scenarios where compliance is required and MPC elsewhere.

The final step is to protect your key from misuse by defining policies concerning key usage such as: verification of the client authentication, rate limit on operations depending on time of day, integration with external checks before the operation, addition of human approval for highly sensitive transactions.

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