Table of Contents

Introduction - Context

Since the beginning of the COVID-19 crisis, security actors are unanimous: the number of cyber threats and attacks is increasing consistently.

On March 25th 2020 Hacknowledge decided to launch the free-of-charge « **Heath Crisis Solidarity Project**» addressed to the health sector in both Luxembourg and Switzerland.

The idea was to support IT teams during the pandemic crisis to prevent an IT disaster from occurring at the same time, as they face the already complicated current situation.

Due to a high demand and because solidarity is important in this crisis time, Hacknowledge has decided to expand the provided service to all actors engaged in the fight against COVID-19 and to make the present newsletter available to other sectors who also have to deal with a unusual situation due to COVID-19.

This provided service can be split in several parts such as:

- Better anticipate threats: a weekly newsletter to stay aware about active threats and campaigns (available to all sectors);
- Better target corrective actions: easy-to-implement workarounds & quick-wins against recent weaknesses;
- Limit the risk exposure and attack surface: OSINT to identify your Internet exposure + simple service discovery scans (**NOT A VULN SCAN SENDING UNCONTROLLED DATA**) in order to identify the “shadow IT” and the services exposed requiring particular attention: **NO EXPLOITATION** in order to exclude any risk of service interruption;
- Allow you to focus on YOUR job: **SAVING LIVES**!

Active Campaign and Advisories

- SQL injection vulnerability and malicious code execution in XG Firewall/SFOS has been fixed

  On Apil 22, 2020, Sophos received an attack using previously unknown pre-auth SQL injection vulnerability to gain access to exposed XG devices, giving the possibility to exfiltrate data residing in the firewall including all local usernames and hashed passwords. Passwords associated with external authentication systems such as Active Directory (AD) or LDAP were not compromised. The CVE is listed as CVE 2020-12271.

  Versions affected: all versions of XG Firewall firmware on both physical and virtual firewalls

  Remediation: Sophos has deployed a hotfix to tackle this issue that should be received automatically for supported versions. Older versions of SFOS should upgrade to a supported version.

  Sophos advisory: https://community.sophos.com/kb/en-us/135412

- Multiple vulnerabilities found in Adobe Bridge could allow arbitrary code execution

  Adobe Bridge is a file management application that manages files across multiple Adobe programs. Several vulnerabilities have been discovered in Adobe Bridge:

  - Stack-based Buffer Overflow vulnerability that could allow for arbitrary code execution. (CVE-2020-9555)
  - Heap Overflow vulnerability that could allow for arbitrary code execution. (CVE-2020-9562, CVE-2020-9563)
  - Out-of-Bounds Read vulnerability that could allow for information disclosure. (CVE-2020-9553, CVE-2020-9557, CVE-2020-9558)
  - Out-of-Bounds Write vulnerability that could allow for arbitrary code execution (CVE-2020-9554, CVE-2020-9556, CVE-2020-9559, CVE-2020-9560, CVE-2020-9561, CVE-2020-9564, CVE-2020-9565, CVE-2020-9569)
  - Use After Free vulnerability that could allow for arbitrary code execution. (CVE-2020-9566, CVE-2020-9567)

  Successful exploitation could result in an attacker gaining the same level of privileges as a logged-on user. Depending on the privilege associated with the user, an attacker could create, change or delete data, including user accounts.

  Affected versions: Adobe Bridge 10.0.1 and earlier

  Remediation: Adobe has released a security update and recommends update to version 10.0.4.

  Adobe advisory: https://helpx.adobe.com/security/products/bridge/apsb20-19.html

- Vulnerability in Microsoft Teams could allow account takeover via a GIF file

  CyberArk teams discovered a flaw in Microsoft Teams that allow an attacker to send a GIF or an image to a victim via chat and get control over their accounts. Fortunately, this issue has already been tackled by Microsoft. However, the detailed steps of the attack are interesting and could serve as example for other attacks using the same vector.

  Attack vectors:

  In Teams, to guarantee that shared media content between users and restricted to those users only, Microsoft has implemented a cookie called "authtoken" and another cookie called "skypetoken_asm".

  The "authtoken" permits authentication of the user to loads images across Microsoft Teams and Skype. It contains a JWT to be sent to *.teams.microsoft.com. On the other hand, actions such as reading or sending messages are handled by another token, the "skypetoken". To get the "skypetoken", only providing "authtoken" is sufficient. With these two tokens, it is possible to make APIs calls/actions through Teams API interfaces, which lets you send/read messages, create groups, add new users, etc.

  An attacker that can get their hands on an "authtoken" can create a "skype token" and have access to all the API calls.

authtoken is only sent to subdomains under teams.microsoft.com. However, two domains were found to be vulnerable to a subdomain takeover:

- aadsync-test.teams.microsoft.com
- data-dev.teams.microsoft.com

An attacker can send a message to a victim with an "src" attribute set to the compromised sub-domain via Teams chat. When the victim opens this message, the victim's browser will try to load the image and this will send the authtoken cookie to the compromised sub-domain.

The attacker will then retrieve the authtoken, finally allowing them to create a skype token, providing access to the victim's data.

The GIF could also be sent to groups (a.k.a Teams), which makes it even easier for an attacker to get control over users faster and with fewer steps.

Remediation: Microsoft has already performed a quick fix by deleting the misconfigured DNS records of the two subdomains that were exposed and could be taken over.

Full article about the steps of the attack can be found at the link here:

https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/

- Compromise of Pulse Secure VPNs after being patched due to stolen credentials

One year after CVE-2019-11510 that could allow unauthenticated attackers to read arbitrary file on the appliance, DHS CISA has observed that many organizations reuse passwords and have failed to update credentials post-compromise. Attackers are using valid accounts tied to external remote services for access and perform lateral movement before exfiltrating data for sale on the dark web.

CVE-2019-11510 arbitrary file reading allows attackers to retrieve /etc/passwd, which contains information about local system accounts. "By requesting the data.mdb object, an attacker can leak plaintext credentials of enterprise users," CISA wrote. "Open-source reporting indicates that cyber threat actors can exploit CVE-2019-11510 to retrieve encrypted passwords." CISA also noted that it was possible to leak the domain administrator password that was used to join the appliance to the domain.

CISA recommended organizations apply the updates to their VPN and change the passwords to all Active Directory accounts, including administrators and service accounts. Administrators should also look for unauthorized applications and scheduled tasks in their environment and remove any remote access programs not approved by the enterprise.

CISA also developed an IOC (indicator of compromise) that searches for evidence of attempted compromise: https://github.com/cisagov/check-your-pulse

Link to the full article: https://healthitsecurity.com/news/amp/dhs-warns-hackers-compromising-patched-vpns-with-stolen-credentials

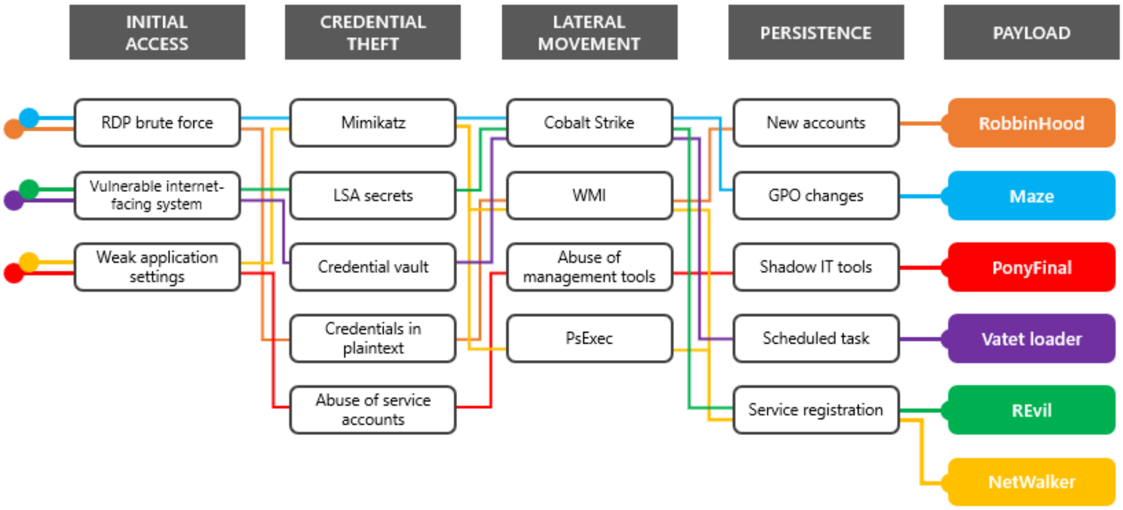
Newsletter #3 updates:

- Ransomware groups targeting healthcare and critical services during COVID-19 crisis (Part 2)

For the first two weeks of April 2020, multiple human-operated ransomwares have targeted healthcare, government institutions and other critical services during the COVID-19 global crisis. Organizations should however be vigilant since these attacks are not limited to critical services.

It has been discovered by incident response teams that many of these compromises have occurred earlier this year and attackers have compromised the target networks months before and have waited to deploy ransomwares when they would see the most financial gain – in this COVID-19 period.

Attackers manage to breach into the target networks by exploiting vulnerable Internet-facing systems with vulnerability discovered at the end of last year, such as Citrix systems affected by CVE-2019-19781, or by doing brute force on services without 2FA authentication. Afterwards, they use lateral movement techniques to spread into the internal networks and deliver their payload.



Microsoft highly recommends paying attention to any sign of compromise related to these ransomwares. This includes:

- Malicious PowerShell, Cobalt Strike, and other penetration-testing tools that can allow attacks to blend in as benign red team activities
- Credential theft activities, such as suspicious access to Local Security Authority Subsystem Service (LSASS) or suspicious registry modifications, which can indicate new attacker payloads and tools for stealing credentials
- Any tampering with a security event log, forensic artifact such as the USNJournal, or a security agent, which attackers do to evade detections and to erase chances of recovering data

Full documented article from Microsoft "Ransomware groups continue to target healthcare, critical services; here's how to reduce risk" article is available at the following link: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Important note to our customers:

For Hacknowledge customers, please contact your TAM to validate or request that corresponding use-cases are in place.

How to Protect: What We Recommend

- Inform users about latest threats and ask them to do not download and/or install any .apk/.exe file from website;

- In case of using IOS or Android, always install Antivirus solution to limit risks – free software exists and, even if not perfect, can prevent from classical malware;

- For **ANY** service or system, even internally exposed only, **apply the latest update**; Validate your patch management policy to ensure all systems are well covered;

- Validate your backups policy to avoid data loss;

- Do not expose useless management interface on the Internet / challenge your exposure;

- If unsure about the authenticity of a website, don't proceed with any login procedures (if you already clicked);

- Implement double factor authentication when possible, specifically on exposed assets (VPN access…);

- **Beware of COVID-19 related phishing schemes** and fake alerts/health advisories;

- Monitor:
    1. Remote access devices;
    2. Abnormal network load peaks (data exfiltration);
    3. Suspicious credential sharing;
    4. Mail gateway/spam alert and covid-19/coronavirus/vaccine URL accessing;
    5. Log all remote access events;

Latest « COVID-19 » Related Papers and Resources

Official papers

- ENISA: https://www.enisa.europa.eu/topics/WFH-COVID19/tips-for-cybersecurity-when-working-from-home
- ECSO: https://www.ecs-org.eu/documents/uploads/covid-19-response-package-1.pdf
- WHO: https://www.who.int/about/communications/cyber-security
- Swiss Government CERT: https://www.govcert.ch/blog/phishing-attackers-targeting-webmasters/

Some news from battlefield

- https://www.darkreading.com/threat-intelligence/microsoft-warns-of-malware-hidden-in-pirated-film-files/d/d-id/1337688
- https://www.darkreading.com/vulnerabilities---threats/advanced-threats/attackers-target-sophos-firewalls-with-zero-day/d/d-id/1337670
- https://www.securityweek.com/code-injection-vulnerability-found-real-time-find-and-replace-wordpress-plugin
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-bridge-could-allow-for-arbitrary-code-execution-apsb20-19_2020-056/
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-magento-cms-could-allow-for-remote-code-execution-apsb20-22_2020-057/
- https://www.zdnet.com/article/microsoft-office-365-us-issues-security-alert-over-rushed-remote-deployments/

Additional Useful Resources

In the event of a ransomware attack, try to identify if the data is recoverable using « no more ransom » project: https://www.nomoreransom.org/fr/index.html

Ransomware prevention advice: https://www.nomoreransom.org/en/prevention-advice.html

Online sandbox for malware analysis: https://www.hybrid-analysis.com/?lang=en

Oracle's commitment to our customers and partners during the COVID-19 crisis (FAQ): https://www.oracle.com/corporate/covid-19.html

Microsoft launch the « Zero Trust Framework »: https://www.microsoft.com/security/blog/2020/04/02/announcing-microsoft-zero-trust-assessment-tool

Contacts

Bourbon Jean-Marie – Head of Offensive Security

Mail: jean-marie@hacknowledge.lu

Phone: (+352) 661 523 211

Barbara Terra – Sales Manager

Mail: barbara@hacknowledge.lu

Phone: (+352) 671 122 709