FLYCAST PARTNERS valencia

☎ 844FLYCAST flycastpartners.com info@flycastpartners.com

# Cybersecurity Threat

## June 2023 Newsletter

## Securing Healthcare

### Healthcare IT Budgets Rise Amid Recession

As organizations are slashing resources to prepare for a looming recession, a new survey reveals that cybersecurity budgets are rising, especially in the healthcare sector. 58% of the 200 CISOs surveyed in the study had increased their cybersecurity budgets to face cybersecurity threats, with 42% planning to pour even more money in the following year. This is attributed to rising attention given to securing software applications and tools.

### HC3: Look Out For FIN11

The US Health Sector Cybersecurity Coordination Center (HC3) is alerting on the rise of the FIN11 group. This advanced persistent threat (APT), said to originate from Russia, is known for exploiting zero-day vulnerabilities against hospitals and healthcare organizations. In its disruptive and lucrative attacks, FIN11 is leveraging Clop ransomware and has been seen using the FORTRA GoAnywhere flaw as well as the more recent MOVEit flaw to compromise healthcare groups.

### A Hospital Closes Because of Ransomware

This June has been especially difficult for healthcare organizations, as high-profile cybersecurity attacks multiplied. Johns Hopkins University and Johns Hopkins Health are in the midst of dealing with a cyberattack and data breach. Johns Hopkins has stuck to calling it a "widely used software tool that impacted thousands of other large organizations across the world"; the timeline would align with the discovery of the MOVEit exploit. This week, we were also reminded of the literal cost of ransomware, with St Margaret's Health in Illinois being forced to close its doors because of the cost from a 2021 cyberattack.

### Hackers Will Always Love Healthcare

Hackers have had an interest in healthcare for years and have been leveraging innovative methods to breach them. Hackers go after healthcare because medical data is sensitive and worth a lot to them. Personal information stolen can then be exploited to carry out further cyberattacks. To hackers, healthcare data is the single largest trove of sensitive data.

### What Should Healthcare Organizations Do?

According to a report drafted by Arete and Cyentia, data exfiltration is the top technique used by hackers to impacthealthcare organizations. This reiterates the importance of **user training** as it relates to social engineering and phishing (with over 50% of breaches in healthcare stemming from phishes), but also of using regularly tested and accurate **backups**. Organizations with codified frequent backup practices showed a lesser likelihood to pay ransom as they could recover ransomed data more easily.

### Healthcare Needs Better Authentication

Also reported in Arete and Cyentia's study is the low adoption rate of **multi-factor authentication (MFA)** across healthcare organizations, which currently sits at 19%. Other proactive measures should include **endpoint detection and response (EDR) solutions**. According to the report, EDRs should be an integral part of healthcare organizations' preventive solutions as they detect threats before they turn into incidents.

## Threat Actor Updates

- A tool known as Terminator is being peddled on Russian-speaking hacking forums. Terminator is said to be able to bypass 24 different antivirus, endpoint detection, and response solutions, as well as extended detection and response security solutions, including Windows Defender.

  **Our Thoughts:** Highlighting the adaptive nature of hackers, Terminator was only detected by a single anti-malware scanning engine.

- Hackers were reported trying to evade detection by impersonating cybersecurity researchers on Twitter and GitHub. They are going to these resources and posting fake proof-of- concept exploits for zero-days targeting Windows and Linux. Quite a bit of effort is going into this endeavor, with profiles and repositories appearing legitimate, oftentimes impersonating real security researchers from renowned security firms such as Rapid7.

  **Our Thoughts:** This is an impressive move, although unfortunately not surprising. Hackers constantly obfuscate and they are now going to the source to do so. Make sure you triangulate the threat intelligence your organization receives with other sources and validate it.

## Exploits and Issued Patches

- The major exploit of early June was a zero-day in the MOVEit Transfer file transfer software. The flaw was an SQL injection weakness in the file transfer product allowing escalated privileges and unauthorized access. The vulnerability is being actively exploited, and constitutes another flaw in MOVEit that was discovered on June 16th

  **Our Thoughts:** The vulnerability affected several victims already, including US federal agencies most recently. If you're using MOVEit, disable HTTP and HTTPs traffic to your transfer environment and apply patches.

- Foxit PDF reader, a popular alternative to Adobe's PDF software, is facing a severe security flaw that could have attackers execute code on the victim's systems. Foxit's Java interface is exposed, which could let attackers write arbitrary files.

  **Our Thoughts:** Patch immediately if you're a Foxit user.

- ESET is alerting about high-severity vulnerabilities found in its Linux and macOS products. ESET has found these during an internal security analysis, the vulnerabilities being local privilege escalation vulnerabilities

  **Our Thoughts:** ESET is a trusted and well known IT organization, it's good to see them being proactive. ESET has issued patches; apply them immediately.

**Subscribe to our newsletter and stay updated.**

- Researchers have released a proof- of-concept exploit for an RCE vulnerability in VMware Aria. The command injection vulnerability sits in the critical severity range and can be exploited by unauthenticated actors in simple attacks – user interaction is not needed for hackers to attain their aim.

  **Our Thoughts:** Exploits that don't require user interaction are always concerning. Vmware has released updates; apply them as soon as possible.

- Google has released updates for Mac, Linux, and PC to address a series of vulnerabilities. These are critical, allowing hackers to use memory after it has been deleted, impacting user privacy and crashing systems.

  **Our Thoughts:** Chrome is among the most popular browsers in the world; update immediately.

## UN Cybercrime Treaty

We are reminded that cybersecurity is an international affair as the UN Cybercrime Treaty makes headway at the UN. The Treaty includes the following items:

- The introduction of over 30 criminal offences related to cyberattacks, including hacking, malware distribution, and cyberbullying.
- Enhanced protection of critical infrastructure, with power, transport, and communication explicitly mentioned.
- Improved procedural safeguards guaranteeing due process to individuals accused of cybercrime.
- Improved international cooperation for cybersecurity threats.
- Recommendations on protection of personal data from unauthorized use via data protection laws.

At the same time, critics point out that other measures in the Treaty, including punishment for insulting religions or humiliating others online, constitute overreach. Others claim that it would legitimize intrusive surveillance and limit civil liberties. As with any development in the cybersecurity landscape, it is not clear if this is a good or a bad thing as of yet. We will be watching this unfold closely