ON2IT AND AMS-IX PRESENT: **THREAT TALKS**

Threat Talks
Healthcare

Responsibilities, regulations and legacies

threat-talks.com

Cyberattacks on healthcare organizations can put patients' lives and entire organizations at risk. There are numerous reasons why cyber attackers seem to favour healthcare facilities as a target: private patient information is worth a lot of money, medical devices are easy entry points, and there's a lot of outdated technology.

When faced with attacks like a ransomware attack, healthcare organizations are faced with a choice: pay ransom or risk patients' lives. The stakes couldn't be higher.

How do you protect patient data? What are the risks associated with legacy systems, and how does one safely modernize these systems without interrupting service or exposing new vulnerabilities? These are a lot of issues to focus on, whilst still remaining compliant with health data regulations like HIPAA and GDPR.

In this episode of Threat Talks we will discuss the following threats:

- DICOM
- CONTI Ransomware - HSE Attack
- ScreenConnect

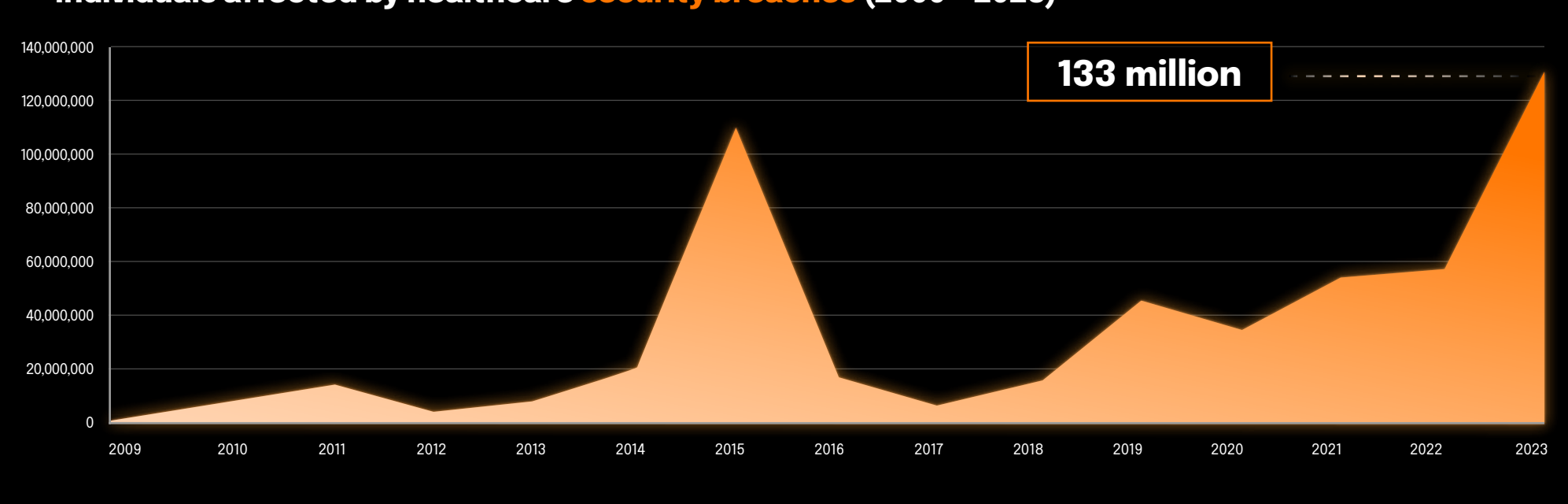
In 2023, an average of 373,788 healthcare records were breached every day.

Source: HIPAA Journal

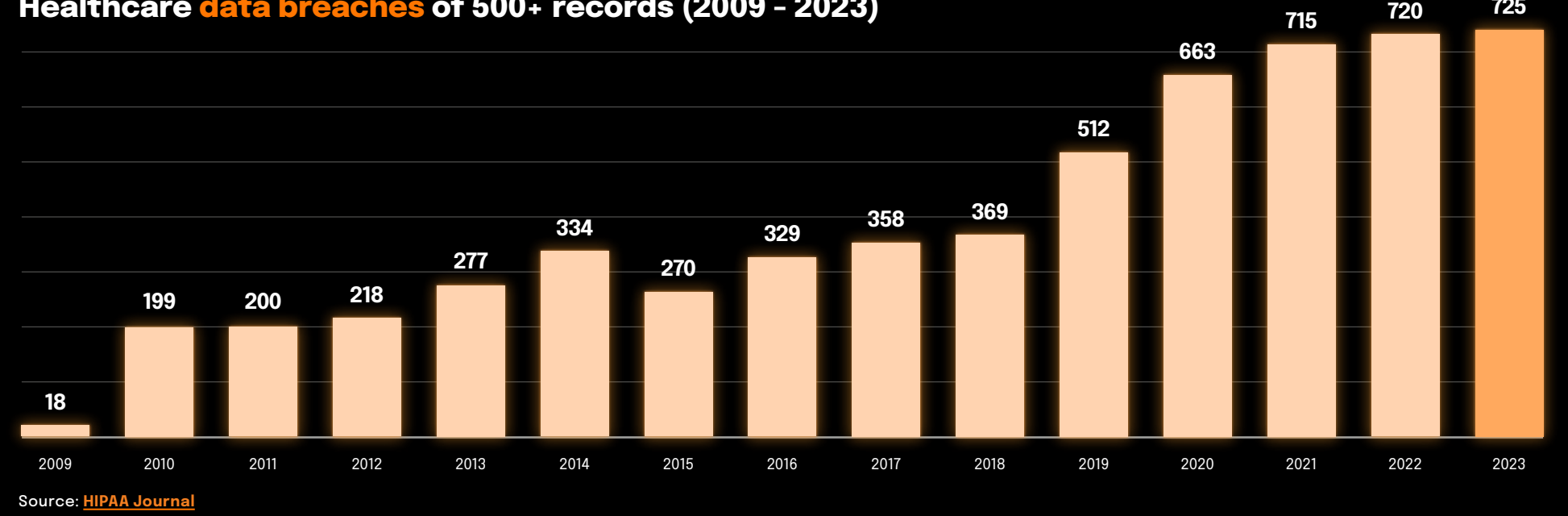
In 2023, the healthcare industry reported data breaches costing an average of $10.93 million per breach – almost double that of the financial industry, which came in second with an average cost of $5.9 million.

Source: World Economic Forum

Individuals affected by healthcare security breaches (2009 - 2023)



Healthcare data breaches of 500+ records (2009 - 2023)



Source: HIPAA Journal

Personal Identifiable Info (PII)

16.1 M

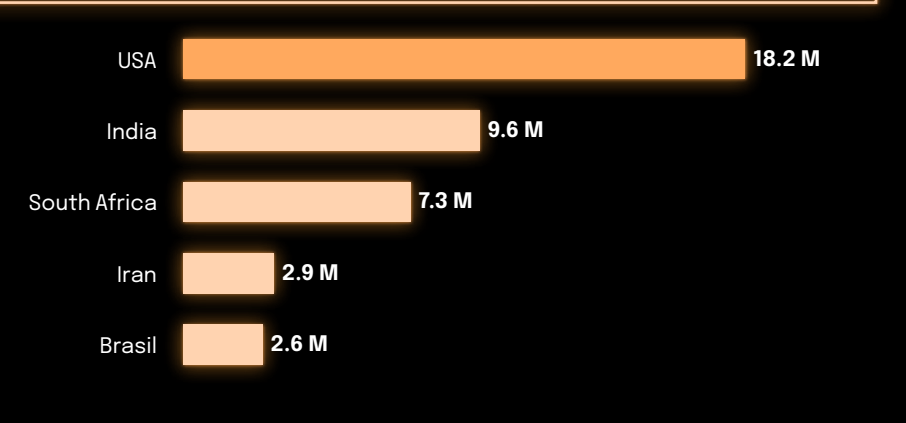
Information like:
- Full name
- Date of Birth
- Address
- Telephone number
- Gender
- In some cases Social Security Number

Protected Health Info (PHI)

43.5 M

Information like:
- Result of examination
- Place, date, and time of examination
- Referring physcian
- Used modality

Top 5 countries out of 111 with the most exposure



DICOM The hidden risks of Legacy Protocols

DICOM (Digital Imaging and Communications in Medicine) is a standard protocol for handling, storing, printing, and transmitting information in medical imaging. Despite its widespread use in the healthcare industry, DICOM is an older legacy protocol, originally designed for use within closed environments and not intended for sharing data across today's open, interconnected environments.

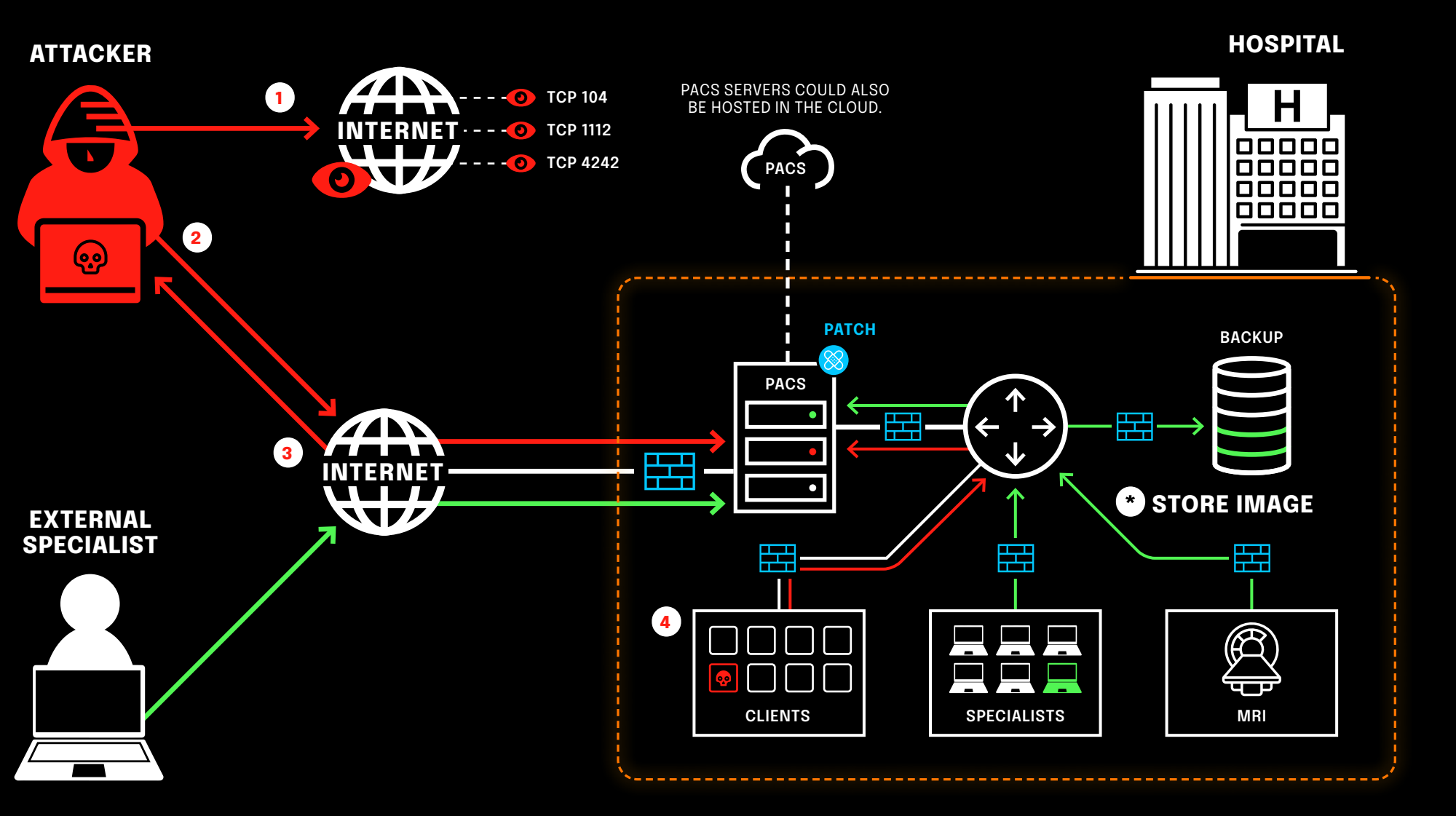
DICOM protocols manage highly sensitive data, including personal identifiable information (PII) and detailed health records. As hospitals integrate newer technologies such as cloud services, the continued reliance on legacy protocols like DICOM presents significant security challenges. Alarmingly, less than 1% of exposed DICOM servers implement effective authorization measures. This vulnerability not only increases the risk of unauthorized data access but also raises concerns about potential data tampering, compromising both patient privacy and care.

These risks were prominently highlighted in the BlackHat presentation "Millions of Patient Records at Risk: The Perils of Legacy Protocols" by Ibrahim Akkulak and Sina Yazdanmehr.

mSOC confidence score	Confirmed
Threat category	Misconfiguration - Insecure settings
Severity	High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1210 - Exploitation of Remote Services	Exploiting vulnerable Internet facing appliances	Impersonation	Low	Healthcare

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1026 - Privileged Account Management M1030- Network Segmentation	Misconfiguration/Poor Security Practices	Anomaly detection, Network monitoring	High	Cybercriminals



*** Image creation and storage**

An image is created by a common medical device (i.e. X-Ray, MRI and Ultrasound machines) and stored on the Picture Archiving and Communication System (PACS).

Scan the Internet for exposed DICOM services

1. The attacker scans the Internet for exposed DICOM services, with special interest in TCP ports; 104, 1112 and 4242.

M Limit access; don't expose the service on the Internet, if remote access is required use strict IP filtering and/or VPNs to further limit access.

Gain access, authorization

2. The attack will connect to the service and see if it requires authentication and if so try default Application Entities Title (AET), which is a way for applications to identify themselves.

M Make sure authentication is enforced and that defaults AETs have changed, if possible enable extended negotiation of user identity. If possible upgrade software to support these features.

Act on objective, retrieve or modify

3. The attacker will act on the objective by either receive files or modify them by using protocol commands like, C-FIND, C-GET, C-MOVE and C-STORE.

M Limit protocols commands where possible, implement network filtering to detect anomalies and have a proper backup in case of tampering.

Threats from inside

4. The attacker may also come from the internal network, by abusing client stations or implementing remote access tools, either in software or hardware.

M Be aware that the threat may also come from the internal network, especially in wide and generally open environments like hospitals, this is a serious threat. Segment the network and limit access to where it is required is a relatively easy mitigation to lower the chances of success for an attacker.

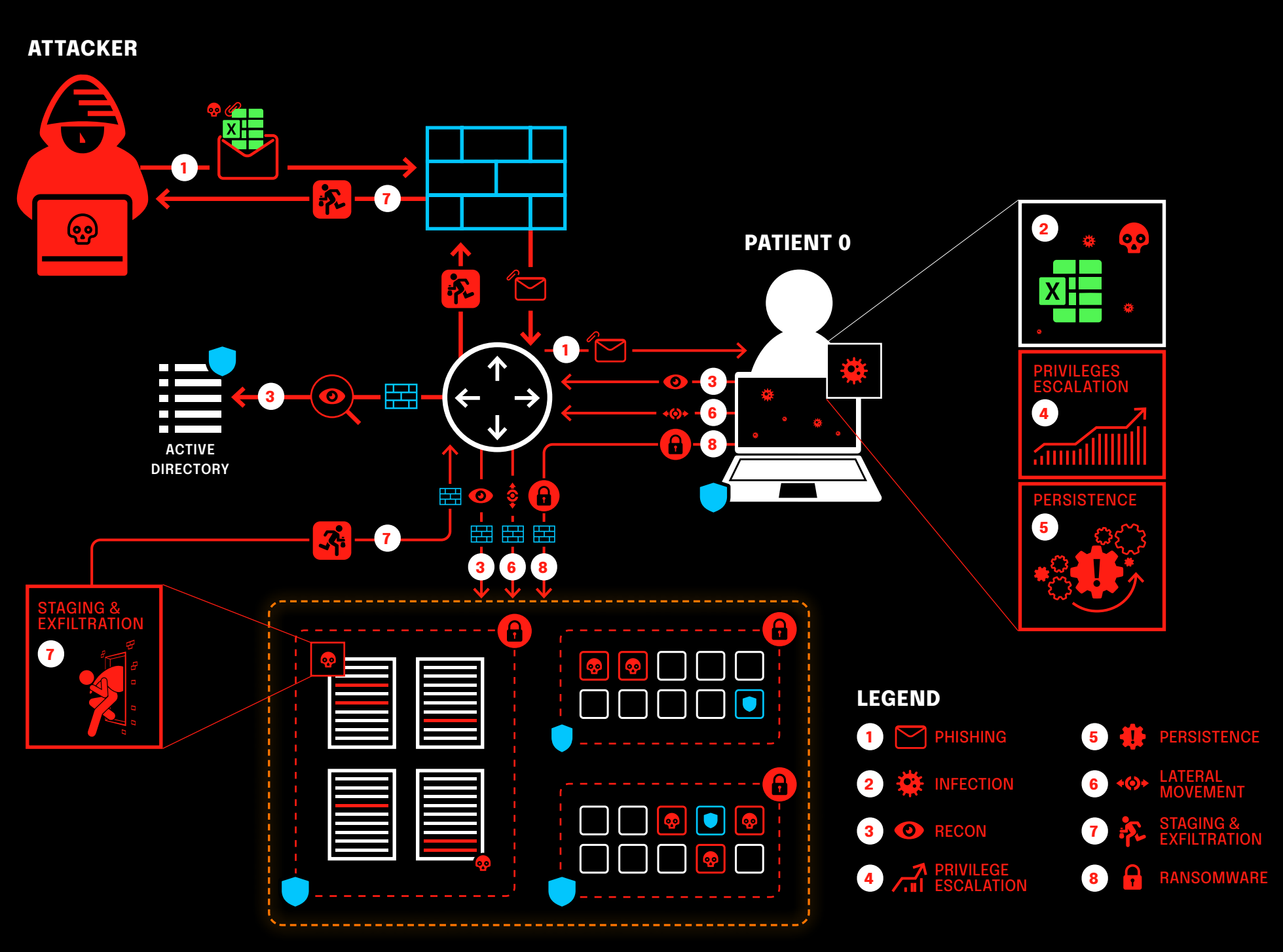
Ireland's HSE Ransomware Attack

The ransomware attack on Ireland's Health Service Executive (HSE) on May 14, 2021, caused significant disruption across the nation's healthcare services. Orchestrated by the cybercrime group Wizard Spider using Conti ransomware, the attack exploited vulnerabilities in unpatched systems and employed double extortion tactics, including threats to release stolen sensitive data. The consequences were severe, impacting about 80% of IT systems, disrupting medical services and patient care, and exposing the need for substantial improvements in cybersecurity measures within the healthcare sector. The recovery and enhancements to prevent future attacks were projected to be costly, highlighting the critical need for up-to-date security protocols and regular system assessments.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - Ransomware Attack
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1486 - Data Encrypted for Impact	Data exfiltration and encryption for extortion	Traffic Obfuscation, Encryption and Tunneling	High	Healthcare (HSE)

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1053 - Data Backup M1040 - Behavior Prevention on Endpoint	Phishing	Network share access, file modification	Critical	Cybercriminal (Wizard Spider)



Although this attack was conducted against the HSE, the following steps are enriched with content extracted from the CONTI ransomware group's playbook leaked in 2021. These steps can serve as a generic explanation of how a typical ransomware attack operates. Attackers may employ various tools such as Cobalt Strike, Metasploit, or other attack frameworks.

It all begins with social engineering!

1. The attacker sends a phishing email to the target containing a malicious Excel document.

M Email filtering solutions can help detect and block phishing attempts. Conduct regular security awareness training to educate users about the risks of opening attachments from untrusted sources.

Infection

2. The target opens the email and executes the malicious Excel document, leading to system infection (patient zero), which installs a backdoor such as TrickBot or BazarLoader.

M EDR solutions can prevent the execution of malicious code and trigger behavioral alerts to inform about possible infections.

Let's take a look around...

3. The attacker begins reconnaissance by attempting to enumerate users and domains, and searches for valuable targets such as domain controllers, file servers, and backup servers, among others.

M Limit user permissions to reduce the effectiveness of enumeration tools and implement monitoring tools that can detect unusual system queries and alert administrators. EDR solutions and firewalls play a crucial role in detecting and blocking enumeration attempts.

More priviliges!

4. At this point the attacker performs privilege escalation to gain higher-level access.

M A least privilege principle for all user accounts, including service accounts, can help preventing privilege escalation. Patching and updating systems regularly to fix vulnerabilities plays a key role as well. EDR solutions can detect and prevent the most common privilege escalation techniques.

I am not going anywhere

5. The attacker will try to establish extra persistence on the host to maintain a foothold. Techniques may vary from installing software such as AnyDesk, to using WMI events, modifying registry keys, or using winlogon.

M Monitoring and restricting changes to registry and startup folders will prevent many common persistence mechanisms. EDR with behavioral analytics can detect anomalous patterns that might indicate attempts at establishing persistence.

I am everywhere

6. In some environments, it will be possible to launch the attack directly from patient zero, while in more secure environments, attackers will need to gain access to as many endpoints as possible. This is achieved through lateral movement.

M Implementing a zero-trust approach will limit lateral movements. Using multi-factor authentication and strengthening credentials management can make lateral movement harder in certain situations. EDR solutions and strict firewall rules play an important role in detecting, preventing, or eventually limiting the targets.

Your data is mine

7. The attacker stages collected sensitive data from compromised systems, often compressing the data using tools such as WinRAR. Once all the data is staged, the attacker proceeds to exfiltrate it using secure transfer protocols or masked traffic to avoid detection.

M Implementing Data Loss Prevention (DLP) strategies can help prevent exfiltration. Encrypting sensitive data both at rest and in transit is crucial. A zero-trust network design limits access to critical data and reduces the risk of unauthorized data movement. Endpoint Detection and Response (EDR) solutions can alert when staging-like events are detected. Traffic monitoring also play a crucial role.

Dropping the bomb

8. The final phase involves deploying the ransomware across the network, encrypting critical files and systems, and then demanding a ransom for the decryption keys. If the ransom is not paid, the attackers may threaten to leak the stolen data.

M Maintaining up-to-date offline backups can enable organizations to restore data without paying the ransom. EDR solutions can utilize hidden canary files, which are monitored for changes such as encryption; any modification to these files triggers an automatic response to block the process and create an alert.

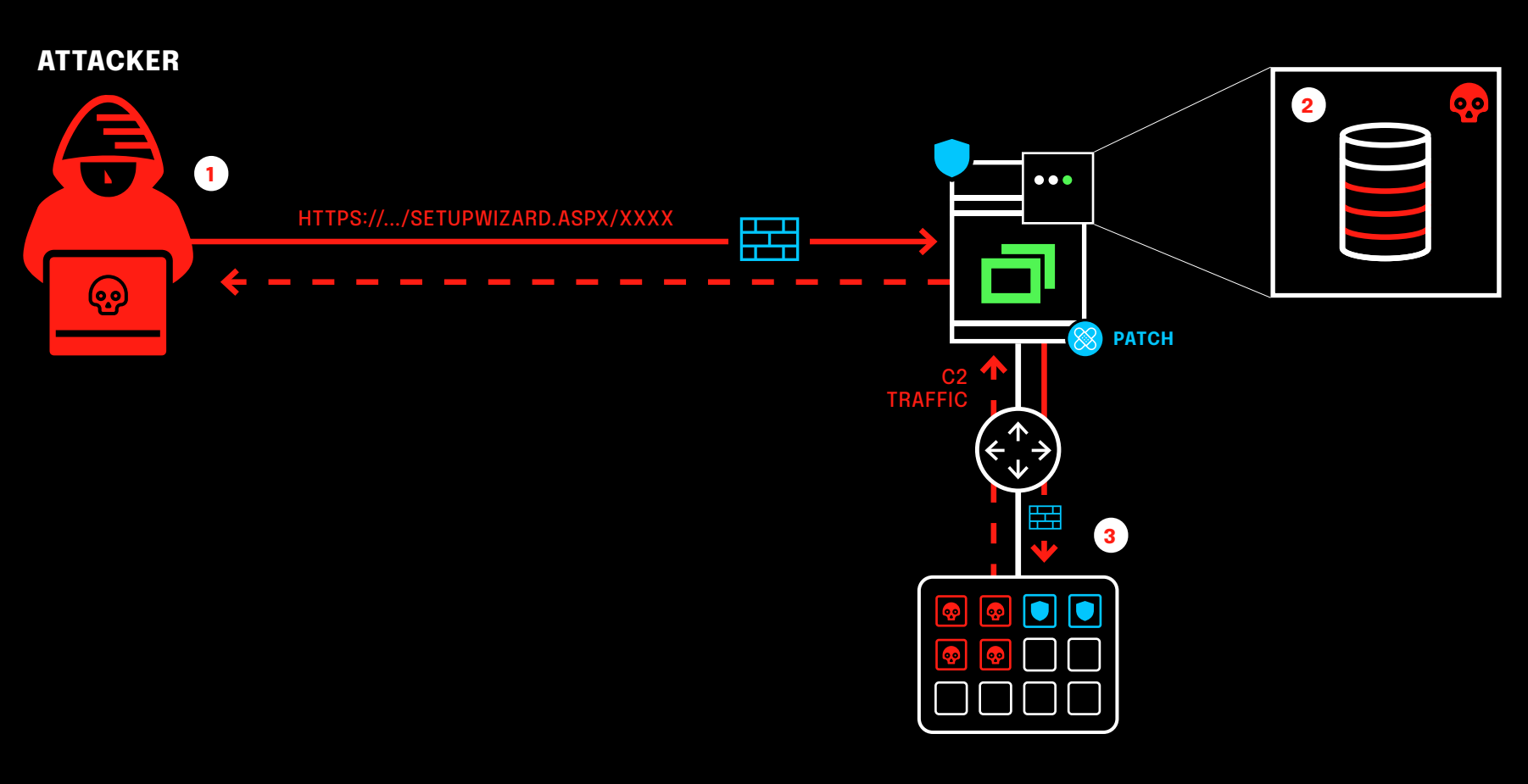
ScreenConnect Authentication Bypass (CVE-2024-1709)

On February 19, 2024, ConnectWise disclosed a critical vulnerability in ScreenConnect, CVE-2024-1709, involving an authentication bypass that could enable remote code execution. This disclosure came just days before a major cyberattack on Change Healthcare, which disrupted services across the healthcare sector. The rapid sequence of events highlighted the vulnerability of healthcare infrastructure to cyber threats and underscored the urgency of robust cybersecurity measures.

mSOC confidence score	Confirmed
Threat category	Vulnerability Disclosures - 0-days
Severity	Critical (CVSS score 10)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1556 - Modify Authentication Process	Exploiting vulnerable public facing application	Traffic Obfuscation	Low	Enterprises

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1047 - Audit	Public facing application	Behavior detection	Behavioral analysis, Logon sessions	Cybercriminals, APTs



Malicious HTTP

1. The attacker crafts a malicious HTTP request to manipulate the URL path, exploiting the improper handling of URL paths in ScreenConnect. This allows the attacker to bypass authentication checks and access the setup wizard of a ScreenConnect instance that has already been configured.

M Next-generation firewalls may be able to block the exploitation of such vulnerabilities once they are known and a signature has been created. Using EDR (Endpoint Detection and Response) solutions with behavioral detection capabilities could help prevent these types of exploits. Timely patching, especially for public-facing applications, is the most crucial action to take.

Setup wizard exploit

2. Using the setup wizard, the attacker can then create an administrative user. This action effectively overwrite the existing user database. All previous local users are removed, leaving only the newly created admin user. This grants the attacker full administrative rights over the ScreenConnect instance.

M Regular audits and user account reviews can help quickly identify and respond to such exploitation. Implementing strict controls on user account management and monitoring for unexpected changes in administrative privileges are essential.

Act on objectives

3. With administrative access, the attacker has the capability to utilize the ScreenConnect server as their own command and control (C2) server. This could facilitate lateral movement within the network, allowing the attacker to execute objectives such as deploying further malware, conducting surveillance, or exfiltrating sensitive data.

M Implementing a zero-trust network design will help limit the blast radius. EDR solutions can also help prevent and detect common steps in the attack chain such as reconnaissance and lateral movement. Enhanced monitoring and alerting for abnormal activities within the network can further mitigate the impact of such attacks.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix