ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Bridging the compliance gap

What's more important: compliance or cybersecurity?

The Chief Information Security Officer (CISO) role has evolved rapidly over the last decade. This is at least in part because the regulatory environment is in constant flux, with new mandates and international sanctions altering compliance requirements almost daily. But what keeps CISOs up at night more: the fear of a cyber attack or the stress of meeting regulatory requirements?

Compliance has become a crucial focus with the implementation of regulations like the GDPR, CCPA, and various global data privacy directives. Whilst regulations exist across all industries, compliance has garnered increased attention because it directly impacts the day-to-day lives of ordinary people.

Is compliance the be-all-end-all when it comes to cybersecurity? Or is there a bridge we need to gap when it comes to compliance versus practical cybersecurity requirements?

In this **'Bridging the Compliance Gap'** episode of Threat Talks we explore how to ensure that your organization is on the same page, what gaps need to be bridged and what CISOs fear more at the end of the day: hackers or auditors?

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

- Accellion file transfer
- OKTA data breach
- Capital One data breach

35% of risk executives said compliance and regulatory risk presents the greatest threat to their company's ability to drive growth. Another 35% said cyber or information risk was.

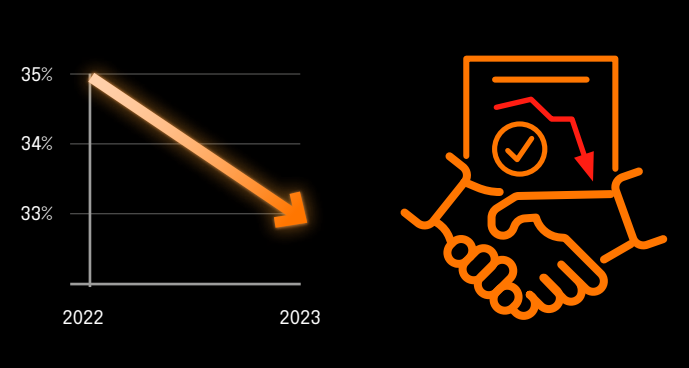
Source: PwC Pulse Survey of CROs and Risk Management Leaders, 2022

Breaches cost almost $220,000 more on average when noncompliance with regulations was indicated as a factor in the event.

Source: IBM's Cost of a Data Breach Report, 2023

Organizations with a high level of noncompliance with regulations showed an average cost of USD 5.05 million. This is a 12.6% increase compared to the average cost of a data breach, or USD 560,000.

Source: IBM's Cost of a Data Breach Report, 2023



33% of respondents predict their compliance teams will grow in the next 12 months, down slightly from 35% in 2022.

Source: Thomson Reuter's Cost of Compliance Report, 2023

Accellion File Transfer Appliance (FTA) Breach

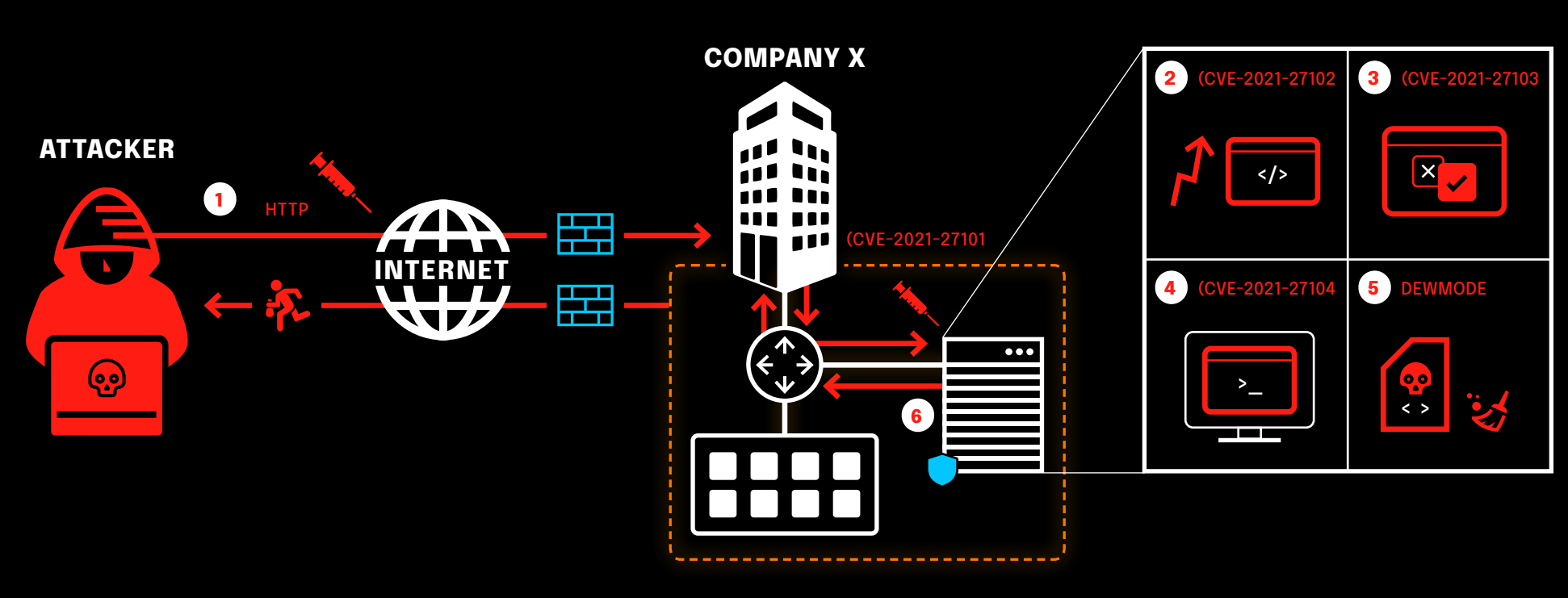
Compliance - Creating Operational Blind Spots

In late 2020 and early 2021, the Accellion File Transfer Appliance (FTA) was the target of multiple sophisticated cyberattacks. Organizations used the Accellion FTA, a legacy file transfer system, because it met the compliance requirements for secure data transfer. Despite being compliant, the FTA was outdated and contained multiple vulnerabilities, leading to data breaches affecting numerous high-profile organizations, including Shell, the Reserve Bank of New Zealand, and the Australian Securities and Investments Commission (ASIC).

mSOC confidence score Confirmed
Threat category Vulnerability - 0-days
Severity Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1071 - Application Layer Protocol	Exploit vulnerabilities to exfiltrate data	Logs Clearing	High	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic M1031 - Network Intrusion Prevention	Act on Objective	Network Traffic Content	High	Cybercriminals



Intial Access via SQL injection (CVE-2021-27101)

1. The attacker exploits CVE-2021-27101 by sending maliciously crafted HTTP requests with a manipulated Host header to exploit an SQL injection vulnerability. This allows them to execute arbitrary SQL commands on the backend database, gaining unauthorized access to the server.

M Modern firewalls can detect and block known exploit signatures, helping to prevent attacks once vulnerabilities are identified. Geofencing can reduce the attack surface by restricting access based on geographic locations, though it is not foolproof. EDR solutions provide continuous monitoring and can detect suspicious activities, such as abnormal SQL queries, that may indicate an ongoing attack. Web Application Firewalls (WAFs) are particularly effective in detecting and blocking SQL injection attempts by filtering and monitoring HTTP requests.

Remote code execution (CVE-2021-27102)

2. The attacker exploits CVE-2021-27102 to execute operating system commands through a local web service call. This grants them higher control over the compromised system.

M Regular patching and updates are crucial to fix known vulnerabilities. Continuous monitoring of web service calls for abnormal behavior can help detect and prevent such exploits.

Server-Side Request Forgery SSRF (CVE-2021-27103)

3. At this point, exploiting CVE-2021-27103, the attacker is able to perform SSRF[1] to make the vulnerable system send unauthorized requests to internal resources, allowing them to interact with and exploit other internal systems.

M Input validation and sanitization are essential to prevent SSRF. Restricting internal network access to essential services can minimize the risk of unauthorized requests.

OS command execution (CVE-2021-27104)

4. By abusing CVE-2021-27104, the attacker is now able to execute further operating system commands through crafted POST requests, solidifying their control over the system.

DEWMODE web shell

5. The attacker installs a webshell named DEWMODE. This webshell allows the attacker to view and download files from the victim machine. It also contains a cleanup function to remove itself and clean traces of the attack.

M Proper segmentation and strict policies on a next-gen firewall would forbid these webshell connections. Additionally, blocking well-known malicious sources (IOCs) could help limit the chance of a successful attack.

[1] Server-Side Request Forgery (SSRF) is a vulnerability where an attacker manipulates a server to make unauthorized requests to internal or external resources on behalf of the server, potentially leading to unauthorized access to sensitive information or internal systems.

Consideration:

Compliance with data transfer regulations led organizations to rely on outdated technology, creating security blind spots that were exploited by attackers. These examples illustrate the complexities of balancing compliance and security, demonstrating that merely adhering to compliance standards does not ensure robust security, and in some cases, can introduce new vulnerabilities.

- **HIPAA** – Health Insurance Portability and Accountability Act – Secure transmission of sensitive healthcare information
- **GDPR** – General Data Protection Regulation – The protection and secure transfer of personal data of EU citizens
- **PCI DSS** – Payment Card Industry Data Security Standard – Secure handling of cardholder data
- **FISMA** – Federal Information Security Management Act – Ensuring the protection of federal information systems

OKTA Customer Support Security Incident

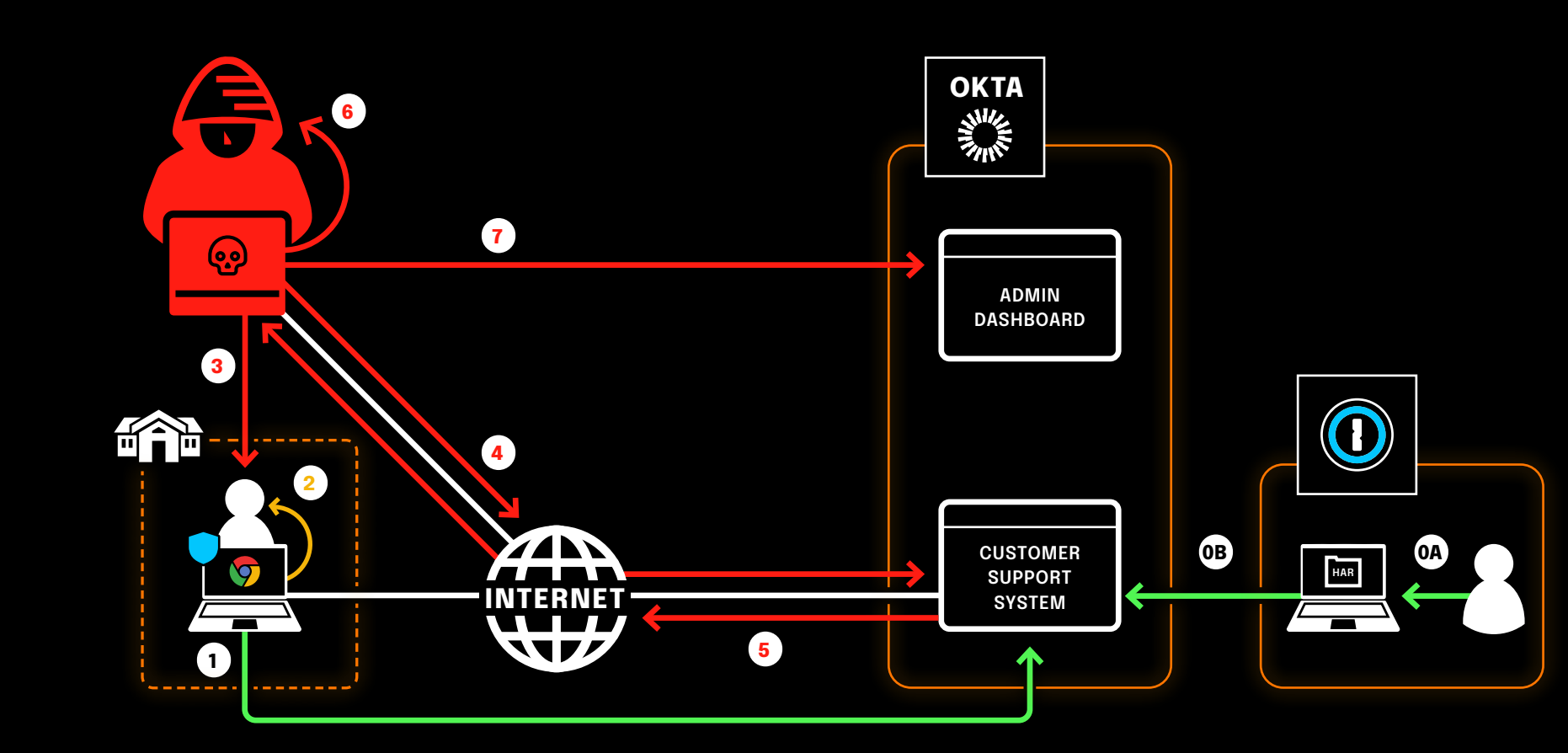
Compliance - Gaps and Human Error

In October 2023, OKTA, a company that specializes in Identity and Access Management (IAM) experienced a security incident stemming from a compliance gap and human error. An OKTA employee inadvertently saved a service account password in their personal Google account by allowing Chrome to save the password while logged in with their personal credentials. The breach came to light when companies such as 1Password, BeyondTrust, and Cloudflare notified OKTA of suspicious activity. This incident highlights the critical need for extending compliance policies to cover the intersection of personal and work-related account usage, ensuring that proper protocols are in place to prevent such vulnerabilities.

mSOC confidence score Confirmed
Threat category Insider threat - Unintentional
Severity Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1071 - Application Layer Protocol	Exploit personal password stores	None	Medium	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic M1041 - Credential Access Protection	Credential Compromise	Network Traffic Content	High	Cybercriminals



Creation of HAR file

0A. An 1password employee was engaged with OKTA support and created a HAR (HTTP Archive) file to help support. This HAR file contains a record of all traffic between the browser and the OKTA servers.

0B. The created HAR file was uploaded to OKTA customer support portal.

Logging into OKTA customer support portal

1. An OKTA employee remotely logs in from home to the OKTA customer support portal using an OKTA service account on a laptop managed by OKTA.

Storing credentials in a personal Google account

2. The employee used a Chrome browser that was logged in with his personal account. After logging in to the OKTA support portal, the OKTA service account credentials were stored within the employee's personal Google account.

Retrieving the credentials

3. An attacker gained access to the credentials stored within the employee's personal Google account. How this access was gained remains unclear, but it could have been through leaked credentials from other data breaches.

M Although the specific attack vector is unclear, an EDR solution might have prevented this attack and could be used later to check if the device was accessed by a malicious adversary.

Accessing the OKTA Customer Support Portal

4. The adversary used the gained OKTA service account to login to the OKTA customer support portal.

M Implementing Multi Factor Authentication (MFA) would make gaining access more difficult. Restricting access to the customer portal with specific IPs, GEO-locations or by using a VPN limits the chance of a successful login.

Retrieving the HAR files

5. Download the HAR files from the OKTA customer support portal.

M Next-gen firewalls can scan the outgoing traffic and data filtering policies can limit or prevent downloading certain files.

Retrieve session tokens

6. The adversary extracts the stored session tokens from the HAR files.

Login to 1password OKTA Dashboard

7. The adversary logs in to the OKTA administrative portal with the retrieved session token. The adversary updated and activated an IDP configuration. When a report was requested of the administrative users an email was being send to a member of the 1password IT team, which caused an alert. 1password investigation on this alert lead to report this incident to OKTA on September 29th.

M Multi Factor Authentication and short lived sessions help to mitigate this risk, OKTA also have a feature called Admin Session Binding, which requires a re-login if the session is being re-used from an IP address with a different ASN (Autonomous System Number).

HTTP Archive (HAR)

A HAR (HTTP Archive) file is a format used to capture and record the sequence of network requests and responses made by a web browser as it loads a webpage. It typically contains detailed information about each HTTP transaction. HAR files are often used for debugging and analyzing web applications, as they provide a comprehensive view of the communication between a web browser and a web server. They are particularly useful for diagnosing performance issues, identifying failed requests, and troubleshooting other network-related problems.

Capital One data breach

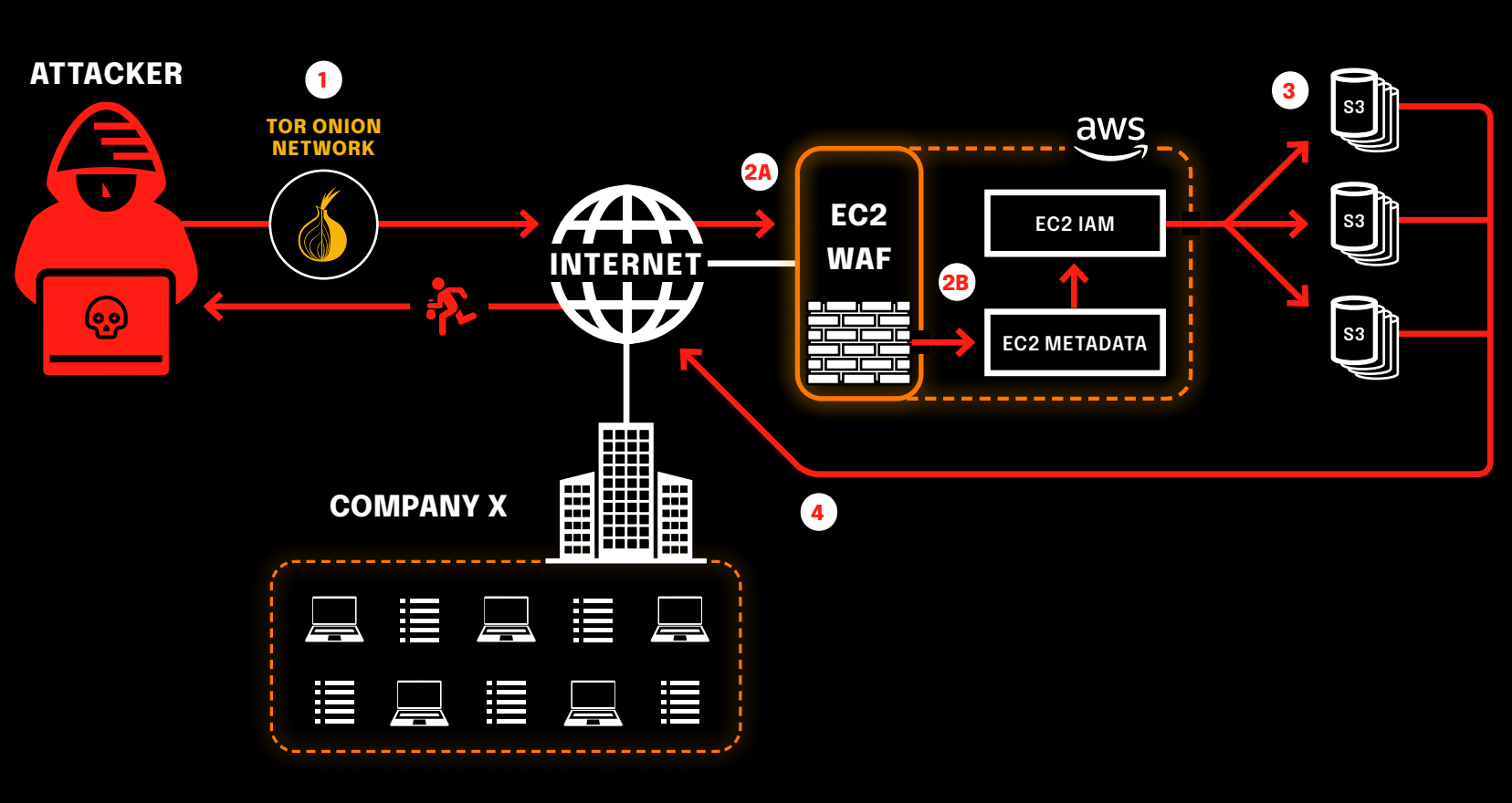
Compliance - Induced False Sense of Security

On August 2, 2019, a former Amazon employee was arrested for stealing over 100 million consumer credit applications from Capital One. Despite compliance with various industry regulations like PCI DSS, Capital One's reliance on cloud security and compliance created a false sense of security, leading to critical oversights. The misconfigured web application firewall (WAF) on AWS allowed a Server-Side Request Forgery (SSRF) attack, which went undetected by internal security measures.

mSOC confidence score Confirmed
Threat category Misconfigurations - Insecure implementation
Severity Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application	Exploit WAF Misconfiguration	Masquerading and Mimicking	Medium	Enterprise

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1030 - Network Segmentation M1016 - Vulnerability Scanning	Misconfiguration	Application Log, Network Traffic	Critical	Cybercriminals



Initial attack

1. The attacker accessed Capital One's AWS EC2[1] instances through anonymizing services such as the TOR network and VPN service provider IPredator. These services were used to obfuscate their identity and avoid detection.

M Restrictive firewall rules and the use of dynamic lists can help block traffic from suspicious sources such as TOR relay nodes. Implementing these measures would make it harder for attackers to use anonymizing services to gain access.

Server-side request forgery

2A. Due to a misconfigured Web Application Firewall (WAF)[2], the attacker was able to perform a Server-Side Request Forgery (SSRF) attack. This involved sending crafted requests as a remote user to internal services that were otherwise inaccessible. Specifically, the attacker used the WAF to access the EC2 instance metadata service.

M Proper configuration and regular audits of WAF settings are essential. Ensuring that WAFs are not overly permissive and correctly validating HTTP requests can prevent SSRF attacks.

Credentials

2B. By accessing the EC2 instance metadata service, the attacker retrieved IAM[3] role credentials assigned to the EC2 instance, including temporary security credentials such as Access Key ID, Secret Access Key, and a security token.

M Using IAM roles with the principle of least privilege and regularly reviewing IAM policies can reduce the risk. Monitoring access to the metadata service and implementing the use of IAM roles with limited permissions are critical defense strategies.

S3 buckets

3. Using the IAM credentials obtained, the attacker gained access to various S3 buckets where sensitive data was stored. The permissions associated with the IAM role were overly permissive, allowing the attacker to list the contents of the buckets and download the data.

M Restricting IAM roles to the minimum necessary permissions and using AWS S3 bucket policies to enforce least privilege can mitigate such risks. Enabling logging and monitoring access to S3 buckets can help detect unauthorized access.

Data exfiltration

4. The attacker used the AWS sync command to copy nearly 30 GB of Capital One credit application data from these buckets to their local machine. According to the FBI report, the attacker accessed more than 700 AWS buckets.

M Implementing data exfiltration detection mechanisms and setting up alerts for unusual data transfer activities can help in early detection of such breaches. Regular audits and the use of encryption for data at rest and in transit are also crucial.

[1] Amazon EC2 is a web service that provides resizable compute capacity in the cloud, allowing users to run virtual servers, known as instances.

[2] WAF is a web application firewall that helps protect web applications by filtering and monitoring HTTP requests. It enables users to define rules that block, allow, or monitor web traffic based on specified conditions.

[3] IAM is a service by Amazon Web Services (AWS) that helps control access to AWS resources. It enables to manage access to AWS services and resources securely.

Consideration:

Capital One's compliance with industry regulations, such as PCI DSS, led to a false sense of security, contributing to critical oversights in their security practices. Despite adhering to these regulations, their firewall was misconfigured, allowing unauthorized access to sensitive data. This breach went undetected by Capital One's internal security measures, highlighting the gap between compliance and actual security practices. The reliance on regulatory compliance led them to neglect essential security measures such as thorough configuration management and continuous monitoring. Moreover, existing regulations did not mandate specific measures for cloud security configurations, which further contributed to the breach.

- **PCI DSS** - Payment Card Industry Data Security Standard – Ensured the secure handling of cardholder data
- **Financial Regulations** – Compliance with various financial industry regulations

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