ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talk 3: The Authentication Apocalypse

Staying Ahead of the Hacker

Every other day, we are faced with yet another news alert about data breaches and stolen credentials. If yours are amongst those, criminals could have acces to your bank accounts, healthcare records, company secrets, and more. Authentication is important, as it makes stealing your information harder: the harder it is to access your data, the more likely that criminals will choose someone else to target.

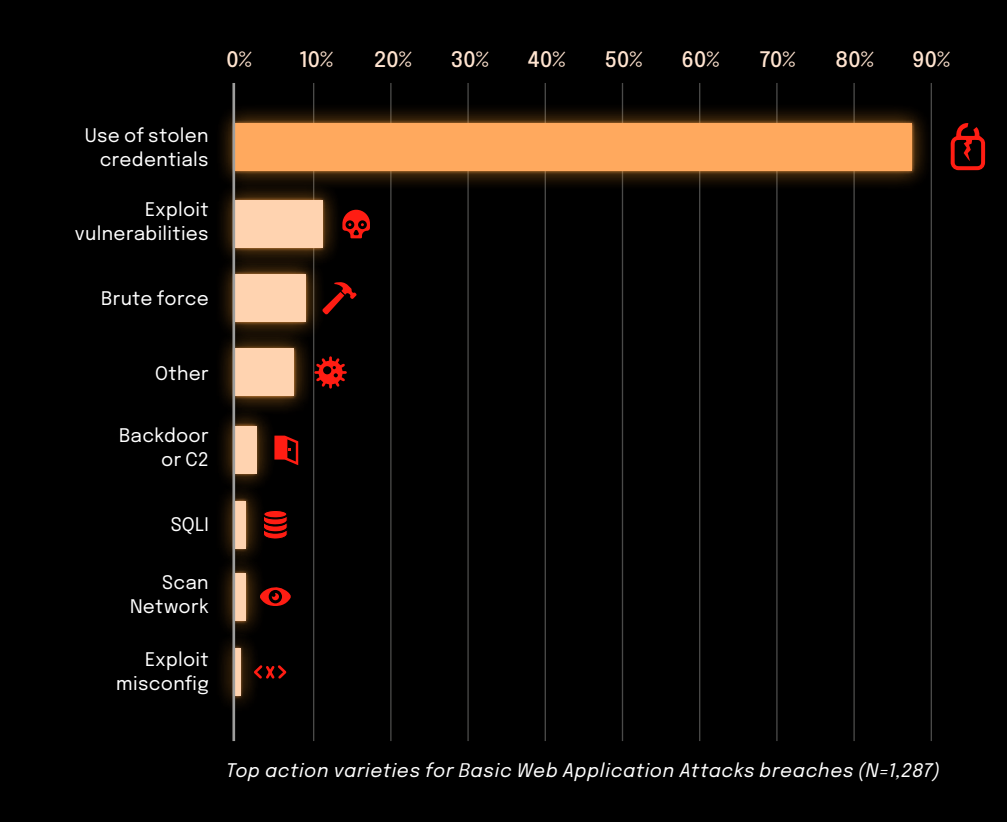
At its core, authentication verifies the identity of users seeking access to various digital services and platforms. There are numerous methods and approaches to this, each offering its own blend of security and convenience. Multi-Factor Authentication is perhaps the most well-known option, though password-less authentication is also on the rise. The future-forward approach of biometric authentication is also an option.

Does your company require authentication methods for signing in? For a deep-dive into modern day authentication, tune in for this episode of Threat Talks: Authentication.

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

- Outlook Vulnerability
- Google OAuth
- Ivanti EPM

86% of data breaches occur due to weak or stolen credentials (like passwords).

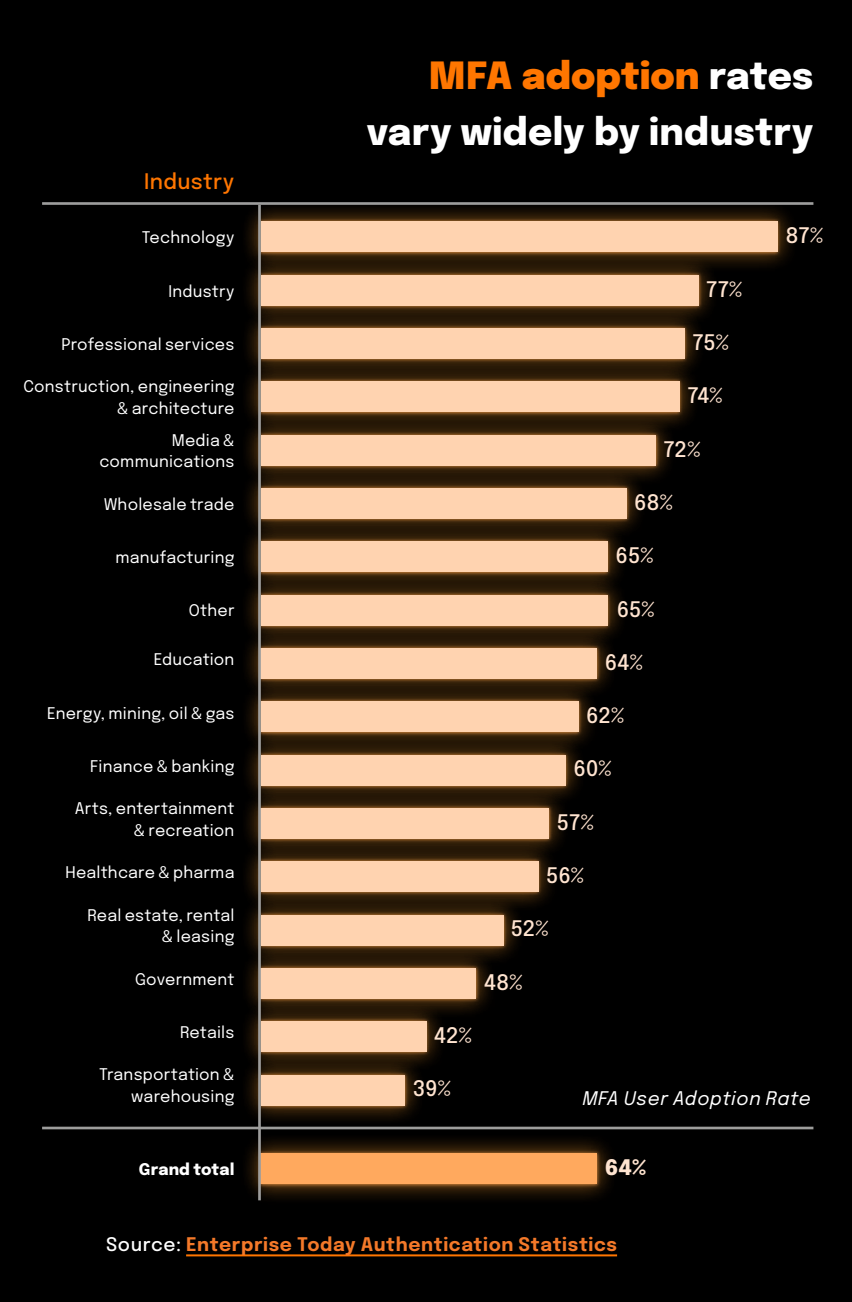


Source: Verizon's 2023 Data Breach Investigations Report

MFA Blocks **99,9%** of modern automated cyberattacks

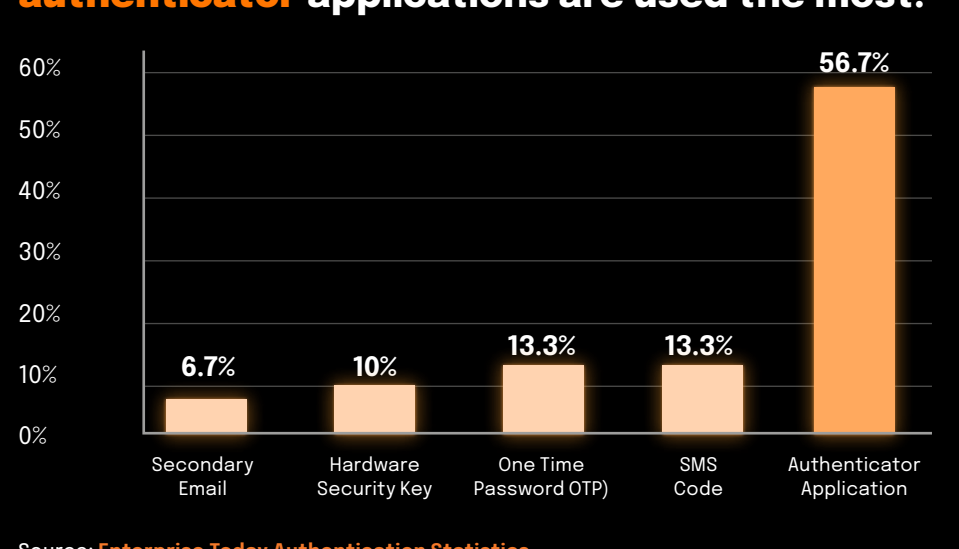
Source: 17 essential Multi-Factor Authentication (MFA) Statistics 2023

MFA adoption rates vary widely by industry



Source: Enterprise Today Authentication Statistics

Out of all authentication methods, authenticator applications are used the most.



Source: Enterprise Today Authentication Statistics

Outlook vulnerability CVE 2023-23397
APT 28 Fancy Bear

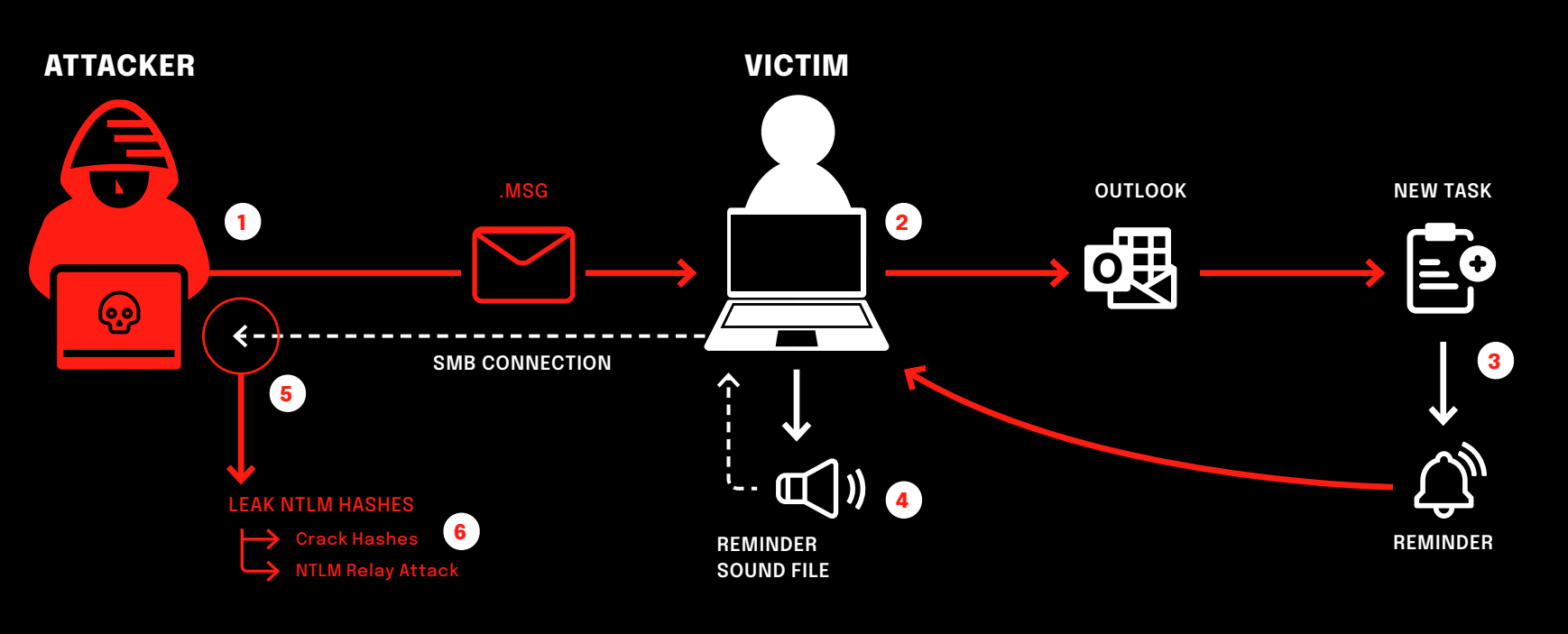
On March 14, 2023, Microsoft disclosed a critical vulnerability in Outlook, identified as CVE-2023-23397. This vulnerability allows a threat actor to craft a malicious email, scheduling a task specifying a custom wave file as a notification sound. The flaw triggers automatically when processed by the Outlook client, leading to exploitation before the email is viewed in the Preview Pane. An attacker who successfully exploits this vulnerability could access a user's Net-NTLMv2 hash, potentially enabling NTLM Relay attacks or hash cracking for authentication on remote services.

This severe flaw in Microsoft's email service has been exploited by the Russian state-sponsored actor APT28, also known as Fancy Bear or Strontium. They have targeted government, energy, transportation, and other key sectors in the United States, Europe, and the Middle East.

mSOC confidence score Confirmed
Threat category Vulnerability Disclosures - 0-days
Severity Critical (CVSS score 9.8)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
TA0006 - Credential access	Obtaining NTLM hashes for password cracking or authentication through pass-the-hash attacks	Bypassing user interaction	Low/medium	Any, Military, Government

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1032 - Multi-factor Authentication	Software vulnerability	Network traffic logs	High	Any, Nation-State Actors, Advanced Persistent Threats



Crafting Malicious Email
1. The attacker sends a malicious email to the victim, containing a parameter (PidLidReminderFileParameter) that enables the attacker to set a custom notification sound for items such as tasks or meeting notifications.

Email Recieved
2. The victim receives the email in their Outlook client.

Scheduled Task
3. The malicious email schedules a task or meeting invite, adding an asynchronous task to play the scheduled reminder, all without requiring any user interaction.

Reminder
4. When the reminder time arrives, the task plays the wave file. Since this file's path points to an attacker-controlled server, Outlook initiates an outbound SMB connection.

M Limiting outbound traffic via restrictive firewall rules can prevent outbound SMB connections to untrusted destinations.

NTLM Leak
5. The threat actor's SMB[1] server receives the inbound request and captures the Net-NTLMv2 hashes of the targeted user

Act on Objective
6. At this point, the attacker can use the hashes to conduct a relay attack, authenticating with other servers that support NTLMv2[2] authentication, or they may attempt to crack the hashes to obtain the underlying plaintext credentials.

ON2IT - What the SOC did

As soon as the vulnerability was disclosed, ON2IT Security Operations Center (mSOC) swiftly reviewed every managed customer environment to adjust overly permissive rules that allowed outbound SMB connections to the internet. Each customer was promptly contacted and advised to patch their Outlook clients as soon as possible.

[1] SMB (Server Message Block) is a network communication protocol used by Windows computers to share access to files, printers, and serial ports over a network. It facilitates the transmission of data between nodes on a network, allowing computers to read and write to files and request services from server programs in a network.

[2] Net-NTLMv2 is an authentication protocol implemented by Microsoft. It employs a challenge-response mechanism for authentication, where a server challenges a client to prove its identity using a hash of the user's password, combined with encryption.

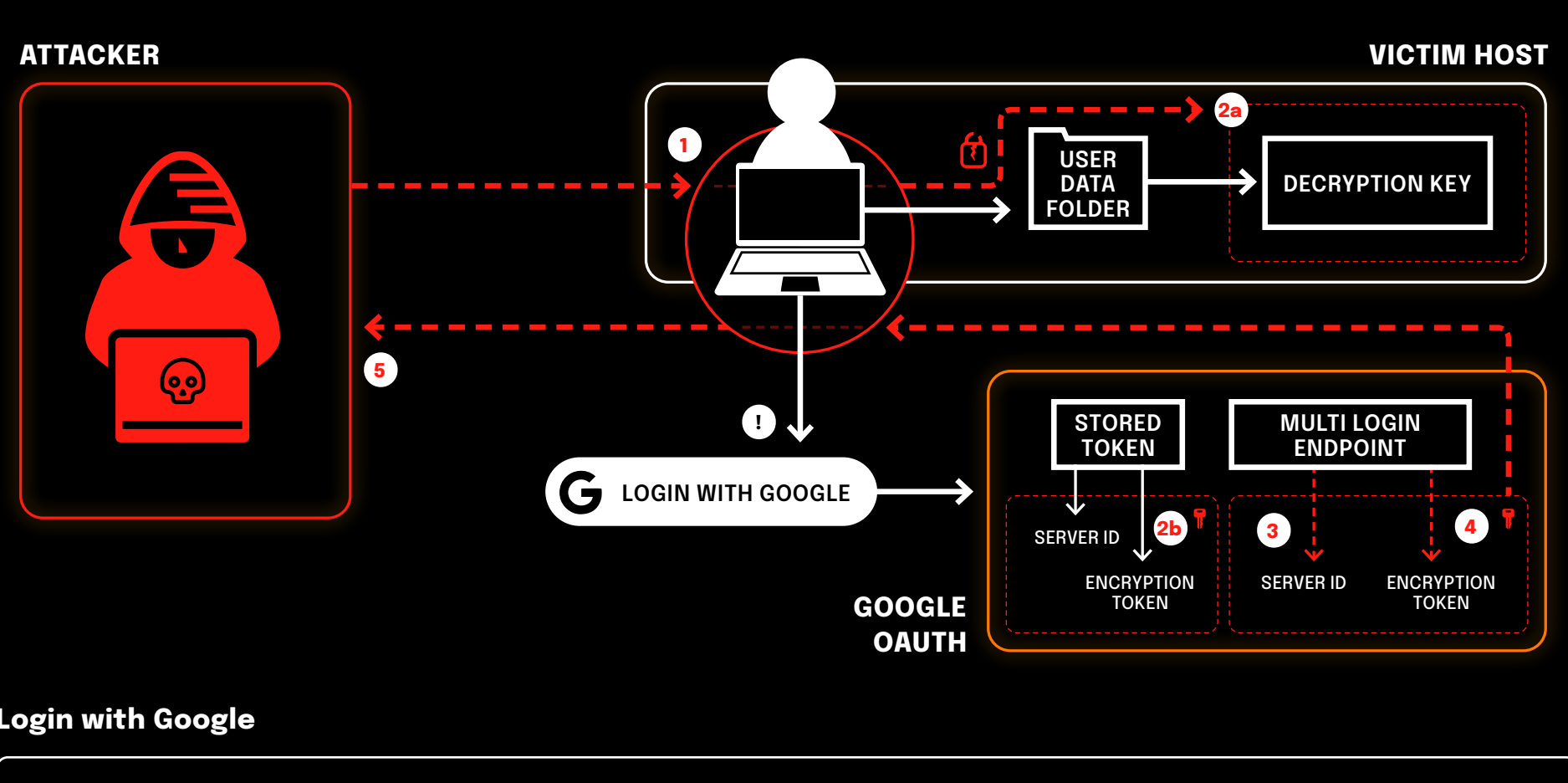
Google OAuth MultiLogin endpoint exploitation

Multiple information-stealing malware strains have been identified exploiting an undocumented Google OAuth endpoint known as "MultiLogin", typically used for synchronizing accounts across different Google services. These malicious programs are designed to regenerate expired authentication cookies, enabling unauthorized access to Google accounts. This capability persists even after the account passwords have been reset, posing a significant security challenge as it circumvents standard account protection measures.

mSOC confidence score Confirmed
Threat category Malware - information-stealing
Severity High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1134 - Access Token Manipulation	Obtaining access to user accounts through malware infection	Encryption, Bypassing Multi-Factor Authentication (MFA)	Medium	Individuals

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1018 - User Account Management M1018 - User Training	Malware infection	Behavioral analysis, logon sessions	High	Cybercriminals



Login with Google

As a prerequisite for this attack to be successful, a user must have authenticated to a service using a Google account at least once, as this type of authentication generates a session cookie[1].

Infection
1. The attacker manages to infect the victim's device with a malware.

Encryption Key:
2a. The malware retrieves an encryption key stored in Chrome's Local State within the User Data directory. This key is similar to the one used for storing passwords on the web browser.

Attacking the Stored Token
2b. The Malware will target Chrome's token_service table of WebData. The table contains the service account ID (GAIA ID) and the encrypted_token. The previously retrieved encryption key is used to decrypt the token.

Attacking the Stored Token
3. By leveraging the MultiLogin endpoint, the attacker is able to generate a new valid token which will bypass multi-factor authentication and persist a password reset.

Protecting Intellectual Property
4. The malware developers use advanced encryption and blackboxing[2] techniques to protect the methodology of their exploit. This encryption acts as a barrier, preventing other threat actors from duplicating their method and evading detection by standard security protocols.

Retrieving the Token
5. The new token is encrypted and sent back to the attacker. The use of encrypted communication between the malware and the MultiLogin endpoint is less likely to trigger alarms in network security systems, allowing the attacker to maintain unauthorized access.

M To protect against this exploit, users should regularly sign out of all sessions and revoke any suspicious connections via their account's device management page.

[1] Small piece of data stored on a user's device by a web browser while the user is browsing a website. It is used to remember stateful information or changes within the browsing session, such as login status or, for example, what items are in a shopping cart.

[2] Concealing the internal workings of a system or process, making it opaque or 'black' to outsiders. This technique is often used to protect proprietary methods or to prevent attackers from understanding and exploiting a system's vulnerabilities.

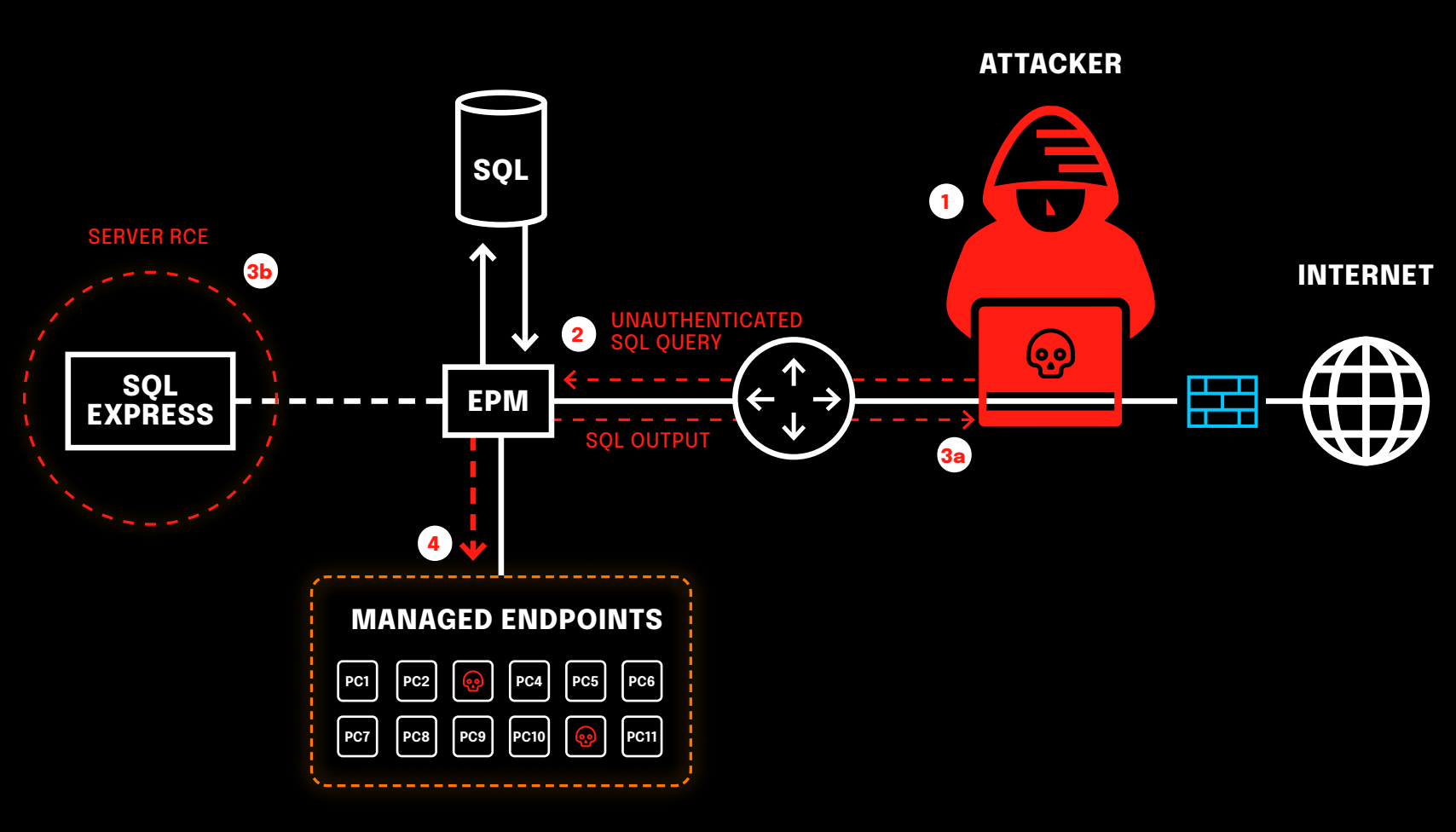
Ivanti EPM SQL Injection

On the 4th of January 2024, Ivanti released a security bulletin reporting a critical vulnerability in its Endpoint Management software, identified as CVE-2023-39336. This vulnerability, if exploited, allows attackers with internal network access to leverage an SQL injection flaw for executing arbitrary SQL queries and controlling devices with the EPM agent, without needing authentication. This risk is present across all MSSQL instances and could potentially lead to Remote Code Execution (RCE) on the core server, when configured with Microsoft SQL Express. Exploiting this vulnerability is trivial due to the low complexity of the attack, which does not require user interaction or privileges, making it necessary to update the affected systems in a timely manner.

mSOC confidence score Confirmed
Threat category Vulnerability Disclosures - CVE Disclosures
Severity Critical (CVSS score 9.6)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1210 - Exploitation of Remote Services	Exploitation of Software Vulnerability	N/A	Low	Enterprises

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1051 - Update Software M1030 - Network Segmentation	Software vulnerability	Application Logs, Network Traffic	Critical	Cybercriminals, APTs



Foothold
1. The attacker requires access to the internal network as a prerequisite for initiating this attack.

M Enhancing prevention and detection involves prioritizing patch management, improving network visibility, strengthening authentication mechanisms, and conducting security awareness training. All these steps can help mitigate the risk of initial footholds.

SQL Injection
2. The threat actor can perform an SQL[1] injection against the EPM server without authentication, to execute arbitrary SQL queries.

M Employing Next-Generation Firewalls (NGFWs) or Web Application Firewalls (WAFs) can help detect and block SQL injection attempts by comparing traffic against known vulnerability signatures. Timely patching of the appliance is essential for effectively mitigating the risk of this attack.

Exploit
3a. Successful exploitation allows the attacker to retrieve output from the SQL server. In scenarios where the core
3b. server uses Microsoft SQL Express, attackers might achieve remote code execution on the core server itself.

Full takeover
4. Following successful exploitation, threat actors could potentially take complete control over any enrolled host.

M Endpoint Detection and Response (EDR) solutions play a crucial role in identifying suspicious activities based on behavioral analysis. These solutions can help pinpoint compromised machines by analyzing patterns and anomalies that deviate from normal operations.

[1] SQL (Structured Query Language) is a programming language designed for managing and manipulating relational databases. It allows manipulate data in a database using simple commands.

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