Threat Talks
Prevent, Pay or Insure?

threat-talks.com

The road to cyber resilience

Days before MGM's computer systems were taken down in a cyberattack, fellow casino operator Caesars paid $15 million to attackers.

MGM chose a different path, involving law enforcement and refusing to pay. Did these different approaches lead to different outcomes, or did the two casino giants lose similar amounts of money down the line?

In the aftermath of these hacks, discussions erupted about how these breaches could have been prevented and whether paying ransom is the right call. While prevention is the cornerstone of cybersecurity, it is not enough on its own. Insurance is becoming vital for organizations facing cyber threats.

To what extent can organizations get insurance against these types of cyber events? Is insurance a primary solution, or just a good fallback to have?

In this **'Prevent, Pay or Insure'** Threat Talk we take a look at how organizations can prepare for stricter insurance demands and make smarter, risk-informed decisions when it comes to cyber threats.

In this Threat Talk we discuss the following threats:

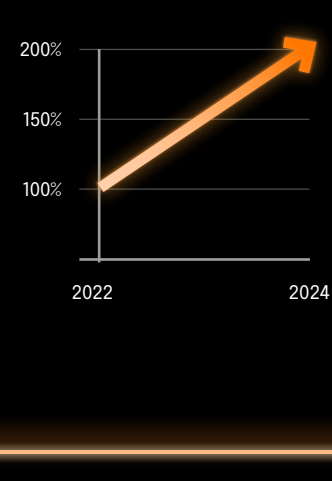
- MGM Resorts Ransomware Attack
- Conti Ransomware Attack on Costarican Government
- Dutch Law Enforcement Data Outleak

The global market for cybersecurity insurance was $7.60 billion in 2021 and is expected to grow to $20.43 billion by 2027.

Source: Network Assured

19% of organizations claimed to have coverage for cyber events beyond $600,000.
55% of organizations claimed to have any cybersecurity insurance at all.

Source: theregister.com, sophos.com



Cyber insurance claims increased by 100% and payouts by 200% in the past 3 years, with the peak claims being 8,100 in 2021.

Source: Network Assured

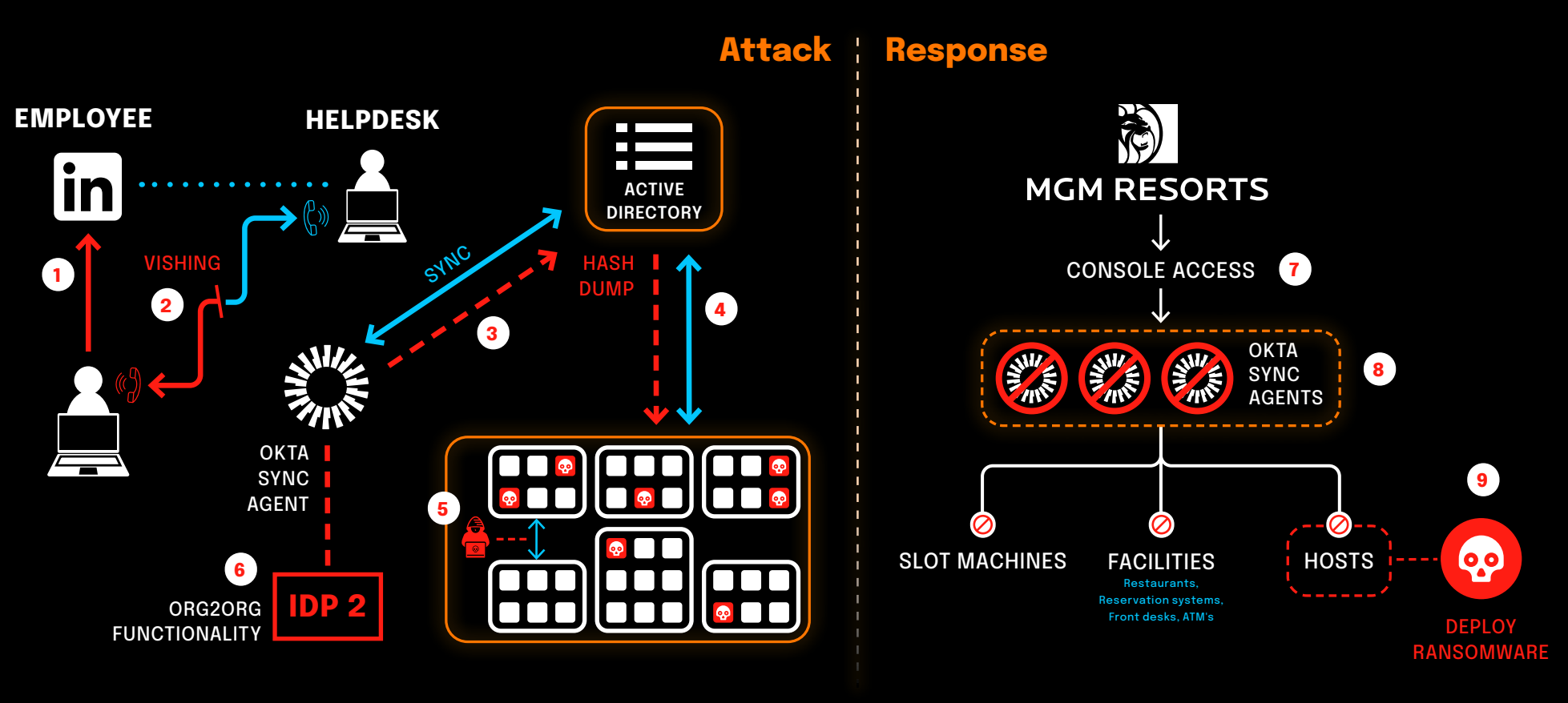
MGM Resorts International
Ransomware Attack

On September 11th, MGM Resorts International, a leading hotel and casino operator, announced a severe cybersecurity issue that disrupted its systems. This included the main website, online reservations, the front desk, restaurant facilities, and in-casino services such as ATMs and slot machines. The problem, which started on a Sunday night, caused widespread outages, especially in Las Vegas. This led to the shutdown of critical systems in an effort to mitigate the issue. Guests faced significant inconveniences, including malfunctioning digital room keys, issues with slot machines, and room charges. The malfunction resulted in substantial revenue losses. MGM reported the incident to the SEC, complying with new regulations for reporting significant cybersecurity incidents. This incident followed a 2020 data breach at MGM, which compromised the personal details of 10.6 million customers.

mSOC confidence score	Verified
Threat category	Cyber Attacks - Ransomware Attacks
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1566.044 - Spearfishing Voice T1486 - Data Encrypted for Impact TA0010 - Exfiltration	Gain a foothold to exfiltrate data and deploy ransomware	Caller ID spoofing, Use of legitimate credentials, Traffic obfuscation, Encryption and Tunneling	High	Enterprise

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1017 - User Training M1030 - Network Segmentation M1053 - Data Backup	Social Engineering, Credential Compromise	Log monitoring (Application, Traffic, Windows events), Unusual login alerts, User behavioral detection	Critical	Cybercriminals



Recon

1. The attackers used LinkedIn to gather information about MGM employees.

M Being mindful of the kind of information we share online can help protect against reconnaissance activities. Social media privacy settings should be restrictive, hiding private information such as date of birth for example.

Social Engineering

2. Using the vishing [1] technique and impersonating a legitimate employee, the attackers deceived MGM's helpdesk, gaining access to the Okta sync agent.

M User training and the use of a validation playbook when resetting accounts, such as calling back on known numbers or using in person/video recognition, can prevent these kinds of attacks.

Credential Gathering

3. With access to the Okta sync agent, the attackers were able to dump credentials from MGM's Active Directory and crack password hashes.

M Conditional access policies can aid in preventing unauthorized access by, for example, blocking attempts from unknown devices. Additionally, access monitoring plays a fundamental role in detecting intrusions at this stage.

Lateral Movement

4. The attackers used lateral movement techniques to further infiltrate MGM's network.

M A Zero Trust network design, combined with the use of EDR (Endpoint Detection and Response) solutions featuring behavioral analysis, can limit the blast radius of such an attack and assist in detecting suspicious activities in a timely manner.

Sniffing Traffic

5. The attackers sniffed additional passwords through their access to the Okta agent servers.

Deploying a Second Malicious IdP

6. The attackers exploited Okta's Org2Org functionality to deploy a second malicious Identity Provider (IdP), establish trust via a federation relationship, and create shadow users linked to real users for extra persistence.

First Response MGM

7. Once it was discovered that the attacker had compromised the Okta environment, MGM implemented conditional restrictions in an attempt to block network access and stop the attack, but this proved insufficient.

8. MGM decided to turn off the Okta sync servers, leading to a shutdown of all network functionalities. This action resulted in disruptions across various facilities, including restaurants, reservation systems, front desks, slot machines and ATM machines.

Act on Objective

9. After a day, the attackers deployed ransomware against over 100 ESXi hosts in MGM's environment. During the attack the threat actors managed to exfiltrate data from the victim environment.

M Certain EDR solutions can detect ransomware activity by using decoy, hidden files. If these files are encrypted, the EDR system can then automatically block the malicious process.

Footnotes

[1] Vishing is a form of phishing that involves using voice communication, like phone calls, to deceive individuals into divulging sensitive information.

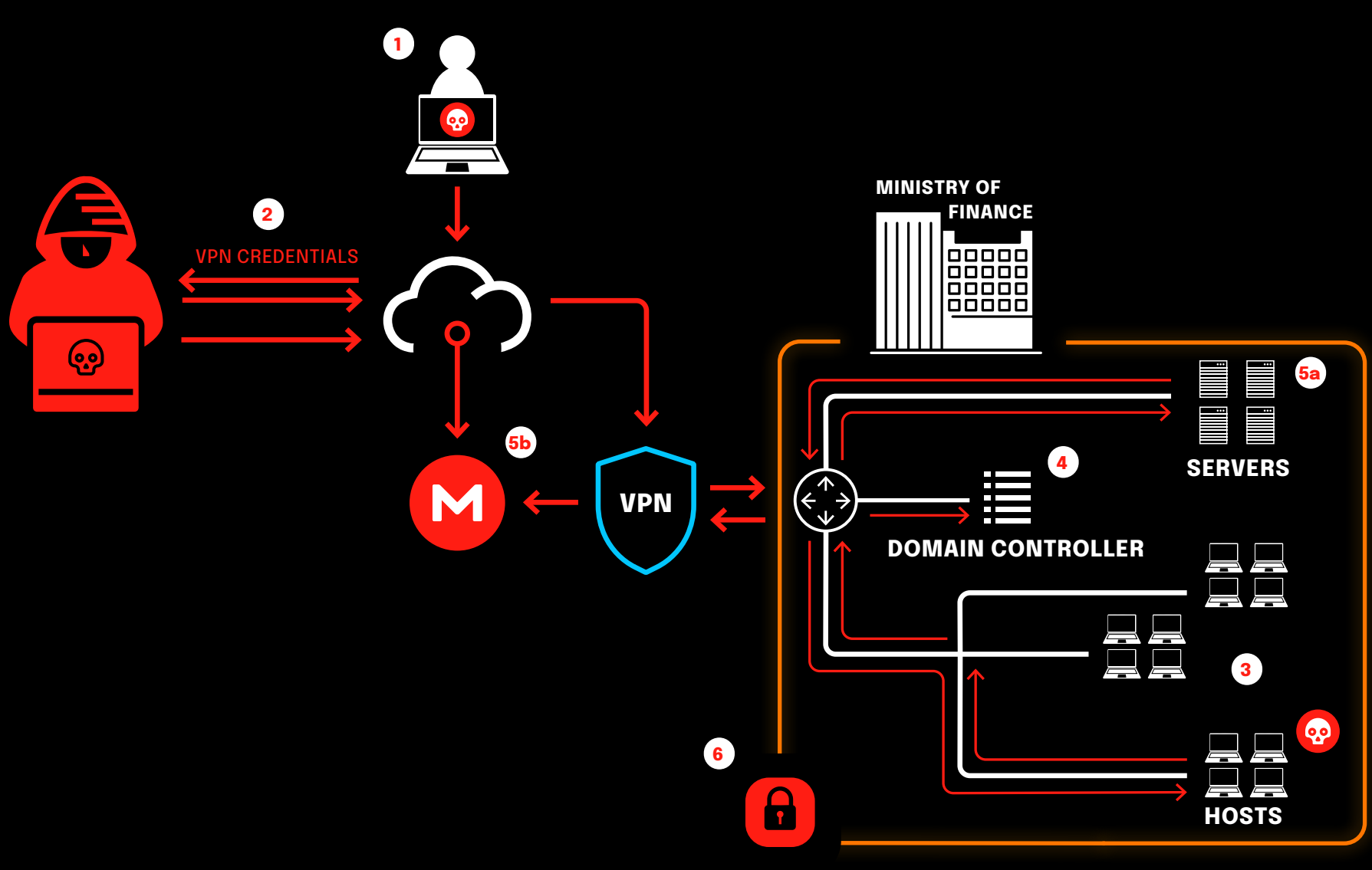
Conti Ransomware Attack
Costarican Government

On April 11, 2022, the Conti ransomware group initiated a cyberattack on Costa Rica's government systems, leading to significant disruptions across multiple ministries. The attackers gained initial access through compromised VPN credentials, conducted reconnaissance, exfiltrated approximately 672 GB of data, and ultimately encrypted critical systems. The breach prompted Costa Rica to declare a national emergency and highlighted vulnerabilities in governmental cybersecurity defenses.

mSOC confidence score	Verified
Threat category	Cyber Attacks - Ransomware Attacks
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1486 - Data Encrypted for Impact TA0010 - Exfiltration	Exploit personal password stores	None	Medium	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1040 - Behavior Prevention on Endpoint M1053 - Data Backup	Credential Compromise	Network Traffic Content	High	Cybercriminals



Initial Access via Compromised VPN Credentials

1. The attacker gained initial access through a system compromised by malware, which allowed them to harvest valid VPN credentials. These credentials enabled unauthorized access to the Ministry of Finance's internal network.

M Implementing multi-factor authentication (MFA) for VPN access can help prevent such attacks or at least add an extra degree of difficulty for the attacker. Regular monitoring of VPN logs for unusual login patterns, along with conducting endpoint security scans, can also help detect and remediate malware infections before they escalate.

Network Infiltration

2. Leveraging the VPN, the attackers infiltrated the Ministry's internal network, establishing a foothold and installing additional Cobalt Strike Beacons [1].

M Updated threat intelligence feeds and Endpoint Detection and Response (EDR) solutions can detect and block malicious activities like Cobalt Strike beacon installation.

Enumeration

3. Inside the network, the attackers performed reconnaissance, gathering information about users, groups, hosts, and domain controllers to map the environment for further exploitation.

M Monitoring for abnormal LDAP queries and Active Directory enumeration attempts can help identify malicious reconnaissance activities. Placing honeytokens on sensitive accounts or resources can also alert defenders to unauthorized access.

Credential Dumping and DCSync Attacks

4. After obtaining local administrator credentials, the attackers used Mimikatz [2] to dump credentials hashes and perform a DCSync attack [3].

M Enforcing privileged account policies, such as just-in-time (JIT) access and removing local admin accounts from endpoints will help prevent these kind of attacks. EDR solutions will alert and block the use of tools like Mimikatz and detect abnormal replication requests from non-domain controllers.

Data Exfiltration Using Rclone and MEGA

5a and 5b. The attackers created Rclone configuration files on several hosts, using them to exfiltrate data to the MEGA file-sharing service.

M Restricting access to unauthorized file-sharing services like MEGA through network policies can prevent this kind of exfiltration. Security teams should monitor for the execution of data exfiltration tools such as Rclone, while implementing data loss prevention (DLP) solutions can detect and block attempts to move sensitive data out of the organization.

Ransomware Deployment and Encryption

6. With elevated privileges and control over the network, the attackers deployed the Conti ransomware, encrypting files and disrupting operations within the Ministry of Finance.

M Maintaining regular, offline backups of critical systems and data is essential to mitigate the impact of ransomware. Organizations should also deploy ransomware detection solutions capable of identifying anomalous encryption activity and conduct regular tabletop exercises to test and refine their incident response plans.

Footnotes

[1] Lightweight implant used by attackers for command-and-control (C2) operations. It allows them to execute commands, and move laterally within a compromised network.

[2] Tool used to extract credentials and password hashes from Windows systems, enabling attacks like credential dumping and privilege escalation.

[3] Technique where an attacker impersonates a domain controller to request and retrieve password hashes from Active Directory, gaining access to sensitive credentials.

Dutch Law Enforcement
Data Breach

On September 27th 2024, news broke about Dutch law enforcement suffering a data breach, initially reported (downplayed) as involving 'only' personal data of 65.000 law enforcement employees (name, email, function). Later it became clear more personal data was leaked. Former employees as well as 'partners', e.g. other parties communicating with law enforcement employees, turned out to have been disclosed ('leaked') as well. Software with an extremely poor security track record (Outlook) was involved. This may well have exacerbated the issue, mainly by lowering the initial exploitation threshold. It should be noted that procurement issues (i.e., the selection of technology unsuitable to the task) is outside the scope of the MITRE ATT&CK framework.

mSOC confidence score	Verified
Threat category	Cyber Attacks - Dataleaks
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1539 - Steal Session Cookie T1563 - Session Highjacking T1567 - Exfiltration	Gain access to device (cookie storage), Obtain and (re)session cookies, Exfiltrate data	-	Medium	Enterprise

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M0913 - Application Developer Guidance M0800 - Authorization Enforcement M1002 - Attestation	Device Comprimise, Credential Compromise, Spearphishing	Log monitoring (Application, Traffic, Windows events), Unusual login alerts, User behavioral detection	Critical	Nation-State Actors

1. User compromised by Spearphish, Drive-by-Download, Executed Attachment, Waterhole Attack, ..

Outlook and session persistence cookies?

Yeehaw!

Attacker obtains session cookie.

2. Attacker reuses session cookie, controls user session.

3. Attacker exfiltrates data from exposed address book.

Obtain Session Cookies

1. This can be realized by way of gaining access to a law enforcement employee device using malware (drive-by download, opening malware-prone documents (Office etc.). Canonic example: attachment masked as a voice memo. This can also be realized by obtaining session cookies can be realised by a remote exploit executing a MitM attack, e.g. using a spearphish attack or a waterhole attack. Proxying to a legitimate backend, for example using Evilnginx2 phishing toolkit.

M Strengthen procurement/deployment, improving endpoint security posture. Employ rigorous endpoint security software to mitigate systemic security flaws, especially when using highly flawed endpoint software. Monitor endpoint and server logs ('events') for irregularities.

Reuse Session Cookies

2. Initiate/resume user session, using session cookie as authentication token.

M Don't uses session cookies as sufficient (re)authentication, validate sessions/ reauthorizations.

Obtain and Exfiltrate Data

3. Readily available, distributed as a global address book.

M Restrict client data transfers. Monitor and analyze data transfers actively and implement data loss prevention (DLP) measures.

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