
maltiverse
Actionable Threat Intelligence
REPORT APR
2025
by LUMU

CONTENT

RESEARCH ARTICLE

- Advisory Alert: Surge in ConnectWise ScreenConnect-Themed Malicious Activity

REPORT

- Indicators by type of activity - april
- Indicators by country - april
- Most active malware families - april

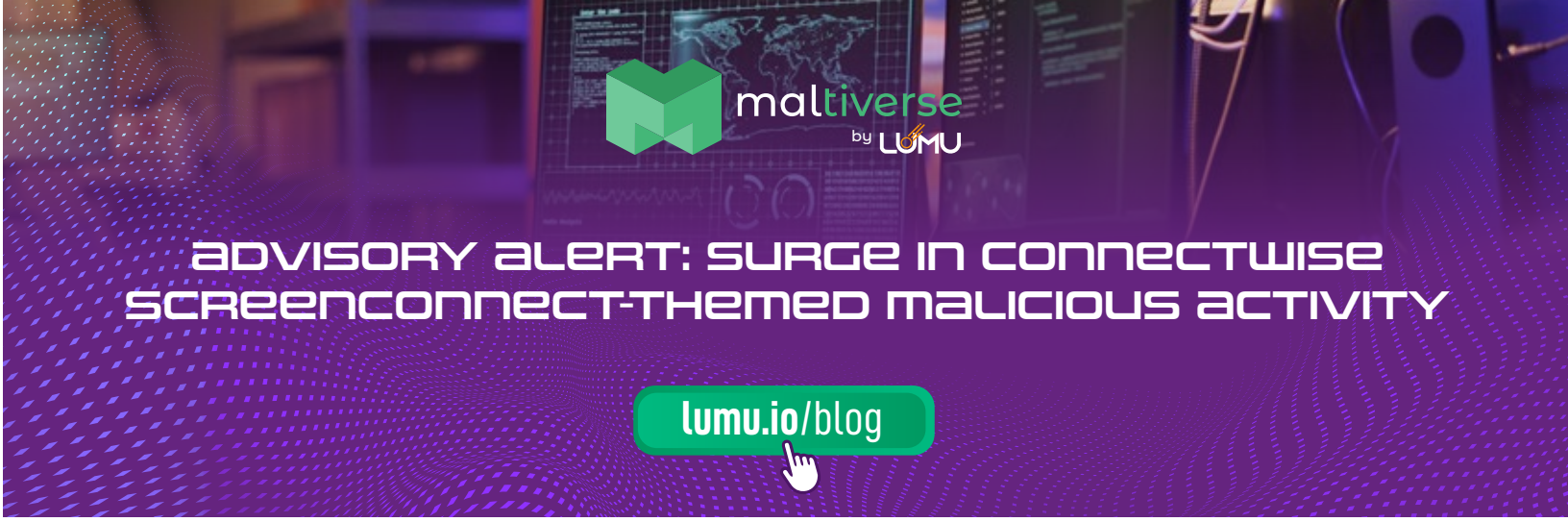
NEWS

- Growing Risk from Autonomous AI Agents
- Data Breach at Co-op Exposes Customers' Personal Information
- Critical "AirBorne" Vulnerability in AirPlay
- Cyberattack on Marks & Spencer Causes £40 Million in Weekly Losses
- Massive Blackout in Spain: Possible Cyberattack Under Investigation
- Spain Approves Historic €1.157 Billion Investment in Cybersecurity

SERVICES

- CTI for Siem
- CTI for Soar
- CTI for Firewalls
- CTI for Routers
- Actionnable threat intelligence
- Threat intelligence platform

maltiverse by LUMU



ADVISORY ALERT: SURGE IN CONNECTWISE SCREENCONNECT-THEMED MALICIOUS ACTIVITY

lumu.io/blog

A rapidly escalating campaign is exploiting ConnectWise ScreenConnect (formerly ConnectWise Control), a widely used remote-support tool, to distribute legitimate client software misused to connect to attacker-controled servers. According to threat-intelligence data from Maltiverse, over 1,300 new Indicators of Compromise (IoCs) mimicking ScreenConnect download paths and binaries have emerged since mid-April 2025. This alert provides a detailed summary of the activity surge, identifies key infrastructure patterns, and offers guidance for detection, hunting, and mitigation to help organizations protect themselves against this evolving threat.

HOW THE THREAT WORKS

The attackers employ belowmethod to exploit ConnectWise ScreenConnect, leveraging social engineering to achieve their goals:

Distribution ScreenConnect Clients for malicious purposes:

TACTIC

Threat actors leverage legitimate, digitally signed ConnectWise ScreenConnect client software, reconfigured to connect to attacker-controlled servers (e.g., connect-004.controlhub.es). These servers are illicitly operated by malicious actors for nefarious purposes. Attackers may target organizations' own ScreenConnect servers through common tactics such as phishing, credential harvesting, exploiting unpatched software flaws or other known misconfigurations (e.g. 2FA not enabled, Not restricted to corp network).

DELIVERY

These clients are distributed through phishing emails, compromised websites, or social-engineering tactics that trick users into downloading and installing them under the guise of legitimate remote-support tools.

IMPACT

Upon execution, the client establishes a connection to the attacker's controlled infrastructure, granting remote access to the victim's system. This enables data theft, deployment of additional malware, or lateral movement across the network.

EDR Detection Struggles

The use of legitimate, signed ScreenConnect clients creates significant challenges for EDR systems:

Trusted Signature

The valid ConnectWise signature (likely issued by a reputable CA like DigiCert) allows the client to bypass signature-based detection, as EDRs generally trust signed binaries from known vendors.

Normal Behavior

The client's core functionality (e.g., remote desktop, session establishment) is indistinguishable from legitimate use, reducing the likelihood of behavioral alerts.

Configuration-Based Attack

The malicious behavior stems from the server connection (connect-004.controlhub.es), not the client's code, making it difficult for EDR to flag the binary itself. EDR must monitor network connections or server reputations, which requires up-to-date threat intelligence.

Living Off The Land

This attack methodology is a prime example of adversaries "Living off the Land" (LotL), or perhaps more precisely, "Living off Trusted Software/Sites." Instead of deploying custom malware for command and control, the attackers leverage a legitimate, widely used, and trusted remote administration tool: ScreenConnect (ConnectWise Control). By embedding malicious configuration into a ScreenConnect client and tricking users into installing it via phishing, they hijack the software's inherent capabilities for remote access, file transfer, and command execution. This approach offers significant advantages for evasion: the malicious traffic blends seamlessly with legitimate ScreenConnect activity, potentially bypassing classic security tools that whitelist or have lower scrutiny for known remote access software. This case shows how the network is the principal way to detect this type of attack. The attacker must connect with the client and in this point the network IOC is relevant to alert to the malicious activity.

Understanding these attack vectors - deceptive client distribution and server exploitation - enables organizations to tailor their defenses effectively against this dual-pronged threat.

Key Observations

#	Indicator / Pattern	Details & Impact
1	**Malicious TLD Concentration**	The .top TLD dominates with 1,005 IoCs, followed by .com (352) and .de (122), highlighting attackers' preference for disposable, low-cost domains.
2	**Sub-domain Farming on Single "Parent" Domains**	Attackers register a single domain and generate numerous sub-domains to host fake clients. Top offenders include: • innocreed[.]com — 193 sub-domains • ratoscreenco[.]com — 15 • controlhub[.]es — 30 • screensconnectpro[.]com — 12 This "domain-burst" tactic maximizes payload distribution while minimizing costs and evading reputation-based detection.
3	**Heavy Use of ASN AS210558 (1 Services GmbH)**	Malicious IPs cluster in AS210558, indicating reliance on a VPS provider with potentially weak abuse oversight.

example IOCs

TYPE	INDICATOR / PATTERN	DETAILS & IMPACT
URL	https://work[.]innocreed[.]com/bin//support.client.exe?i=&e=Support&y=Guest&r=	One of 193 malicious sub-domains under innocreed.com.
DOMAIN	connect-004[.]controlhub[.]es	Parent domain hosting 15 malicious sub-domains.
IP	2[.]58[.]56[.]90	Malicious IPv4 that resolves a hostname tied to ScreenConnect abuse.
HASH	Support[.]client[.]exe 1d5195c858b1fb7f3b8193705bb9aec4f224d000c daf546f27cb29eed6ea7865	SHA256 binary with malicious configuration

A comprehensive, regularly updated IoC list is available on Maltiverse.

Last year, ConnectWise Screen Connect 23.9.7 and prior suffered two critical vulnerabilities, CVE-2024-1708 and CVE-2024-1709, related to Authentication Bypass via path-traversal vulnerability, which could allow an attacker to execute remote code or directly affect sensitive data or critical systems. These vulnerabilities were fixed in subsequent releases. Lumu created a tool to check if your infrastructure is vulnerable to the aforementioned CVEs.

DETECTION & HUNTING GUIDANCE

- **Network & Proxy Logs:** Search for URLs ending in support.client.exe, /ScreenConnect.Client.exe, or containing query strings like i=&e=Support&y=Guest.
- **DNS Filtering:** Block or monitor sub-domains of known malicious parent domains (e.g., *.innocreed.com, *.controlhub.es).
- **ASN Watchlists:** Add AS210558 to high-risk or alerting lists; scrutinize new connections to unfamiliar IPs within this ASN.
- **Endpoint Sweeps:** Identify unexpected ScreenConnect binaries or services; cross-check installations against a whitelist of approved tools.
- **Email & Web Gateway Rules:** Quarantine messages or downloads mentioning "ScreenConnect" unless originating from the official ConnectWise domain.
- **Threat-Intel Feeds:** Integrate connectwise and screenconnect tags from Maltiverse, URLhaus, ThreatFox, and similar sources to track emerging infrastructure.

MITRE ATT&CK TTPS OBSERVED IN THIS CAMPAIGN

To effectively combat the ConnectWise ScreenConnect misuse campaign, it's critical to understand the Tactics, Techniques, and Procedures (TTPs) employed by the attackers. Mapped to the MITRE ATT&CK framework, these TTPs highlight the specific methods used in this campaign, offering actionable insights for detection and mitigation. Below is a detailed breakdown of the observed TTPs, with examples from the campaign and tailored recommendations:

TTP	DESCRIPTION	EXAMPLE IN THIS CAMPAIGN	DETECTION & MITIGATION
T1566 – Phishing	Phishing emails deliver malware or trick users into installing malicious software.	Phishing campaigns distribute misused ScreenConnect clients via links to domains like connect-004.controlhub.es.	– Conduct user awareness training on phishing risks. – Use email gateways to filter malicious links and attachments. – Integrate Maltiverse Phishing Feed to block phishing domains
Compromise Infrastructure (T1584)	Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, network devices.	Attackers cracked ScreenConnect Server installations to allow misused clients to connect to them in their attacker-controled servers.	– Whitelist approved remote access tools. – Block known malicious IOCs, IPs and domains (e.g., AS210558). – Audit systems for unauthorized ScreenConnect instances.
Masquerading (T1036)	Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.	The ScreenConnect client configuration is manipulated to connect to the malicious infrastructure.	– Whitelist approved remote access tools. – Block known malicious IOCs, IPs and domains (e.g., AS210558). – Audit systems for unauthorized ScreenConnect instances.
T1219 – Remote Access Software	Adversaries leverage legitimate remote access tools for persistence and control.	Misused ScreenConnect clients contain a malicious configuration to connect to cracked ScreenConnect servers hosted on malicious infrastructure.	– Whitelist approved remote access tools. – Block known malicious IOCs, IPs and domains (e.g., AS210558). – Audit systems for unauthorized ScreenConnect instances.

MITIGATION & RESPONSE

INDICATOR / PATTERN	DETAILS & IMPACT
Block High-Confidence IoCs (domains, IPs, URLs) in firewalls, proxies, and DNS resolvers.	Disrupts attackers' connection channels and client delivery pipelines with malicious configurations
Patch ScreenConnect Servers to the latest release (post-CVE-2024-1708/1709).	Prevents exploitation of vulnerabilities in legitimate deployments.
Audit Remote-Access Software Usage and enforce MFA for all remote-support sessions.	Reduces the risk of unauthorized access.
User Awareness Training: Warn employees about unsolicited "screen-connect" or "remote-support" prompts; instruct them to verify requests via official channels.	Mitigates social-engineering attacks that rely on user interaction.

CONCLUSION

This campaign demonstrates a sophisticated abuse of ConnectWise ScreenConnect, with attackers mass-registering parent domains and spinning up hundreds of sub-domains—particularly under .top and .com—to distribute client software misused to connect to attacker-controlled servers. Their reliance on AS210558 and "domain-burst" techniques offers defenders clear opportunities to disrupt the threat. By incorporating the provided IoCs, detection strategies, and mitigation actions into security controls and incident-response playbooks, organizations can effectively counter this growing menace.

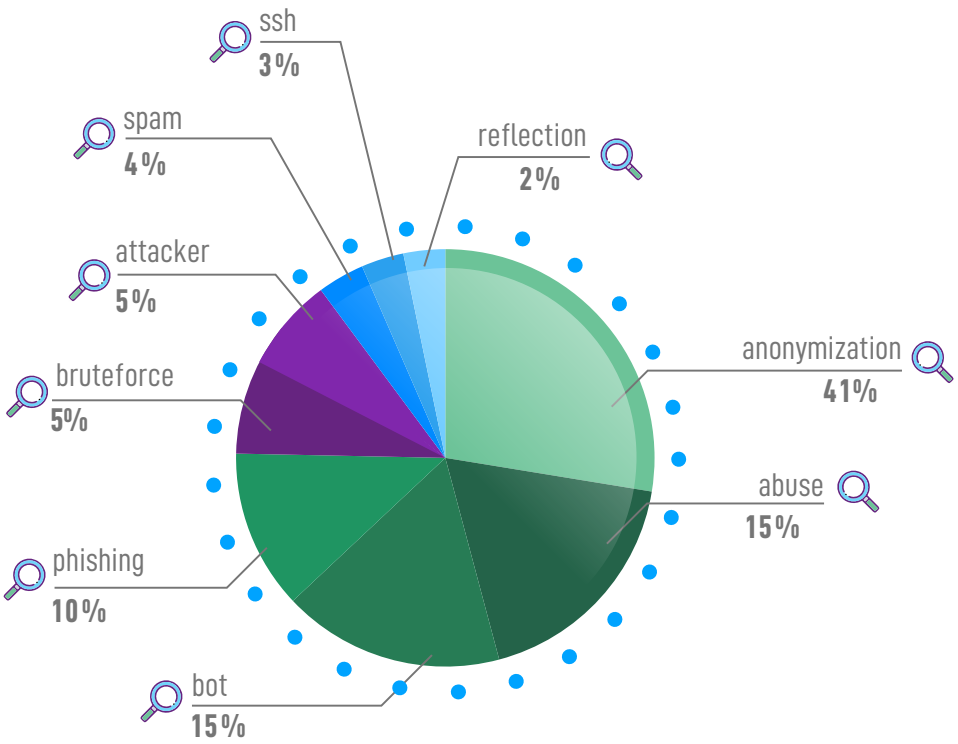
ABOUT MALTIVERSE BY LUMU

Maltiverse delivers real-time, customized threat intelligence, offering in-depth insights and emerging trend analysis. Since joining forces with Lumu in March 2025, Maltiverse enhances the contextual depth of Lumu's detections, while still providing invaluable stand-alone threat intelligence.

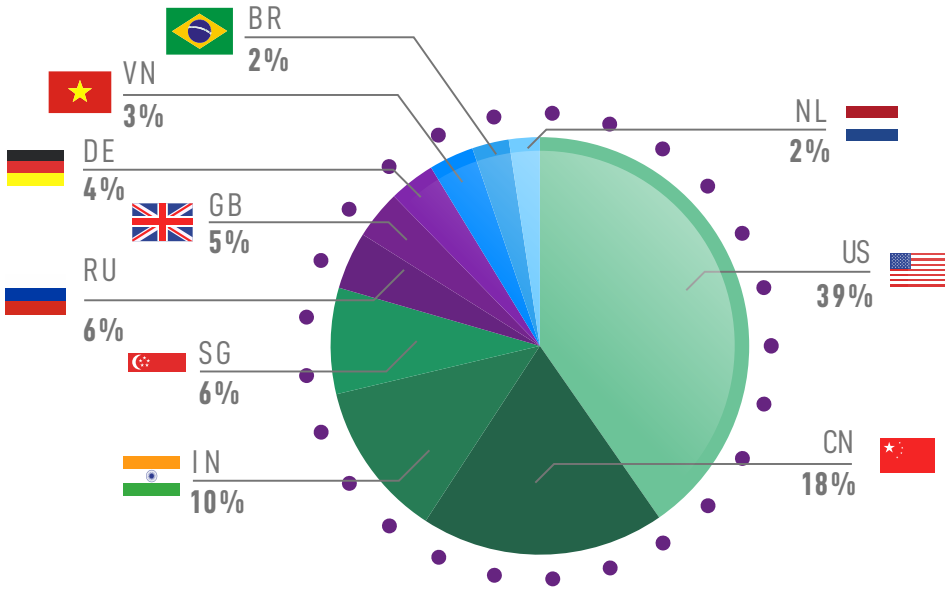
maltiverse
Actionable Threat Intelligence

REPORT

INDICATORS BY TYPE OF ACTIVITY - APRIL



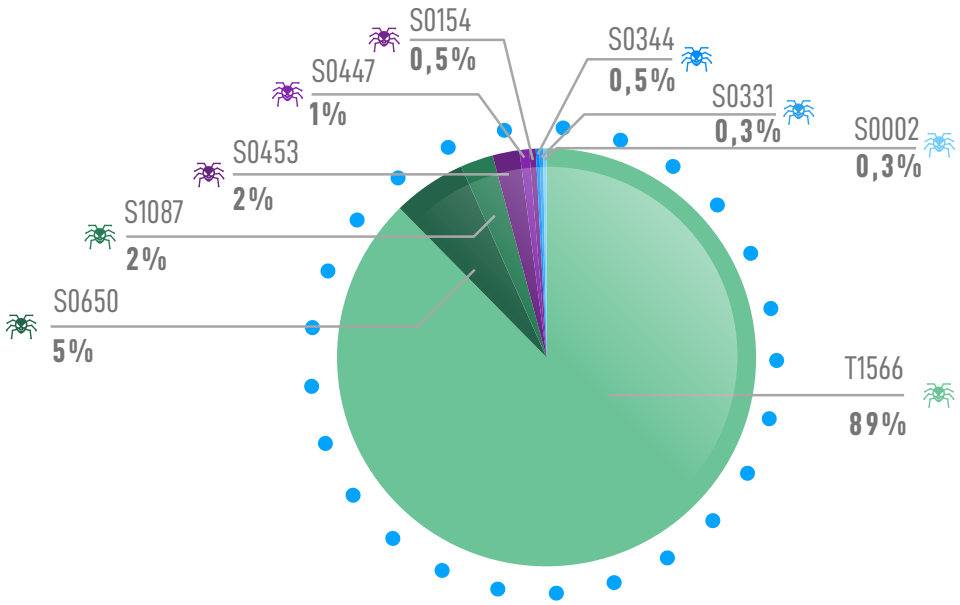
INDICATORS BY COUNTRY - APRIL



maltiverse
Actionable Threat Intelligence

REPORT

MOST ACTIVE MALWARE FAMILIES - APRIL



ID: T1566

Type: MALWARE
Platforms: Google Workspace, Linux, Office 365, SaaS, Windows, macOS
Version: 2.5

PHISHING

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering.

PROCEDURE EXAMPLES

G0001 - Axiom / G0115 - GOLD SOUTHFIELD / S0009 - Hikit / S1073 - Royal

ID: S0650

Type: MALWARE
Platforms: Windows
Version: 1.2

QAKBOT

Is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007.

GROUPS THAT USE THIS SOFTWARE

G0127 - TA551

ID: S0453

Type: MALWARE
Platforms: Windows
Version: 1.0

PONY

Is a credential stealing malware, though has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.

maltiverse
Actionable Threat Intelligence

REPORT

ID: S0447
Type: MALWARE
Platforms: Windows
Version: 2.0

LOKIBOT
Is a widely distributed information stealer that was first reported in 2015.

GROUPS THAT USE THIS SOFTWARE

G0083

ID: S0154
Type: MALWARE
Platforms: Windows, Linux, macOS
Version: 1.12

COBALT STRIKE
Is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors".

GROUPS THAT USE THIS SOFTWARE

G0129 - Mustang Panda / G0027 - Threat Group-3390 / G0050 - APT32 / G1022- ToddyCat
G0073 - APT19 / G0037 - FIN6 / G0092 - TA505

ID: S1111
Type: MALWARE
Platforms: Windows
Version: 1.3

CAMBIAR
Is a commercial Trojan that is used to steal information from compromised hosts.

GROUPS THAT USE THIS SOFTWARE

G0092 - TA505

ID: S1087
Type: MALWARE
Platforms: Windows
Version: 1.0

DARKGATE
DarkGate first emerged in 2018 and has evolved into an initial access and data gathering tool associated with various criminal cyber operations.

ID: S0344
Type: MALWARE
Platforms: Windows
Version: 1.3

AZORULT
Is a commercial Trojan that is used to steal information from compromised hosts.

GROUPS THAT USE THIS SOFTWARE

G0092 - TA505

ID: S0332
Type: TOOL
Platforms: Windows
Version: 1.3

REMCOS
is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security.

GROUPS THAT USE THIS SOFTWARE

G0140 - G0078

maltiverse
Actionable Threat Intelligence

news

Growing risk from autonomous AI agents

The cybersecurity industry is facing a growing risk due to the adoption of autonomous artificial intelligence (AI) agents in critical business tasks. These agents, which operate similarly to employees, pose unique security challenges if not properly managed. Without strict controls, AI agents can lead to data leaks, misuse of access credentials, or disclosure of confidential information. At the RSA Conference in San Francisco, securing the identities of AI agents emerged as a key topic. Deloitte estimates that 25% of companies using generative AI will launch AI agent pilots in 2025, rising to 50% by 2027. While there is experience in securing non-human identities, the potential harm from unregulated AI agents increases the urgency to implement robust identity management.

A knowledge gap exists among companies regarding these risks, prompting security vendors to raise awareness. As agent deployment accelerates, experts like Jason Clinton, CISO of Anthropic, stress the importance of acting now to ensure security, compliance, and trust.

Data breach at Co-op exposes customers' personal information

Co-op has confirmed a significant cyberattack in which personal information of a large number of current and former customers was stolen. The compromised data includes names, contact details, and dates of birth; however, passwords, credit card information, and transaction data were not affected. The attack has been described as "highly complex" and is currently under investigation by the UK's National Crime Agency and the National Cyber Security Centre. The breach came to light after hackers approached the BBC with evidence of the stolen data. In response, Co-op shut down certain IT systems to safeguard remaining data, causing disruptions to administrative operations.

The company apologized for the breach and emphasized the importance of data protection. Co-op stated it has taken proactive steps to mitigate further risks while minimizing the impact on customers and partners. This incident follows a similar cyberattack on Marks & Spencer that disrupted store operations.

Critical "AirBorne" vulnerability in AirPlay

A critical vulnerability named "AirBorne" has been discovered in Apple's AirPlay protocol and SDK, putting billions of Apple users at risk of malware attacks. The flaw allows hackers on the same Wi-Fi network to deploy malware, access private data, or even eavesdrop on conversations. Public spaces like cafés and airports are especially vulnerable. Cybersecurity experts urge users to immediately update all Apple devices and disable AirPlay if unused to reduce risk. While Apple has released security updates, many third-party devices such as smart TVs, speakers, and in-car systems remain exposed, as they rely on the affected AirPlay SDK and may not receive timely patches.

Experts warn these unpatched devices could act as backdoors, giving attackers network access even if an iPhone is fully updated. The flaw involves 23 software vulnerabilities and may undermine consumer trust in Apple's ecosystem, particularly since Apple cannot control third-party hardware patching.

maltiverse
Actionable Threat Intelligence

news

Cyberattack on Marks & Spencer causes £40 million in weekly losses

Marks & Spencer (M&S) is facing a major cyberattack that began over the Easter weekend, orchestrated by a hacker group known as Scattered Spider. The attack forced the retailer to shut down large parts of its IT systems, including online ordering and contactless payment services. Executives, including CEO Stuart Machin and Head of Digital Rachel Higham, held overnight crisis meetings. The ransomware attack involved hackers stealing and decrypting staff passwords and deploying malware to cripple M&S's operations. As a result, the company has faced widespread stock shortages, click-and-collect delays, and a hiring freeze - costing an estimated £40 million per week in lost sales. Despite recent financial gains - a 17% rise in pre - tax profits to £408 million - M&S risks reputational damage if customer data is confirmed to be compromised. Experts from Microsoft, Fenix24, and CrowdStrike have been brought in to manage the crisis.

The UK's National Cyber Security Centre is involved, and M&S has declined to comment on data security. Analysts suggest the attack could fast-track long-needed IT infrastructure refo rms. The company has not paid the ransom and is using workarounds as full restoration efforts continue.

Massive blackout in Spain: possible cyberattack under investigation

On April 28, 2025, a massive blackout left millions without power across much of Spain and Portugal for several hours. Although Red Eléctrica de España initially reported no clear signs of a cyberattack—attributing the outage to a technical failure in critical power transmission infrastructure—the government has not ruled out the possibility of a cyber incident due to the scale and synchronization of the failure. The National Intelligence Center (CNI), the National Cryptologic Center (CCN), and the National Cybersecurity Institute (INCIBE) have activated investigative protocols, working alongside Spain's National Court, which has opened proceedings for potential sabotage. The blackout severely impacted rail transport, healthcare centers, and telecommunications networks. Security experts warn that if a malicious origin is confirmed, it could represent one of the most sophisticated cyberattacks ever on critical infrastructure in Europe, with significant geopolitical implications. A preliminary government report is expected by the end of May.

Spain approves historic €1.157 billion investment in cybersecurity

The Spanish government has approved a €1.157 billion cybersecurity plan as part of the Industrial and Technological Plan for Security and Defense. The initiative aims to strengthen the country's resilience against cyberattacks, which have surged by 300% over the past decade, with over 100,000 incidents reported in 2024 alone. Of the total budget, 60.4% will be managed by the Ministry of Defense, including the National Intelligence Center (CNI) and the Joint Cyberspace Command. The plan includes projects to reinforce the Cybersecurity Operations Center for small municipalities and enhance the State's alert systems and digital platforms. It also promotes AI development and collaboration with universities in this field.

Additionally, the plan aims to strengthen Spain's national cybersecurity industry, amid the growing threat of cybercrime, which now accounts for one in every five crimes committed in the country.

maltiverse
Actionable Threat Intelligence

SERVICES

CTI FOR SIEM

A SIEM correlates logs, using user and entity behavior analysis to identify threats and send alerts. While it is effective, it can generate too many alerts, resulting in alert fatigue.

CTI FOR SOAR

SOAR technologies helps coordinate, execute and automate tasks between various people and tools all within a single platform. Maltiverse provides IoC context information and accurate classifications to create Playbooks and dramatically improve the quality of the decision making process.

CTI FOR FIREWALL

At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. Maltiverse provides Threat Intelligence feeds that can be automatically synchronized with Firewalls to improve security for outbound connections to Command & Control servers or Malware distribution sites.

CTI FOR SIEM

A SIEM correlates logs, using user and entity behavior analysis to identify threats and send alerts. While it is effective, it can generate too many alerts, resulting in alert fatigue.

The Enteprise Plan offers a **14-day free trial for Enterprise customers**

Upgrade your **detection capabilities**

START 14 days TRIAL

Actionnable threat INTELLIGENCE

Maltiverse Intelligence Plan provides a cloud based solution to delegate the collection, classification, filtering and delivery of Indicators of Compromise. It provides a powerful baseline protection aggregated from more than 100 different public and private intelligence sources that can be integrated in less than 30 minutes. Forget about setup and maintenance, delegate to highly skilled cybersecurity professionals at Maltiverse.

START 14 days TRIAL

Threat intelligence PLATFORM

Maltiverse Platform is a cloud-based TIP that seamlessly integrates your intelligence from MISP and other sources, enriching and filtering out false positives to ensure your data is ready for delivery to your security devices, such as SIEMs, SOARs, Firewalls, or EDRs. Beyond leveraging your own intelligence, Maltiverse also offers industry-leading intelligence feeds, delivering the most powerful and reliable Threat Intelligence available in the market.

START 14 days TRIAL