PSTA

Public Safety Threat Alliance

Public Safety ISAO

TLP:GREEN

PSTA CyberBytes

Public Safety Threat Alliance

31 December 2024 - 14 January 2025

MOTOROLA SOLUTIONS

TLP:GREEN

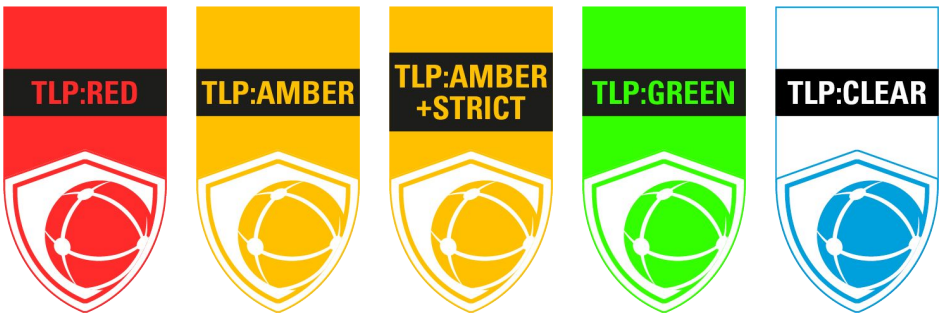
Table of Contents

Disclosure

As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group.

Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

Please note the Traffic Light Protocol signifiers on each page of this document and see the document Traffic Light Protocol APPENDIX for more details.



Cyberattacks to Public Safety Mission Space

Winston-Salem IT Systems Offline After Likely Extortion Attack

A North Carolina municipality took its IT network offline after a cyberattack impacted local systems. On 30 December 2024, defenders from Winston-Salem identified an ongoing compromise against unspecified municipal systems. The attack did not impact 9-1-1 or emergency services, based on available reporting.

The city is still dealing with degraded systems from the attack. “Right now we can only tell you it was a cyber event that impacted our systems and we're taking precautions," City Manager Patrick Pate said. Local news claimed “servers” were impacted, but it is not stated whether this was from a successful ransomware infection or preemptive disabling by city IT personnel.

The United States Federal Bureau of Investigation (FBI), North Carolina Joint Cyber Task Force, and the National Guard are purportedly assisting with the investigation, which is ongoing. Based on the involvement of state and federal entities, it is probable the compromise involved ransomware.

Analyst Note

Extortion attacks fell 35% in December, consistent with similar dips observed in prior years. Ransomware usually spikes in Q1, and we expect more public safety compromises to occur in the coming months as established extortion groups return with new tools and novel groups begin conducting attacks.

TLP:GREEN

Resources and Links

Source: Article 1

Article 2

TLP:GREEN

Kingston, Ontario Police Shuts Down Network after Cyberattack

A police department in Canada disabled their IT network after detecting a cyberattack. On 03 January 2025, Kingston Police in Ontario, Canada identified an undisclosed “network issue,” which soon escalated into a full cyberattack, likely involving ransomware. Defenders disconnected the network and began mitigation efforts, which were ongoing as of 06 January 2025.

The compromise did not disrupt 9-1-1 or emergency services and was limited to “nonemergency functions,” according to local news. The department launched an investigation with the aid of federal law enforcement and third party vendors to determine the full scope of the attack. It is currently unknown whether attackers stole any data.

Analyst Note

Historically, attacks tend to increase at the start of the new year. However, established extortion syndicates operating on observable channels yet to claim responsibility. It is likely more compromises will emerge from both established extortion groups as well as novel groups in the coming months.

Resources and Links

Source: Article

Turks and Caicos Islands 'Critical' Systems Offline

British overseas territory Turks and Caicos Islands suffered a ransomware infection, impacting local systems. According to available reporting, on 18 December 2024, unknown adversaries accessed the territory's government IT infrastructure through undisclosed means. The attack impacted 'critical' systems, according to a special Cabinet meeting.

At the time of writing, it is unclear if emergency services were impacted. However, reporting indicates "priority [for restoration] will be given to the processing of payments," with no mention of mission-critical systems. This suggests the 'critical' systems impact were likely related only to day-to-day business operations.

"A detailed report on the nature of the attack and the steps taken to prevent future incidents will be submitted once the recovery process is complete," the Cabinet stated. Forensic investigators funded by the United Kingdom government are in the process of investigating the attack.

Analyst Note

The attack on Turks and Caicos Islands is emblematic of most extortion activity facing state, local, and tribal territories (SLTT) in late 2024 and early 2025. Namely, victims often experience widespread system disruptions either through ransomware deployment or preemptive network disabling actions.

A review of available dark web and criminal forum locations did not reveal any claims by extortion syndicates. However, we identified a December 2024 post advertising personally identifiable information (PII), including credit cards, purportedly sourced from Turks and Caicos Islands. However, commenters on the post claimed the stolen credit cards were inactive, though the expiration dates of most cards had not expired.

Resources and Links

Source: Article 1

Article 2

NoName057(16) Disrupts Multiple French Municipal Websites

The pro-Russian hacktivist group *NoName057(16)* claimed responsibility for a distributed-denial-of-service (DDoS) attack against several French websites. On 31 December 2024, *NoName057(16)* used the Telegram messaging platform to state they had disrupted sites belonging to the Préfecture de Police. They also struck the city of Poitiers and nine other municipal websites.

The group provided Check-Host links as proof of their claim, showing the sites as temporarily unavailable. At the time of writing, impacted sites are again operational.

Analyst Note

NoName057(16) remains extremely active, hitting public safety entities multiple times a month. While their attacks are common, they have a generally low impact, and are unlikely to cause serious business disruption when compared to more dangerous attacks, such as ransomware.

Resources and Links

Source: Article

TLP:GREEN

Headline Cyber News

Extortion Gang Uses Artificial Intelligence to Lower Attack Entry Barriers

A known public safety attacker likely employed artificial intelligence (AI) to help prepare for attacks and develop malware. On 10 January 2025, Check Point Research detailed the emergence of *FunkSec*, a hybrid hacktivist and extortion group which began targeting United States and Middle-Eastern countries in late 2024.

FunkSec reportedly "extensively" employed undisclosed AI systems to develop tooling. The code of their Scorpion distributed-denial-of-service (DDoS) tool was likely fully or partially generated by a large language model (LLM) agent, evidenced by the perfect English code comments which differ from *FunkSec's* usually basic fluency. This goes too for the group's Rust-based ransomware.

The group is associated with AI in other ways. They published a custom AI running off (or based on) Miniapps, a program that can create AI tools without the restrictions found in regulated systems like ChatGPT. "The bot [...] is specifically designed to support malicious activities."

Like full-time hacktivists, the hybrid *FunkSec* also tends to inflate claims. In December 2024, they took responsibility for 85 victims on their dedicated data-leak blog. However, "many of the group's leaked data sets are recycled from previous hacktivism campaigns, raising doubts about the authenticity of their disclosures," according to Check Point.

Analyst Note

We observed five purported attacks from *FunkSec* since they emerged, all of which occurred in December 2024. While the group posted data samples alongside most of their claims, it is currently unclear to what extent they accurately represented attacks.

However, the highly likely use of AI tooling to establish a cyberattack-capable operation clearly highlights the effect growing AI tool availability has on the criminal ecosystem. AI is increasingly lowering the barrier to entry for less sophisticated threat actors and making it easier for individuals to create custom malware and tooling. Public Safety is likely to see further AI-assisted attacks or malware from other low-sophistication groups in 2025.

Resources and Links

Source: Article

Vulnerability and Exploit News

Ivanti Connect Buffer Overflow Flaw Actively Exploited

A flaw impacting Ivanti products could allow a remote, unauthenticated attacker to execute arbitrary code on vulnerable systems. On 08 January 2025, Ivanti released a security advisory warning of CVE-2025-0282, a stack-based buffer overflow vulnerability affecting Connect Secure, Policy Secure, and Neurons for Zero-trust Access.

Undisclosed adversaries exploited CVE-2025-0282 as a zero-day, which occurred as recently as 08 January 2025, according to multiple sources. While victims were not publicly disclosed, most organizations using vulnerable Ivanti products may likely be targeted, as CVE-2025-0282 impacts default configurations.

The flaw affects three distinct Ivanti products. These are described below:

- Neurons For Zero-trust Access — version 22.7 R2 through 22.7 R2.3
- Connect Secure — version 22.7 through 22.7 R2.4
- Policy Secure — version 22.7 through 22.7 R1.2

Patching is available for all impacted products except for Policy Secure, for which a patch is planned to be released on 21 January 2025. For Connect Secure, Ivanti recommends a factory reset for appliances with a clean scan prior to upgrading to version 22.7R2.5 “out of an abundance of caution.”

Analyst Note

At the time of writing, there is no publicly available proof-of-concept code online. The PSTA anticipates increased targeting from threat actors in the near future, as CVE-2025-0282 facilitates remote code execution (RCE) and affects a secure socket layer (SSL) virtual private network (VPN).

Resources and Links

Source: Article

TLP:GREEN

LEVELS OF ANALYTIC CONFIDENCE

HIGH CONFIDENCE

Generally indicates judgments based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and still carries a risk of being wrong.

MODERATE CONFIDENCE

Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.

LOW CONFIDENCE

Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

OUR SHARED MISSION

The Public Safety Threat Alliance (PSTA) serves as a cyber threat intelligence sharing, collaboration and information hub for the evolving cyber security challenges faced by the global public safety community. The PSTA strives to improve the cyber security posture, defense and resilience of our members. We collaborate with trusted partners to collect and analyze cyber threat information to protect public safety organizations and the communities they serve. The PSTA is recognized by the Cybersecurity and Infrastructure Security Agency (CISA) as an official cyber threat Information Sharing and Analysis Organization (ISAO).

Learn more about the Public Safety Threat Alliance

PSTA
PUBLIC SAFETY THREAT ALLIANCE
PUBLIC SAFETY ISAO

MOTOROLA SOLUTIONS

Motorola Solutions Inc., 500 W Monroe St, Chicago, IL 60661. U.S.A. motorolasolutions.com
MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2023 Motorola Solutions, Inc. All rights reserved. 09-2022

TLP:GREEN

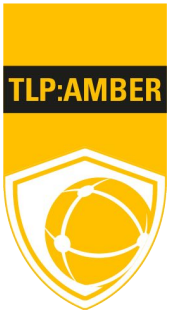
APPENDIX:
TRAFFIC LIGHT PROTOCOL

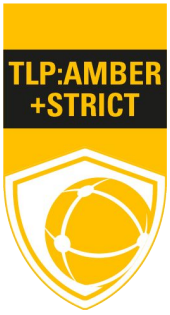
As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

NOT FOR DISCLOSURE:
Restricted to the immediate PSTA participants only

When should it be used? - Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.

How may it be shared? - Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.





LIMITED DISCLOSURE:
Restricted to participants' organizations

When should it be used? - Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

How may it be shared? - Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. TLP:AMBER+STRICT Restricts sharing to the organization only.

LIMITED DISCLOSURE
Restricted to the community

When should it be used? - Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.

How may it be shared? - Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

DISCLOSURE IS NOT LIMITED

When should it be used? - Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

How may it be shared? - Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.