PSTA

Public Safety Threat Alliance

Public Safety ISAO

TLP:GREEN

PSTA CyberBytes

Public Safety Threat Alliance

26 August — 09 September 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. Please share any observed IOCs to pstaioc@motorolasolutions.com.

IOCs can take multiple forms, such as suspicious or malicious IP addresses and malware hashes. All sensitive information to your organization that is shared with the PSTA will be redacted from any IOCs before they are shared with the Full Access member community through the secure PSTA portal. We advise all members to provide any possible threat information and reach out to the PSTA with questions or concerns.

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.

TLP:GREEN

Cyberattacks to public safety mission space

State of Nevada attack disrupts dispatch and police records

A cyberattack on the State of Nevada caused widespread disruptions, affecting computer-aided-dispatch (CAD) and records and evidence systems. On 24 August 2025, the State of Nevada identified a "cybersecurity incident" impacting the state IT network, reporting it publicly a day later. The compromise affected at least one CAD server connected to the state IT network, disrupting law enforcement dispatch communications.

The attack also disrupted access to in-person services at state offices, phone lines, and some state websites. It likewise impacted a shared records management portal used by Nevada police to store and download reports and evidence. The attack also likely impacted the Nevada Highway Patrol administrative and online functions. However, the state indicated that 9-1-1 and emergency services remain operational and that no personally identifiable information (PII) was exposed, though adversaries stole "some data."

The United States Federal Bureau of Investigation (FBI) is assisting the governor's technology office with attack remediation and investigation. These efforts are ongoing at the time of writing.

The *Qilin* extortion syndicate appears to be responsible for the attack based on information from trusted sources, though conflicting reporting blames the *SP1D3R HUNTERS* joint cybercrime operation. At the time of writing, *Qilin* has not publicly claimed responsibility for the Nevada attack, and it is not known how the compromise began. However, officials warned of unsolicited calls, emails, or texts asking for personal information, suggesting social engineering techniques such as phishing may have been involved.

Analyst note

This attack marks the 21st mission-critical disruption observed in 2025. These disruptions occurred across 16 different agencies, disrupting CAD, public safety radio, and 9-1-1 call-handling. *Qilin* accounts for 31% of these disruptions, making them the top attributed adversary responsible for mission-critical impacts this year.

Resources and links

Source: article

Novel ransomware group attacks Ohio municipality twice in one month

A novel ransomware group targeted the same Ohio municipality after previously attacking them two weeks prior. On 26 August 2025, officials from West Chester Township reported that their email server was struck with ransomware right after a previous attack was conducted on their IT network on 12 August 2025. In the second incident, the group purportedly stole 2 TBs of data that included personally identifiable information of residents and employees.

On 15 August 2025, the *PEAR* ransomware group listed West Chester Township as a victim on their data leak site, where they claimed to have exfiltrated an unspecified amount of data. The first attack was not publicly acknowledged by the township, however, it was publicly acknowledged after officials reported this second attack.

The details regarding how the threat actor gained access both times remain unknown. However, local reporting suggests that the municipality's IT environment likely had multiple vulnerable entry points, allowing for repeat exploitation.

Analyst note

While it is uncommon for municipalities to be struck twice in quick succession, this incident demonstrates how failing to completely remove the threat actor's persistent access points in incident response can leave organizations vulnerable to follow-on attacks. This marks the sixth ransomware incident against an Ohio public safety agency in 2025. Notably, in August 2025, Middletown, Ohio, also experienced a ransomware attack within days of the initial West Chester compromise, though it remains unclear whether there is any correlation between the two events.

Resources and Links

Source: article

INC extortion group claims attack on Canadian municipality

A prominent public safety attacker claimed an attack against a municipality in Canada. On 29 August 2025, the *INC Ransomware* group listed the City of Sainte-Brigitte-de-Laval as a victim on their dedicated data-leak site. The group provided samples of municipal documents as proof of their claim.

Currently, the municipality has not yet publicly acknowledged the attack. However, there are no reports of disruptions to 9-1-1 or emergency services. Information on the attack remains limited and the PSTA will continue to monitor for relevant updates.

Analyst note

This incident marks INC's 12th public safety compromise in 2025 and their fourth attack in just the past month, underscoring the group's sustained operational tempo. This tempo suggests that INC is likely to continue targeting public safety agencies at a similar rate in the near future.

Resources and links

Source: article

Qilin claims attack on Chatham, Massachusetts

A prominent public safety adversary purportedly struck a Massachusetts city with ransomware, stealing data. On 28 August 2025, the Qilin extortion syndicate added Chatham, Massachusetts to their dedicated data-leak site. The group posted samples of purportedly stolen data as proof of their claim. However, the group did not specify the amount of data that was compromised.

The samples posted consist of financial and logistic documents, likely sourced from the municipal IT network. There is no indication of any compromise or disruption to 9-1-1 or emergency services.

Chatham officials have yet to publicly acknowledge the alleged compromise and minimal information is available regarding the attack. The PSTA will continue to monitor for relevant updates.

Analyst Note

Qilin continues to be a top threat in the public safety space. This incident marks the group's 15th ransomware attack against a public safety agency in 2025. Qilin remains the most responsible for impacts to mission critical systems and will likely continue to remain a top threat as the year continues.

Resources and links

Source: article

Multiple Czechia government agencies attacked by NoName057(16)

The hacktivist group *NoName057(16)* launched a distributed-denial-of-service (DDoS) attack against multiple websites in Czechia. In late-August 2025, the pro-Russian threat actor claimed responsibility for disruptions to the official websites of the following victims:

- Plzeňský region
- Olomoucký region
- Municipal Police of Ostrava

NoName057(16) provided Check-Host links showing the websites as temporarily unavailable as proof of their claim. At the time of writing, the sites are once again available.

Analyst note

While we have observed the group continuing attacks on city halls and nonpublic safety organizations, the majority of their recent attacks on public safety were against Czechia entities. This marks a shift away from their German focus throughout most of August. At the time of writing, NoName057(16) is attacking public safety approximately once every two days, a drop from their one attack a day average in the last week of August.

Resources and links

Source: article

Headline cyber news

Ransomware takedowns foster new, smaller extortion groups

Extortion groups are now smaller and more numerous following law enforcement disruptions of major syndicates. The MalwareBytes State of Ransomware 2025 report identified 60 total ransomware operations active at the same time in 2025, the highest number since MalwareBytes began tracking adversaries. A total of 41 new extortion groups emerged from July 2024 and June 2025, targeting a range of industries across the globe.

According to research by Flashpoint, many of these "new" operations are instead rebrands and splinters of prior threat groups. This is consistent with assessments the PSTA made in 2024 that exit scams and major law enforcement takedowns would cause the affiliates of high-profile syndicates to establish their own groups or flee to smaller, more secure operations.

Researcher Allan Liska from RecordedFuture stated it is now "incredibly dangerous" to be a large ransomware-as-a-service (RaaS) group. "Ransomware affiliates are left with two choices: try to join one of the still operating closed groups like *Qilin* or *Akira* or start up their own ransomware operation," Liska assessed.

Analyst note

The splintering of extortion groups is likely a contributing factor as to why public safety has seen a fall in ransomware activity, as these entities are now more divided, targeting a larger array of sectors and victim types. However, when adversaries like *Qilin* and *INC Ransomware* do strike public safety, they have a tendency to disrupt public safety radio, computer-aided-dispatch, or 9-1-1 call handling services, making their attacks more likely to net ransom payouts. In the meantime, smaller groups like *Cephalus* and *PEAR* are beginning to attack the sector, meaning public safety ransomware may rise as these threat actors establish their footing and targeting preferences.

Resources and links

Source: article

Vulnerability and exploit news

Citrix NetScaler critical flaw under exploitation

A patch is now available for a critical vulnerability impacting Citrix NetScaler devices. On 26 August 2025, Citrix released a Security Bulletin for CVE-2025-7775, a memory overflow flaw which can let remote, unauthenticated attackers execute code on vulnerable systems. According to Citrix, exploits "of CVE-2025-7775 on unmitigated appliances have been observed."

CVE-2025-7775 impacts the following NetScaler devices:

- NetScaler ADC and NetScaler Gateway 14.1-47.48 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-59.22 and later releases of 13.1
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.241 and later releases of 13.1-FIPS and 13.1-NDcPP
- NetScaler ADC 12.1-FIPS and 12.1-NDcPP 12.1-55.330 and later releases of 12.1-FIPS and 12.1-NDcPP

Citrix did not provide any workaround mitigations for organizations unable to patch. The PSTA Threat Intelligence team has not identified any publicly-available proofs-of-concept (POCs), but observed open-source scanning scripts on GitHub designed to identify vulnerable instances of NetScaler.

Currently, Citrix rates CVE-2025-7775's attack complexity as 'High,' suggesting it is difficult to exploit. According to research from Rapid7, memory overflow flaws may "be complex and prone to failure due to unexpected memory layouts or other indeterminisms in the target system."

Analyst note

Even complex CVEs may be exploited in high-impact extortion attacks. Flaws which enable remote code execution (RCE) are favorites of threat actors who target such vulnerabilities to obtain initial access on victim networks. While the threat actors who exploited CVE-2025-7775 are not publicly disclosed, we assess extortion groups and access brokers are likely to target the flaw.

Resources and links

Source: article

High-severity Hikvision flaw allows unauthenticated admin access

A vulnerability in Hikvision security software could lead to compromises of camera environments. On 29 August 2025, Hikvision released a security advisory for CVE-2025-39247, an access control vulnerability impacting HikCentral Professional, rated CVSS 8.6 (High).

According to Hikvision, CVE-2025-39247 exploitation could let an unauthenticated attacker obtain administrative privileges on vulnerable instances. As described by Security Affairs, the bug is a "direct path to manipulating configurations, tampering with logs, or even shutting down critical monitoring functions."

The flaw impacts the following HikCentral Professional systems:

- Versions between v2.2.1 and v2.3.2
- Version v3.0.0

There is a patch available for the flaw. Hikvision did not provide any workaround mitigations for organizations unable to patch. At the time of writing, there is no publicly-reported exploitation in the wild, and no POCs on sites such as GitHub.

Analyst note

When cameras are not set on isolated networks, they can be accessed from the open internet or connected environments. We have observed threat actors deploying malware against public safety entities' camera systems in the past, and while these attacks rarely move beyond the camera network, they can serve as footholds to enterprise environments.

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

TLP:GREEN

APPENDIX:
TRAFFIC LIGHT PROTOCOL

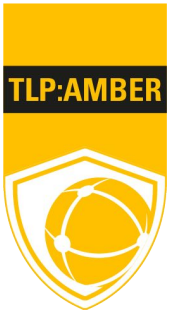
As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light 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.

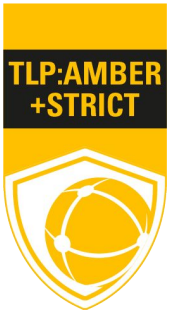
NOT FOR DISCLOSURE:
Restricted to the immediate PSTA participants only

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.