PSTA
Public Safety Threat Alliance
Public Safety ISAO

TLP:GREEN

PSTA CyberBytes

Public Safety Threat Alliance
21 October — 04 November 2025

MOTOROLA SOLUTIONS

Table of contents

[Cyberattacks to public safety mission space](#) 3

1. Oxford County, Canada suffers ransomware attack
2. Mentor, Ohio recovering from ransomware attack
3. NoName057(16) attacks multiple municipal websites in Canada

[Headline cyber news](#) 6

1. Hacktivists disrupt industrial control systems in Canada
2. Ransomware profits continue to drop in 2025

[Vulnerability and exploit news](#) 8

1. Critical Microsoft WSUS flaw exploited in wild

[Levels of analytic confidence](#) 9

[Appendix: traffic light protocol](#) 10

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:RED TLP:AMBER TLP:AMBER +STRICT TLP:GREEN TLP:CLEAR

Cyberattacks to public safety mission space

Oxford County, Canada suffers ransomware attack

A likely ransomware attack disrupted a municipality in Canada, resulting in the theft of local data. On 20 October 2025, the *Brain Cipher* extortion syndicate used their dedicated data-leak site to claim responsibility for compromising Oxford County in Ontario.

Brain Cipher did not provide proof of their claim. However, in September 2025, Oxford County reported a “cybersecurity incident” which resulted in the theft or exposure of over 4,000 citizens’ personal data.

The extent of ransomware disruption to Oxford County systems remains unclear. There is no indication of impacts to emergency services. Oxford County Warden Marcus Ryan stated the attack was "still an ongoing issue, and frankly, will be for months," suggesting either widespread impact or significant difficulty in restoring affected services. However, local news reported that all of the county’s systems were "operating normally," which would imply that Brain Cipher or the group responsible for the attack failed to deploy ransomware.

Analyst note

Brain Cipher is known for attacking data centers and demanding large ransoms. This is the first observed attack to a public safety entity the group allegedly conducted. Because of the lack of data provided as proof, we cannot verify *Brain Cipher’s* claim. However, the timing is appropriate for an attack occurring a month prior; ransom negotiations may take time, and threat actors who failed to deploy ransomware may also be initially hesitant to claim attacks as they sort through stolen data.

Resources and Links

Source: article 1

article 2

Mentor, Ohio recovering from ransomware attack

A municipality in Ohio experienced a ransomware attack resulting in disruptions to administrative services and phone lines. On 25 October 2025, defenders from Mentor, Ohio shut down enterprise servers after detecting a ransomware infection on the network. The attack delayed unspecified city services and disrupted administrative phone lines at the police department and municipal court.

The threat actor behind the compromise remains unknown or unreported, as is whether attackers stole data during the incident. The attack appeared to be limited to the enterprise network as 9-1-1 and emergency services were not affected, according to the city. The city is currently undergoing recovery in accordance with their cyber attack plan.

Analyst note

This is the 14th ransomware attack against a public safety agency in October, with the Qilin ransomware group responsible for 50% of the attacks this month. Qilin often delays claiming victims, likely while ransomware negotiations are underway; however, their involvement in this attack remains unconfirmed.

Resources and links

Source: article

NoName057(16) attacks multiple municipal websites in Canada

The hacktivist group NoName057(16) launched a distributed-denial-of-service (DDoS) attack against multiple municipal websites in Canada. On 21 October 2025, the pro-Russian threat actor claimed responsibility for disruptions to the following municipal websites:

- Thunder Bay
- Burlington
- Vancouver
- Quebec City

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

Analyst note

NoName057(16) continues to attack municipal websites as part of their routine DDoS campaign. This was only its second attack on Canada this year, with the first occurring in January. It remains unclear whether the group will begin focusing on Canadian municipalities, as the number of attacks on Canada is too low to establish a clear trend.

Resources and links

Source: article

Headline Cyber News

Hacktivists disrupt industrial control systems in Canada

Ideologically-motivated threat actors purportedly disrupted industrial control systems (ICS) in Canada, prompting an investigation from the Royal Canadian Mounted Police (RCMP). On 29 October 2025, the RCMP and Canadian Cyber Centre released a threat alert detailing how hacktivists accessed ICS devices across multiple organizations to inflict minor disruptions including changing the water pressure at a local water utility.

The attack on the water utility organization resulted in "degraded service for [the] community," marking one of the few instances where threat actors have successfully disrupted or altered water provisioning. Attackers also struck a Canadian oil and gas company, "where an Automated Tank Gauge (ATG) was manipulated, triggering false alarm," according to the alert.

The RCMP did not publicly attribute the compromises to any specific threat group, only stating that the culprits were hacktivists. The RCMP likewise indicated that impacted organizations were not specifically targeted, but were instead victims of opportunistic attacks from adversaries who are "increasingly exploiting internet-accessible ICS devices to gain media attention, discredit organizations, and undermine Canada's reputation."

The alert provides a series of suggested mitigation measures which can be employed to reduce the risk and impact of a successful compromise. For more information, please see the full alert.

Analyst Note

The PSTA observed a recent uptick in hacktivist related activity against Canadian public safety entities. Both the *DarkStorm* and *NoName057(15)* groups attacked Canadian municipalities in October this year using low-impact distributed-denial-of-service (DDoS) to disrupt internet-facing websites.

While we have yet to observe hacktivists disrupting mission-critical systems, the RCMP alert suggests some groups are capable of accessing isolated and protected networks such as ICS. The PSTA Threat Intelligence team will continue to monitor for relevant updates.

Resources and Links

Source: article

Ransomware profits continue to drop in 2025

Ransomware payments continue to decline, likely prompting extortion syndicates to test out new tactics when striking victims. On 24 October 2025, Coveware released a blog describing how the changing economics of running an extortion group and improving victim defenses has made it harder to get paid as an attacker.

According to Coveware, ransomware payment rates have dropped to a historic low of 23% in Q3 2025, meaning only a quarter of ransomware victims are now agreeing to threat actors' demands. This is a consistent trend; in Q3 2020, 60% of victims Covware monitored paid ransoms. That fell to 45% the following year and has continued to drop since. Ransomware's "overall success rate is contracting," Coveware states.

Similarly, actual payment amounts have started to fall. With the average ransom payment Covware observed spiking to over $1,000,000 USD in Q2 2025, it has dropped to only $376,941 USD in Q3. However, this is a more volatile trend, and may not hold in the long term.

Coveware attributes dropping profits to changes in the extortion economy. The "framework that brought groups like Conti, Hive, and Lockbit to prominence is unlikely to succeed in today's climate," the blog states, referencing previous top public safety adversaries' use of opportunistic initial access brokers (IABs). Groups are increasingly forced to pivot from opportunistic targeting to more intentional attacks, as victims' patch management and security controls are making it more time-consuming to breach the average network.

Analyst note

The shift Coveware observed likely drove the recent information sharing agreement between *LockBit*, *Qilin*, and *DragonForce*. This partial operational merger has likely led to a recent spike in public safety attacks from the *Qilin* group and a mission-critical attack from *DragonForce*. The PSTA also previously assessed that, as ransomware attacks fell, they would individually become more impactful as groups put more effort into hitting sensitive data and systems to force victims to pay ransoms.

Resources and links

Source: article

Vulnerability and Exploit News

Critical Microsoft WSUS flaw exploited in wild

A vulnerability impacting Microsoft's Windows Server Update Services (WSUS) is under active exploitation, requiring patching for impacted organizations. On 23 October 2025, Microsoft released an out-of-band patch for CVE-2025-59287, a critical (9.8 CVSS) flaw in WSUS which an "unsafe deserialization of untrusted data" could lead to remote code execution (RCE). CVE-2025-59287 could let an unauthenticated, remote adversary execute code against vulnerable Windows servers.

The flaw affects servers in which WSUS Server Role is turned on. This is not a default feature, meaning CVE-2025-59287 only impacts organizations which have altered this default WSUS setting. The following Microsoft Windows Servers are vulnerable: versions 2012, 2012 R2, 2016, 2019, 2022 (including 23H2 Edition) and 2025.

A patch is available for the vulnerability. However, Microsoft also recommends disabling the WSUS Server Role on impacted servers if patching is unavailable. Defenders may also stop "inbound traffic to Ports 8530 and 8531 on the host firewall (as opposed to blocking only at the network/perimeter firewall) to render WSUS nonoperational."

Analyst Note

According to Unit42 research, threat actors are abusing CVE-2025-59287 a number of ways. Ports 8530 (HTTP) and 8531 (HTTPS) are being targeted for initial access. PowerShell is employed for the execution stage of attacks, with defenders identifying two possible process chains to-date: wsusservice.exe → cmd.exe → cmd.exe → powershell.exe and w3wp.exe → cmd.exe → cmd.exe → powershell.exe. For more information, please review Unit42's blog on ongoing CVE-2025-59287 exploitation.

The PSTA has not observed any public safety compromises in which CVE-2025-59287 was exploited. However, proof-of-concept code is available online, and given the severe nature of the flaw and ongoing exploitation we recommend patching at the earliest opportunity.

Resources and Links

Source: article

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

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

TLP:RED

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

TLP:AMBER

TLP:AMBER +STRICT

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

TLP:GREEN

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

TLP:CLEAR

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.