PSTA

Public Safety Threat Alliance

Public Safety ISAO

TLP:GREEN

PSTA CyberBytes

Public Safety Threat Alliance

08 - 22 April 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

Gooding County, Idaho Data Accessed During Extortion Attack

An undisclosed adversary struck an Idaho county network, resulting in the alleged theft of citizen's personal information. On 25 March 2025, Gooding County defenders identified an ongoing cyberattack against the county IT network. Little information is available regarding the compromise, but there is no indication 9-1-1 or emergency services were disrupted.

An 04 April 2025 notice to residents stated investigators, "determined that this incident likely involved unauthorized acquisition of personal information," and that the county is "working with legal counsel and the digital forensics firm to review the impacted data"

No extortion syndicate has to-date claimed responsibility for the attack.

Analyst Note

In 2025, 23 extortion attacks were observed impacting United States public safety entities, with 16 of those targeting municipalities. Municipalities are the most commonly attacked public safety entities due to their broad networks and large number of users, applications, services, and connections to/from the open internet. These factors are often opportunities for financially-motivated adversaries who can abuse remote services, logins, and vulnerabilities to access public safety networks.

TLP:GREEN

Resources and Links

Source: Article

TLP:GREEN

Ransomware Attack Paralyzes Municipal Network in Belgium

A municipality in Belgium suffered an extortion attack which disabled the municipal IT network. On 14 April 2025, defenders from Jemeppe-sur-Sambre, Belgium reported a ransomware infection disrupting the city's enterprise network overnight. The attack caused administrative municipal services to become inoperable.

An investigation was initiated alongside unnamed third-party experts to investigate and restore services. According to local sources, the municipality refused to pay the ransom of $700,000 USD. However, defenders did not disclose the responsible extortionists.

According to initial investigations, it appears attackers were present inside the enterprise network for roughly two weeks before detonating ransomware. The undisclosed group allegedly stole over one TB of data. There is no evidence of disruption to emergency services.

Analyst Note

The severe disruption caused by this ransomware attack indicates the group possessed a high level of sophistication. There was likely no managed detection and response capability within the municipality since the attackers were persistent in the network for two weeks. As of 18 April 2025, no threat actor has claimed responsibility for the compromise.

Resources and Links

Source: Article

Darkstorm Claims Attack on Multiple French Municipal Websites

A hacktivist group launched distributed denial-of-service (DDoS) attacks that disrupted websites belonging to multiple French municipalities. On 11 April 2025, Darkstorm claimed responsibility for disrupting websites belonging to the cities of Nice and Nantes on their Telegram channel.

The group posted links to Check-Host, showing the websites as temporarily unavailable. At the time of writing, impacted sites are again operational

Analyst Note

In 2025, *Darkstorm* has carried out its fifth public safety compromise, suggesting the group is escalating the frequency of attacks against organizations across Europe. The group's activities could potentially reach the same scale as the disruptions caused by *NoName057(16),* indicating additional low-impact attacks could occur on public safety websites.

TLP:GREEN

Resources and Links

Source: Article

Headline Cyber News

The Riskiest Connected Devices of 2025

A report from Forescout describes the connected devices most likely to enable cyberattacks, based on systems located in Forescout's device cloud. According to the 09 April 2025 report, government systems are at an elevated risk compared to other industries. This is due in part to continued use of outdated operating systems and insecure services.

The report indicates over 50% of devices with "the most critical vulnerabilities" are routers and similar systems. This is exacerbated by malicious campaigns targeting edge devices, allowing threat actors to access victim networks through vulnerability exploitation. Routers and firewalls are both exploited by extortion syndicates and advanced persistent threat actors (APTs) and are commonly abused due to their internet-facing nature. Domain controllers likewise represent serious risk. "Threat actors frequently compromise them post-initial access using them as pivot points for lateral movement within a network,"

Vulnerabilities and open ports drove most Forescout-observed issues. Adversaries can brute force logins against unsecure remote services and through automated vulnerability exploitation to execute code on vulnerable systems. Consistent with PSTA reporting, remote desktop protocol (RDP), server message block (SMB) and secure shell (SSH) are among the most targeted protocols when attackers abuse internet-facing services.

Analyst Note

Forescout's report is highly consistent with malicious activity observed against public safety systems. Specifically, public safety adversaries persistently target domain controllers, firewalls, routers, and unsecured ports to access victim networks, move laterally, elevate privileges, and deploy ransomware.

Resources and Links

Source: Article

State-sponsored Adversaries Begin Using ClickFix Tactic

Multiple APTs from North Korea, Russia, and Iran are abusing a popular social engineering technique when targeting the United States and other nations. ClickFix, previously associated with extortion syndicates and other cybercriminals, is a method by which attackers use pop-up dialog boxes to convince users to copy and run PowerShell and install malware. According to a 17 April 2025 report from Proofpoint, *TA427*, *MuddyWater*, and *APT28* are using ClickFix in attacks.

"The incorporation of ClickFix is not revolutionizing the campaigns [...] but instead is replacing the installation and execution stages in existing infection chains," Proofpoint stated. APTs appear to be using the technique mostly against government and financial institutions.

ClickFix-led infections generally begin via navigation to compromised websites or through phishing emails containing malicious links, HTML attachments, or documents. Once a user clicks on the link or document, a pop-up alert urges the individual to perform a series of actions to fix an alleged software or operating system issue. An attacker-created script is then automatically run *or* the user is advised how to manually open PowerShell and copy-paste a malicious command. This facilitates malware installation, including information stealers or command-and-control beacons.

Analyst Note

While not an entirely novel tactic, social engineering techniques like ClickFix which focus on software or hardware problems can increase user interaction with phishing emails and malicious prompts. Defenders are advised to educate end-users and employees about the nature of and threat posed by ClickFix and similar tactics. This is based on the use of ClickFix by both cybercriminals and APTs and associated risk of potential compromises to public safety networks through social engineering.

Resources and Links

Source: Article

Vulnerability and Exploit News

CentreStack and Triofox Critical Flaw Under Exploitation

A critical remote code execution (RCE) vulnerability disclosed on 03 April 2024 is under active exploitation. On 14 April 2025, researchers at Huntress detailed the targeting of CVE-2025-30406, a deserialization flaw in Gladinet CentreStack and the Triofox remote access platform, which exists due to the use of hard-coded cryptographic keys. This flaw could allow remote adversaries to execute arbitrary code against internet-facing systems.

Adversaries must know the machineKey, but Triofox and CentreStack instances have the "same hardcoded cryptographic keys in their configuration file, and can be easily abused for remote code execution," Huntress stated. In an observed attack, adversaries abused the vulnerability in addition to "encoded PowerShell to download and sideload a [malicious] DLL."

Public proof-of-concept code is not yet available, based on cursory searches of major sites like GitHub. However, in-the-wild exploitation began as early as March, though 11 April 2025 is the first confirmed sighting by Huntress. It is recommended that vulnerable organizations update to the latest versions of CentreStack and Triofox. Organizations unable to patch should change machineKeys via the process outlined in the CentreStack and Triofox guides.

Analyst Note

A list of known indicators-of-compromise (IOCs) are available through the Huntress blog. Based on the addition of CVE-2025-30406 to the United States Cybersecurity and Infrastructure Security Agency's (CISA) known exploited vulnerability catalog (KEV), we advise organizations who use Centrestack or Triofox on internet-facing systems to patch at the soonest opportunity.

TLP:GREEN

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

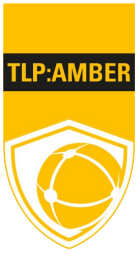
As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light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

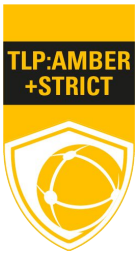
NOT FOR DISCLOSURE:
Restricted to the immediate PSTA participants only

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.