Ontinue

Threat Intelligence Report

2H 2024

Executive Summary

Ontinue's 2H 2024 Threat Intelligence Report delivers an in-depth analysis of the evolving cyber threat landscape, based on insights from Ontinue's Advanced Threat Operations (ATO) team. The report highlights key attack trends, emerging techniques, and vulnerabilities that organizations must address to strengthen their security posture.

The report found that info stealers, PlugX RAT, and suspicious PowerShell activity remain among the most frequently detected threats in Ontinue ION MXDR. Threat actors continue to exploit built-in Microsoft tools, such as Quick Assist and Windows Hello, to establish persistence and evade detection. Additionally, zero-day vulnerabilities are being weaponized at an accelerated rate by both nation-state actors and cybercriminals.

Key Trends

1. **Malware Delivery via Browser Extensions and Malvertising**
   Threat actors leverage browser extensions for reinfection and use deceptive ads to execute malicious PowerShell commands.

2. **Advanced Phishing & Vishing Tactics**
   Man-in-the-middle (AiTM) phishing, trusted cloud services (e.g., SharePoint, Google Drive), and vishing scams are increasingly used to steal credentials.

3. **Exploitation of IoT & OT Environments**
   As enterprise networks expand, attackers are targeting IoT and OT devices with greater frequency.

4. **Ransomware Evolution**
   Cybercriminals employ more sophisticated delivery methods and abuse legitimate tools to bypass security controls.

To mitigate these threats, Ontinue emphasizes proactive defense measures, including continuous monitoring, rapid patching, and strengthening authentication mechanisms. Staying informed through threat intelligence and best practices remains critical for organizations looking to enhance their cybersecurity resilience.

Cyber Trends to Watch

Ransomware in 2024: Trends, Metrics, and Response Strategies

Evolving Tactics of Ransomware Operators

Ransomware operators continue to refine their approaches, prioritizing IT skills over programming expertise. Affiliates are often selected for their ability to navigate enterprise networks, assess and disable backups, and target databases and virtualized environments. This shift underscores the growing sophistication of ransomware attacks and the increasing need for robust cybersecurity measures.

Ransomware Trends and Financial Impact

Two of the most widely reported ransomware metrics are total payments made and the industries most affected. However, these figures only represent a portion of the broader impact. Many organizations choose not to pay, yet still face significant operational and financial consequences.

Estimated Ransom Payments in 2024:

Analysis suggests that ransomware payments in 2024 totaled approximately $810 million, a decrease from $1.25 billion in 2023 but an increase from $665 million in 2022. This decline may indicate a growing resistance to ransom payments, coupled with law enforcement actions disrupting ransomware groups. However, it does not necessarily reflect a reduction in overall attacks.

Year	Estimated Ransom Payments
2024	$813,550,000
2023	$1,250,000,000
2022	$665,440,000

Source: "The 2025 Crypto Crime Report" by Chainalysis

Ransomware Attacks by Industry Sector

Data shows manufacturing, services, and healthcare were among the most frequently targeted industries in 2024. However, the distribution of attacks highlights that no sector is immune.

Sector	Reported Incidents
Manufacturing	538
Services	496
Healthcare/Pharma	406
Transport	372
IT/Telecom	354
Government/Society	274

Source: Ecrime.ch

Payment Rate vs. Attack Rate:

Data suggests that while ransom payments declined in 2024, the number of reported breaches increased. This could indicate that ransomware groups are conducting more attacks to compensate for lower ransom success rates.

Month	Estimated Payments	Reported Leaks
Jan	470	310
May	380	575
Nov	180	720

Source: "The 2025 Crypto Crime Report" by Chainalysis

Ransomware Group Disruptions

Law enforcement agencies have increasingly targeted ransomware groups, with the LockBit takedown in February 2024 being a notable success. This joint operation involved multiple countries, demonstrating the international cooperation required to combat ransomware. However, history suggests that disrupted groups often reorganize, or affiliates move to new operations.

Ransomware Victims by Company Size

Ransomware attacks affect organizations of all sizes. Data suggests that while large enterprises remain targets, smaller organizations are frequently impacted, often struggling with recovery due to limited resources.

Company Size	Reported Incidents
50 employees	1,589
200 employees	846
1,000 employees	513

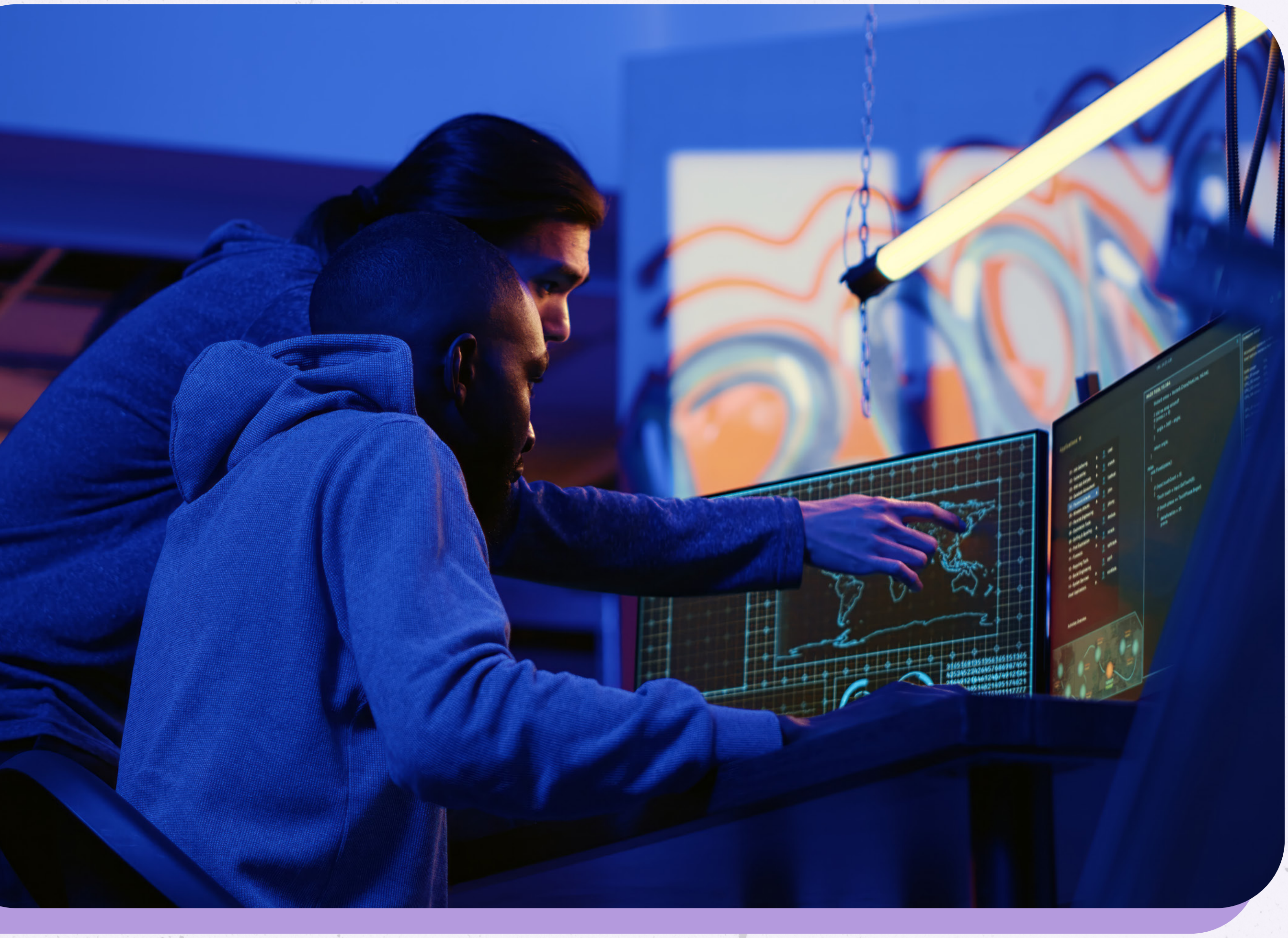
Source: Ecrime.ch

Mitigation and Prevention Strategies

The British Library cyberattack in late 2023, which left the institution dealing with disruptions well into 2024, underscores the long-term consequences of ransomware. Prevention remains the most effective defense. Organizations should consider the following:

- **Patching and Vulnerability Management**: Most ransomware attacks exploit known vulnerabilities. Regular patching can prevent these entry points.
- **Strong Authentication Practices**: Multi-factor authentication (MFA) and passkeys reduce the risk of credential-based attacks.
- **Phishing Awareness and Detection**: Ransomware often begins with phishing. Employee training and email security solutions can reduce risk.
- **Proactive Security Monitoring**: Partnering with a cybersecurity provider can enhance detection and response capabilities.

While the decline in ransomware payments in 2024 is a positive development, the continued rise in attack numbers indicates that organizations must remain vigilant. A strong cybersecurity posture, combined with proactive monitoring and incident response, remains essential in mitigating the impact of ransomware.

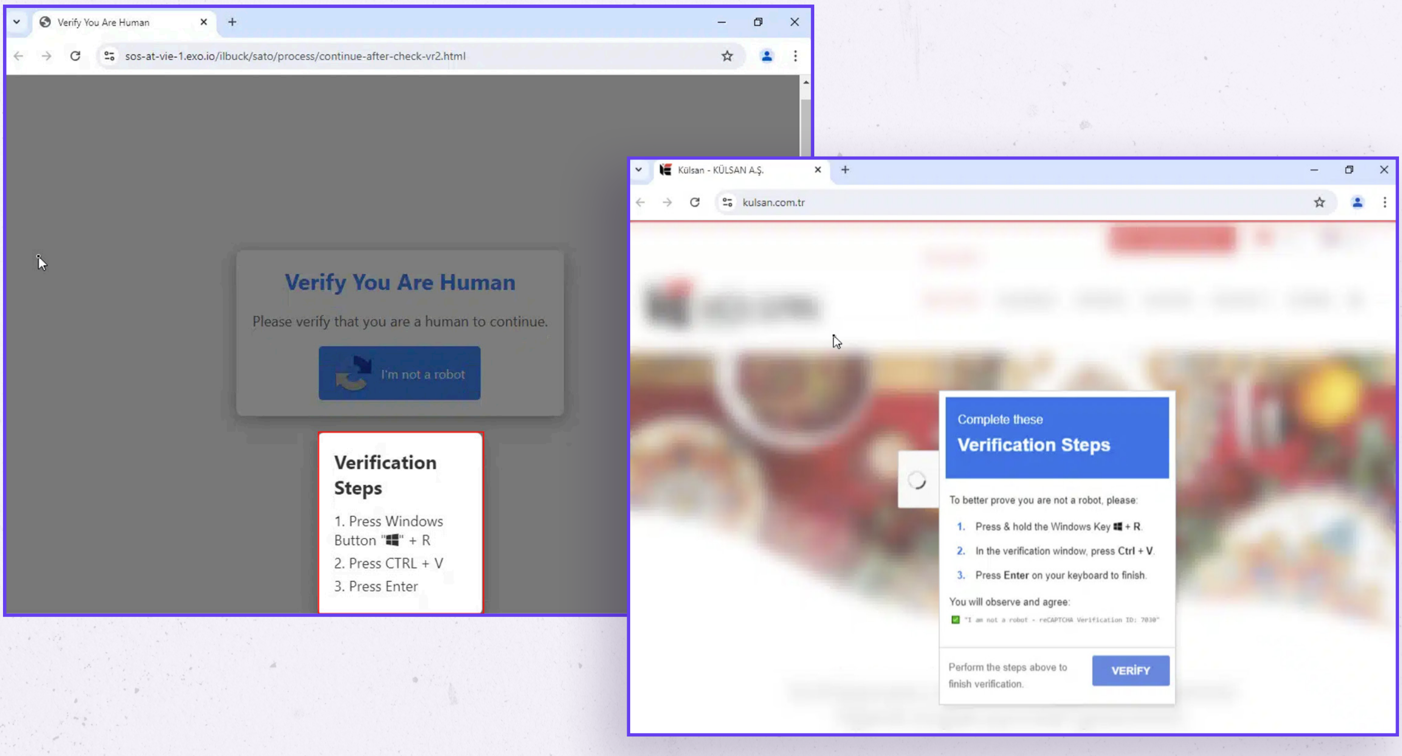


Malware Delivery Mechanisms are Shifting

As cyber defenses evolve, threat actors are continuously adapting their delivery methods to evade detection and maximize persistence. Traditional malware delivery techniques, such as email-based phishing and exploit kits, remain prevalent, but attackers are increasingly leveraging browser extensions and malvertising as stealthier alternatives. These methods exploit user behavior and system recovery processes, making them particularly effective at reinfecting devices even after remediation efforts.

Examples of exploitation:

- Browser extensions, especially those on Chrome, are being exploited to deliver information-stealing malware. This method is particularly effective because the malicious extensions can persist even after a system is reimaged. Users often unknowingly reintroduce the threat by reimporting their browser profiles, including the infected extensions, during the recovery process.
- Malvertising campaigns are coercing users into executing malicious PowerShell commands by instructing them to copy and paste the code directly into their system. These campaigns often guide users to open the 'Run' dialog using the Windows + R shortcut and then paste the commands using CTRL + V.



Verify You Are Human

Please verify that you are a human to continue.

Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

Complete these

Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key ⊞ + R.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard to finish.

You will observe and agree:

✅ "I am not a robot - reCAPTCHA Verification ID: 7030"

Perform the steps above to finish verification.

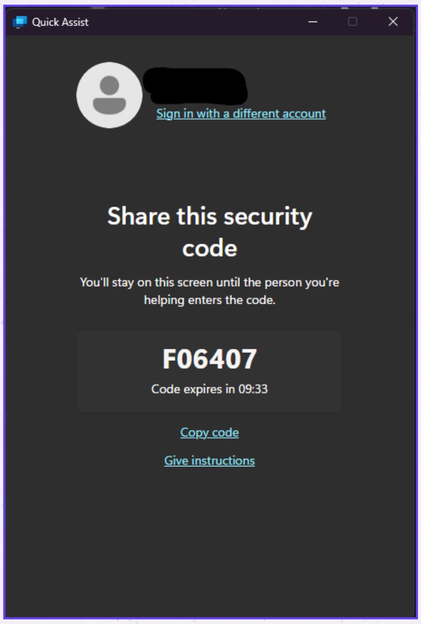
Threat Spotlights

Leveraging Built-in Microsoft Tools

Threat actors are turning trusted Microsoft tools into silent weapons, exploiting built-in features to slip past defenses and infiltrate customer environments. By abusing legitimate services like Quick Assist and Windows Hello, attackers can establish access and operate under the radar. These tactics highlight the urgent need for organizations to rethink security around trusted applications, ensuring that convenience doesn't come at the cost of compromise.

QuickAssist: A Convenient Tool Turned Cyber Threat

Quick Assist is a tool built into the Microsoft Windows operating system, designed to facilitate remote access for supporting end users. It allows an individual from another endpoint to connect to and control the target host device using a unique code that the user must provide from their device. As this tool is pre-installed, it can be exploited by threat actors who use social engineering techniques to impersonate technical support personnel to infiltrate the user's target endpoint.



[redacted]

Share this security code

You'll stay on this screen until the person you're helping enters the code.

F06407

Code expires in 09:33

Attack Vector Overview

- **Spam Bomb Attack:** The attacker inundates the victim's email or phone with a high volume of spam messages, thereby disrupting normal communications. This tactic is intended to overwhelm the recipient, creating a sense of urgency and confusion.
- **Fake Tech Support Scams**: In this scenario, the attacker establishes a fraudulent website, posing as tech support, to persuade the user to contact the phone number displayed on the site.
- **Quick Assist Exploitation**: When the victim contacts the scam hotline, the attacker directs them to launch QuickAssist.exe, a legitimate Microsoft tool pre-installed on Windows systems. By providing a code to initiate a Quick Assist session, the attacker can gain remote control over the victim's machine.

Potential Post-Access Activities

A threat actor could utilize this tool to deploy malware onto the victim's device, enabling various malicious activities, including:

- **Persistence:** The threat actor establishes mechanisms to maintain continuous access to the compromised endpoint, such as registry modifications, scheduled tasks, or backdoor creation.
- **Execution:** Additional malware or scripts are deployed to further compromise the system, potentially executing remote commands or downloading secondary payloads.
- **Command and Control (C2) & Exfiltration:** The attacker communicates with an external server to receive commands and exfiltrate sensitive data from the victim's machine, including personal files, credentials, and system information.
- **Data Theft:** The attacker may browse files, harvest credentials, or extract confidential information, which can be leveraged for further attacks or sold on underground markets.
- **System Sabotage:** The attacker might disable security software, encrypt files for extortion (ransomware), manipulate system settings, or corrupt essential data to disrupt operations and evade detection.

Mitigation and Recommendations

Awareness Training:

- Educate users on the risks associated with spam bomb attacks and fake tech support scams.
- Emphasise the importance of verifying contact numbers and avoiding unsolicited technical assistance.

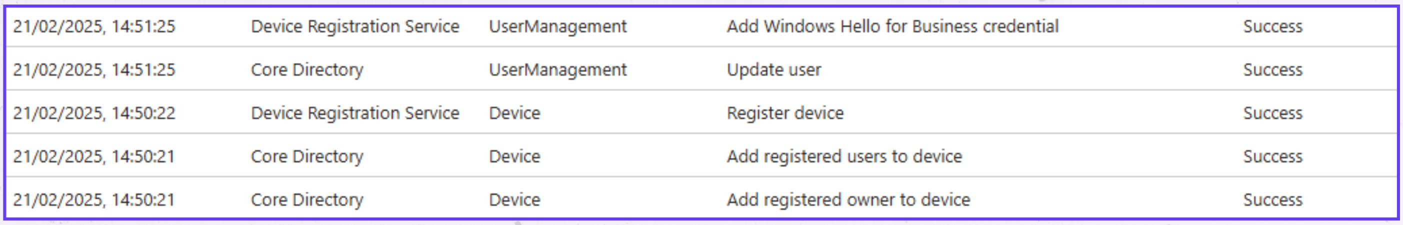
Technical Safeguards

- Disable Quick Assist via Group Policy on enterprise devices where it is not explicitly required.
- Monitor and log the usage of QuickAssist.exe to detect any anomalous activities.

Windows Hello

Windows Hello is Microsoft's passwordless authentication technology designed to enhance security while improving user convenience. It supports biometric (facial recognition, fingerprint) or PIN-based authentication and is categorized into:

- Windows Hello is Microsoft's passwordless authentication system that allows users to log in using biometrics (fingerprint/face) or PIN.
- Windows Hello for Business (WHfB) extends this authentication to Microsoft Entra (Azure AD) and third-party apps via SSO (Single Sign-On).



21/02/2025, 14:51:25	Device Registration Service	UserManagement	Add Windows Hello for Business credential	Success
21/02/2025, 14:51:25	Core Directory	UserManagement	Update user	Success
21/02/2025, 14:50:22	Device Registration Service	Device	Register device	Success
21/02/2025, 14:50:21	Core Directory	Device	Add registered users to device	Success
21/02/2025, 14:50:21	Core Directory	Device	Add registered owner to device	Success

Windows Hello is often considered **phishing-resistant** since authentication is bound to a specific device. However, attackers have identified ways to bypass these protections, compromising both persistence and Multi-Factor Authentication (MFA) security.

How Attackers Exploit Windows Hello

✓ Device Enrollment & MFA Bypass

Attack Type: Registering a Rogue Device or Bypassing MFA

- In some misconfigured enterprise environments, attackers with a valid user credential can enroll a new Windows Hello for Business device and authenticate without passwords.
- Real-world scenario: If an attacker steals a user's Active Directory credentials, they might be able to register their own device with WHfB and gain persistent access.

✓ Key Abuse in Active Directory & Azure AD

Attack Type: Stolen or Compromised Authentication Keys

- WHfB replaces passwords with asymmetric key pairs stored in TPM or software.
- Attackers can target private keys if they:
  - Gain access to a compromised endpoint.
  - Exploit a weakly protected TPM implementation.
  - Extract keys from memory in non-Hyper-V secured environments.

Security Recommendations

Security teams must rethink trusted applications and authentication mechanisms to prevent these attacks:

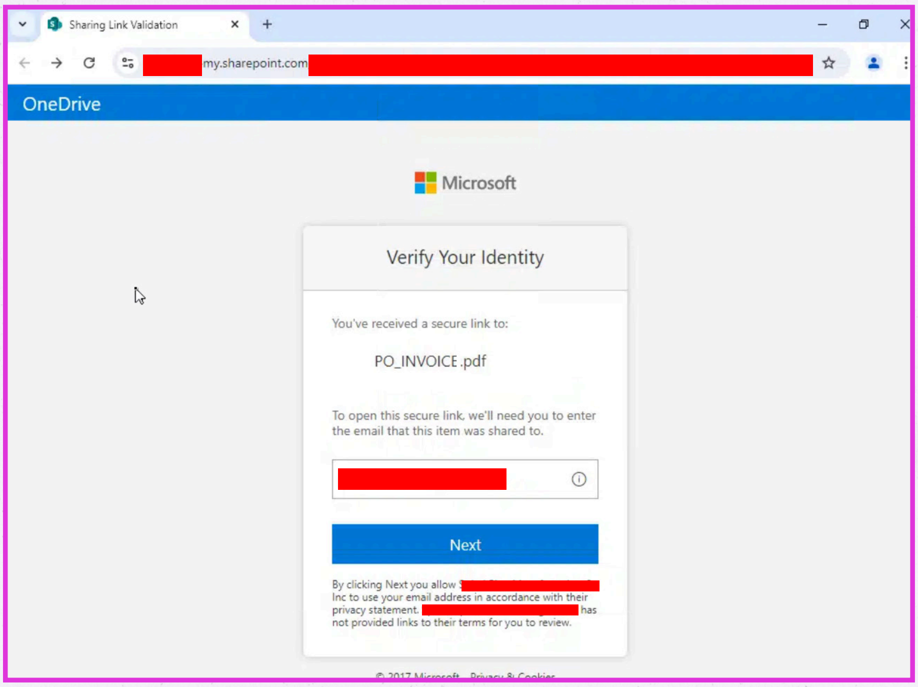
- Monitor and audit device registrations to detect unauthorized Windows Hello enrollments in Entra ID and Active Directory.
- Enforce strict conditional access policies to restrict WHfB registration to managed and compliant devices only.
- Enable FIDO2 security keys for phishing-resistant authentication and disable software-based biometric authentication.
- Require TPM 2.0 for WHfB keys and enforce Credential Guard to prevent key extraction and relay attacks.
- Revoke compromised Windows Hello credentials by removing unauthorized devices and resetting WHfB registrations.
- Regularly review Entra ID sign-ins and authentication logs to identify anomalies in authentication activity. By addressing these evolving tactics, organizations can ensure that convenience doesn't come at the cost of security.

Phishing

Phishing emails continue to be a significant threat as they remain a common entry point for threat actors. Ontinue has noted several trends in phishing schemes that have effectively lured users to 'Man in the Middle' (AiTM) sites, resulting in the theft of their credentials and session tokens.

Using legit sites for the first landing page

- The URLs contained in phishing emails often lead to legitimate websites which redirect users to a more obscure and malicious domain. This tactic helps evade email security mechanisms which scan URLs and are more familiar to users increasing the likelihood they will interact with it. Such sites include compromised SharePoint domains, Microsoft Forms, WeTransfer and Google Drive.



Verify Your Identity

You've received a secure link to:

PO_INVOICE.pdf

To open this secure link, we'll need you to enter the email that this item was shared to.

[redacted]

Next

By clicking Next you allow [redacted] Inc to use your email address in accordance with their privacy statement. [redacted] has not provided links to their terms for you to review.

© 2017 Microsoft Privacy & Cookies

Using 'noreply' sender addresses

- In line with the tactic above, threat actors frequently use legitimate 'no-reply' email addresses (e.g., 'noreply@wetransfer.com') to send phishing emails. This approach can circumvent email security checks that assess the sender's address and appear more legitimate to recipients.

Using legitimate domains to redirect users

- Ontinue has also observed that threat actors commonly exploit legitimate domains with obscure URLs, such as those from google.com, apple.com, and bing.com, to redirect users to AiTM sites. These legitimate domains help in evading detection.

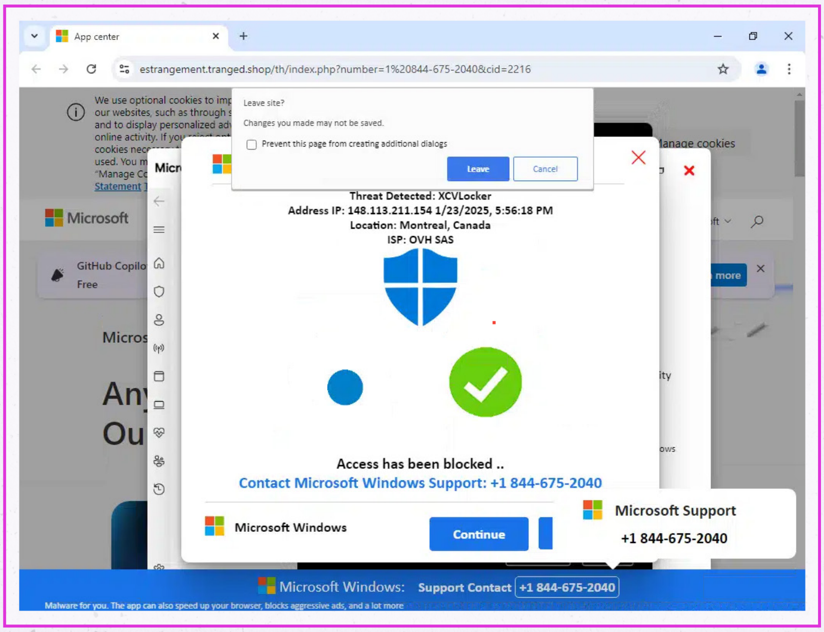
Vishing

Ontinue has observed a significant increase in Vishing attacks over the past six months as an initial method for compromising hosts. Vishing is particularly effective because it bypasses the automated security filters that phishing emails must navigate. Additionally, most organizations lack telemetry over phone calls made to users' mobile devices, further reducing their ability to detect and mitigate these attacks. The threat actors will attempt to convince the user to grant them remote access to their host via tools such as Quick Assist or ScreenConnect. Once the actors have control, they infect the host with their malware loaders.

Microsoft report that APT Storm-1811 have been particularly active leveraging this technique in 2024. The end goal is usually Black Basta Ransomware.

There have been two notable techniques where Ontinue observed threat actors leveraging to create fictious scenarios before vishing attacks occur:

- **Email bombing** – A tactic where threat actors flood multiple users' inboxes with an overwhelming volume of junk emails, rendering them unusable. Following this disruption, the attackers pose as Help Desk personnel, calling the victims and claiming they need remote access to their systems to resolve the issue. This social engineering technique exploits the user's frustration and urgency, increasing the likelihood of them granting access.
- **Malvertising** – Ontinue has frequently observed users being redirected from malicious adverts to web pages which mislead users into believing their devices have been compromised, urging them to call a so-called 'Microsoft Support' number. Following this the threat actors will then try to convince the user to install a remote desktop application and give them control of their machine.



estrangement.tranged.shop/th/index.php?number=1%20844-675-2040&cid=2216

Leave site?

Changes you made may not be saved.

□ Prevent this page from creating additional dialogs

Threat Detected: XCVLocker
Address IP: 148.113.211.154 1/23/2025, 5:56:18 PM
Location: Montreal, Canada
ISP: OVH SAS

Access has been blocked ..
Contact Microsoft Windows Support: +1 844-675-2040

Microsoft Support
+1 844-675-2040

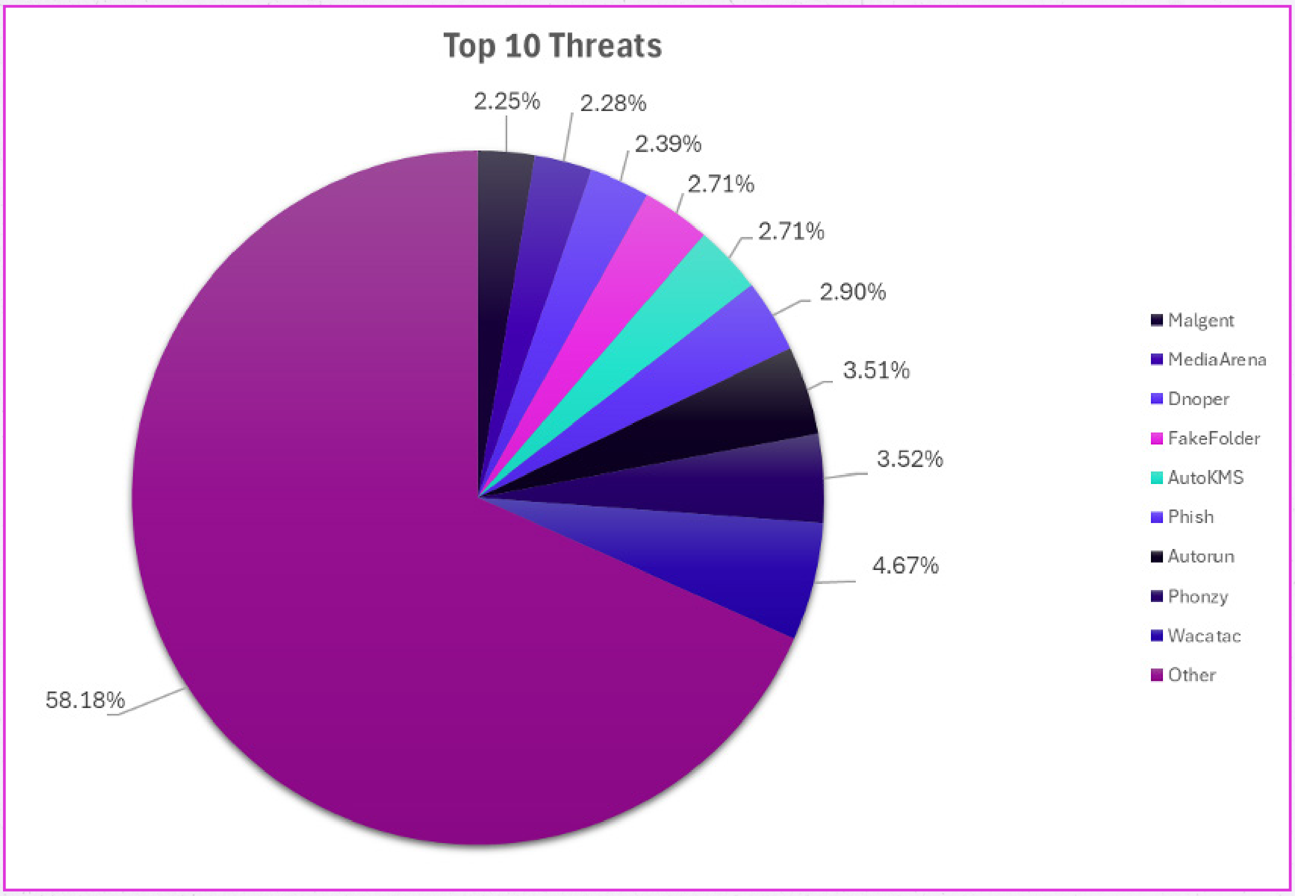
Microsoft Windows: Support Contact +1 844-675-2040

Malware for you. The app can also speed up your browser, blocks aggressive ads, and a lot more

Vishing has become increasingly popular among threat actors as they continue to leverage artificial intelligence. By utilizing AI-driven voice cloning technologies, cybercriminals can create highly realistic audio deepfakes, impersonating trusted individuals to deceive victims into divulging sensitive information or transferring funds. The ATO team has observed a staggering 1633% increase in Vishing-related incidents compared to the previous quarter, often involving users accessing web pages hosted on '.shop' domains. As threat actors continue refining their tactics, the ATO team predicts that Vishing will remain an escalating threat in 2025 and beyond.

Network Exploitation and Zero-day Development 🦠

Since the beginning of 2024, we have seen an accession of actively exploited zero-day vulnerabilities in various network security products. Ontinue's Advanced Threat Operations (ATO) Team reported these threats on the 25th of October.



Various sources (like, National Cyber Security Center, security researchers, reports) have been warning about internet facing services, and especially edge network devices being in the crosshairs of *continuous* and widely successful *offensive security development.*

How Large is the Threat?

Nation-states have dedicated offensive cyber units. Sizes vary, but the largest cyber armies can have several thousand members comprised of military personnel, defense subcontractors, and university research teams. Many of these teams are dedicated to the extensive research of impactful products and services for the express purpose of developing and weaponizing exploits.

How Do Zero-day Vulnerabilities Get Reported?

The most common way that zero-day vulnerabilities are reported is through threat analysts and intelligence teams tracing back breach investigations. This work is often done in conjunction with the security providers who built the products and services that have been exploited.

Vulnerability research is expensive and takes a lot of resource and man power to find vulnerabilities. Using a Zero day has to be carefully planned, once used it has a high chance of being discovered and then mitigated. Zero-days are often used by APT groups in:

- highly impactful targets (e.g. governments)
- where long-term access and staying undetected is important

The (Re-)use of Zero-days

Nation-state actors are highly organized. Once campaigns are detected / exposed a wider range of cyber attacks follow almost immediately with the same weaponized exploit, for different purposes. This effective sharing has increased the economic benefits favouring the aggressors.

What Can Security Teams Do?

If a system is vulnerable and online, it will be hit within hours—there's no if, just when. Attackers continuously scan the entire IPv4 address space, meaning exposed services are discovered almost immediately. Security teams must establish resilient emergency patching procedures for internet-facing services and edge devices. Depending on the operational and business risk, patching should ideally happen within hours, not days—and certainly not weeks. Leaving the front door open, even briefly, almost guarantees costly network remediation efforts, even if just one compromised edge device is detected.

Zero-days vs. "Regular" Vulnerabilities

According to several vulnerability research reports, the overwhelming majority of exploitations are still happening through regular reported vulnerabilities. This is due to the sheer number of publicly disclosed, easily exploitable vulnerabilities that even less skilled attackers can easily weaponize.

Noteworthy News & Rising Threats

The Rise in IoT & OT Threats

When we think about cybersecurity, IT networks and corporate systems usually come to mind—but what about the countless devices that operate outside of traditional IT oversight? Industrial machinery, power grids, surveillance cameras, and even smart thermostats all fall under the umbrella of Operational Technology (OT) and the Internet of Things (IoT). Unlike corporate IT environments, these devices often lack centralized security controls, making them prime targets for cyber threats. As attackers shift their focus to these critical systems, businesses must rethink their security strategies to account for the growing risks in IoT and OT environments.

When Consumer and Proprietary Collide

For simplicity, IoT can be considered a subset of OT, even though IoT devices are primarily designed for and marketed to consumers for non-industrial use.

Indeed, IoT-like hardware and software combinations often end up in OT products that are outwardly ruggedized, but internally similar or even identical to low-cost consumer devices. Notably, IoT devices are typically built so they can operate remotely and autonomously without being plugged into a laptop or any other computing device.

Despite having price tags as low as just a few dollars or tens of dollars, IoT devices typically include a miniature but complete computer of their own packaged into a single chip called a SoC, short for *System-on-Chip*.

They usually run a general-purpose operating system, frequently a stripped-down Linux distribution; include their own wireless networking hardware, often both Bluetooth and Wi-Fi; and run on their own USB-rechargeable battery power.

Today, we're seeing that even those devices that are squarely aimed at consumers commonly find their way into and onto corporate networks, directly and indirectly, for several important reasons:

- **Staff working from home often hook up their IoT devices to the same SoHo network as their work laptops and phones**, so the IoT devices end up directly adjacent on the network to their work computers.
- **IoT devices such as webcams and light switches don't care whether they're on a company network or a home network**, so they are easy and convenient to deploy at work, with or without the approval of the IT or cybersecurity team.
- **Non-consumer OT devices may be based on IoT-like internals**, so even specialized devices such as weather monitors or plant control systems could be exposed by the same already-known vulnerabilities as off-the-shelf consumer products.

Typical Abuses of IoT/OT

When IoT devices are built down to a price, their firmware is often built down to a price, too. IoT web services, for example, often rely on stripped-down networking software that runs with root privilege and performs its configuration operations simply by passing user-supplied data to the system via a command shell.

This makes IoT devices notoriously vulnerable to command injection, remote code execution, and privilege escalation attacks.

These low-security devices usually have outbound access to the internet, even when they sit alongside work-related computers, with the result that hacked or badly configured IoT products can be exploited for a wide range of cybercrimes.

These include:

- **Distributed denial of service attacks (DDoS).** By generating innocent-looking but useless network traffic aimed at chosen targets, compromised IoT devices can affect your internal networks, or leave the finger of blame pointing back at you for attacks against third parties.
- **Network mapping and vulnerability scans**. Rogue IoT devices can typically map out your private networks from the inside and report back on vulnerable systems, either for immediate criminal use or for sale on dark web cybercrime forums.
- **Remote access backdoors**. Insecure devices can be abused to set up reverse shells, where a compromised device "calls home" and connects outwards, but then uses the inbound channel of that connection to provide a criminals on the outside with a command prompt inside the network.
- **Hidden VPN services**. Some criminals specialize in using backdoors on IoT devices to set up hidden proxies or VPN servers so they can "rent out" your bandwidth and your network identity to other criminals. This leaves you to face the investigatory probing of regulators, lawyers, and law enforcement.

- **Click fraud**. By triggering outbound web requests from a wide range of otherwise trustworthy networks, cybercriminals can often circumvent fraud detection tools. Other criminals willingly pay for artificial clicks and recommendations, for example to earn bogus ad revenue, promote fake news, or legitimize rogue products and services.
- **Unauthorized configuration and manipulation of systems**. Wrongly configured devices may end up externally manageable by unauthorized visitors. This is worrying enough if the device provides a real-time video feed of a secure area, but potentially devastating if the device regulates flood control valves, or switchgear in an electrical grid.

Recent IoT/OT Attack Scenarios

The rapid rise of IoT and OT threats presents a significant challenge for defenders, as these devices often lack the same security controls and visibility as traditional IT systems. Unlike corporate networks, where security teams can deploy monitoring tools and enforce strict policies, IoT and OT environments frequently operate in silos, with little oversight and limited ability to detect or respond to threats. This lack of visibility makes it difficult to measure the true scale of the risk, but recent attacks have shown just how vulnerable these systems can be. From large-scale botnets leveraging unpatched IoT devices to sophisticated nation-state actors targeting industrial control systems, the evidence is clear: IoT and OT threats are not only increasing in frequency but also growing in complexity and impact.

Examples of Iot/OT attacks from the 2024 include:

- Matrix Threat Actor – This double-pronged actor targeted both cloud services (e.g., Hadoop clusters) and IoT devices such as webcams, DVRs, and SoHo routers, launching widespread DDoS campaigns.
- Mirai-Based DDoS Attacks – An unnamed threat actor leveraged old Mirai malware to conduct large-scale global DDoS attacks, demonstrating the persistent threat of repurposed malware.
- Rising IoT Malware Infections – Researchers reported a 12% increase in IoT malware infection attempts, with most active samples derived from Mirai and Bashlite botnets, capable of launching attacks and self-updating to evade detection
- Flax Typhoon Botnet Takedown – The U.S. DOJ disrupted a 20,000-node botnet operated by Flax Typhoon (assessed to be China-based). During the takedown, the FBI faced retaliatory DDoS attacks from undismantled parts of the botnet
- Flax Typhoon's Raptor Train Campaign – This group has spent years infecting and reinfecting IoT devices with malware variants designed to operate across ARM, MIPS, Intel, SH4, and PPC architectures
- Volt Typhoon Resurgence – Despite a U.S. government takedown, researchers observed renewed activity from Volt Typhoon, which exploits unpatchable, end-of-life SoHo routers to conceal cyber operations

- Threats to European Power Grids – Researchers identified vulnerabilities in a widely used remote power control protocol, revealing that unauthenticated commands could disrupt up to 40GW of power supply, potentially leading to brownouts or blackouts.
- Water System Vulnerabilities – The U.S. government warned of misconfigured infrastructure control systems in water facilities. Pro-Russian actors were reportedly able to alter pumping parameters, disable alarms, and lock operators out of their systems.

Best Practices for Securing IoT and OT Assets

Achieve Full Visibility of IoT and OT Assets

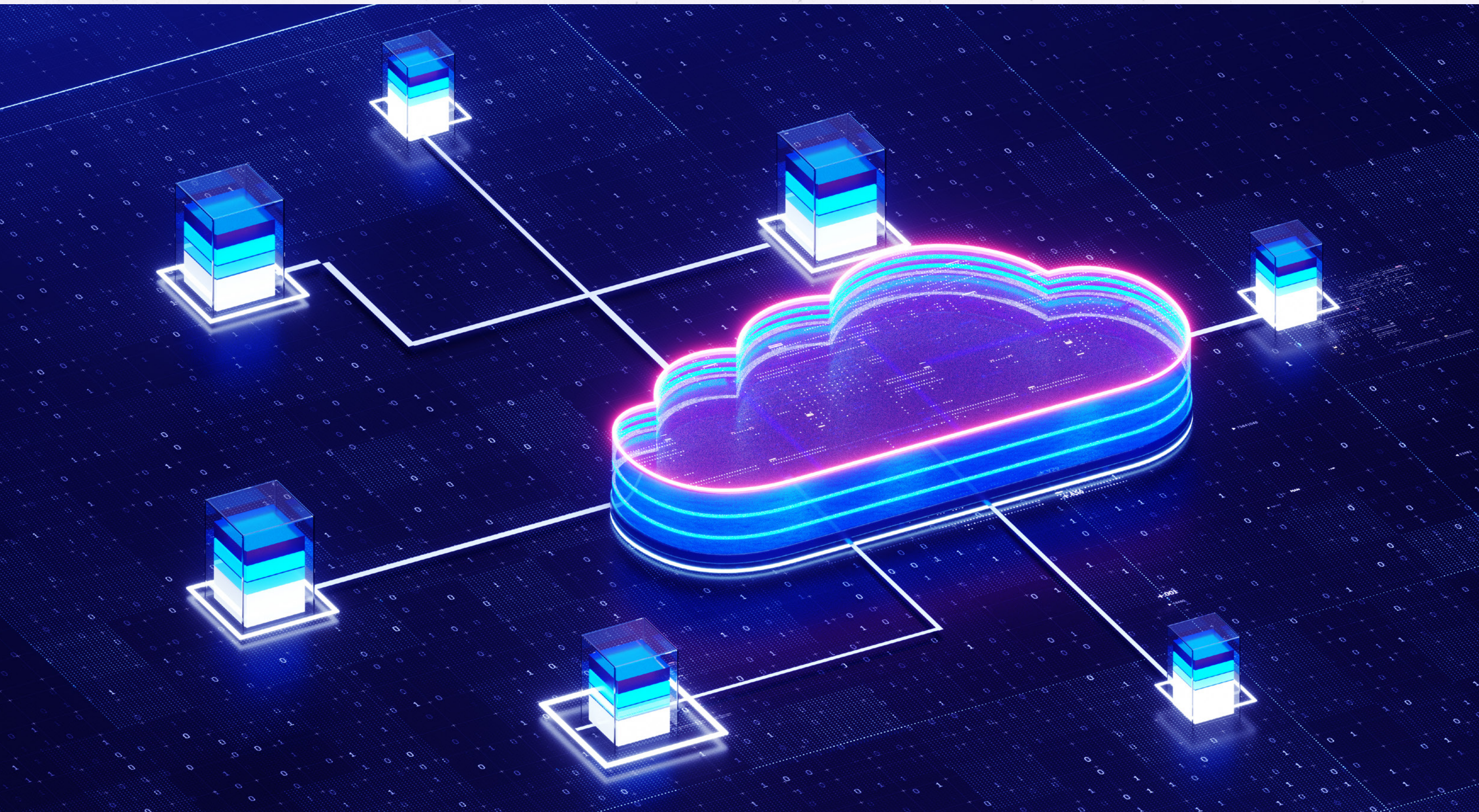
- Maintain an up-to-date inventory of all connected devices, including unauthorized shadow IoT/OT systems.
- Use network monitoring tools to detect and classify IoT/OT traffic separately from traditional IT assets.

Segment Networks and Restrict Access

- Separate IT, OT, and IoT devices into distinct network zones to prevent lateral movement by attackers.
- Enforce least privilege access and restrict direct internet connectivity for IoT/OT devices.

Continuously Monitor and Respond to Threats

- Deploy threat detection solutions that identify anomalies in IoT/OT environments.
- Integrate IoT/OT risks into the organization's broader incident response framework.



Top 15 True Positive Detections Observed on the Ontinue ION MXDR

Ontinue's ATO team identified the top 15 True Positive detections across the ION customer base, revealing key cyber threats targeting organizations in 2H 2024. The most prevalent threats included **info stealers, emerging threats, Adversary-in-the-Middle (AiTM) attacks, PlugX Remote Access Trojan (primarily targeting NGOs), suspicious PowerShell and DLL activity, and phishing—often leading to initial access breaches**.

This year, AiTM attacks emerged as a dominant theme, along with significant activity from PlugX, command-and-control (C2) traffic, and phishing campaigns. However, the ATO team also observed a **notable uptick in emerging threats and information stealers**, signaling evolving tactics from threat actors.

Below are the top 15 True Positive detections flagged by the Ontinue ION platform:

1. **AO-EXE-MDFE-04** – Potential Lumma stealer activity via PowerShell download
2. **Suspicious DLL** launched from an unusual location
3. **Suspicious process execution** by Rundll32.exe
4. **EX-CRE-AAD-01** – Password spray attack targeting Microsoft Entra ID applications
5. **Possible PlugX Remote Access Trojan (RAT) activity**
6. **Suspicious PowerShell** command detected in the Windows registry
7. **Potential initial access attempt** from an emerging threat
8. **Connection to an AiTM phishing site**, indicating credential theft attempts
9. **Information-stealing malware** in active use
10. **1EX-INA-AAD-02** – Possible AiTM phishing attempt targeting Microsoft Entra ID
11. **Encoded PowerShell execution**, suggesting obfuscation tactics
12. **PowerShell command execution** by a suspicious process
13. **AO-INA-MDO-AADIP-01** – Correlation between a potentially malicious URL click and AADIP alerts
14. **Suspicious URL clicked,** possibly leading to malware or credential theft
15. **EX-INA-AAD-01** – Risky sign-in attempt with a newly registered MFA method

These findings highlight the **persistent and evolving nature of cyber threats**, with adversaries continuously refining their methods to bypass security defenses. Ontinue's ATO team remains vigilant, leveraging real-time threat intelligence and proactive detection to safeguard organizations from these advanced threats.

Getting Cyber Serious

To mitigate emerging threats, organizations should implement the following security measures:

Strengthen Ransomware Defenses

- Enforce regular data backups with offline storage.
- Implement endpoint detection and response (EDR) solutions.
- Use threat intelligence to proactively detect ransomware indicators.

Secure Authentication Methods

- Enforce multi-factor authentication (MFA) with phishing-resistant options (e.g., FIDO2 security keys).
- Monitor and restrict device registrations to prevent unauthorized access.
- Regularly audit authentication logs for anomalies.

Monitor and Secure Built-in System Tools

- Restrict access to Quick Assist and other remote support tools.
- Enforce strong policies for Windows Hello to prevent unauthorized device enrollment.
- Regularly review security configurations to detect and mitigate abuse of native tools.

Implement Rapid Patching and Vulnerability Management

- Establish emergency patching procedures for critical zero-day vulnerabilities.
- Prioritize updates for edge devices and network security products.
- Continuously monitor for new exploit disclosures and apply patches promptly.

Enhance Web and Email Security

- Block unauthorized browser extensions and monitor installed add-ons.
- Train employees to recognize malvertising and phishing attempts.
- Deploy email filtering solutions to detect AiTM phishing attempts.

Improve Incident Response and Threat Hunting

- Conduct regular tabletop exercises to test incident response plans.
- Leverage threat intelligence to proactively detect adversarial tactics.
- Utilize behavioral analytics to identify suspicious activity before compromise occurs.

As cyber threats continue to evolve, organizations must adopt a proactive approach to cybersecurity. The 2H 2024 Threat Intelligence Report underscores the importance of rapid threat detection, robust authentication controls, and an agile response strategy. By implementing these best practices, businesses can reduce risk exposure and build a more resilient security posture against emerging threats.

Contributors

Ontinue's **Advanced Threat Operations** (ATO) team leverages proactive threat identification, analysis, and mitigation to empower our customers with the resilience needed to tackle the constantly evolving threat landscape.

Special thanks to **Will Bailey,** ION Senior SOC Analyst, and **Lenka Sykorova**, Director of Threat Detection, for their contributions.

Ontinue

© 2025 Ontinue. All Rights Reserved. Approved for public use

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.

Continuous protection. AI-powered Nonstop SecOps. That's Ontinue.

CONTACT US

LEARN MORE