TIR-20260819CaptiveCrunch: Hotel Wi-Fi Attacks Target Corporate Travelers

8/19/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

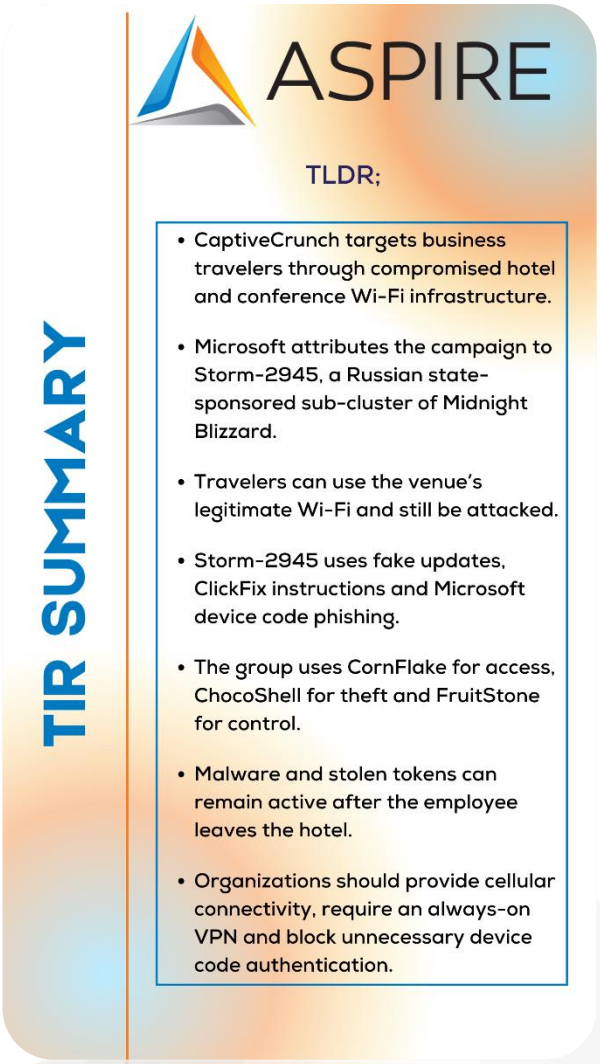
Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

CaptiveCrunch is an ongoing hotel Wi-Fi attack campaign that turns a routine hotel or conference network connection into an opportunity to compromise corporate accounts and devices. Microsoft has tracked the cyberespionage activity since early May 2026 and attributes it to Storm-2945, a sub-cluster of the Russian state-sponsored threat actor Midnight Blizzard.

A traveler can connect to a hotel or conference venue's legitimate Wi-Fi network and still be exposed to CaptiveCrunch. Storm-2945 uses its access to the captive portal infrastructure to interfere with DNS and HTTP traffic, replacing the normal login process with a fake Microsoft sign-in page or software update message. If the traveler enters a device code or follows the update instructions, the threat actor may gain access to the traveler's Microsoft 365 account or install malware that collects credentials, authentication tokens, files and other data from the device.



Microsoft is still investigating how Storm-2945 gained access to these environments. Several affected networks used similar equipment and management systems, which raises the possibility that the group compromised a service used by multiple venues instead of targeting each location separately.

For organizations, the threat continues after a guest disconnects from the hotel Wi-Fi. Malware installed during the stay can remain active when the guest returns home or to the office. Stolen cloud tokens could also allow the group to access corporate email and other Microsoft 365 data without needing the guest's password again.

STORM-2945 AND THE CAPTIVECRUNCH CAMPAIGN

Storm-2945 is a Russia-based, state-sponsored threat cluster that Microsoft considers part of Midnight Blizzard. Microsoft first observed activity attributed to Storm-2945 in February 2026, when the group was conducting device code and OAuth phishing against Microsoft 365 users. The CaptiveCrunch campaign began several months later, in early May 2026.

Midnight Blizzard is also known as APT29, Cozy Bear, NOBELIUM and the Dukes. The U.S. and U.K. governments have linked the group to Russia's Foreign Intelligence Service, the SVR. It is an espionage group rather than a financially motivated cybercriminal operation. Its goal is to maintain access to targeted organizations and collect intelligence that supports Russian foreign policy.

The broader Midnight Blizzard operation has historically targeted government agencies, diplomatic organizations, nongovernmental organizations and IT service providers, mainly in the United States and Europe. CaptiveCrunch can reach people from many other industries simply because they travel and use shared Wi-Fi. ReliaQuest observed connections from financial services, professional services, legal, healthcare, energy and retail organizations. Compromised gateways were found in several U.S. cities as well as India and Saudi Arabia. This does not necessarily mean Storm-2945 chose every organization or country in advance. Anyone using an affected network could be exposed.

Microsoft connected Storm-2945 to Midnight Blizzard partly through its similarities to Storm-2372, another Midnight Blizzard sub-cluster. Both groups have used device code and OAuth phishing to access Microsoft 365 accounts. They also share similar targets and have used Microsoft Graph to collect email. CaptiveCrunch takes this existing method and places it inside the Wi-Fi sign-in process, where the request is less likely to raise suspicion.

Microsoft also found signs that artificial intelligence supported parts of the operation. ChocoShell contains unusually detailed developer comments explaining how the

malware avoids specific Microsoft detections. Microsoft believes the wording and structure of those comments may point to AI-assisted development.

Connections to Midnight Blizzard and Other Russian Threat Actors

Storm-2945 shares technical similarities with Storm-2372, another Midnight Blizzard sub-cluster known for device code and OAuth phishing. Both have targeted similar victims and used Microsoft Graph to collect email from compromised Microsoft 365 accounts.

Microsoft noted that CaptiveCrunch uses DNS manipulation similar to an earlier operation associated with Forest Blizzard, also known as APT28 or Fancy Bear. However, Microsoft attributes CaptiveCrunch to Storm-2945, a Midnight Blizzard sub-cluster, rather than Forest Blizzard.

How the CaptiveCrunch Attack Works

Hotel Wi-Fi Captive Portal Traffic Manipulation

Hotels, airports and conference venues often require guests to pass through a captive portal before connecting to the internet. A device checks for internet access as soon as it joins the network. On networks affected by CaptiveCrunch, Storm-2945 can interfere with this process and redirect the device to its own infrastructure.

The guest is not connecting to a fake Wi-Fi network. The network name, password and connection instructions may all be legitimate. The problem is that the captive portal or the infrastructure supporting it has been compromised, allowing the threat actor to control what appears during the connection process.

In the activity observed by ReliaQuest, the attackers changed DNS settings on compromised gateways. This allowed them to send users to malicious systems when they attempted to visit legitimate websites. The attackers also tested Web Proxy Auto-Discovery abuse, which could route more of the device's application traffic through their proxy.

Fake Browser Updates and ClickFix

One CaptiveCrunch attack path presents the traveler with a fake software update or repair message. The page may look like a Windows update, browser update, security scan or network troubleshooting tool. Its timing makes it more believable because it appears just after the device connects to the network.

Some pages use ClickFix instructions that ask the user to copy a command and run it through Windows Terminal or PowerShell. The malware runs because the user follows the instructions, not because the page automatically installs it. Microsoft also found pages that instructed Android users to download an APK file, although confirmed Android infections have not been reported.

The CTI team previously covered ClickFix and fake browser updates in a cyber threat intelligence report. CaptiveCrunch uses the same type of social engineering, but the prompt reaches the victim through manipulated Wi-Fi traffic instead of an email or an unrelated website.

Microsoft Device Code Phishing

Storm-2945 can also redirect travelers into Microsoft's legitimate device code authentication process. The attacker starts a sign-in attempt and then gives the victim a code to enter on Microsoft's real website.

Entering the code signs the attacker into the account. Microsoft then issues access and refresh tokens that can be used to reach Microsoft 365 services. Because the victim enters the code on a legitimate Microsoft page, there may be no obvious fake login page to recognize.

The CTI team previously covered token theft and device code phishing in its cyber threat intelligence report on initial access brokers. CaptiveCrunch places the request inside the hotel Wi-Fi connection process, where an extra sign-in step may not seem unusual.

CornFlake RAT Malware

CornFlake is the main malware Storm-2945 uses to maintain access to Windows devices. While a fake progress window keeps the victim occupied, the RAT copies itself to %APPDATA%\svchost32\svchost32.exe.

The malware creates a Windows service called svchost32, which appears as Cloud Sync Service. It can also use Registry Run keys and scheduled tasks to start again after a reboot. A built-in watchdog recreates these persistence methods if security software removes them.

Once installed, CornFlake can:

- Record keystrokes and clipboard activity
- Capture screenshots and record audio or video
- Steal browser credentials and files
- Monitor connected removable drives
- Run commands through a remote shell

These functions allow Storm-2945 to continue monitoring the device after the traveler disconnects from the network and leaves the venue.

ChocoShell Infostealer and FruitStone

Storm-2945 uses ChocoShell, an in-memory PowerShell infostealer, to collect information that can provide access to a victim's accounts. It steals browser cookies, saved passwords, Microsoft 365 single sign-on tokens, Web Account Manager tokens and saved Wi-Fi credentials.

Before collecting the data, ChocoShell attempts to disable PowerShell scanning through the Antimalware Scan Interface. It also checks for sandbox environments and tries several methods to bypass User Account Control. The malware sends the stolen information over HTTPS using web paths that resemble normal traffic.

Storm-2945 also uses the FruitStone command-and-control panel to manage infected devices and build new CornFlake payloads. FruitStone is disguised as a business cloud-management console. Operators can use it to issue commands, search files, change malware settings and review stolen information.

WHY CAPTIVECRUNCH THREATENS ORGANIZATIONS

The hotel network is the entry point, but the traveler's organization is the intended target. A work laptop may already be signed in to corporate email, Microsoft 365 and other business applications. It may also contain local files and active browser sessions that Storm-2945 can use or steal.

If malware is installed, it can remain on the device when the guest returns to work/home and reconnects to the corporate environment. Stolen Microsoft 365 tokens can also give the threat actor remote access to email and cloud data. Because those tokens may remain valid after a password change, resetting the target's password may not be enough to remove the attacker.

Any organization with employees who travel could be affected. This includes education, public sector, retail, manufacturing, finance, legal and professional services. Executives and employees with elevated access are attractive targets, but an ordinary user account can still give Storm-2945 a way into the organization.

CONCLUSION

CaptiveCrunch abuses a normal part of business travel. Connecting to legitimate hotel Wi-Fi is not careless behavior, and recognizing the correct network name does not prevent this attack.

Organizations should reduce their reliance on public Wi-Fi and control what company devices can access before reaching trusted corporate infrastructure. Employees should also understand that a captive portal should never require them to install software, run commands or authorize access to a corporate account.

ASPIRE'S RECOMMENDATIONS

Recommendations for Organizations

- Give employees a company-managed hotspot or eSIM before business travel. Make cellular service the default connection for company devices instead of hotel, airport or conference Wi-Fi.
- Configure company laptops to connect automatically to a full-tunnel VPN. Send all internet and DNS traffic through the corporate network and enable a kill switch that blocks internet access if the VPN disconnects.
    - Only captive portal registration and the traffic needed to establish the VPN should be allowed outside the tunnel.
- Create a Microsoft Entra Conditional Access policy that blocks device code authentication for all users. Add exceptions only for approved accounts with a documented business need.
    - Alert whenever an excluded account uses the device code flow.
- Move employees to passkeys or FIDO2 security keys. Require new authentication methods to be registered from a compliant company device or trusted location.
    - Use Entra sign-in risk policies to block high-risk attempts and require another sign-in when suspicious activity is detected.
- Use mobile device management to stop employees from manually adding wireless networks to company devices. Push approved Wi-Fi profiles through the management platform.
    - Employees who must use venue Wi-Fi should connect through a managed travel router that establishes an encrypted corporate tunnel.
- Disable Web Proxy Auto-Discovery through Group Policy if the organization does not use it. If WPAD is required, allow proxy configuration files to come only from approved internal servers.
- Create endpoint alerts for files downloaded or created within minutes of a captive portal connectivity check. Security teams should also monitor for svchost32.exe, a service named Cloud Sync Service, new Registry Run keys and scheduled tasks.
    - Other signs include AMSI being disabled, UAC bypass activity and unusual PowerShell commands.

- Review Entra logs for device code authentication from unfamiliar locations and new devices registered without approval. If an employee may have been affected, isolate the laptop and revoke the user's active sessions and refresh tokens.
    - Remove unauthorized devices from Entra ID and reset the account credentials. Reimage the laptop if CornFlake, ChocoShell or another unknown payload may have run.

Recommendations for Employees Who Travel for Work

- Use the hotspot or eSIM provided by your employer. If company policy allows it, use your phone's hotspot as a backup.
    - Do not connect a company laptop to hotel, airport or conference Wi-Fi when cellular service is available.
- A guest Wi-Fi page should never require you to install software. Close the page if it offers an update, certificate, security scan or network repair tool.
    - Never copy instructions from the page into PowerShell, Command Prompt or Windows Terminal.
- Do not enter your work password or a Microsoft device code during Wi-Fi registration. If a Microsoft sign-in page appears unexpectedly, disconnect from the network and report it to your security team or help desk.
- Update your laptop before leaving for a business trip. Install Windows, browser and application updates through the company's management tool or the software's built-in update feature. Restart the laptop so pending updates are completed.
- If you must use hotel Wi-Fi, provide only the information required to pass through the captive portal. Start the corporate VPN as soon as the portal closes and wait until the VPN client shows that it is connected.
    - Do not open email or other company applications before the connection is active. If the VPN will not connect, stop using the network and switch to cellular service.

MITRE MAP

Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1204.002 – User Execution: Malicious File T1204.004 – User Execution: Malicious Copy and Paste
Persistence	T1053.005 – Scheduled Task/Job: Scheduled Task T1543.003 – Create or Modify System Process: Windows Service T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
Defense Evasion	T1112 – Modify Registry T1562.001 – Impair Defenses: Disable or Modify Tools
Credential Access	T1557 – Adversary-in-the-Middle T1555.003 – Credentials from Password Stores: Credentials from Web Browsers T1528 – Steal Application Access Token
Discovery	T1082 – System Information Discovery T1518.001 – Software Discovery: Security Software Discovery T1120 – Peripheral Device Discovery
Collection	T1005 – Data from Local System T1113 – Screen Capture T1115 – Clipboard Data T1123 – Audio Capture
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols
Exfiltration	T1041 – Exfiltration Over C2 Channel

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from

endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts acts as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Indicators of Compromise (IoCs)

Domains

- ms365-device[.]com
- ms365-live[.]com
- m365-owa[.]com
- owa-ms365[.]com

IP Addresses

- 31[.]57[.]243[.]154
- 38[.]146[.]28[.]75

- 38[.]146[.]28[.]132
- 104[.]194[.]159[.]150
- 104[.]145[.]210[.]184
- 107[.]189[.]26[.]194
- 192[.]142[.]52[.]31
- 213[.]145[.]86[.]112

SHA-256 Hashes

- 918fa52ae45ed60ba7cc8bdc99c3cbe9ab92e0375ec31fc05d0d4513be11c593
- be99857449d2856dd5a84e21c8a3d5e0e01456adb44062ddec5a6b4970d8d42c

Email Address

- chikolimdrid[at]gmail[.]com

File Name

- svchost32.exe

SUPPORTING DOCUMENTATION

Hotel Wi-Fi Attack: Fake Updates and Phishing Explained | Mirage Threat Watcher

Russian hackers behind large-scale hotel Wi-Fi attack

DNS Poisoning Tactics Expand to Hospitality Wi-Fi | ReliaQuest Threat Spotlight

Storm-2945 - The Threat Codex

CaptiveCrunch: Storm-2945 Hijacks Captive Portal Traffic for Credential Theft and Malware Delivery — Vega Threat Intel

Storm-2372 conducts device code phishing campaign | Microsoft Security Blog

Travelers targeted when logging into hotel Wi-Fi networks | Malwarebytes

CaptiveCrunch Targets Travelers via Hijacked Wi-Fi

Midnight Blizzard launches CaptiveCrunch | ThreatLabz

Russian State APT Linked to Recent Public Wi-Fi Gateway Hacking - SecurityWeek

Midnight Blizzard Targets Travelers via Captive Portals - Infosecurity Magazine

CaptiveCrunch: Midnight Blizzard targets travelers worldwide for malware delivery and credential theft | Microsoft Security Blog

SVR Cyber Actors Adapt Tactics for Initial Cloud Access | CISA

Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication | Volexity

APPENDIX: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.