Research Threat intelligence Microsoft Defender Social engineering / phishing
10 min read

Financially motivated threat actors misusing App Installer

By Microsoft Threat Intelligence

December 28, 2023

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Attacker techniques, tools, and infrastructure

Threat actors

Since mid-November 2023, Microsoft Threat Intelligence has observed threat actors, including financially motivated actors like Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674, utilizing the ms-appinstaller URI scheme (App Installer) to distribute malware. In addition to ensuring that customers are protected from observed attacker activity, Microsoft investigated the use of App Installer in these attacks. In response to this activity, Microsoft has disabled the ms-appinstaller protocol handler by default.

The observed threat actor activity abuses the current implementation of the ms-appinstaller protocol handler as an access vector for malware that may lead to ransomware distribution. Multiple cybercriminals are also selling a malware kit as a service that abuses the MSIX file format and ms-appinstaller protocol handler. These threat actors distribute signed malicious MSIX application packages using websites accessed through malicious advertisements for legitimate popular software. A second vector of phishing through Microsoft Teams is also in use by Storm-1674.

Threat actors have likely chosen the ms-appinstaller protocol handler vector because it can bypass mechanisms designed to help keep users safe from malware, such as Microsoft Defender SmartScreen and built-in browser warnings for downloads of executable file formats.

In this blog, we provide an analysis of activity by financially motivated threat actors abusing App Installer observed since mid-November 2023.

Threat actors abusing App Installer since mid-November 2023

Microsoft Threat intelligence observed several actors—including Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674—using App Installer as a point of entry for human-operated ransomware activity. The observed activity includes spoofing legitimate applications, luring users into installing malicious MSIX packages posing as legitimate applications, and evading detections on the initial installation files.

Storm-0569

At the beginning of December 2023, Microsoft observed Storm-0569 distributing BATLOADER through search engine optimization (SEO) poisoning with sites spoofing legitimate software downloads such as Zoom, Tableau, TeamViewer, and

AnyDesk. Users who search for a legitimate software application on Bing or Google may be presented with a landing page spoofing the original software provider's landing pages that include links to malicious installers through the ms-appinstaller protocol. Spoofing and impersonating popular legitimate software is a common social engineering tactic. These software are not affected by the attacks directly, but this information can help users better spot malicious spoofing by threat actors.

Figure 1. A malicious landing page spoofing Zoom accessed via malicious search engine advertisement for Zoom downloads

Figure 2. Sample malicious App Installer experience. Note the Publisher is not who a user should expect to be publishing this software.

Users who click the links to the installers are presented with the desktop App Installer experience. If the user clicks "Install" in the desktop App Installer, the malicious application is installed and eventually runs additional processes and scripts that lead to malware installation.

Storm-0569 then uses PowerShell and batch scripts that lead to the download of BATLOADER. In one observed instance, Storm-0569's BATLOADER dropped a Cobalt Strike Beacon followed by data exfiltration using the Rclone data exfiltration tools and Black Basta ransomware deployment by Storm-0506.

Storm-0569 is an access broker that focuses on downloading post-compromise payloads, such as BATLOADER, through malvertising and phishing emails containing malicious links to download sites. The threat actor also provides malicious installers and landing page frameworks to other actors. They cover multiple infection chains that typically begin with maliciously signed Microsoft Installer (MSI) files posing as legitimate software installations or updates for applications such as TeamViewer, Zoom, and AnyDesk. Storm-0569 infection chains have led to additional dropped payloads, including IcedID, Cobalt Strike Beacon, and remote monitoring and management (RMM) tools, culminating in a handoff to ransomware operators like Storm-0846 and Storm-0506.

Storm-1113

Since mid-November 2023, Microsoft observed Storm-1113's EugenLoader delivered through search advertisements mimicking the Zoom app. Once a user accesses a compromised website, a malicious MSIX installer (EugenLoader) is downloaded on a device and used to deliver additional payloads. These payloads could include previously observed malware installs, such as Gozi, Redline stealer, IcedID, Smoke Loader, NetSupport Manager (also referred to as NetSupport RAT), Sectop RAT, and Lumma stealer.

Storm-1113 is a threat actor that acts both as an access broker focused on malware distribution through search advertisements and as an "as-a-service" entity providing malicious installers and landing page frameworks. In Storm-1113 malware distribution campaigns, users are directed to landing pages mimicking well-known software that host installers, often MSI files, that lead to the installation of malicious payloads. Storm-1113 is also the developer of EugenLoader, a commodity malware first observed around November 2022.

Sangria Tempest

In mid-November 2023, Microsoft observed Sangria Tempest using Storm-1113's EugenLoader delivered through malicious MSIX package installations. Sangria Tempest then drops Carbanak, a backdoor used by the actor since 2014, that in turn delivers the Gracewire malware implant. In other cases, Sangria Tempest uses Google ads to lure users into downloading malicious MSIX application packages—possibly relying on Storm-1113 infrastructure—leading to the delivery of POWERTRASH, a highly obfuscated PowerShell script. POWERTRASH is then used to load NetSupport and Gracewire, a malware typically affiliated with the threat actor Lace Tempest, whom Sangria Tempest has cooperated with in past intrusions.

Sangria Tempest (previously ELBRUS, also tracked as Carbon Spider, FIN7) is a financially motivated cybercriminal group currently focusing on conducting intrusions that often lead to data theft, followed by targeted extortion or ransomware deployment such as Clop ransomware.

Storm-1674

Since the beginning of December 2023, Microsoft identified instances where Storm-1674 delivered fake landing pages through messages delivered using Teams. The landing pages spoof Microsoft services like OneDrive and SharePoint, as well as other companies. Tenants created by the threat actor are used to create meetings and send chat messages to potential victims using the meeting's chat functionality.

Screenshot of landing page pretending to be a SharePoint site

Figure 3. Landing page pretending to be a SharePoint site for a spoofed employment opportunity site; target users are led to this landing page via malicious URLs sent via Teams messages.

Screenshot of fake error message

Figure 4. Fake error the user receives when clicking on any of the PDFs in the SharePoint. Clicking OK invokes ms-appinstaller.

Screenshot of sample malicious App Installer experience

Figure 5. Sample malicious App Installer experience. Note the Publisher is not who a user should expect to be publishing Adobe software.

Screenshot of malicious landing page pretending to be a networking security tool

Figure 6. Malicious landing page pretending to be a networking security tool; target users are led to this landing page via malicious URLs sent via Teams messages.

Screenshot of JavaScript code

Figure 7. Sample JavaScript invokes ms-appinstaller handler from malicious landing page at time of user click.

Screenshot of sample malicious App Installer experience

Figure 8. Sample malicious App Installer experience. Note the Publisher is not who a user should expect to be publishing this software.

The user is then lured into downloading spoofed applications like the ones shown in figures 5 and 8, which will likely drop SectopRAT or DarkGate. In these cases, Storm-1674 was using malicious installers and landing page frameworks provided by Storm-1113.

Microsoft assesses this technique was used to avoid the accept/block screen shown in one-on-one and group chats. The Teams client now shows an accept/block screen for meeting chats sent by an external user.

Microsoft has taken action to mitigate the spread of malware from confirmed malicious tenants by blocking their ability to send messages thus cutting off the main method used for phishing.

Storm-1674 is an access broker known for using tools based on the publicly available TeamsPhisher tool to distribute DarkGate malware. Storm-1674 campaigns have typically relied on phishing lures sent over Teams with malicious attachments, such as ZIP files containing a LNK file that ultimately drops DarkGate and Pikabot. In September 2023, Microsoft observed handoffs from Storm-1674 to ransomware operators that have led to Black Basta ransomware deployment.

Recommendations

The ms-appinstaller URI scheme handler has been disabled by default in App Installer build 1.21.3421.0. Refer to the Microsoft Security Response Blog for App Installer protection tips.

Microsoft recommends the following mitigations to reduce the impact of this threat. Check the recommendations card for the deployment status of monitored mitigations.

- Pilot and deploy phishing-resistant authentication methods for users.
- Implement Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Educate Microsoft Teams users to verify 'External' tagging on communication attempts from external entities, be cautious about what they share, and never share their account information or authorize sign-in requests over chat.
- Apply Microsoft's security best practices for Microsoft Teams to safeguard Teams users.
- Educate users to review sign-in activity and mark suspicious sign-in attempts as "This wasn't me".
- Encourage users to use Microsoft Edge and other web browsers that support Microsoft Defender SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
- Educate users to use the browser URL navigator to validate that upon clicking a link in search results they have arrived at an expected legitimate domain.
- Educate users to verify that the software that is being installed is expected to be published by a legitimate publisher.
- Configure Microsoft Defender for Office 365 to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages, other Microsoft Office applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to

the regular anti-spam and anti-malware protection in inbound email messages in Microsoft Exchange Online Protection (EOP). Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.

- Turn on PUA protection in block mode.
- Turn on attack surface reduction rules to prevent common attack techniques:
  - Use advanced protection against ransomwareBlock executable files from running unless they meet a prevalence, age, or trusted list criterion

Appendix

Microsoft Defender XDR detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the malware listed below. Enterprise customers managing updates should select the detection build 1.403.520.0 or newer and deploy it across their environments.

- TrojanDownloader:Win32/CryptedLoader
- Backdoor:PowerShell/CryptedLoader.PS

Microsoft Defender Antivirus detects associated post-compromise activity as the following:

- Trojan:Python/BatLoader
- Trojan:PowerShell/BatLoader
- Trojan:Win32/Batloader
- TrojanDownloader:PowerShell/EugenLoader
- Trojan:Win32/EugenLoader
- TrojanDownloader:PowerShell/Malgent
- Trojan:Win64/Lumma
- Trojan:Win32/Gozi
- Trojan:Win64/IcedID
- Trojan:Win32/Smokeloader
- Backdoor:MSIL/SectopRAT
- Behavior:Win32/CobaltStrike
- Backdoor:Win64/CobaltStrike
- HackTool:Win64/CobaltStrike
- Ransom:Win32/BlackBasta
- Ransom:Linux/BlackBasta

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- An executable loaded an unexpected dll
- A process was injected with potentially malicious code
- Suspicious sequence of exploration activities
- Activity that might lead to information stealer
- Possible theft of passwords and other sensitive web browser information

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- A file or network connection related to ransomware-linked actor Storm-0569 detected
- Storm-1113 threat actor detected
- Ransomware-linked Sangria Tempest threat activity group detected
- Potential BATLOADER activity
- Potential IcedID activity
- Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)

- Human-operated attack using Cobalt Strike
- Possible POWERTRASH loader activity
- Carbanak backdoor detected

Microsoft Defender for Office 365

Microsoft Defender for Office 365 detects malicious activity associated with this threat.

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, and respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Actor profile: Sangria Tempest
- Actor profile: Storm-0506
- Tool profile: BATLOADER
- Tool profile: Cobalt Strike
- Tool profile: DarkGate
- Tool profile: Black Basta ransomware
- Tool profile: Lumma stealer
- Tool profile: Pikabot

Microsoft 365 Defender Threat analytics

- Activity profile: Qakbot distributor Storm-0464 shifts to DarkGate and IcedID
- Storm-0569: Malvertising and phishing deliver fake software installers and lead to ransomware
- Actor profile: Sangria Tempest
- IcedID's frosty arrival can lead to data theft

Hunting queries

Microsoft Defender XDR

Use this query to review all the ms-appinstaller protocol handler invoked network connections in your environment.

```
DeviceNetworkEvents
| where InitiatingProcessCommandLine == '"AppInstaller.exe" -ServerName:App.AppX9rwyqtrq9gw3wnmrap
```

Indicators of compromise

Storm-0569 indicators related to App Installer abuse

SHA-256

- 48aa2393ef590bab4ff2fd1e7d95af36e5b6911348d7674347626c9aaafa255e
- 11b71429869f29122236a44a292fde3f0269cde8eb76a52c89139f79f4b97e63
- 7e646dfe7b7f330cb21db07b94f611eb39f604fab36e347fb884f797ba462402
- ffb45dc14ea908b21e01e87ec18725dff560c093884005c2b71277e2de354866
- b79633917e51da2a4401473d08719f493d61fd64a1b10fe482c12d984d791ccb

URLs

- hxxps://scheta[.]site/api.store/ZoomInstaller.msix
- hxxps://scheta[.]site/api.store/Setup.msix

Domain names

- teannviewer.ithr[.]org
- tab1eu.ithr[.]org
- amydeks.ithr[.]org
- zoonn.ithr[.]org
- scheta[.]site
- tnetworkslicense[.]ru
- 1204knos[.]ru
- 1204networks[.]ru
- abobe.ithr[.]org

Storm-0506 Cobalt Strike beacon C2:

- gertefin[.]com
- septcntr[.]com

Storm-1113 indicators related to App Installer abuse

SHA-256

- 44cac5bf0bab56b0840bd1c7b95f9c7f5078ff417705eeaaf5ea5a2167a81dd5

Domain names

- info-zoomapp[.]com
- zoonn[.]meetlng[.]group

Sangria Tempest indicators related to App Installer abuse

Domain names

- storageplace[.]pro
- sun1[.]space

SHA-256

- 2ba527fb8e31cb209df8d1890a63cda9cd4433aa0b841ed8b86fa801aff4ccbd
- 06b4aebbc3cd62e0aadd1852102645f9a00cc7eea492c0939675efba7566a6de

Storm-1674 indicators related to App Installer abuse

SHA-256

- 2ed5660c7b768b4c2a7899d00773af60cd4396f24a2f7d643ccc1bf74a403970

Domain names:

- nixonpeabody[.]tech-department[.]us
- amgreetings[.]tech-department[.]us
- cbre[.]tech-department[.]us
- tech-department[.]us
- kellyservices-hr[.]com
- hubergroup[.]tech-department[.]us
- formeld[.]tech-department[.]us
- kellyhrservices-my[.]sharepoint[.]com
- kellyserviceshr-my[.]sharepoint[.]com
- kellyservicesrecruitmentdep-my[.]sharepoint[.]com
- kellyservicesheadhunter-my[.]sharepoint[.]com
- mckinseyhrcompany-my[.]sharepoint[.]com
- webmicrosoftservicesystem[.]com
- perimeter81support-my[.]sharepoint[.]com

- cabotcorpsupport-my[.]sharepoint[.]com

References

- Malvertising Surges to Distribute Malware (Intel471)
- Microsoft Security Response Blog
- CVE-2021-43890

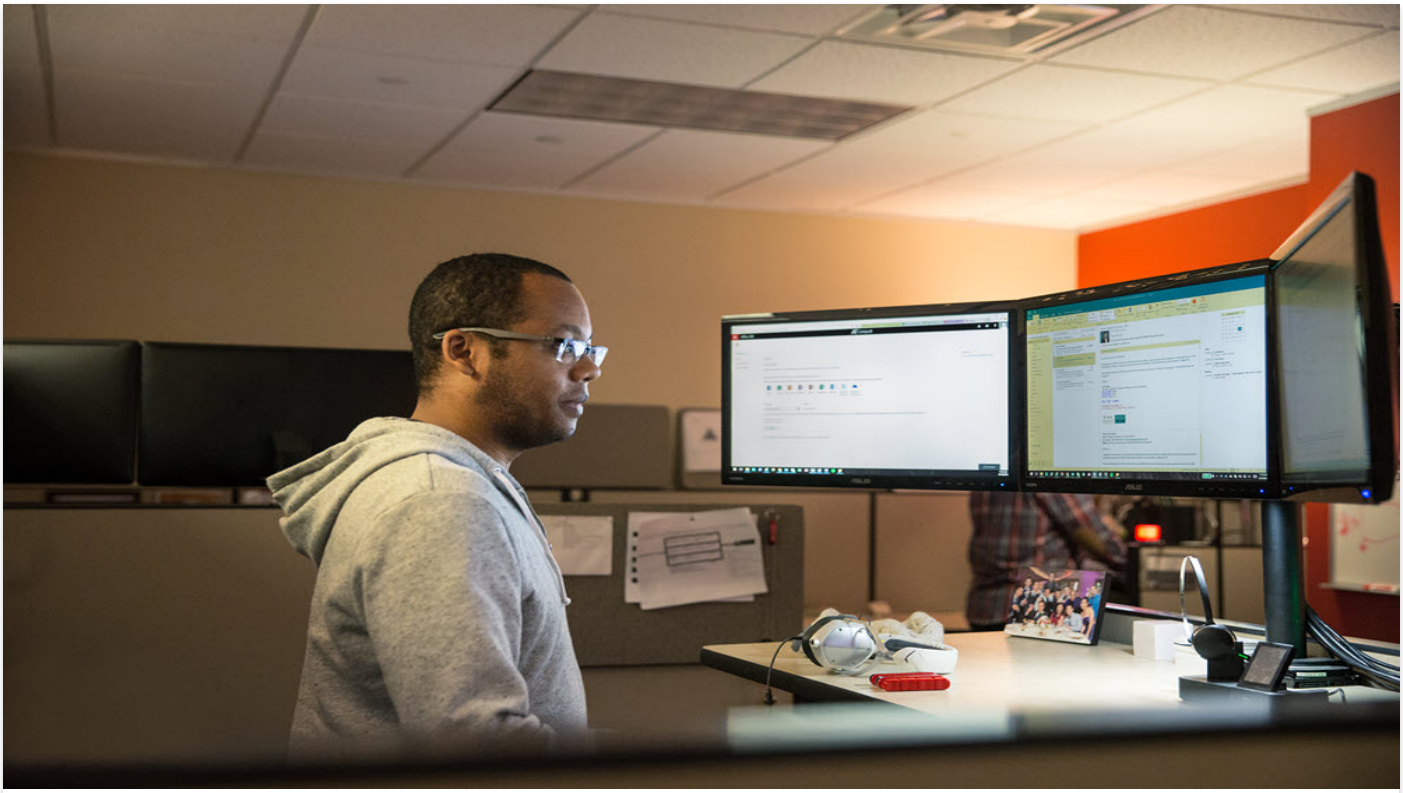
Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

Related Posts

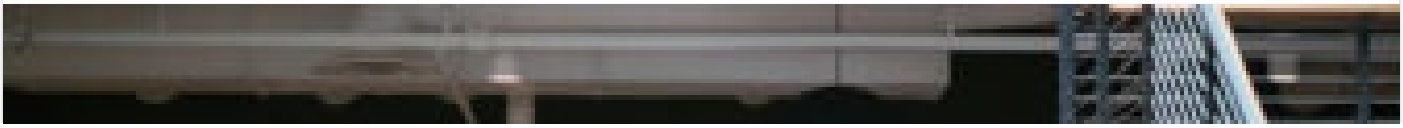


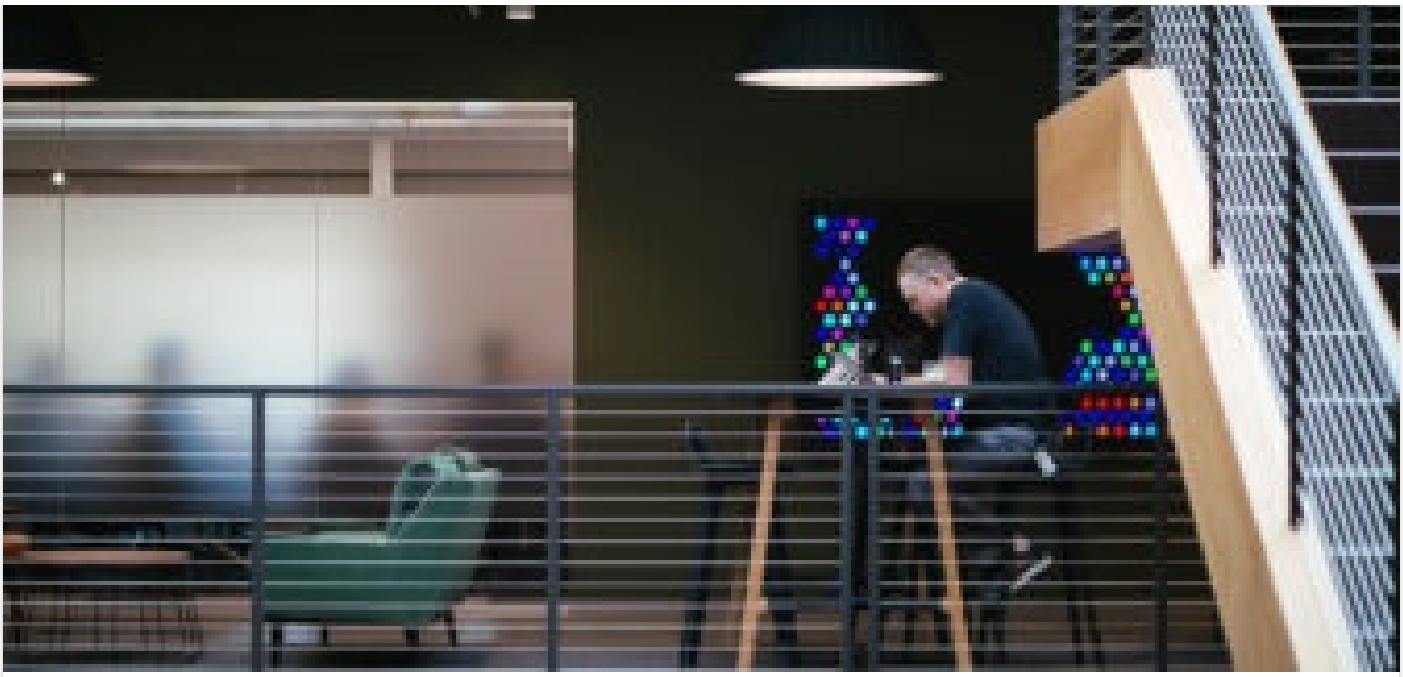
News
Threat intelligence

Nov 17
7 min read

DEV-0569 finds new ways to deliver Royal ransomware, various payloads

DEV-0569's recent activity shows their reliance on malvertising and phishing in delivering malicious payloads. The group's changes and updates in delivery and payload led to distribution of info stealers and Royal ransomware.





Research
Endpoint security
Microsoft Defender XDR
Threat actors

Sep 12
8 min read

Malware distributor Storm-0324 facilitates ransomware access

The threat actor that Microsoft tracks as Storm-0324 is a financially motivated group known to gain initial access using email-based initial infection vectors and then hand off access to compromised networks to other threat actors. These handoffs frequently lead to ransomware deployment. Beginning in July 2023, Storm-0324 was observed distributing payloads using an open-source tool [...]

Research

Threat intelligence
Microsoft Incident Response
Threat actors

Oct 25
17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for many organizations across multiple industries.

Research
Threat intelligence
Microsoft Defender
Threat actors

Jul 11
7 min read

Storm-0978 attacks reveal financial and espionage motives

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, which included a zero-day remote code execution vulnerability exploited via Microsoft Word documents.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy