Black Basta and Cactus Ransomware Groups Add BackConnect Malware to Their Arsenal

By Catherine Loveria, Stephen Carbery, Jovit Samaniego, Adam O'Connor, Ian Kenefick, Gabriel Cardoso, Lucas Silva, Jack Walsh (words)

Published: 2025-03-03 · Archived: 2026-04-05 22:43:59 UTC

Ransomware

In this blog entry, we discuss how the Black Basta and Cactus ransomware groups utilized the BackConnect malware to maintain persistent control and exfiltrate sensitive data from compromised machines.

By: Catherine Loveria, Stephen Carbery, Jovit Samaniego, Adam O'Connor, Ian Kenefick, Gabriel Cardoso, Lucas Silva, Jack Walsh Mar 03, 2025 Read time: 10 min (2650 words)

Summary

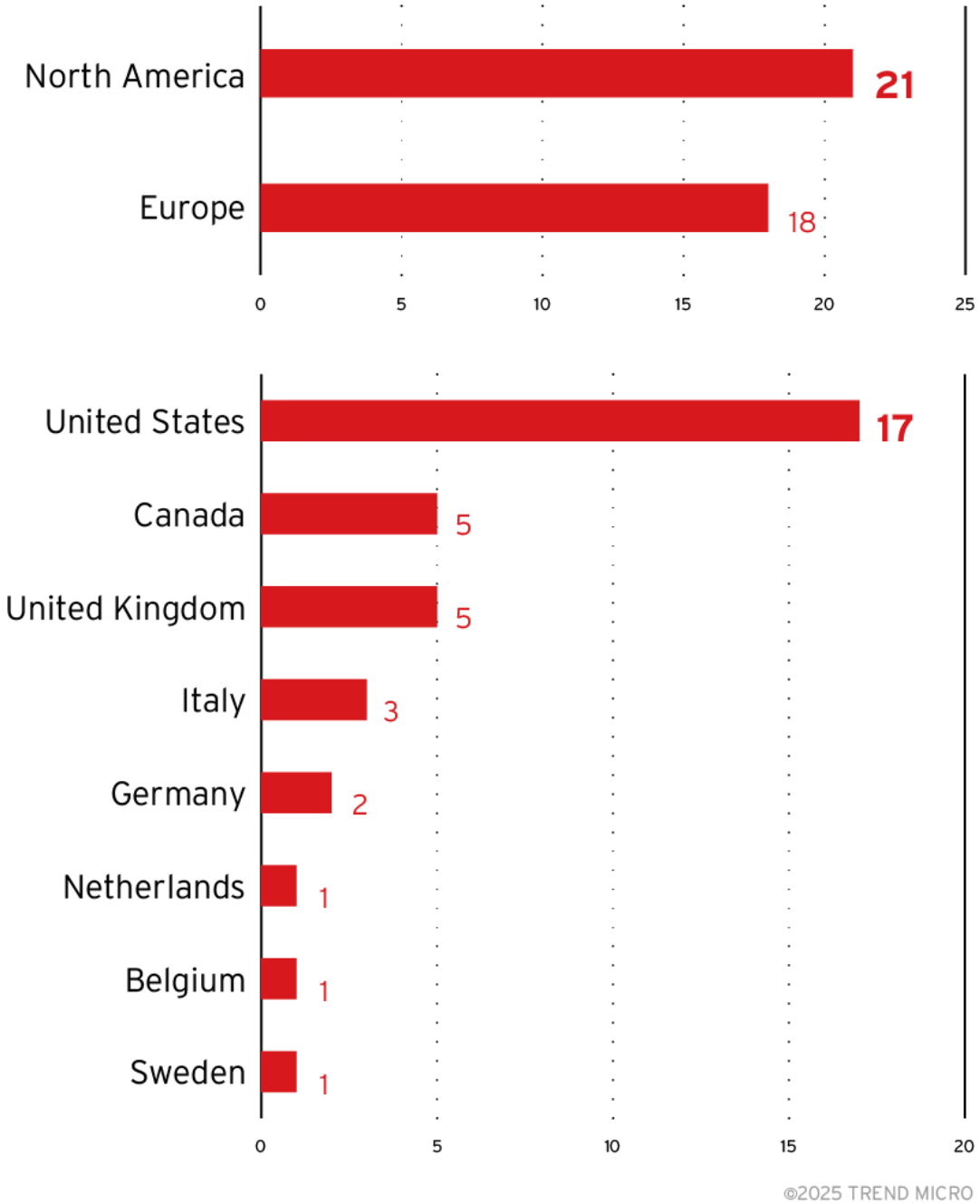
- Attackers utilized social engineering to lure the victims into giving them initial access. Attackers abused Microsoft Teams for impersonation and privilege escalation. Attackers abused Quick Assist and similar remote access software to manipulate users into granting unauthorized access.
- OneDriveStandaloneUpdater.exe, which is responsible for updating OneDrive, was abused to side-load malicious DLLs, which provided the attackers access to internal networks.The attacker utilized the BACKCONNECT malware to control the compromised machine persistently.
- As reported by researchersopen on a new tab, this new BackConnect malware (which Trend Micro detects as QBACKCONNECT) has artefacts which suggest links to QakBot, a loader malware which was the subject of a takedown effort dubbed ‘Operation Duckhunt’ in 2023. QakBot infections were the predominant initial access method utilised by Black Basta threat actors before the takedown forced the threat actors to find alternative methods.
- WinSCP usage was utilized soon after.
- Attackers hosted and distributed malicious files using a commercial cloud storage service, taking advantage of its ease of use, widespread adoption, and misconfigured or publicly accessible storage buckets.
- Trend Micro Threat Intelligence data indicates that since October 2024, most incidents occurred in North America (21 breaches), followed by Europe (18). The US was the hardest hit, with 17 affected organizations, while Canada and the UK each experienced five breaches.

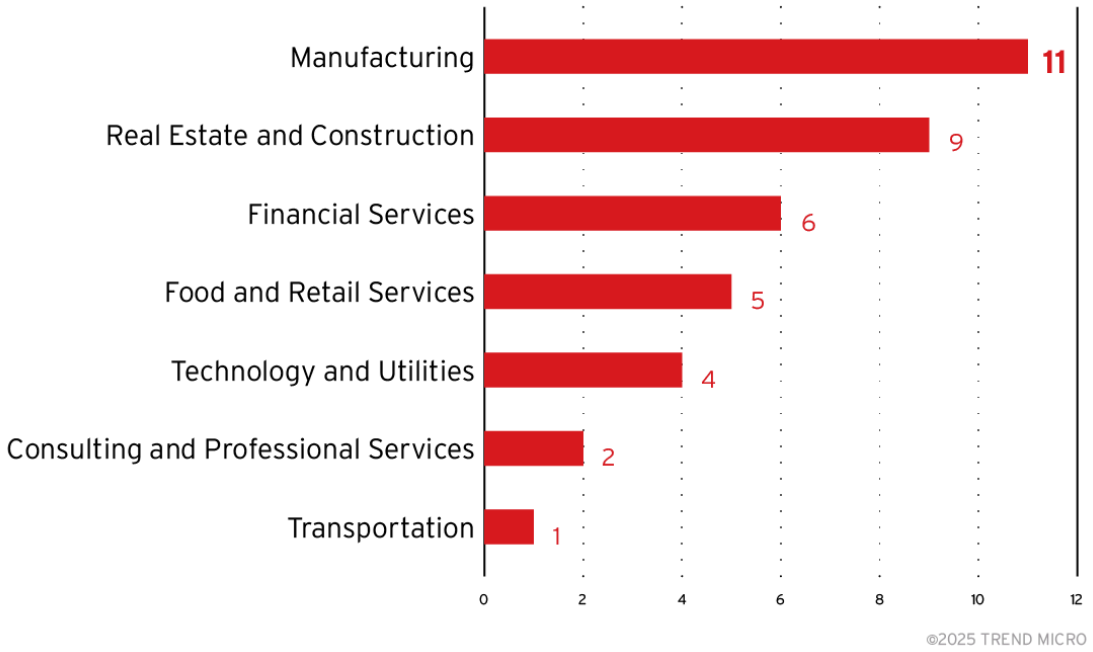
The Trend Micro™ Managed XDRopen on a new tab and Incident Response (IR) teams recently analyzed incidents where threat actors deploying Black Basta and Cactus ransomware used the same BackConnect malware to strengthen their foothold on compromised machines.

The BackConnectopen on a new tab malware is a tool that cybercriminals use to establish and maintain persistent control over compromised systems. Once infiltrated, it grants attackers a wide range of remote control capabilities, allowing them to execute commands on the infected machine. This enables them to steal sensitive data, such as login credentials, financial information, and personal files.

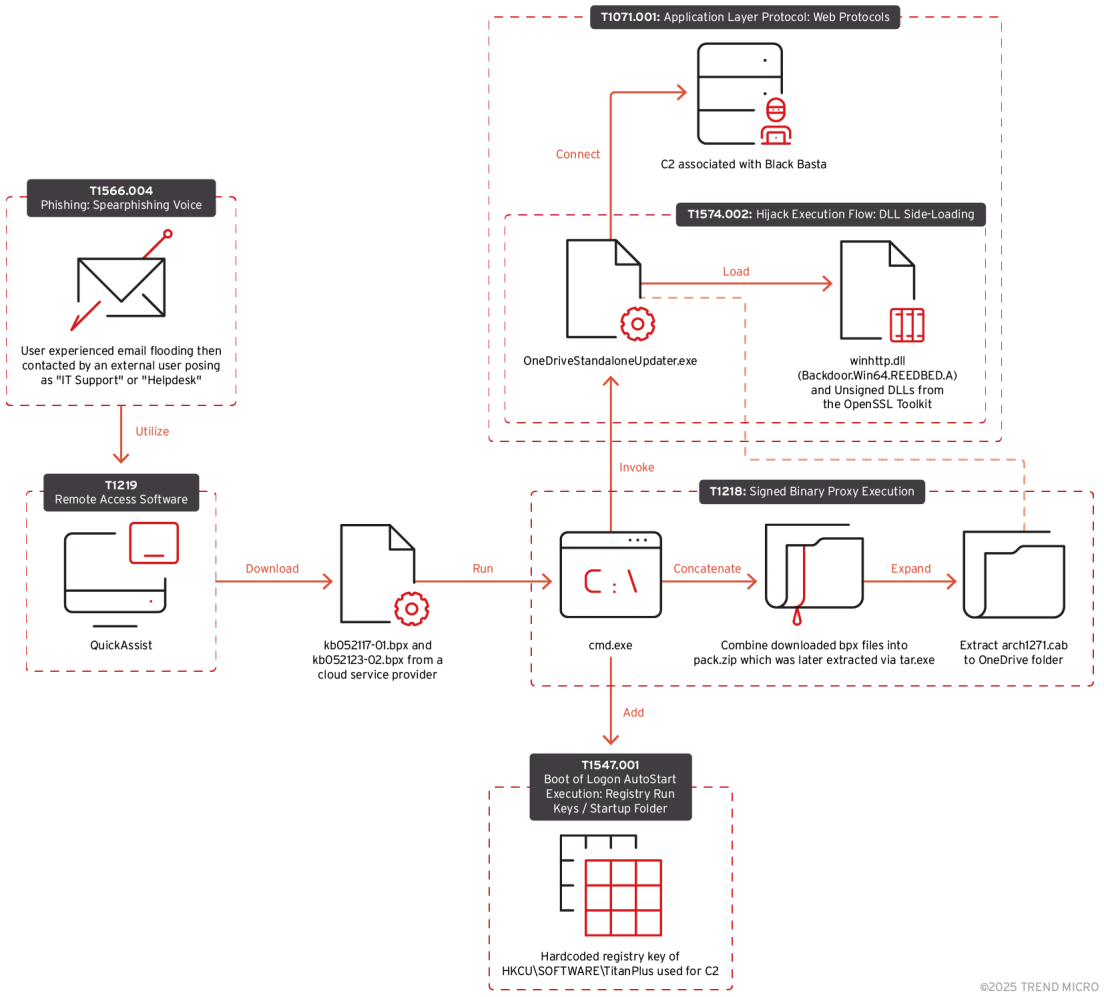
In 2023, the group behind Black Bastaopen on a new tab reportedly extorted US$107 millionopen on a new tab in Bitcoins from their victims. Based on data from Trend Micro Threat Intelligenceopen on a new tab on the attacks carried out by the Black Basta ransomware group since October 2024, the majority of incidents occurred in North America, accounting for 21 breaches, followed by Europe with 18. The US was the hardest hit, with 17 affected organizations, while Canada and the UK each had five breaches. In terms of Black Basta's impact across industries, manufacturing had the highest number of attacks with 11 victims, followed by real estate and construction with nine victims, then financial services with six victims.

The attack chains' methods might not be technically groundbreaking, but how they layer social engineering with the abuse of legitimate tools and cloud-based infrastructure enables them to blend malicious activity into normal enterprise workflows.





Black Basta ransomware attack chain



Initial access

Our Managed XDR team analyzed a case involving a technique similar to the one used by the DarkGate malwareopen on a new tab where the user experienced email flooding before being contacted by external actor posing as IT support or helpdesk. In this sample case, the external email address is ***admin_52351@brautomacao565[.]onmicrosoft[.]com***.

Logged	LogType	principalName	actionName	service
2025-01-16 18:06:11	messaging	admin_52351@brautomacao565.onmicrosoft.com	MessageSent	MicrosoftTeams
2025-01-16 18:03:33	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:42:34	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:41:09	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:41:07	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams

eventSubId	101 - TELEMETRY_FILE_CREATE
objectFilePath	C:\Windows\Prefetch\QUICKASSIST.EXE-B2423231.pf

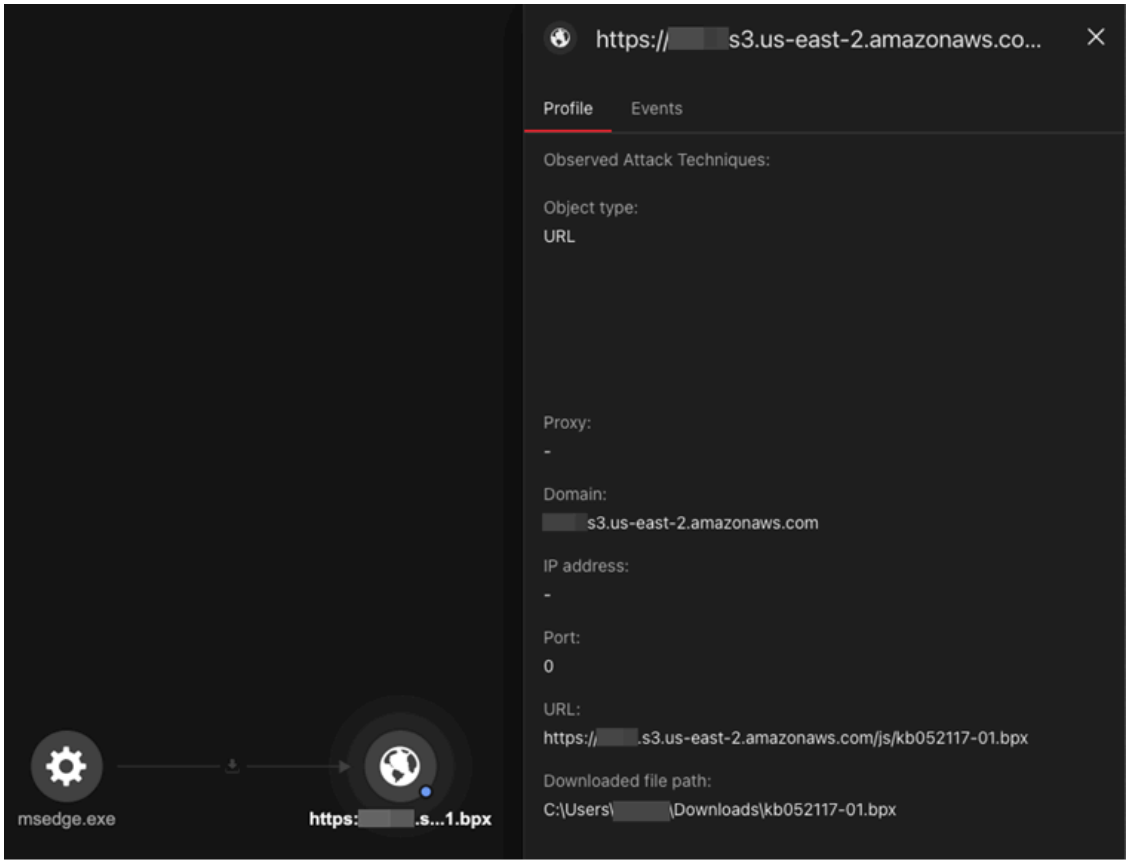
During the call, the user was persuaded by the attacker to grant him access through the built-in Quick Assist tool. It allows users to share their Windows device remotely, enabling screen viewing, annotations, and full control for troubleshooting. Microsoft has previously published their own analysisopen on a new tab of how threat actors exploit this by impersonating IT support to gain unauthorized access. This tactic, observed since late last year, has been attributed to Black Basta ransomwareopen on a new tab.

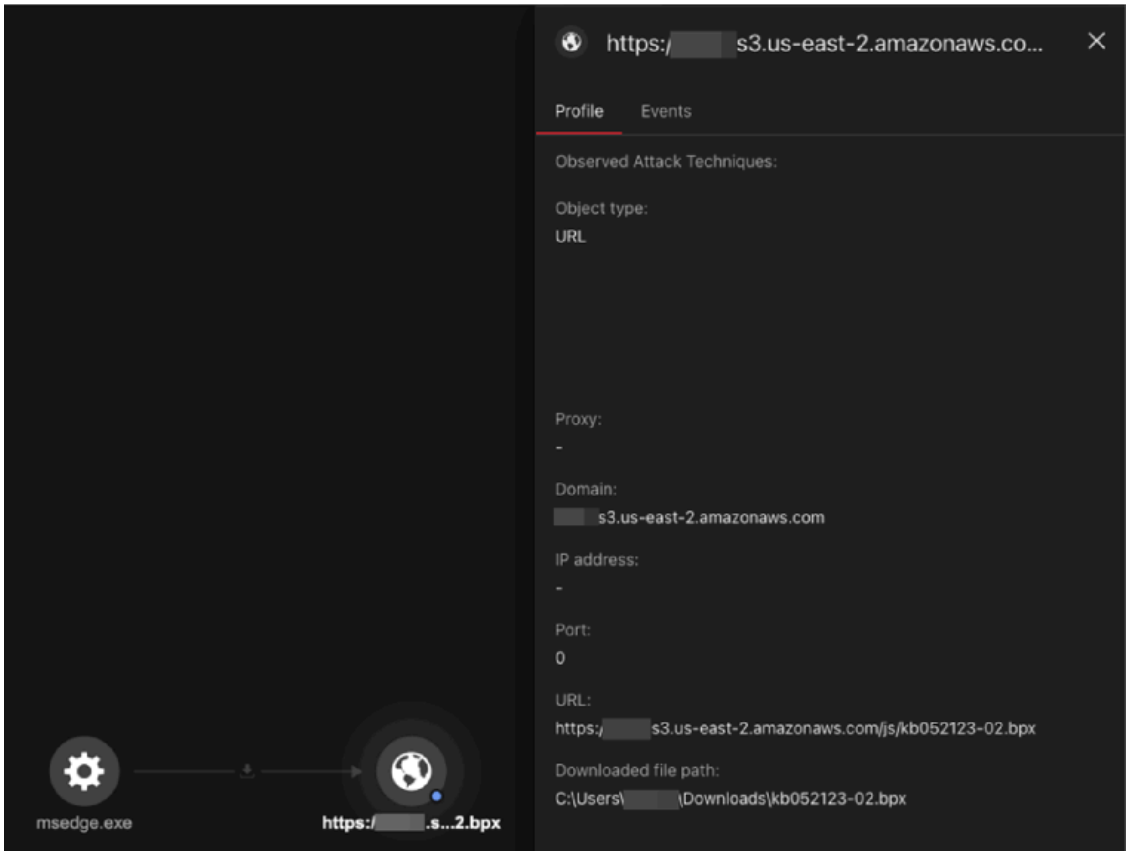
Execution

After gaining initial access, the attacker downloaded two different malicious .bpx files from a commercial cloud storage provider. Reportsopen on a new tab have observed how threat actors frequently abuse commercial cloud storage services for malware distribution due to their ease of use, widespread adoption, and the risk of misconfigured or publicly accessible buckets.

The following are the downloaded files from the first case:

- C:\Users\<user>\Downloads\kb052117-01.bpx
- C:\Users\<user>\Downloads\kb052123-02.bpx





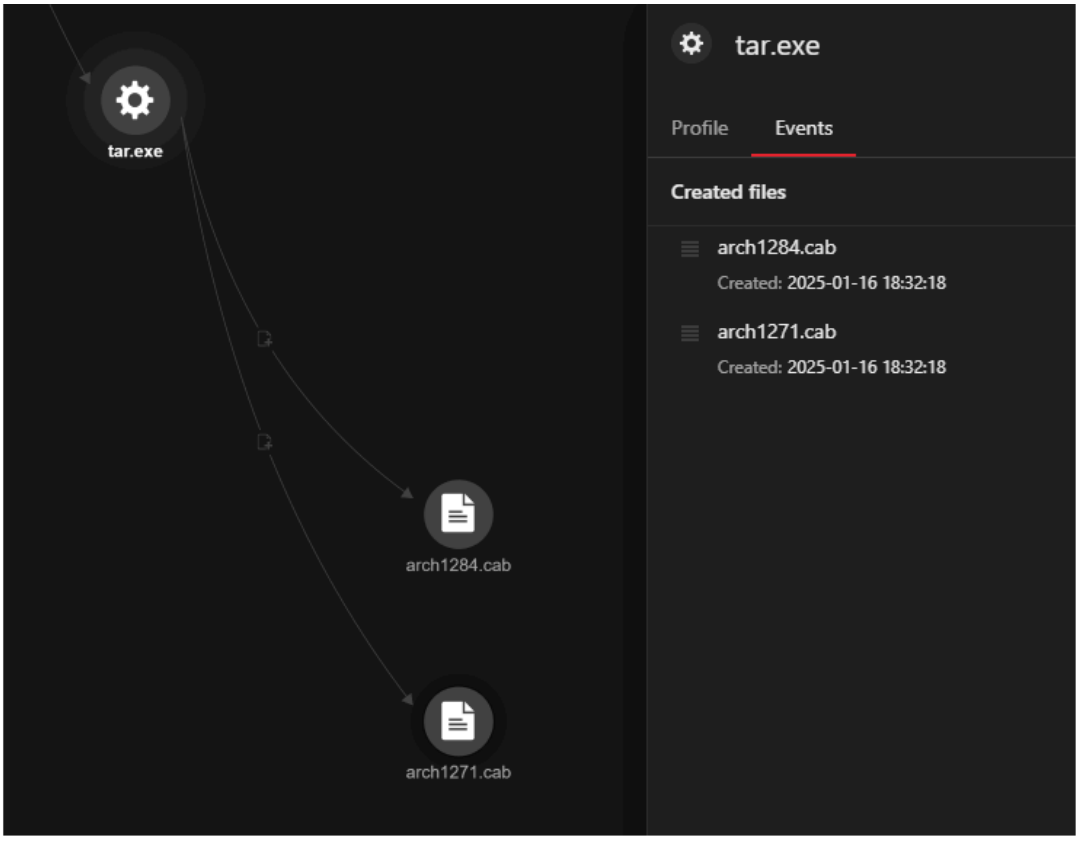
Based on our threat intelligence, the attacker concatenates the two .bpx files into “pack.zip”. In this case, the attacker used the command ***type kb052117-01.bpx kb052123-02.bpx > pack.zip*** that will concatenate the two .bpx files into a pack.zip, the content of which will be unpacked using Tar. The name of the bpx files varies from case to case.

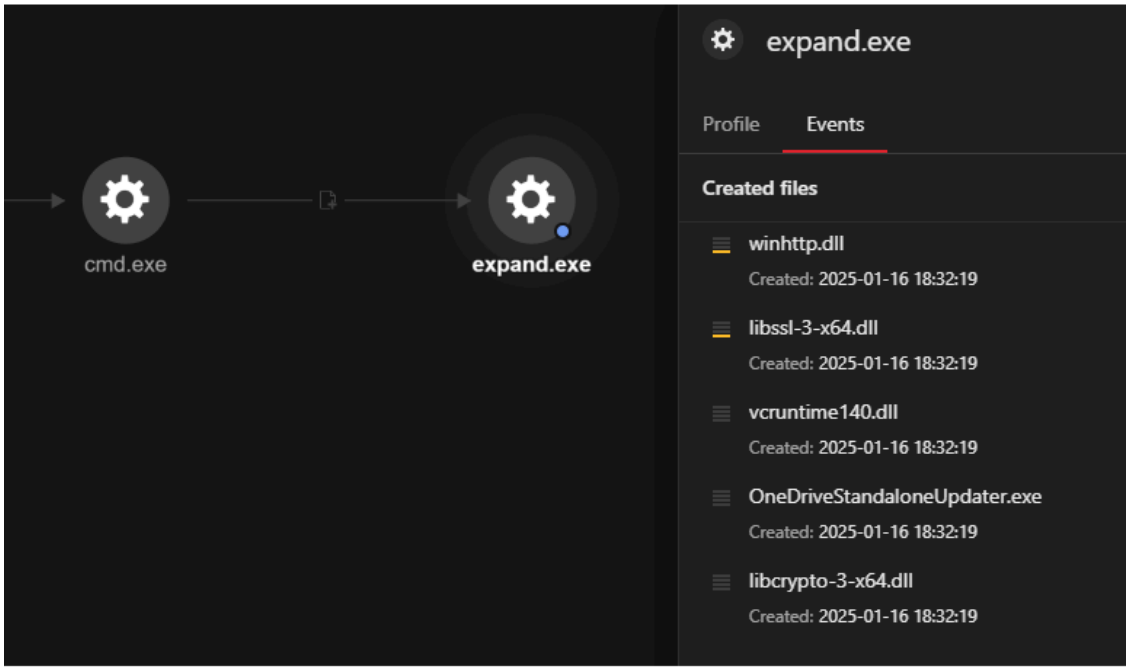
processCmd	"C:\Windows\System32\cmd.exe"
eventSubId	101 - TELEMETRY_FILE_CREATE
objectFilePath	C:\Users\[redacted]\Downloads\pack.zip

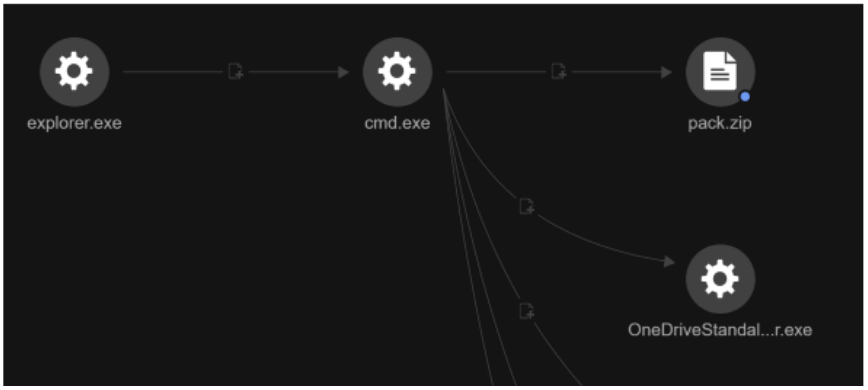
objectFilePath	C:\Windows\System32\tar.exe
objectCmd	tar xf pack.zip -C "C:\Users\[redacted]\AppData\Local\Temp"

The following files were created after the extraction of pack.zip:

- C:\Users\<user>\AppData\Local\Temp\arch1284.cab
- C:\Users\<user>\AppData\Local\Temp\arch1271.cab


tar.exe
arch1284.cab
arch1271.cab
tar.exe
Profile
Events
Created files
arch1284.cab
Created: 2025-01-16 18:32:18
arch1271.cab
Created: 2025-01-16 18:32:18


cmd.exe
expand.exe
expand.exe
Profile
Events
Created files
winhttp.dll
Created: 2025-01-16 18:32:19
libssl-3-x64.dll
Created: 2025-01-16 18:32:19
vcruntime140.dll
Created: 2025-01-16 18:32:19
OneDriveStandaloneUpdater.exe
Created: 2025-01-16 18:32:19
libcrypto-3-x64.dll
Created: 2025-01-16 18:32:19


explorer.exe
cmd.exe
pack.zip
OneDriveStandal...r.exe

The file ***arch1271.cab*** was extracted to place those extracted files into the OneDrive folder:

Command: expand "C:\Users\<user>\AppData\Local\Temp\arch1271.cab" -F: "C:\Users\<user>\AppData\Local\Microsoft\OneDrive"*

The following files were created/dropped after the extraction:

- C:\Users\<user>\AppData\Local\Microsoft\OneDrive\winhttp.dll
- C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libssl-3-x64.dll
- C:\Users\<user>\AppData\Local\Microsoft\OneDrive\vcruntime140.dll
- C:\Users\<user>\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
- C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libcrypto-3-x64.dll

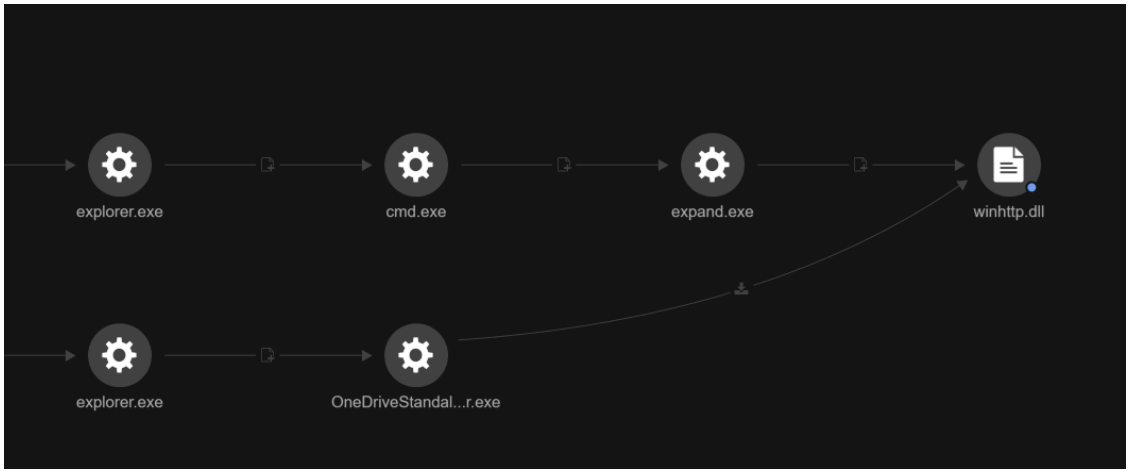
The OneDriveStandaloneUpdater.exe process was later launched noninteractively via cmd.exe with the following command-line instruction:

- CLI command: "C:\Users\<user>\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe" -Embedding.

Researchopen on a new tab says that winhttp.dll is a malicious loader that is sideloaded by the Onedrive executable. This loader decrypts the backdoor from a dat file named settingsbackup.dat which is also contained in pack.zip

Contents of pack.zip:

- libcrypto-3-x64.dll (e45b73a5f9cdf335a17aa97a25644489794af8e1)
- libssl-3-x64.dll (9c8dea7602a99aa15f89a46c2b5d070e3ead97f9)
- Settingsbackup.dat (11ec09ceabc9d6bb19e2b852b4240dc7e0d8422e)
- Vcruntime140.dll (00149b7a66723e3f0310f139489fe172f818ca8e)
- Winhttp.dll (232fdfde3c0e180ad91ebeb863bfd8d58915dd39)

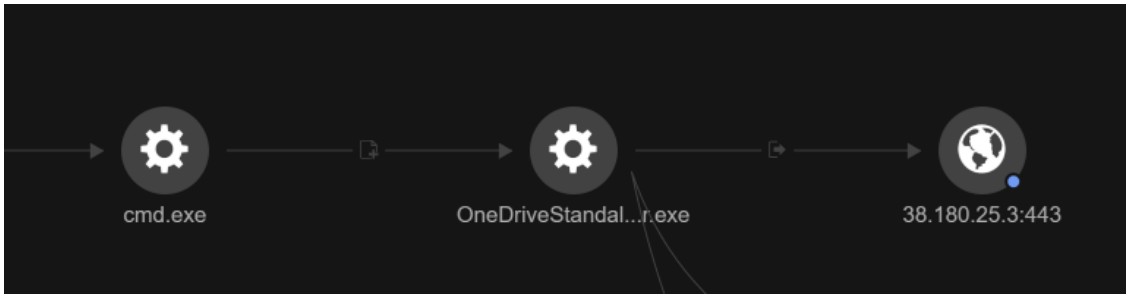


After the update process, several key configuration files were modified by the **OneDrive Standalone Updater**:

- **C:\Users\<user>\AppData\Local\Temp\.ses**
- **C:\Users\<user>\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\PreSignInSettingsConfig.json**
- **C:\Users\<user>\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\Update.xml**

Command and control (C&C) and post-installation activities

We observed OneDrive Standalone Updater connecting to the external IP ***38.180.25[.]3***, which is flagged as Dangerous and categorized as C&C server.



The attacker also added the following registry entry to store their BackConnect IPs:

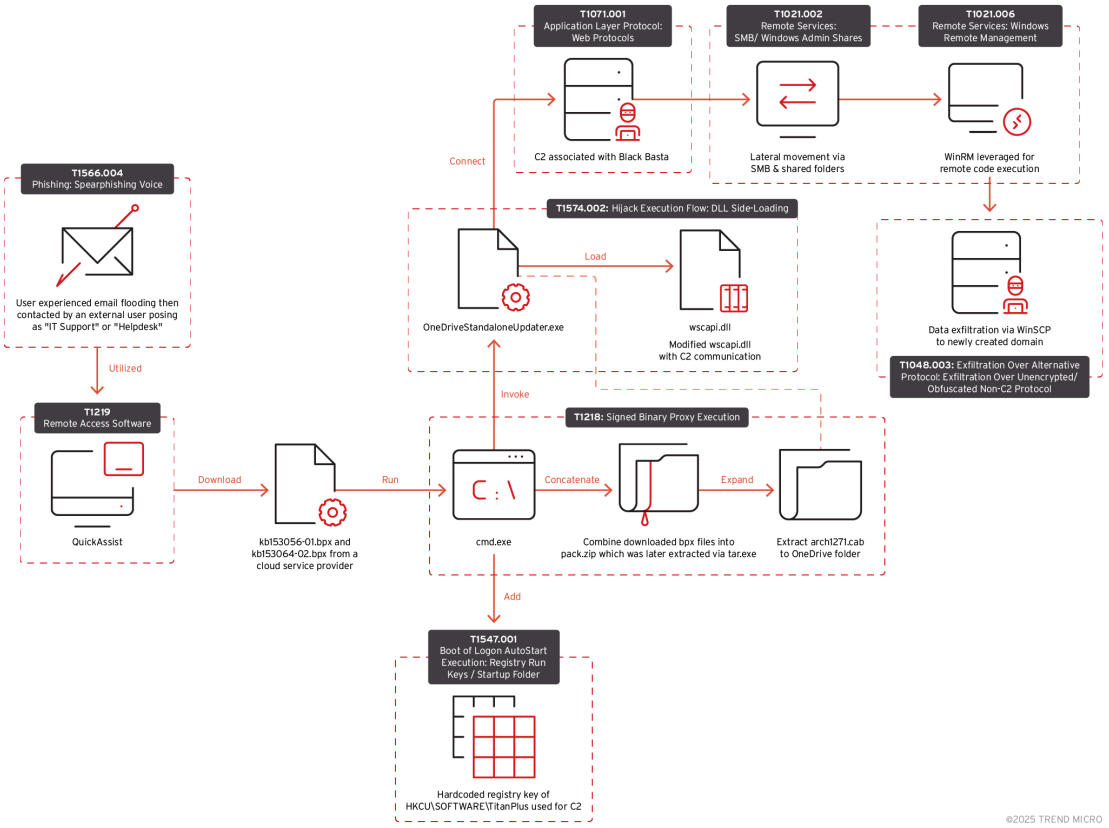
reg add "HKCU\SOFTWARE\TitanPlus" /v 1 /t REG_SZ /d "38.180.25.3A443;45.8.157.199A443;5.181.3.164A443" /f

Based on Trend Micro Threat Intelligenceopen on a new tab, the IPs used in the above registry key are associated with Black Basta, with the IPs classified as C&C servers.

Cactus ransomware attack chain

The Trend Micro IR team encountered an evolution of the attack chain we detailed earlier. While the initial tactics closely mirrored the campaign, we observed several additional techniques that provide further insight into the adversary's evolving methods.

Attack chain and initial intrusion



The campaign used familiar methods:

- **Email bombing and social engineering:** An email flood was launched, followed by contact via Microsoft Teams from the address admin_734@gamicalstudio[.]onmicrosoft[.]com. Using the previously observed social engineering techniques, the victim was persuaded to grant remote access via Quick Assist.
- **Malicious file downloads and archive manipulation:** Two .bpx files were downloaded, then concatenated into a single archive (pack.zip), which, upon extraction, produced files similar to those seen in the earlier attack.:
  - C:\Users\<user>\Downloads\kb153056-01.bpx
  - C:\Users\<user>\Downloads\kb153064-02.bpx
- The same files were created upon extracting the '.cab' archives:
  - C:\Users\<user>\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
  - C:\Users\<user>\AppData\Local\Microsoft\OneDrive\wscapi.dll
  - C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libssl-3-x64.dll
  - C:\Users\<user>\AppData\Local\Microsoft\OneDrive\vcruntime140.dll
  - C:\Users\<user>\AppData\Local\Microsoft\OneDrive\libcrypto-3-x64.dll
- "HKCU\SOFTWARE\TitanPlus" was also added as registry to store BACKCONNECTC2 IP addresses:
  - add "HKLM\SOFTWARE\TitanPlus" /v 1 /t REG_SZ /d "45B8B157B199A443;5B181B3B164A443;38B180B25B3A443"
    - 45.8.157[.]199;443;5.181.3[.]164;443;38.180.25[.]3;443
- The same C&C infrastructure was observed in case with Black Basta, being utilized with BackConnect:
  - 45[.]8[.]157[.]199
    - 5[.]181[.]3[.]164
    - 38[.]180[.]25[.]3
    - 185[.]190[.]251[.]16
    - 207[.]90[.]238[.]52

- 89[.]185[.]80[.]86

Lateral movement and ransom

Building on the initial foothold, the adversary used advanced lateral movement techniques to expand their presence:

Server Message Block (SMB) and Windows Remote Management (WinRM): The attacker utilized SMB via shared folders and used WinRM to remotely execute commands and scripts, allowing them to traverse the network.

processCmd	src	dpt	dst
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.13[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.13[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.13[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]
"C:\Users\[redacted]\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.ex...	10.226[redacted]	135	10.1.[redacted]

parentCmd	processFilePath	objectCmd
C:\Windows\system32\svchost.exe -k DcomLaunch -p	C:\Windows\System32\winrshost.exe	C:\Windows\system32\cmd.exe /C schtasks.exe /Create /RU "NT AUTHORITY\SYST...
	C:\Windows\System32\svchost.exe	C:\Windows\system32\WinrsHost.exe -Embedding
C:\Windows\system32\WinrsHost.exe -Embedding	C:\Windows\System32\cmd.exe	reg add "HKLM\SOFTWARE\TitanPlus" /v 1 /t REG_SZ /d "45B8B157B199A443;5B1...
C:\Windows\system32\svchost.exe -k DcomLaunch	C:\Windows\System32\winrshost.exe	C:\Windows\system32\cmd.exe /C reg add "HKLM\SOFTWARE\TitanPlus" /v 1 /t R...

ESXi host compromise: Notably, we identified the compromise of ESXi hosts. A binary, socks.out — believed to be the SystemBC proxy malware — was deployed. By enabling an SSH session as the root user, they:

- Disabled the ExecInstalledOnly setting (which normally restricts execution to binaries installed via official VIBs).
- Turned off the firewall, thereby permitting unauthorized binaries to run.

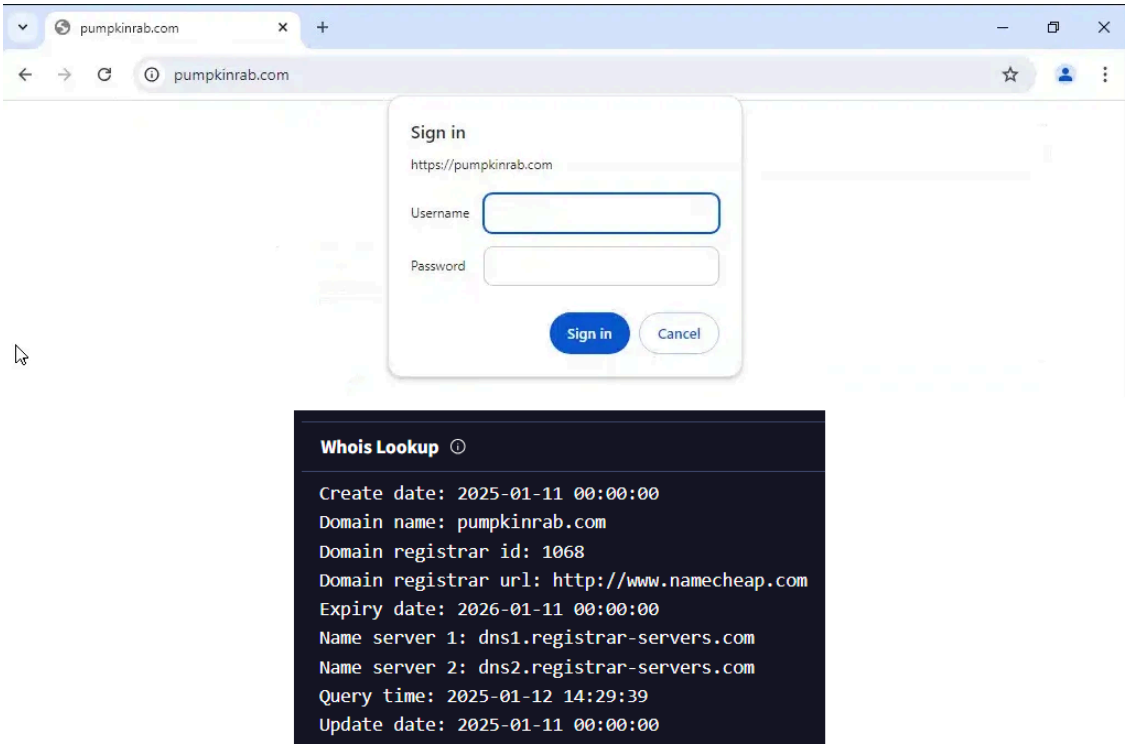
This sequence of actions culminated in the execution of the socks.out binary without interference from system protections.

- Analysis further revealed that the attackers leveraged WinSCP—an open-source file transfer client—as part of their operational process:**Leveraging WinSCP:** WinSCP was employed to facilitate file transfers within the compromised environment. Firewall logs confirmed notable network activity involving WinSCP connecting to a newly registered, suspicious domain.Pumpkinrab[.]com – 208[.]115[.]200[.]146.

The adversary deployed WinSCP across multiple compromised hosts, suggesting that the tool was distributed to streamline their operations.

eventSubId	processCmd	objectFilePath
101 - TELEMETRY_FILE_CREATE	C:\Windows\Explorer.EXE	C:\ProgramData\WinSCP-6.3.6-Portable.zip

eventSubId	processFilePath	dst	hostName
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
301 - TELEMETRY_DNS_QUERY	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe		pumpkinrab.com
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
301 - TELEMETRY_DNS_QUERY	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe		pumpkinrab.com
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	
204 - TELEMETRY_CONNECTION_CONNECT_...	C:\ProgramData\WinSCP-6.3.6-Portable\WinSCP.exe	208.115.200.146	



Our incident response efforts successfully subverted the attempt to encrypt the victim's network. However, the sequence of events clearly indicates that encryption was their intended next step. A ransom note was sent via email, with the attackers identifying themselves as the "Cactus Group."

The Black Basta chat log leaks

On February 11, 2025, a significant leak exposed the internal communications and organizational structure of the Black Basta group. According to the published information, the data was released due to an internal misunderstanding. The group has reportedly targeted Russian banks. The leaked archive contains messages exchanged in Black Basta's internal chat rooms between September 18, 2023, and September 28, 2024.

Analysis of the messages uncovers a broad spectrum of information, such as phishing templates and their target emails, cryptocurrency addresses, victims' credentials, and information about gang members. The information was firstly published by PRODAFT.open on a new tab

While reviewing the leak data we have observed messages indicating that Black Basta operators **recognize Trend Micro as a significant obstacle** and discuss ways to bypass it. Here are their key views:

1. Trend Micro is a Major Security Challenge

- One actor explicitly states that **Trend Micro is widely used** and must be bypassed:
  "TrendMicro много где стоит, надо обходить" ("Trend Micro is used in many places, we need to bypass it").
- Another user confirms that **Trend Micro XDR is particularly difficult to evade**:
  "мелкий не может обходить Trend Micro XDR" ("Melky can't bypass Trend Micro XDR").

2. Testing and Workarounds

- Some group members discuss **testing Trend Micro detection capabilities** using brute-force techniques:
  "с трендом все ок на бруте должно быть" ("With Trend, everything should be fine on brute").
- There is also mention of **Trend Micro being a persistent issue in their operations**, frustrating them when trying to bypass its protections.

Additionally, some of the key members of Black Basta have left the group to join the Cactus Ransomware operation, as observed in the TTPs overlaps between the two groups. Based on that context, Trend assesses that Cactus will remain highly active, and the experienced members of Basta will carry on their attacks under the Cactus operation. The future of Black Basta is unknown at this moment. It might implode because of the leaks, as was the case with Conti.

Securing the enterprise beyond traditional defenses

Since early October 2024, activity related to the Black Basta ransomware social engineeringopen on a new tab campaign has surged. First reported in May, the campaign has evolved with updated tacticsopen on a new tab, improved malware payloads, and the use of Microsoft Teams for lures.

The attacks start with an email bombing campaign, followed by direct contact via Teams, where the attacker impersonates an IT staff. Victims are tricked into installing remote management tools or executing a remote shell, sometimes bypassing multifactor authentication (MFA) via QR codes. Once granted access, additional malware such DarkGate, and custom payloads are deployed to enumerate the environment, extract credentials, and steal VPN configuration files.

Our intelligence indicates that threat actors are using these tactics, techniques, and procedures (TTP) — vishing, Quick Assist as a remote tool, and BACKCONNECT — to deploy Black Basta ransomware.

Since January 2025, our Threat Intelligence teams have observed a likely shift in affiliations among certain threat actors associated with Black Basta. Specifically, there is evidence suggesting that members have transitioned from the Black Basta ransomware group to the Cactus ransomware group. This conclusion is drawn from the analysis of similar tactics, techniques, and procedures (TTPs) being utilized by the Cactus group."

To mitigate the risk of ransomware and similar attacks, organizations should consider the following key measures:

- **Restrict remote assistance tools.** Disable unauthorized usage of remote access tools. Implement strict policies for remote assistance usage, requiring approval or verification. Layering access control, monitoring, and authentication measures helps reduce the risks associated with remote assistance tools.
- **Train employees on social engineering**. Regularly educate users about phishing scams and fake remote assistance attempts, reinforcing verification of all unsolicited requests. Companies should actively test, measure, and improve user response rates through behavior-driven training programs to enhance employee resilience against evolving social engineering tactics.
- **Apply Microsoft's security** best practices for Microsoft Teamsopen on a new tab to safeguard Teams users. Companies should also treat Teams as a critical enterprise communication tool that requires the same level of security monitoring as email. Apply security to third-party integrations and external communications to prevent impersonation attacks.

Proactive security with Trend Vision One

Trend Vision Oneopen on a new tab™ is an enterprise cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise's attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One open on a new tabcustomers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and

allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Vision One Intelligence Reports App [IOC Sweeping]

- Black Basta and Cactus Ransomware Groups Add BackConnect Malware to Their Arsenal

Trend Vision One Threat Insights App

- Emerging Threats: Black Basta and Cactus Ransomware Groups Add BackConnect Malware to Their Arsenalopen on a new tab

Hunting queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post using data within their environment. **Note that this can also be triggered by normal activity.**

Detection of DLL side-loading involves identifying modified DLLs that replace legitimate ones to execute unauthorized code.

- eventSubId: 603 AND (request:filters*.s3.us-east-2.amazonaws.com OR request:sfu*.s3.us-east-2.amazonaws.com) AND objectFilePath:kb*.bpx
- service: MicrosoftTeams AND principalName: *.onmicrosoft.com AND actionName:(ChatCreated OR MessageSent)
-

- tags:
- XSAE.F8809 (QuickAssist Remote Session Established)
- XSAE.F11212 (TitanPlus Installation)
- XSAE.F11530 (Anomalous Connection from OneDrive Binary)
- XSAE.F11531 (Cabinet File Expanded via Lolbin)
- XSAE.F11532 (Cabinet File Expansion via Lolbin)
- XSAE.F11534 (TitanPlus Installation - Process Create)

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledopen on a new tab.

Indicators of compromise (IoCs)

Sha256	Filename	Detection
b79c8b7fabb650bcae274b71ee741f4d2d14a626345283a268c902f43edb64fd	winhttp.dll	Backdoor.Win64.REEDBED.A
60bca9f0134b9499751f6a5b754a9a9eff0b44d545387fffc151b5070bd3a26a	wscapi.dll	
623a43b826f95dc109f7b46303c6566298522b824e86a928834f12ac7887e952	run2.bat	

URL/IP	Rating - Category
38.180.25[.]3	C&C Server

45.8.157[.]199	C&C Server
5[.]181[.]3[.]164	C&C Server
185[.]190[.]251[.]16	C&C Server
207[.]90[.]238[.]52	C&C Server
89[.]185[.]80[.]86	C&C Server
pumpkinrab[.]com	Malware Accomplice
hxxps://sfu11[.]s3[.]us-east-2[.]amazonaws[.]com/js/kb052117-01[.]bpx	
hxxps://sfu11[.]s3[.]us-east-2[.]amazonaws[.]com/js/kb052123-02[.]bpx	
hxxps[://]filters14[.]s3[.]us-east-2[.]amazonaws[.]com/	

Threat hunting

Here are other BACKCONNECT-related IPs based on Trend Micro Threat Intelligence:

- 5.181.159[.]48
- 45.128.149[.]32
- 207.90.238[.]46
- 45.8.157[.]158
- 195.123.233[.]19
- 178.236.247[.]173
- 195.123.241[.]24
- 20.187.1[.]254
- 5.78.41[.]255
- 38.180.192[.]243
- 207.90.238[.]52
- 89.185.80[.]251
- 91.90.195[.]91
- 45.8.157[.]162
- 20.82.136[.]218
- 45.8.157[.]146
- 5.181.3[.]164
- 195.123.233[.]148
- 45.8.157[.]199
- 89.185.80[.]86
- 195.211.96[.]135
- 38.180.25[.]3
- 38.180.135[.]232
- 185.190.251[.]16

Tags
