Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network

microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

October 31, 2024

Skip to main content

By

Since August 2023, Microsoft has observed intrusion activity targeting and successfully stealing credentials from multiple Microsoft customers that is enabled by highly evasive password spray attacks. Microsoft has linked the source of these password spray attacks to a network of compromised devices we track as CovertNetwork-1658, also known as xlogin and Quad7 (7777). Microsoft is publishing this blog on how covert networks are used in attacks, with the goal of increasing awareness, improving defenses, and disrupting related activity against our customers.

Microsoft assesses that credentials acquired from CovertNetwork-1658 password spray operations are used by multiple Chinese threat actors. In particular, Microsoft has observed the Chinese threat actor Storm-0940 using credentials from CovertNetwork-1658. Active since at least 2021, Storm-0940 obtains initial access through password spray and brute-force attacks, or by exploiting or misusing network edge applications and services. Storm-0940 is known to target organizations in North America and Europe, including think tanks, government organizations, non-governmental organizations, law firms, defense industrial base, and others.

As with any observed nation-state threat actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to help secure their environments. In this blog, we provide more information about CovertNetwork-1658 infrastructure, and associated Storm-0940 activity. We also share mitigation recommendations, detection information, and hunting queries that can help organizations identify, investigate, and mitigate associated activity.

What is CovertNetwork-1658?

Microsoft tracks a network of compromised small office and home office (SOHO) routers as CovertNetwork-1658. SOHO routers manufactured by TP-Link make up most of this network. Microsoft uses “CovertNetwork” to refer to a collection of egress IPs consisting of compromised or leased devices that may be used by one or more threat actors.

CovertNetwork-1658 specifically refers to a collection of egress IPs that may be used by one or more Chinese threat actors and is wholly comprised of compromised devices. Microsoft assesses that a threat actor located in China established and maintains this network. The threat actor exploits a vulnerability in the routers to gain remote code execution capability. We continue to investigate the specific exploit by which this threat actor compromises these routers. Microsoft assesses that multiple Chinese threat actors use the credentials acquired from CovertNetwork-1658 password spray operations to perform computer network exploitation (CNE) activities.

Post-compromise activity on compromised routers

After successfully gaining access to a vulnerable router, in some instances, the following steps are taken by the threat actor to prepare the router for password spray operations:

1. Download Telnet binary from a remote File Transfer Protocol (FTP) server
2. Download xlogin backdoor binary from a remote FTP server
3. Utilize the downloaded Telnet and xlogin binaries to start an access-controlled command shell on TCP port 7777
4. Connect and authenticate to the xlogin backdoor listening on TCP port 7777
5. Download a SOCKS5 server binary to router

6. Start SOCKS5 server on TCP port 11288

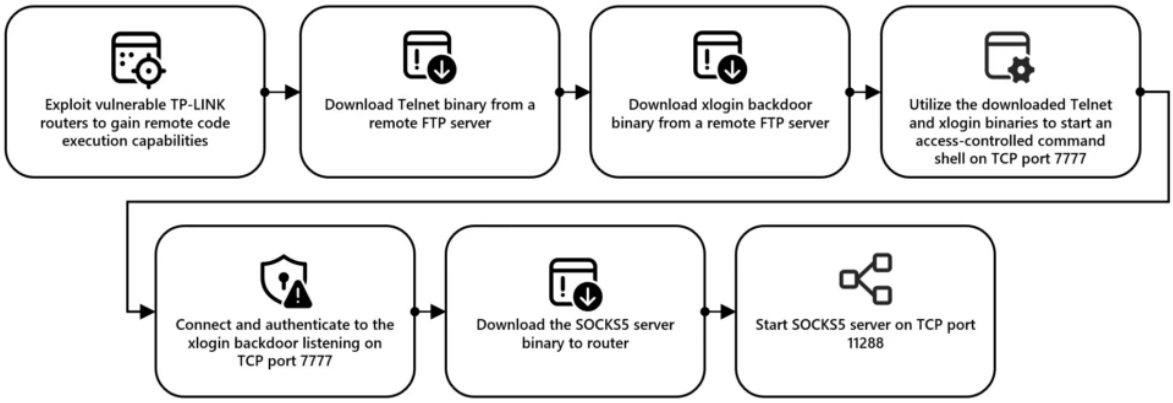


Figure 1. Steps taken to prepare the router for password spray operations

CovertNetwork-1658 is observed conducting their password spray campaigns through this proxy network to ensure the password spray attempts originate from the compromised devices.

Password spray activity from CovertNetwork-1658 infrastructure

Microsoft has observed multiple password spray campaigns originating from CovertNetwork-1658 infrastructure. In these campaigns, CovertNetwork-1658 submits a very small number of sign-in attempts to many accounts at a target organization. In about 80 percent of cases, CovertNetwork-1658 makes only one sign-in attempt per account per day. Figure 2 depicts this distribution in greater detail.

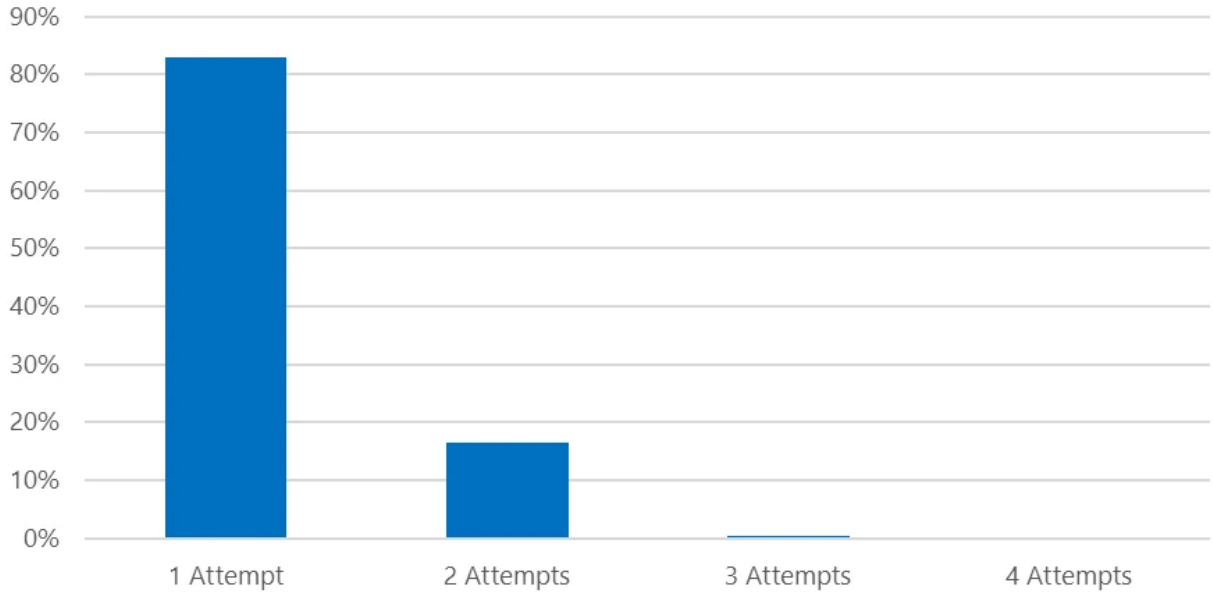


Figure 2. CovertNetwork-1658 count of sign-in attempts per account per day.

CovertNetwork-1658 infrastructure is difficult to monitor due to the following characteristics:

- The use of compromised SOHO IP addresses
- The use of a rotating set of IP addresses at any given time. The threat actors had thousands of available IP addresses at their disposal. The average uptime for a CovertNetwork-1658 node is approximately 90 days.
- The low-volume password spray process; for example, monitoring for multiple failed sign-in attempts from one IP address or to one account will not detect this activity

Various security vendors have reported on CovertNetwork-1658 activities, including Sekoia (July 2024) and Team Cymru (August 2024). Microsoft assesses that after these blogs were published, the usage of CovertNetwork-1658 network has declined substantially. The below chart highlights a steady and steep decline in the use of CovertNetwork-1658's original infrastructure since their activities have been exposed in public reporting as observed in Censys.IO data.

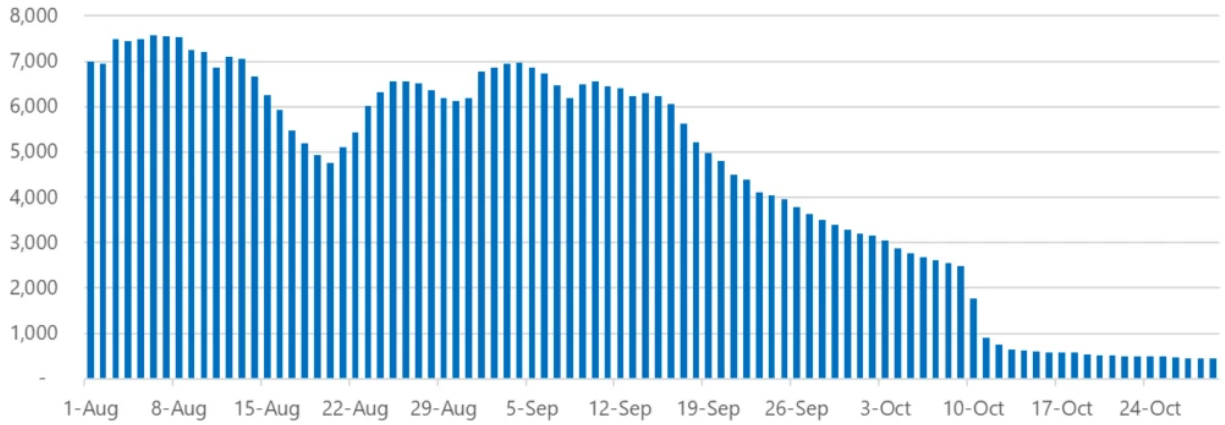


Figure 3. Chart showing the drop in CovertNetwork-1658's available nodes between August 1, 2024 and October 29, 2024

Microsoft assesses that CovertNetwork-1658 has not stopped operations as indicated in recent activity but is likely acquiring new infrastructure with modified fingerprints from what has been publicly disclosed. An observed increase in recent activity may be early evidence supporting this assessment.

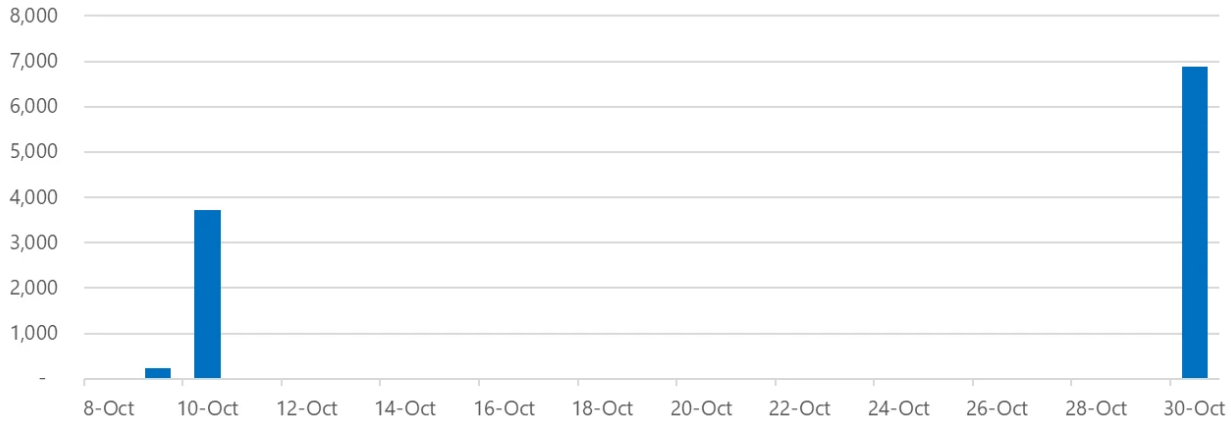


Figure 4. Chart showing number of Microsoft Azure tenants targeted by day between October 8, 2024-October 30, 2024.

Historically, Microsoft has observed an average of 8,000 compromised devices actively engaged in the CovertNetwork-1658 network at any given time. On average, about 20 percent of these devices perform password spraying at any given time. Any threat actor using the CovertNetwork-1658 infrastructure could conduct password spraying campaigns at a larger scale and greatly increase the likelihood of successful credential compromise and initial access to multiple organizations in a short amount of time. This scale, combined with quick operational turnover of compromised credentials between CovertNetwork-1658 and Chinese threat actors, allows for the potential of account compromises across multiple sectors and geographic regions.

Below are User Agent Strings* observed in the password spray activity:

- Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

**Note: We updated this list of User Agent Strings on November 4, 2024 to fix typos.*

Observed activity tied to Storm-0940

Microsoft has observed numerous cases where Storm-0940 has gained initial access to target organizations using valid credentials obtained through CovertNetwork-1658's password spray operations. In some instances, Storm-0940 was observed using compromised credentials that were obtained from CovertNetwork-1658 infrastructure on the same day. This quick operational hand-off of compromised credentials is evidence of a likely close working relationship between the operators of CovertNetwork-1658 and Storm-0940.

After successfully gaining access to a victim environment, in some instances, Storm-0940 has been observed:

- Using scanning and credential dumping tools to move laterally within the network;

- Attempting to access network devices and install proxy tools and remote access trojans (RATs) for persistence; and
- Attempting to exfiltrate data.

Recommendations

Organizations can defend against password spraying by building credential hygiene and hardening cloud identities. Microsoft recommends the following mitigations to reduce the impact of this threat:

- Educate users on the importance of credential hygiene and avoiding password reuse.
- Enforce multi-factor authentication (MFA) on all accounts, remove users excluded from MFA, and strictly require MFA from all devices, in all locations, at all times. Microsoft continues to expand MFA defaults for products and services like Azure to broaden MFA adoption.
    Consider transitioning to a passwordless primary authentication method, such as Azure MFA, certificates, or Windows Hello for Business.
    Secure Remote Desktop Protocol (RDP) or Windows Virtual Desktop endpoints with MFA to harden against password spray or brute force attacks.
- Enable passwordless authentication methods (for example, Windows Hello, FIDO keys, or Microsoft Authenticator) for accounts that support passwordless. For accounts that still require passwords, use authenticator apps like Microsoft Authenticator for MFA.
- Disable legacy authentication.
- Use a cloud-based identity security solution to identify and detect threats or compromised identities.
- Disable stale or unused accounts.
- Reset account passwords for any accounts targeted during a password spray attack. If a targeted account had system-level permissions, further investigation may be warranted.
- Implement the Azure Security Benchmark and general best practices for securing identity infrastructure, including:
    Create conditional access policies to allow or disallow access to the environment based on defined criteria.
-
    Block legacy authentication with Azure AD by using Conditional Access. Legacy authentication protocols don’t have the ability to enforce MFA, so blocking such authentication methods will prevent password spray attackers from taking advantage of the lack of MFA on those protocols.
    Enable AD FS web application proxy extranet lockout to protect users from potential password brute force compromise.

- Secure accounts with credential hygiene:
  - Practice the principle of least privilege and audit privileged account activity in your Azure AD environments to slow and stop attackers.
  - Deploy Azure AD Connect Health for ADFS. This captures failed attempts as well as IP addresses recorded in ADFS logs for bad requests via the *Risky IP report*.
  - Use Azure AD password protection to detect and block known weak passwords and their variants.
  - Turn on identity protection in Azure AD to monitor for identity-based risks and create policies for risky sign ins.
- Educate users about phishing attempts and MFA fatigue attacks. Encourage users to report unsolicited MFA authentication prompts.
- Review your Anomaly detection policies in Defender for Cloud Apps under Microsoft 365 Defender Policies by going to Cloud Apps > Policies > Policy management. Then select Anomaly detection policy.

Detection details

Alerts with the following titles in the Security Center can indicate threat activity on your network:

Microsoft Defender for Endpoint

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

> Storm-0940 actor activity detected

Microsoft Defender XDR

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

> Password spray attacks originating from single ISP

Microsoft Defender for Identity

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

- Password Spray
- Unfamiliar Sign-in properties
- Atypical travel
- Suspicious behavior: Impossible travel activity

Microsoft Defender for Cloud Apps

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

- Suspicious Administrative Activity
- Impossible travel activity

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

Potential Storm-0940 activity

This query identifies UserAgents obtained from observed activity and AAD SignInEvent attributes that identify potential activity to guide investigation:

```
//Advanced Hunting Query
let suspAppRes = datatable(appId:string, resourceId:string)
[
    "1950a258-227b-4e31-a9cf-717495945fc2", "00000003-0000-0000-c000-000000000000"
];
let userAgents = datatable(userAgent:string)
[
    "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.149 Safari/537.36" //Low fidelity
];
AADSignInEventsBeta
| where Timestamp >=ago(30d)
| where ApplicationId in ((suspAppRes | project appId)) and ResourceId in
((suspAppRes | project resourceId)) and UserAgent in ((userAgents| project
userAgent))
Failed sign-in activity
The following query identifies failed attempts to sign-in from multiple sources that
originate from a single ISP. Attackers distribute attacks from multiple IP addresses
across a single service provider to evade detection
IdentityLogonEvents
| where Timestamp > ago(4h)
| where ActionType == "LogonFailed"
| where isnotempty(AccountObjectId)
| summarize TargetCount = dcount(AccountObjectId), TargetCountry = dcount(Location),
TargetIPAddress = dcount(IPAddress) by ISP
| where TargetCount >= 100
| where TargetCountry >= 5
| where TargetIPAddress >= 25
```

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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

Potential Storm-0940 activity

This query identifies UserAgents obtained from observed activity and AAD SignInEvent attributes that identify potential activity to guide investigation:

```
//sentinelquery
let suspAppRes = datatable(appId:string, resourceId:string)
[
    "1950a258-227b-4e31-a9cf-717495945fc2", "00000003-0000-0000-c000-000000000000"
];
let userAgents = datatable(userAgent:string)
[
    "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.149 Safari/537.36" //Low fidelity
];
SigninLogs
| where TimeGenerated >=ago(30d)
| where AppId  in ((suspAppRes | project appId)) and ResourceIdentity in ((suspAppRes
| project resourceId)) and UserAgent in ((userAgents| project userAgent))
```

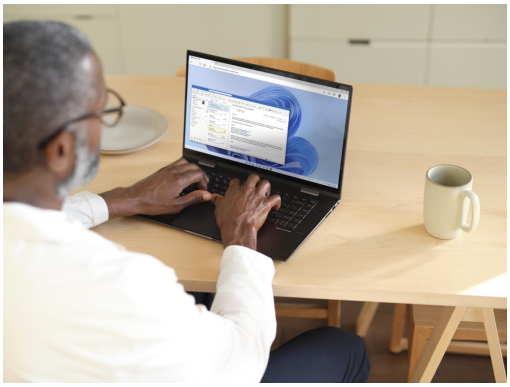
Learn more

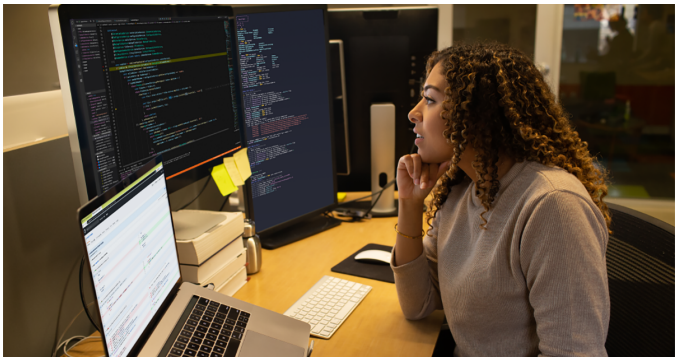
For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

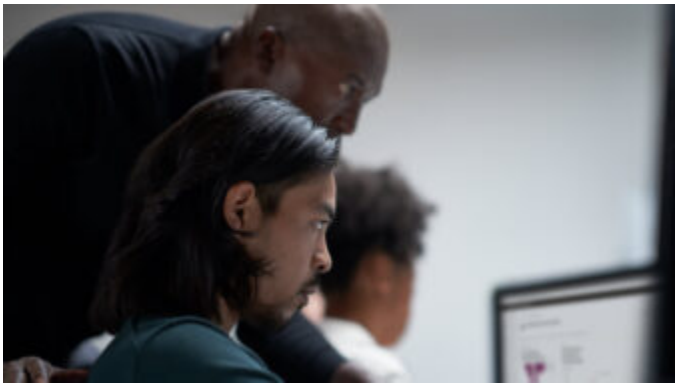
To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

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







Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets

Since February 2023, Microsoft has observed a high volume of password spray attacks attributed to Peach Sandstorm, an Iranian nation-state group. In a small number of cases, Peach Sandstorm successfully authenticated to an account and used a combination of publicly available and custom tools for persistence, lateral movement, and exfiltration.

Chained for attack: OpenVPN vulnerabilities discovered leading to RCE and LPE

Microsoft researchers found multiple vulnerabilities in OpenVPN that could lead to an attack chain allowing remote code execution and local privilege escalation. This attack chain could enable attackers to gain full control over targeted endpoints, potentially resulting in data breaches, system compromise, and unauthorized access to sensitive information.