Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files

microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

October 29, 2024

Skip to main content

By

Since October 22, 2024, Microsoft Threat Intelligence has observed Russian threat actor Midnight Blizzard sending a series of highly targeted spear-phishing emails to individuals in government, academia, defense, non-governmental organizations, and other sectors. This activity is ongoing, and Microsoft will continue to investigate and provide updates as available. Based on our investigation of previous Midnight Blizzard spear-phishing campaigns, we assess that the goal of this operation is likely intelligence collection. Microsoft is releasing this blog to notify the public and disrupt this threat actor activity. This blog provides context on these external spear-phishing attempts, which are common attack techniques and do not represent any new compromise of Microsoft.

The spear-phishing emails in this campaign were sent to thousands of targets in over 100 organizations and contained a signed Remote Desktop Protocol (RDP) configuration file that connected to an actor-controlled server. In some of the lures, the actor attempted to add

credibility to their malicious messages by impersonating Microsoft employees. The threat actor also referenced other cloud providers in the phishing lures.

While this campaign focuses on many of Midnight Blizzard's usual targets, the use of a signed RDP configuration file to gain access to the targets' devices represents a novel access vector for this actor. Overlapping activity hasalso been reported by the Government Computer Emergency Response Team of Ukraine (CERT-UA) under the designation UAC-0215 and also by Amazon.

Midnight Blizzard is a Russian threat actor attributed by the United States and United Kingdom governments to the Foreign Intelligence Service of the Russian Federation, also known as the SVR. This threat actor is known to primarily target governments, diplomatic entities, non-governmental organizations (NGOs), and IT service providers, primarily in the United States and Europe. Its focus is to collect intelligence through longstanding and dedicated espionage of foreign interests that can be traced to early 2018. Its operations often involve compromise of valid accounts and, in some highly targeted cases, advanced techniques to compromise authentication mechanisms within an organization to expand access and evade detection.

Midnight Blizzard is consistent and persistent in its operational targeting, and its objectives rarely change. It uses diverse initial access methods, including spear phishing, stolen credentials, supply chain attacks, compromise of on-premises environments to laterally move to the cloud, and leveraging service providers' trust chain to gain access to downstream customers. Midnight Blizzard is known to use the Active Directory Federation Service (AD FS) malware known as FOGGYWEB and MAGICWEB. Midnight Blizzard is identified by peer security vendors as APT29, UNC2452, and Cozy Bear.

As with any observed nation-state actor activity, Microsoft is in the process of directly notifying customers that have been targeted or compromised, providing them with the necessary information to secure their accounts. Strong anti-phishing measures will help to mitigate this threat. As part of our commitment to helping protect against cyber threats, we provide indicators of compromise (IOCs), hunting queries, detection details, and recommendations at the end of this post.

Spear-phishing campaign

On October 22, 2024, Microsoft identified a spear-phishing campaign in which Midnight Blizzard sent phishing emails to thousands of users in over 100 organizations. The emails were highly targeted, using social engineering lures relating to Microsoft, Amazon Web Services (AWS), and the concept of Zero Trust. The emails contained a Remote Desktop Protocol (RDP) configuration file signed with a LetsEncrypt certificate. RDP configuration

(.RDP) files summarize automatic settings and resource mappings that are established when a successful connection to an RDP server occurs. These configurations extend features and resources of the local system to a remote server, controlled by the actor.

In this campaign, the malicious .RDP attachment contained several sensitive settings that would lead to significant information exposure. Once the target system was compromised, it connected to the actor-controlled server and bidirectionally mapped the targeted user's local device's resources to the server. Resources sent to the server may include, but are not limited to, all logical hard disks, clipboard contents, printers, connected peripheral devices, audio, and authentication features and facilities of the Windows operating system, including smart cards. This access could enable the threat actor to install malware on the target's local drive(s) and mapped network share(s), particularly in AutoStart folders, or install additional tools such as remote access trojans (RATs) to maintain access when the RDP session is closed. The process of establishing an RDP connection to the actor-controlled system may also expose the credentials of the user signed in to the target system.

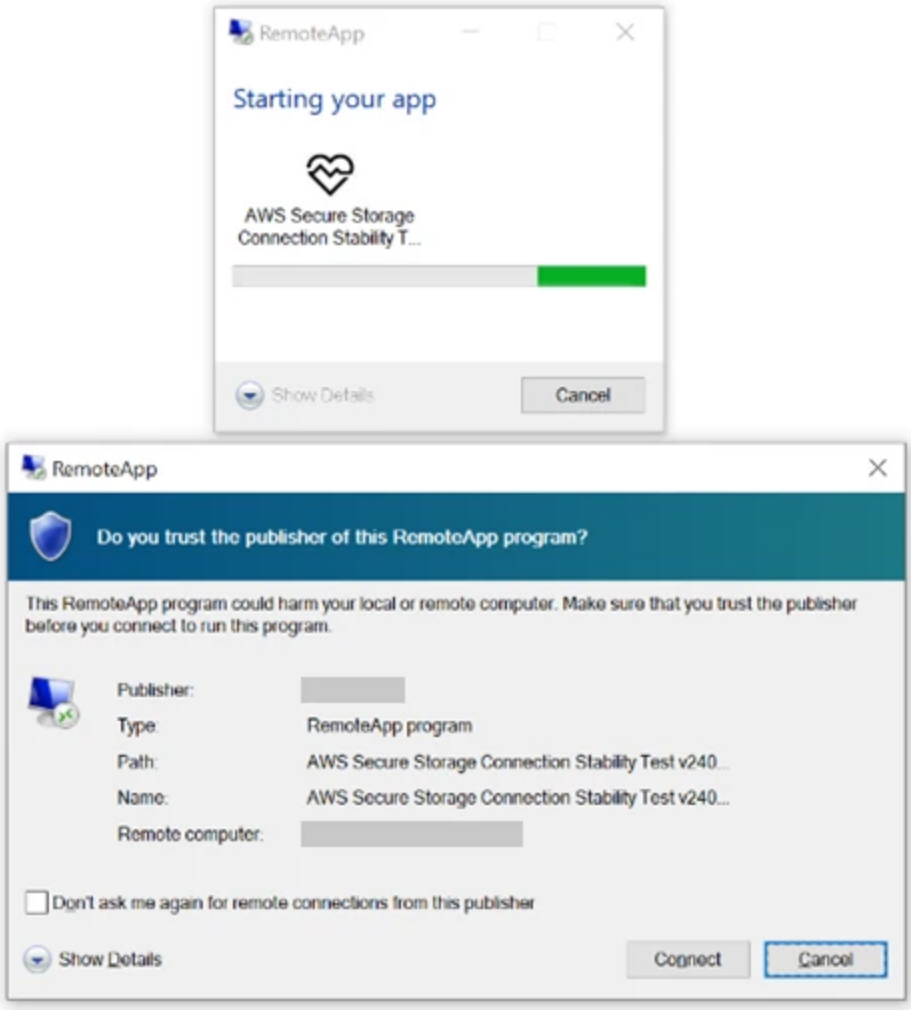


Figure 1. Malicious remote connection

RDP connection

When the target user opened the .RDP attachment, an RDP connection was established to an actor-controlled system. The configuration of the RDP connection then allowed the actor-controlled system to discover and use information about the target system, including:

- Files and directories
- Connected network drives
- Connected peripherals, including smart cards, printers, and microphones
- Web authentication using Windows Hello, passkeys, or security keys
- Clipboard data
- Point of Service (also known as Point of Sale or POS) devices

Targets

Microsoft has observed this campaign targeting governmental agencies, higher education, defense, and non-governmental organizations in dozens of countries, but particularly in the United Kingdom, Europe, Australia, and Japan. This target set is consistent with other Midnight Blizzard phishing campaigns.

Email infrastructure

Midnight Blizzard sent the phishing emails in this campaign using email addresses belonging to legitimate organizations that were gathered during previous compromises. The domains used are listed in the IOC section below.

Mitigations

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

Strengthen operating environment configuration

- Utilize Windows Firewall or Windows Firewall with Advanced Security to help prevent or restrict outbound RDP connection attempts to external or public networks external or public networks
- Require multifactor authentication (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 number matching. Avoid telephony-based MFA methods to avoid risks associated with SIM-jacking.
- Implement 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 help blocks malicious websites, including phishing sites, scam sites, and sites that host malware.

Strengthen endpoint security configuration

If you are using Microsoft Defender for Endpoint take the following steps:

- Ensure tamper protection is turned on in Microsoft Defender for Endpoint.
- Turn on 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 help 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 help 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 help resolve breaches, significantly reducing alert volume.
- Microsoft Defender XDR customers can turn on the following attack surface reduction rules to help 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

Strengthen antivirus configuration

- Turn on cloud-delivered protection in Microsoft Defender Antivirus, or the equivalent for your antivirus product, to help cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections help 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.

Strengthen Microsoft Office 365 configuration

- Turn on Safe Links and Safe Attachments for Office 365.
- Enable Zero-hour auto purge (ZAP) in Office 365 to help 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.

Strengthen email security configuration

- Invest in advanced anti-phishing solutions that monitor incoming emails and visited websites. For example, Microsoft Defender for Office 365 merges incident and alert management across email, devices, and identities, centralizing investigations for email-based threats. Organizations can also leverage web browsers that automatically identify and help block malicious websites, including those used in phishing activities.

- If you are using Microsoft Defender for Office 365, configure it to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages, other Microsoft 365 applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Microsoft Exchange Online Protection (EOP). Safe Links scanning can help protect an organization from malicious links used in phishing and other attacks.
- If you are using Microsoft Defender for Office 365, 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.

Conduct user education

Robust user education can help mitigate the threat of social engineering and phishing emails. Companies should have a user education program that highlights how to identify and report suspicious emails.

Microsoft Defender XDR detections

Microsoft Defender for Endpoint

The following alerts may 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.

- Midnight Blizzard Actor activity group
- Suspicious RDP session

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects at least some of the malicious .RDP files as the following signature:

Backdoor:Script/HustleCon.A

Microsoft Defender for Cloud

The following alerts may 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 outgoing RDP network activity
- Traffic detected from IP addresses recommended for blocking

Microsoft Defender for Office 365

Microsoft Defender for Office 365 raises alerts on this campaign using email- and attachment-based detections. Additionally, hunting signatures and an RDP file parser have been incorporated into detections to block similar campaigns in the future. Defenders can identify such activity in alert titles referencing RDP, for example, *Trojan_RDP**.

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 threat intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Midnight Blizzard targets NGOs in new wave of initial access campaigns.
- Midnight Blizzard targets diplomatic, NGOs, and humanitarian organizations in global spear phishing activity.

Hunting queries

Microsoft Defender XDR

Identify potential Midnight Blizzard targeted recipients

Surface possible targeted email accounts within the environment where the email sender originated from a Midnight Blizzard compromised domain related to the RDP activity.

```
EmailEvents
| where SenderFromDomain in~ ("sellar.co.uk", "townoflakelure.com",
"totalconstruction.com.au", "swpartners.com.au", "cewalton.com")
| project SenderFromDomain, SenderFromAddress, RecipientEmailAddress, Subject,
Timestamp
```

Surface potential targets of an RDP attachment phishing attempt

Surface emails that contain a remote desktop protocol (RDP) file attached. This may indicate that the recipient of the email may have been targeted in an RDP attachment phishing attack attempt.

```
EmailAttachmentInfo
| where FileName has ".rdp"
| join kind=inner (EmailEvents) on NetworkMessageId
| project SenderFromAddress, RecipientEmailAddress, Subject, Timestamp, FileName,
FileType
```

Identify potential successfully targeted assets in an RDP attachment phishing attack

Surface devices that may have been targeted in an email with an RDP file attached, followed by an RDP connection attempt from the device to an external network. This combined activity may indicate that a device may have been successfully targeted in an RDP attachment phishing attack.

```
// Step 1: Identify emails with RDP attachments
let rdpEmails = EmailAttachmentInfo
| where FileName has ".rdp"
| join kind=inner (EmailEvents) on NetworkMessageId
| project EmailTimestamp = Timestamp, RecipientEmailAddress, NetworkMessageId,
SenderFromAddress;
// Step 2: Identify outbound RDP connections
let outboundRDPConnections = DeviceNetworkEvents
| where RemotePort == 3389
| where ActionType == "ConnectionAttempt"
| where RemoteIPType == "Public"
| project RDPConnectionTimestamp = Timestamp, DeviceId, InitiatingProcessAccountUpn,
RemoteIP;
// Step 3: Correlate email and network events
rdpEmails
| join kind=inner (outboundRDPConnections) on $left.RecipientEmailAddress ==
$right.InitiatingProcessAccountUpn
| project EmailTimestamp, RecipientEmailAddress, SenderFromAddress,
RDPConnectionTimestamp, DeviceId, RemoteIP
```

Threat actor RDP connection files attached to email

Surface users that may have received an RDP connection file attached in email that have been observed in this attack from Midnight Blizzard.

```
EmailAttachmentInfo
| where FileName in~ (
    "AWS IAM Compliance Check.rdp",
    "AWS IAM Configuration.rdp",
    "AWS IAM Quick Start.rdp",
    "AWS SDE Compliance Check.rdp",
    "AWS SDE Environment Check.rdp",
    "AWS Secure Data Exchange - Compliance Check.rdp",
    "AWS Secure Data Exchange Compliance.rdp",
    "Device Configuration Verification.rdp",
    "Device Security Requirements Check.rdp",
    "IAM Identity Center Access.rdp",
    "IAM Identity Center Application Access.rdp",
    "Zero Trust Architecture Configuration.rdp",
    "Zero Trust Security Environment Compliance Check.rdp",
    "ZTS Device Compatibility Test.rdp"
)
| project Timestamp, FileName, SHA256, RecipientEmailAddress, SenderDisplayName,
SenderFromAddress
```

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.

Indicators of compromise

Email sender domains

Domains	Last seen
sellar[.]co.uk	October 23, 2024
townoflakelure[.]com	October 23, 2024
totalconstruction[.]com.au	October 23, 2024
swpartners[.]com.au	October 23, 2024
cewalton[.]com	October 23, 2024

RDP file names

- AWS IAM Compliance Check.rdp
- AWS IAM Configuration.rdp

- AWS IAM Quick Start.rdp
- AWS SDE Compliance Check.rdp
- AWS SDE Environment Check.rdp
- AWS SDE Environment Check.rdp
- AWS Secure Data Exchange – Compliance Check.rdp
- AWS Secure Data Exchange Compliance.rdp
- Device Configuration Verification.rdp
- Device Security Requirements Check.rdp
- IAM Identity Center Access.rdp
- IAM Identity Center Application Access.rdp
- Zero Trust Architecture Configuration.rdp
- Zero Trust Security Environment Compliance Check.rdp
- ZTS Device Compatibility Test.rdp

RDP remote computer domains

ap-northeast-1-aws.s3-ua[.]cloud	ap-northeast-1-aws.ukrainesec[.]cloud
ca-central-1.gov-ua[.]cloud	ca-central-1.ua-gov[.]cloud
ca-west-1.aws-ukraine[.]cloud	ca-west-1.mfa-gov[.]cloud
ca-west-1.ukrtelecom[.]cloud	central-2-aws.ua-mil[.]cloud
central-2-aws.ua-sec[.]cloud	central-2-aws.ukrainesec[.]cloud
central-2-aws.ukrtelecom[.]cloud	eu-central-1.difesa-it[.]cloud
eu-central-1.mfa-gov[.]cloud	eu-central-1.mil-be[.]cloud
eu-central-1.mil-pl[.]cloud	eu-central-1.minbuza[.]cloud
eu-central-1.mindef-nl[.]cloud	eu-central-1.msz-pl[.]cloud
eu-central-1.quirinale[.]cloud	eu-central-1.regeringskansliet-se[.]cloud
eu-central-1.s3-be[.]cloud	eu-central-1.s3-esa[.]cloud
eu-central-1.s3-nato[.]cloud	eu-central-1.ua-gov[.]cloud
eu-central-1.ua-sec[.]cloud	eu-central-1.ukrtelecom[.]cloud
eu-central-1-aws.amazonsolutions[.]cloud	eu-central-1-aws.dep-no[.]cloud
eu-central-1-aws.gov-pl[.]cloud	eu-central-1-aws.gov-sk[.]cloud
eu-central-1-aws.gov-trust[.]cloud	eu-central-1-aws.mfa-gov[.]cloud
eu-central-1-aws.minbuza[.]cloud	eu-central-1-aws.mindef-nl[.]cloud
eu-central-1-aws.msz-pl[.]cloud	eu-central-1-aws.mzv-sk[.]cloud
eu-central-1-aws.ncfta[.]cloud	eu-central-1-aws.presidencia-pt[.]cloud
eu-central-1-aws.quirinale[.]cloud	eu-central-1-aws.regeringskansliet-se[.]cloud
eu-central-1-aws.s3-be[.]cloud	eu-central-1-aws.s3-ua[.]cloud
eu-central-1-aws.ua-gov[.]cloud	eu-central-1-aws.ukrainesec[.]cloud
eu-central-2-aws.amazonsolutions[.]cloud	eu-central-2-aws.aws-ukraine[.]cloud
eu-central-2-aws.dep-no[.]cloud	eu-central-2-aws.gov-pl[.]cloud
eu-central-2-aws.gov-sk[.]cloud	eu-central-2-aws.mil-be[.]cloud
eu-central-2-aws.mil-pl[.]cloud	eu-central-2-aws.mindef-nl[.]cloud

eu-central-2-aws.msz-pl[.]cloud	eu-central-2-aws.mzv-sk[.]cloud
eu-central-2-aws.presidencia-pt[.]cloud	eu-central-2-aws.regeringskansliet-se[.]cloud
eu-central-2-aws.s3-be[.]cloud	eu-central-2-aws.ua-gov[.]cloud
eu-central-2-aws.ua-mil[.]cloud	eu-central-2-aws.ukrtelecom[.]cloud
eu-east-1-aws.amazonsolutions[.]cloud	eu-east-1-aws.dep-no[.]cloud
eu-east-1-aws.gov-sk[.]cloud	eu-east-1-aws.gov-ua[.]cloud
eu-east-1-aws.mil-be[.]cloud	eu-east-1-aws.mil-pl[.]cloud
eu-east-1-aws.minbuza[.]cloud	eu-east-1-aws.mindef-nl[.]cloud
eu-east-1-aws.msz-pl[.]cloud	eu-east-1-aws.mzv-sk[.]cloud
eu-east-1-aws.quirinale[.]cloud	eu-east-1-aws.regeringskansliet-se[.]cloud
eu-east-1-aws.s3-be[.]cloud	eu-east-1-aws.s3-de[.]cloud
eu-east-1-aws.ua-gov[.]cloud	eu-east-1-aws.ua-sec[.]cloud
eu-east-1-aws.ukrtelecom[.]cloud	eu-north-1.difesa-it[.]cloud
eu-north-1.gov-trust[.]cloud	eu-north-1.gov-ua[.]cloud
eu-north-1.gv-at[.]cloud	eu-north-1.mil-be[.]cloud
eu-north-1.mil-pl[.]cloud	eu-north-1.mzv-sk[.]cloud
eu-north-1.ncfta[.]cloud	eu-north-1.regeringskansliet-se[.]cloud
eu-north-1.s3-be[.]cloud	eu-north-1.s3-de[.]cloud
eu-north-1.s3-ua[.]cloud	eu-north-1-aws.dep-no[.]cloud
eu-north-1-aws.difesa-it[.]cloud	eu-north-1-aws.gov-pl[.]cloud
eu-north-1-aws.gov-sk[.]cloud	eu-north-1-aws.mil-be[.]cloud
eu-north-1-aws.mil-pl[.]cloud	eu-north-1-aws.minbuza[.]cloud
eu-north-1-aws.ncfta[.]cloud	eu-north-1-aws.presidencia-pt[.]cloud
eu-north-1-aws.quirinale[.]cloud	eu-north-1-aws.regeringskansliet-se[.]cloud
eu-north-1-aws.s3-be[.]cloud	eu-north-1-aws.s3-de[.]cloud
eu-north-1-aws.ua-energy[.]cloud	eu-north-1-aws.ua-gov[.]cloud

eu-south-1-aws.admin-ch[.]cloud	eu-south-1-aws.dep-no[.]cloud
eu-south-1-aws.difesa-it[.]cloud	eu-south-1-aws.gov-pl[.]cloud
eu-south-1-aws.gov-trust[.]cloud	eu-south-1-aws.mfa-gov[.]cloud
eu-south-1-aws.mil-be[.]cloud	eu-south-1-aws.minbuza[.]cloud
eu-south-1-aws.mzv-sk[.]cloud	eu-south-1-aws.quirinale[.]cloud
eu-south-1-aws.s3-be[.]cloud	eu-south-1-aws.s3-de[.]cloud
eu-south-1-aws.ua-gov[.]cloud	eu-south-2.dep-no[.]cloud
eu-south-2.gov-pl[.]cloud	eu-south-2.gov-sk[.]cloud
eu-south-2.mil-be[.]cloud	eu-south-2.mil-pl[.]cloud
eu-south-2.mindef-nl[.]cloud	eu-south-2.s3-be[.]cloud
eu-south-2.s3-de[.]cloud	eu-south-2.s3-esa[.]cloud
eu-south-2.s3-nato[.]cloud	eu-south-2.ua-sec[.]cloud
eu-south-2.ukrainesec[.]cloud	eu-south-2-aws.amazonsolutions[.]cloud
eu-south-2-aws.dep-no[.]cloud	eu-south-2-aws.gov-pl[.]cloud
eu-south-2-aws.gov-sk[.]cloud	eu-south-2-aws.mfa-gov[.]cloud
eu-south-2-aws.mil-be[.]cloud	eu-south-2-aws.mil-pl[.]cloud
eu-south-2-aws.mil-pt[.]cloud	eu-south-2-aws.minbuza[.]cloud
eu-south-2-aws.msz-pl[.]cloud	eu-south-2-aws.mzv-sk[.]cloud
eu-south-2-aws.ncfta[.]cloud	eu-south-2-aws.quirinale[.]cloud
eu-south-2-aws.regeringskansliet-se[.]cloud	eu-south-2-aws.s3-be[.]cloud
eu-south-2-aws.s3-de[.]cloud	eu-south-2-aws.s3-esa[.]cloud
eu-south-2-aws.s3-nato[.]cloud	eu-south-2-aws.s3-ua[.]cloud
eu-south-2-aws.ua-gov[.]cloud	eu-southeast-1-aws.amazonsolutions[.]cloud
eu-southeast-1-aws.aws-ukraine[.]cloud	eu-southeast-1-aws.dep-no[.]cloud
eu-southeast-1-aws.difesa-it[.]cloud	eu-southeast-1-aws.gov-sk[.]cloud
eu-southeast-1-aws.gov-trust[.]cloud	eu-southeast-1-aws.mil-be[.]cloud

eu-southeast-1-aws.mil-pl[.]cloud	eu-southeast-1-aws.mindef-nl[.]cloud
eu-southeast-1-aws.msz-pl[.]cloud	eu-southeast-1-aws.mzv-cz[.]cloud
eu-southeast-1-aws.mzv-sk[.]cloud	eu-southeast-1-aws.quirinale[.]cloud
eu-southeast-1-aws.s3-be[.]cloud	eu-southeast-1-aws.s3-de[.]cloud
eu-southeast-1-aws.s3-esa[.]cloud	eu-southeast-1-aws.s3-ua[.]cloud
eu-southeast-1-aws.ua-energy[.]cloud	eu-southeast-1-aws.ukrainesec[.]cloud
eu-west-1.aws-ukraine[.]cloud	eu-west-1.difesa-it[.]cloud
eu-west-1.gov-sk[.]cloud	eu-west-1.mil-be[.]cloud
eu-west-1.mil-pl[.]cloud	eu-west-1.minbuza[.]cloud
eu-west-1.msz-pl[.]cloud	eu-west-1.mzv-sk[.]cloud
eu-west-1.regeringskansliet-se[.]cloud	eu-west-1.s3-de[.]cloud
eu-west-1.s3-esa[.]cloud	eu-west-1.s3-ua[.]cloud
eu-west-1.ua-gov[.]cloud	eu-west-1.ukrtelecom[.]cloud
eu-west-1-aws.amazonsolutions[.]cloud	eu-west-1-aws.aws-ukraine[.]cloud
eu-west-1-aws.dep-no[.]cloud	eu-west-1-aws.gov-pl[.]cloud
eu-west-1-aws.gov-sk[.]cloud	eu-west-1-aws.gov-trust[.]cloud
eu-west-1-aws.gov-ua[.]cloud	eu-west-1-aws.mil-be[.]cloud
eu-west-1-aws.mil-pl[.]cloud	eu-west-1-aws.minbuza[.]cloud
eu-west-1-aws.quirinale[.]cloud	eu-west-1-aws.s3-be[.]cloud
eu-west-1-aws.s3-de[.]cloud	eu-west-1-aws.s3-esa[.]cloud
eu-west-1-aws.s3-nato[.]cloud	eu-west-1-aws.ua-sec[.]cloud
eu-west-1-aws.ukrainesec[.]cloud	eu-west-2-aws.amazonsolutions[.]cloud
eu-west-2-aws.dep-no[.]cloud	eu-west-2-aws.difesa-it[.]cloud
eu-west-2-aws.gov-pl[.]cloud	eu-west-2-aws.gov-sk[.]cloud
eu-west-2-aws.gv-at[.]cloud	eu-west-2-aws.mil-be[.]cloud
eu-west-2-aws.mil-pl[.]cloud	eu-west-2-aws.minbuza[.]cloud

eu-west-2-aws.mindef-nl[.]cloud	eu-west-2-aws.msz-pl[.]cloud
eu-west-2-aws.mzv-sk[.]cloud	eu-west-2-aws.quirinale[.]cloud
eu-west-2-aws.s3-be[.]cloud	eu-west-2-aws.s3-de[.]cloud
eu-west-2-aws.s3-esa[.]cloud	eu-west-2-aws.s3-nato[.]cloud
eu-west-2-aws.s3-ua[.]cloud	eu-west-2-aws.ua-sec[.]cloud
eu-west-3.amazonsolutions[.]cloud	eu-west-3.aws-ukraine[.]cloud
eu-west-3.mil-be[.]cloud	eu-west-3.mil-pl[.]cloud
eu-west-3.minbuza[.]cloud	eu-west-3.mindef-nl[.]cloud
eu-west-3.msz-pl[.]cloud	eu-west-3.mzv-sk[.]cloud
eu-west-3.presidencia-pt[.]cloud	eu-west-3.s3-be[.]cloud
eu-west-3.s3-ua[.]cloud	eu-west-3.ukrainesec[.]cloud
eu-west-3.ukrtelecom[.]cloud	eu-west-3-aws.aws-ukraine[.]cloud
eu-west-3-aws.dep-no[.]cloud	eu-west-3-aws.difesa-it[.]cloud
eu-west-3-aws.gov-pl[.]cloud	eu-west-3-aws.gov-sk[.]cloud
eu-west-3-aws.gov-trust[.]cloud	eu-west-3-aws.mil-be[.]cloud
eu-west-3-aws.mil-pl[.]cloud	eu-west-3-aws.mil-pt[.]cloud
eu-west-3-aws.minbuza[.]cloud	eu-west-3-aws.mindef-nl[.]cloud
eu-west-3-aws.msz-pl[.]cloud	eu-west-3-aws.mzv-sk[.]cloud
eu-west-3-aws.quirinale[.]cloud	eu-west-3-aws.regeringskansliet-se[.]cloud
eu-west-3-aws.s3-be[.]cloud	eu-west-3-aws.s3-ua[.]cloud
eu-west-3-aws.ua-mil[.]cloud	us-east-1-aws.mfa-gov[.]cloud
us-east-1-aws.s3-ua[.]cloud	us-east-1-aws.ua-gov[.]cloud
us-east-1-aws.ua-sec[.]cloud	us-east-2.aws-ukraine[.]cloud
us-east-2.gov-ua[.]cloud	us-east-2.ua-sec[.]cloud
us-east-2.ukrainesec[.]cloud	us-east-2-aws.gov-ua[.]cloud
us-east-2-aws.ua-gov[.]cloud	us-east-2-aws.ukrtelecom[.]cloud

us-east-console.aws-ukraine[.]cloud	us-east-console.ua-energy[.]cloud
us-west-1.aws-ukraine[.]cloud	us-west-1.ua-energy[.]cloud
us-west-1.ua-gov[.]cloud	us-west-1.ukrtelecom[.]cloud
us-west-1-amazon.ua-energy[.]cloud	us-west-1-amazon.ua-mil[.]cloud
us-west-1-amazon.ua-sec[.]cloud	us-west-1-aws.gov-ua[.]cloud
us-west-2.gov-ua[.]cloud	us-west-2.ua-energy[.]cloud
us-west-2.ua-sec[.]cloud	us-west-2-aws.mfa-gov[.]cloud
us-west-2-aws.s3-ua[.]cloud	us-west-2-aws.ua-energy[.]cloud

References

- https://cert.gov.ua/article/6281076
- https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/
- https://media.defense.gov/2024/Oct/09/2003562611/-1/-1/0/CSA-UPDATE-ON-SVR-CYBER-OPS.PDF
- https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/?msockid=392e4194f0f26165030055c3f1de6080
- https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/?msockid=392e4194f0f26165030055c3f1de6080

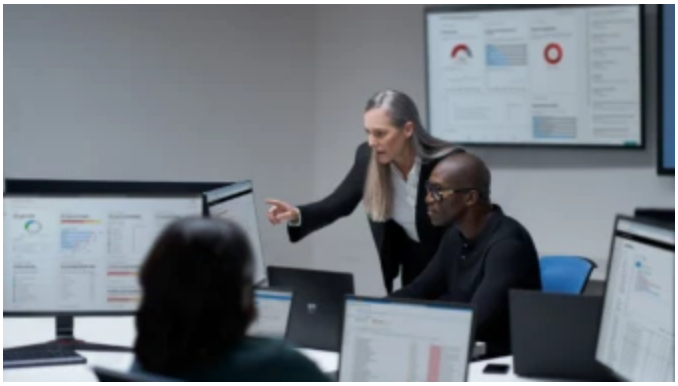
Learn more

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.

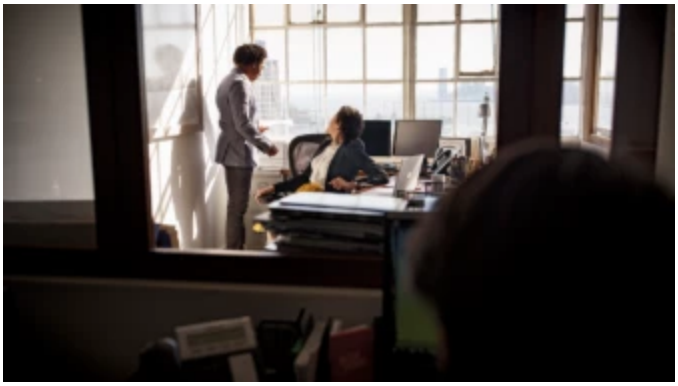
To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

Related Posts



Midnight Blizzard: Guidance for responders on nation-state attack

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.



Midnight Blizzard conducts targeted social engineering over Microsoft Teams

Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by the threat actor that Microsoft tracks as Midnight Blizzard (previously tracked as NOBELIUM).

MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone

Microsoft security researchers have discovered a post-compromise capability we're calling MagicWeb, which is used by a threat actor we track as NOBELIUM to maintain persistent access to compromised environments.