THREAT BULLETINS

Russian Threat Actor Midnight Blizzard Conducts Large Scale Spearphishing Campaign Containing RDP Files

TLP:WHITE

Oct 29, 2024

On October 29, 2024, Microsoft Threat Intelligence released a blog report regarding the observance of Russian threat actor Midnight Blizzard conducting a spearphishing campaign delivering phishing emails to individuals in government, academia, defense, non-governmental organizations, and other sectors. According to Microsoft's investigation, the objective of the ongoing activity is assessed to be likely based on reconnaissance.

During their phishing campaign, the threat actors were observed impersonating Microsoft employees and sending emails with social engineering lures related to Microsoft, Amazon Web Services (AWS), and the concept of Zero Trust. Through the phishing emails, remote desktop protocol (RDP) configuration files signed with a LetsEncrypt certificate were delivered. The RDP configuration files contain automatic settings and resource mappings that are established after successfully connecting to an RDP server controlled by the threat actor.

Successfully executed attacks provided threat actors with sensitive information from the compromised device as the threat actor-controlled server mapped the victims' local device 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. Additionally, the unauthorized access could allow the threat actor to deploy malware on local drives and mapped network shares to maintain persistence once the RDP session is terminated.

Health-ISAC is sharing this report for your situational awareness and encourages members to incorporate the mitigation strategies provided in this report.

The full alert, which includes additional information, mitigations, hunting queries, and indicators of compromise, can be found here.

Recommendations:

Health-ISAC recommends that organizations review and assess their level of risk to the reported activity and take the necessary actions to ensure appropriate security measures are implemented. Additionally, organizations should review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Indicators contained within this alert are available in the H-ISAC WHITE TAXII feed:

Reference(s)	Microsoft Blog, HHS, Security Week

Threat Indicator(s)

Domain(s):

eu-south-2[.]gov-sk[.]cloud
eu-southeast-1-aws[.]ukrainesec[.]cloud
us-west-1[.]aws-ukraine[.]cloud
eu-south-2-aws[.]mfa-gov[.]cloud
eu-west-1-aws[.]s3-esa[.]cloud
eu-central-2-aws[.]gov-sk[.]cloud
eu-west-3-aws[.]mil-pt[.]cloud
eu-west-3[.]amazonsolutions[.]cloud

eu-south-2-aws[.]mil-pt[.]cloud
eu-east-1-aws[.]dep-no[.]cloud
eu-west-3-aws[.]regeringskansliet-se[.]cloud
eu-west-1-aws[.]s3-nato[.]cloud
ca-central-1[.]ua-gov[.]cloud
eu-west-1-aws[.]amazonsolutions[.]cloud
eu-east-1-aws[.]ua-gov[.]cloud
eu-central-1[.]ua-sec[.]cloud
us-west-2[.]gov-ua[.]cloud
us-east-1-aws[.]s3-ua[.]cloud
us-east-2-aws[.]ukrtelecom[.]cloud
eu-north-1[.]s3-be[.]cloud
central-2-aws[.]ua-mil[.]cloud
eu-south-2-aws[.]s3-ua[.]cloud
eu-north-1[.]mil-be[.]cloud
us-west-1[.]ukrtelecom[.]cloud
eu-north-1-aws[.]ua-energy[.]cloud
eu-south-2[.]ua-sec[.]cloud
eu-west-3-aws[.]aws-ukraine[.]cloud
eu-central-2-aws[.]amazonsolutions[.]cloud
eu-west-1-aws[.]ua-sec[.]cloud
eu-south-2[.]ukrainesec[.]cloud
eu-north-1[.]ncfta[.]cloud
eu-south-2[.]mil-pl[.]cloud
eu-south-2[.]dep-no[.]cloud
eu-central-1-aws[.]mindef-nl[.]cloud
central-2-aws[.]ukrainesec[.]cloud
eu-central-2-aws[.]dep-no[.]cloud
eu-south-2[.]gov-pl[.]cloud
eu-north-1[.]mil-pl[.]cloud
us-west-2[.]ua-energy[.]cloud
eu-west-2-aws[.]mzv-sk[.]cloud
eu-central-1[.]s3-nato[.]cloud
eu-west-1-aws[.]dep-no[.]cloud
eu-central-1[.]mindef-nl[.]cloud
eu-southeast-1-aws[.]dep-no[.]cloud
eu-central-2-aws[.]ua-gov[.]cloud
eu-central-1-aws[.]ncfta[.]cloud
eu-east-1-aws[.]ua-sec[.]cloud
eu-west-2-aws[.]s3-esa[.]cloud
us-east-2-aws[.]ua-gov[.]cloud
central-2-aws[.]ukrtelecom[.]cloud
eu-south-2-aws[.]regeringskansliet-se[.]cloud
eu-south-2-aws[.]quirinale[.]cloud
eu-central-1-aws[.]msz-pl[.]cloud

eu-north-1-aws[.]regeringskansliet-se[.]cloud
eu-west-3-aws[.]gov-sk[.]cloud
eu-west-1[.]minbuza[.]cloud
eu-south-1-aws[.]ua-gov[.]cloud
eu-east-1-aws[.]amazonsolutions[.]cloud
eu-south-2-aws[.]s3-esa[.]cloud
us-east-2[.]ukrainesec[.]cloud
eu-southeast-1-aws[.]s3-ua[.]cloud
eu-central-1-aws[.]gov-trust[.]cloud
eu-west-3-aws[.]mzv-sk[.]cloud
eu-west-3[.]mindef-nl[.]cloud
eu-southeast-1-aws[.]gov-sk[.]cloud
eu-west-3[.]s3-ua[.]cloud
ap-northeast-1-aws[.]ukrainesec[.]cloud
eu-central-1-aws[.]quirinale[.]cloud
us-east-console[.]ua-energy[.]cloud
eu-west-3-aws[.]s3-ua[.]cloud
eu-north-1-aws[.]ua-gov[.]cloud
eu-south-1-aws[.]dep-no[.]cloud
eu-central-2-aws[.]gov-pl[.]cloud
eu-west-2-aws[.]gov-pl[.]cloud
us-east-1-aws[.]ua-sec[.]cloud
eu-southeast-1-aws[.]mzv-sk[.]cloud
ap-northeast-1-aws[.]s3-ua[.]cloud
eu-central-1-aws[.]ua-gov[.]cloud
eu-west-3-aws[.]msz-pl[.]cloud
eu-central-1[.]mfa-gov[.]cloud
eu-west-1[.]msz-pl[.]cloud
eu-west-1[.]gov-sk[.]cloud
eu-central-2-aws[.]s3-be[.]cloud
eu-south-2[.]s3-de[.]cloud
eu-north-1-aws[.]minbuza[.]cloud
eu-west-1-aws[.]mil-be[.]cloud
eu-south-2-aws[.]mil-be[.]cloud
eu-north-1-aws[.]gov-sk[.]cloud
eu-west-2-aws[.]mindef-nl[.]cloud
eu-central-1[.]s3-be[.]cloud
eu-east-1-aws[.]mzv-sk[.]cloud
us-east-1-aws[.]mfa-gov[.]cloud
eu-west-1-aws[.]mil-pl[.]cloud
eu-west-1-aws[.]aws-ukraine[.]cloud
eu-west-1[.]ua-gov[.]cloud
eu-west-1[.]mil-be[.]cloud
eu-south-2-aws[.]mzv-sk[.]cloud
eu-east-1-aws[.]ukrtelecom[.]cloud

eu-central-2-aws[.]mzv-sk[.]cloud
eu-north-1-aws[.]mil-pl[.]cloud
eu-west-2-aws[.]s3-ua[.]cloud
eu-central-2-aws[.]mil-pl[.]cloud
eu-central-1[.]ukrtelecom[.]cloud
eu-west-3[.]mil-be[.]cloud
eu-west-1[.]s3-ua[.]cloud
eu-west-2-aws[.]gov-sk[.]cloud
eu-west-2-aws[.]mil-be[.]cloud
eu-west-2-aws[.]dep-no[.]cloud
eu-central-1[.]minbuza[.]cloud
eu-east-1-aws[.]gov-sk[.]cloud
eu-west-3[.]presidencia-pt[.]cloud
eu-west-2-aws[.]gv-at[.]cloud
eu-north-1[.]difesa-it[.]cloud
eu-south-1-aws[.]gov-trust[.]cloud
eu-west-3[.]minbuza[.]cloud
eu-west-3-aws[.]gov-pl[.]cloud
eu-east-1-aws[.]quirinale[.]cloud
ca-west-1[.]mfa-gov[.]cloud
eu-west-3[.]ukrainesec[.]cloud
us-west-1-amazon[.]ua-mil[.]cloud
eu-south-2-aws[.]amazonsolutions[.]cloud
us-west-1-amazon[.]ua-energy[.]cloud
eu-south-1-aws[.]mfa-gov[.]cloud
eu-west-2-aws[.]difesa-it[.]cloud
eu-west-1[.]s3-de[.]cloud
eu-north-1[.]s3-ua[.]cloud
eu-east-1-aws[.]s3-de[.]cloud
eu-east-1-aws[.]mil-pl[.]cloud
eu-south-1-aws[.]mzv-sk[.]cloud
eu-southeast-1-aws[.]mzv-cz[.]cloud
eu-south-1-aws[.]s3-de[.]cloud
eu-central-1-aws[.]presidencia-pt[.]cloud
eu-central-1[.]msz-pl[.]cloud
eu-central-1-aws[.]gov-sk[.]cloud
eu-southeast-1-aws[.]amazonsolutions[.]cloud
eu-west-2-aws[.]ua-sec[.]cloud
us-west-2-aws[.]ua-energy[.]cloud
eu-southeast-1-aws[.]difesa-it[.]cloud
eu-west-3-aws[.]minbuza[.]cloud
eu-central-2-aws[.]aws-ukraine[.]cloud
eu-south-2-aws[.]ncfta[.]cloud
eu-central-1-aws[.]mzv-sk[.]cloud
eu-southeast-1-aws[.]s3-esa[.]cloud

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

eu-south-2[.]mindef-nl[.]cloud
eu-east-1-aws[.]mindef-nl[.]cloud
eu-south-1-aws[.]difesa-it[.]cloud
eu-west-3[.]s3-be[.]cloud
eu-west-1[.]difesa-it[.]cloud
eu-north-1[.]regeringskansliet-se[.]cloud
eu-central-1-aws[.]s3-ua[.]cloud
eu-west-2-aws[.]amazonsolutions[.]cloud
eu-southeast-1-aws[.]aws-ukraine[.]cloud
us-east-2[.]aws-ukraine[.]cloud
eu-west-3-aws[.]mindef-nl[.]cloud
eu-south-2-aws[.]msz-pl[.]cloud
eu-west-1[.]regeringskansliet-se[.]cloud
eu-north-1[.]mzv-sk[.]cloud
eu-west-3-aws[.]s3-be[.]cloud
eu-southeast-1-aws[.]gov-trust[.]cloud
us-west-1-aws[.]gov-ua[.]cloud
us-west-1[.]ua-gov[.]cloud
central-2-aws[.]ua-sec[.]cloud
eu-central-1[.]quirinale[.]cloud
eu-southeast-1-aws[.]msz-pl[.]cloud
eu-west-3-aws[.]dep-no[.]cloud
eu-north-1[.]gv-at[.]cloud
eu-east-1-aws[.]minbuza[.]cloud
eu-north-1-aws[.]gov-pl[.]cloud
eu-south-1-aws[.]minbuza[.]cloud
eu-west-2-aws[.]s3-de[.]cloud
eu-north-1-aws[.]dep-no[.]cloud
ca-west-1[.]ukrtelecom[.]cloud
eu-north-1-aws[.]quirinale[.]cloud
eu-central-1-aws[.]regeringskansliet-se[.]cloud
eu-west-3-aws[.]mil-pl[.]cloud
eu-south-2[.]s3-esa[.]cloud
eu-central-1[.]regeringskansliet-se[.]cloud
eu-south-1-aws[.]mil-be[.]cloud
eu-east-1-aws[.]regeringskansliet-se[.]cloud
eu-north-1-aws[.]mil-be[.]cloud
eu-central-2-aws[.]ukrtelecom[.]cloud
eu-north-1[.]gov-ua[.]cloud
us-east-2-aws[.]gov-ua[.]cloud
eu-west-1-aws[.]gov-sk[.]cloud
eu-east-1-aws[.]msz-pl[.]cloud
eu-south-1-aws[.]gov-pl[.]cloud
eu-west-2-aws[.]s3-nato[.]cloud
eu-south-2[.]s3-nato[.]cloud

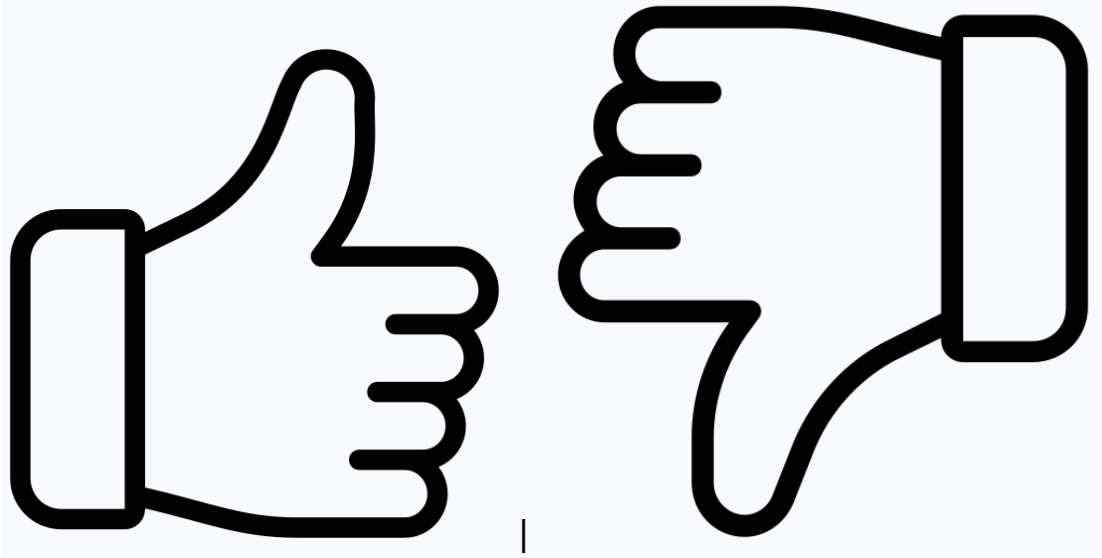
eu-southeast-1-aws[.]quirinale[.]cloud
ca-west-1[.]aws-ukraine[.]cloud
eu-west-1-aws[.]gov-pl[.]cloud
eu-west-2-aws[.]minbuza[.]cloud
eu-southeast-1-aws[.]mil-pl[.]cloud
eu-central-1-aws[.]gov-pl[.]cloud
us-east-2[.]gov-ua[.]cloud
us-east-1-aws[.]ua-gov[.]cloud
eu-north-1-aws[.]presidencia-pt[.]cloud
eu-west-1-aws[.]s3-de[.]cloud
eu-southeast-1-aws[.]s3-de[.]cloud
eu-central-1[.]mil-be[.]cloud
eu-west-3-aws[.]gov-trust[.]cloud
us-east-console[.]aws-ukraine[.]cloud
eu-west-3-aws[.]quirinale[.]cloud
eu-west-2-aws[.]msz-pl[.]cloud
eu-southeast-1-aws[.]s3-be[.]cloud
eu-south-2[.]s3-be[.]cloud
eu-south-1-aws[.]s3-be[.]cloud
eu-west-1[.]mzv-sk[.]cloud
eu-central-1-aws[.]ukrainesec[.]cloud
us-west-2[.]ua-sec[.]cloud
eu-south-2-aws[.]gov-pl[.]cloud
eu-west-3[.]mzv-sk[.]cloud
us-west-1-amazon[.]ua-sec[.]cloud
eu-north-1-aws[.]s3-de[.]cloud
eu-west-3-aws[.]ua-mil[.]cloud
eu-south-2-aws[.]s3-de[.]cloud
eu-central-1-aws[.]mfa-gov[.]cloud
eu-north-1-aws[.]ncfta[.]cloud
eu-west-1-aws[.]minbuza[.]cloud
eu-west-1[.]s3-esa[.]cloud
eu-central-2-aws[.]mil-be[.]cloud
eu-south-2[.]mil-be[.]cloud
eu-central-1-aws[.]s3-be[.]cloud
eu-west-1-aws[.]ukrainesec[.]cloud
eu-north-1-aws[.]difesa-it[.]cloud
eu-west-1-aws[.]s3-be[.]cloud
eu-west-1-aws[.]quirinale[.]cloud
eu-south-2-aws[.]dep-no[.]cloud
eu-north-1[.]gov-trust[.]cloud
eu-central-1-aws[.]minbuza[.]cloud
eu-south-2-aws[.]ua-gov[.]cloud

Alert ID 8df81209

This Alert has 3 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback
was this helpful?



Tags Midnight Blizzard, White, UNC2452, spearphishing, APT29, COZY BEAR

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.