Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks

: 12/17/2024

APT & Targeted Attacks

APT group Earth Koshchei, suspected to be sponsored by the SVR, executed a large-scale rogue RDP campaign using spear-phishing emails, red team tools, and sophisticated anonymization techniques to target high-profile sectors.

By: Feike Hacquebord, Stephen Hilt December 17, 2024 Read time: 12 min (3117 words)

Summary

- Earth Koshchei's rogue remote desktop protocol (RDP) campaign used an attack methodology involving an RDP relay, rogue RDP server, and a malicious RDP configuration file, leading to potential data leakage and malware installation.
- Earth Koshchei is known for constantly innovating and using a variety of methods. In this campaign, they leveraged red team tools for espionage and data exfiltration.
- The spear-phishing emails used in Earth Koshchei's campaign were designed to deceive recipients into using a rogue RDP configuration file, causing their machines to connect to one of the group's 193 RDP relays.

- Earth Koshchei's campaign showed significant preparation, registering more than 200 domain names between August and October of this year.
- The group used anonymization layers like commercial VPN services, TOR, and residential proxies to mask their operations, enhance their stealthiness, and complicate attribution efforts.

Red teaming provides essential tools and testing methodologies for organizations to strengthen their security defenses. Cybercriminals and advanced persistent threat (APT) actors pay close attention to new methods and tools red teams develop, and they may repurpose them with a malicious intent.

In October 2024, an APT group that Trend Micro tracks as Earth Koshchei (also known as APT29 and Midnight Blizzard), likely used a rogue remote desktop protocol (RDP) attack methodology against numerous targets. This methodology was described earlier in 2022 by Black Hills Information Security in detail. The attack technique is called “rogue RDP”, which involves an RDP relay, a rogue RDP server, and a malicious RDP configuration file. A victim of this technique would give partial control of their machine to the attacker, potentially leading to data leakage and malware installation.

Earth Koshchei’s rogue RDP campaign reached its peak on October 22, when spear-phishing emails were sent to governments and armed forces, think tanks, academic researchers and Ukrainian targets. These emails were designed to deceive recipients into using a rogue RDP configuration file attached to the message. When opened, this RDP configuration file would instruct the target computer to try to connect to a foreign RDP server through one of the 193 RDP relays Earth Koshchei had set up.

Even though many of the targeted organizations are likely to have outgoing RDP connections blocked, it is still possible that in some cases RDP connections were not; for example, like in a home office environment or organizations that have less strict security in place. In the attack setup, it is also possible to use a non-standard port for the RDP relay, thus avoiding firewall rules. We believe that the spear-phishing email wave was preceded by earlier, very targeted and barely audible campaigns that ended abruptly with a final loud bang on October 22.

Microsoft and Amazon publicly attributed the rogue RDP campaign to Midnight Blizzard and APT29, which we track as Earth Koshchei. While we cannot make an independent attribution with high confidence to Earth Koshchei, we noticed they used some of their typical tactics, techniques and procedures (TTP) in the campaign and we could significantly expand on the indicators of compromise (IOCs) that had been made public so far by Microsoft and Cert-UA.

The threat group behind Earth Koshchei is allegedly sponsored by the Russian Foreign Intelligence Service (SVR), according to US and UK law enforcement. Earth Koshchei is characterized by its persistent targeting of diplomatic, military, energy, telecom, and IT companies in Western countries over many years, with the motivation believed to be primarily espionage. Earth Koshchei is known for adapting their TTPs and has deployed several techniques in the past like password spraying, brute forcing dormant accounts and watering hole attacks.

In Trend Micro’s global threat intelligence, the rogue RDP spear-phishing emails were found to have been sent to many targets, including the military, ministries of foreign affairs, targets in Ukraine and academic researchers. The scale of the RDP campaign was huge: The number of high-profile targets – about 200 – we saw in one day was about the same size as another APT group like Pawn Storm targets in weeks.

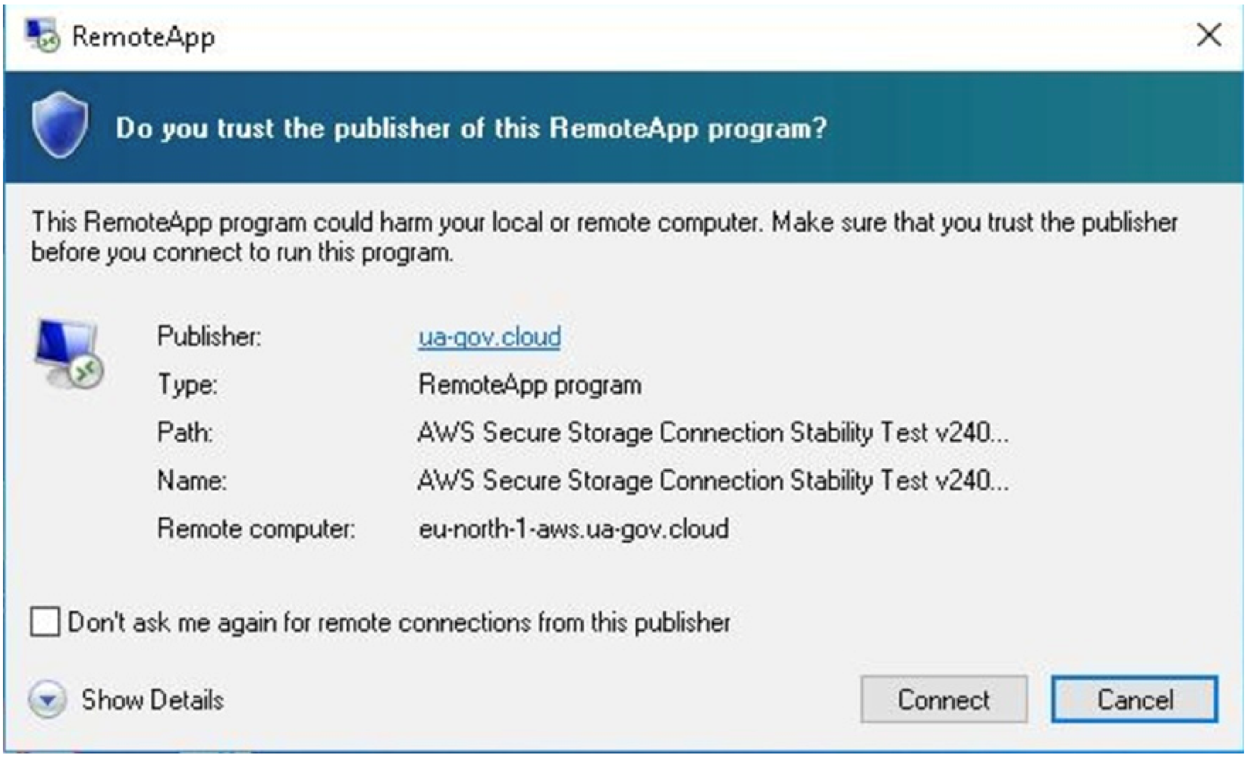
This was not the first time Earth Koshchei was linked to a massive spear-phishing campaign: In May 2021, they also sent spear-phishing emails to thousands of individual accounts.

Preparations for the campaign had already started as early as August 7-8, when the adversary began to register domain names whose names suggest they would be used against targets that have a relationship with the Australian and Ukrainian governments. The last domain, registered on October 20, was apparently meant to target an organization with a link to the Netherlands' Ministry of Foreign Affairs. In between, almost 200 domain names were registered, many of which suggest the target the adversaries had in mind.

This report aims to give a detailed explanation of what happened around Earth Koshchei's RDP campaign, how the previously published red team methodology was used, to describe the scale of the campaign, and what anonymization layers were used. In particular, we discuss the infrastructure of the attack: We reveal 193 domains that were actively used against various organizations and 34 rogue RDP backend servers. In our assessment, these 193 domain names served as proxies to the 34 backends that look like the real rogue RDP servers of Earth Koshchei. We have seen evidence that some of the suspected rogue RDP backend servers, in combination with some of the RDP relays, were used for data exfiltration from October 18 to 21 for two military organizations and one cloud provider.

Rogue RDP configuration file: From red team tool to targeted attacks

We investigated one of the RDP configuration files that was sent to an academic researcher in Europe. The file specified a remote server to contact: *eu-south-2-aws[.]zero-trust[.]solutions*. Although the hostname suggests a legitimate Amazon Web Services (AWS) server, it is controlled by Earth Koshchei. The configuration redirects all local drives, printers, COM ports, smart cards, and clipboards, allowing remote access to the victim's local machine. Obviously, this can be exploited for data exfiltration. After a successful connection is established, a remote application called *AWS Secure Storage Connection Stability Test v24091285697854* is executed. At the time of our analysis, the remote servers were already down, so we could not check what action this remote application would execute.



RemoteApp

Do you trust the publisher of this RemoteApp program?

This RemoteApp program could harm your local or remote computer. Make sure that you trust the publisher before you connect to run this program.

Publisher: ua-gov.cloud
Type: RemoteApp program
Path: AWS Secure Storage Connection Stability Test v240...
Name: AWS Secure Storage Connection Stability Test v240...
Remote computer: eu-north-1-aws.ua-gov.cloud

☐ Don't ask me again for remote connections from this publisher

Figure 1. RDP connection (Source: VirusTotal)
download

This kind of attack scenario was described in 2022 by Mike Felch in a Black Hill blog post. It is more complex to set up than it might initially appear. An attacker's goal is to minimize suspicious warnings and reduce the need for user interaction as much as possible. Therefore, Felch proposed an idea of using a man-in-the-middle (MITM) proxy in front of the actual rogue RDP servers and use the Python Remote Desktop Protocol MITM tool (PyRDP).

As described in Black Hill's blog, the RDP attack begins when the victim attempts to use the .RDP file that was sent in a spear-phishing attack. This then makes an outbound RDP connection to the attacker's first system (Figure 2). Here, the attacker employs PyRDP to act as a MITM proxy, intercepting the victim's connection request. Instead of connecting the victim to what they think is a legitimate server, the PyRDP proxy redirects the session to a rogue server controlled by the attacker. This setup enables the attacker to pose as the legitimate server to the victim, effectively hijacking the session. By doing so, the attacker gains full visibility and control over the communication between the victim and the RDP environment.

Upon establishing the connection, the rogue server mimics the behavior of a legitimate RDP server and exploits the session to carry out various malicious activities. A primary attack vector involves the attacker deploying malicious scripts or altering system settings on the victim's machine. Additionally, the PyRDP proxy facilitates access to the victim's file system, enabling the attacker to browse directories, read or modify files, and inject malicious payloads. This capability renders the attack particularly hazardous, as it permits immediate and untraceable compromise of the victim's endpoint.

The final stage of the attack often involves data exfiltration, where the attacker utilizes the compromised session to extract sensitive information such as passwords, configuration files, proprietary data, or other confidential materials. The PyRDP proxy ensures that any data stolen or commands executed are funneled back to the attacker without alerting the victim. Tools like RogueRDP further enhance the attacker's capabilities by automating the creation of convincing RDP files, enticing users to initiate compromised sessions.

This method not only demonstrates the danger of MITM attacks in RDP environments but also emphasizes the critical need for security measures within organizations.

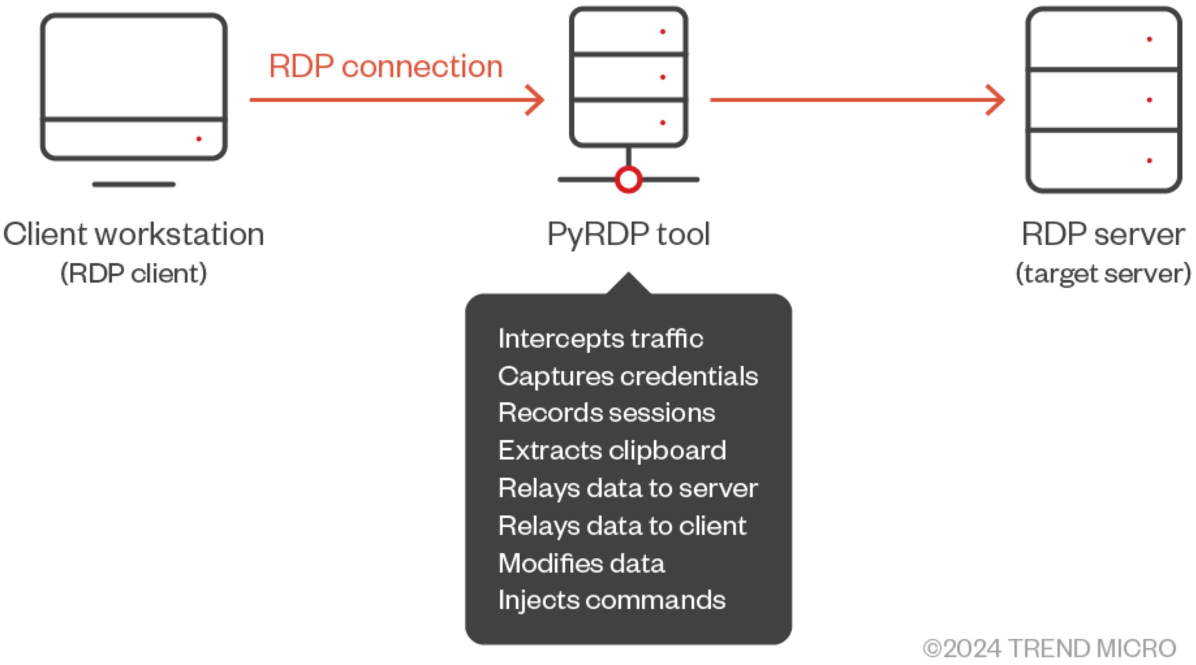


Figure 2. Setup of the RDP attack method
download

Configuration setting	Value	Purpose in attack
full address	eu-north-1.regeringskansliet-se.cloud	Redirects the victim to a malicious server.
alternate full address	eu-north-1.regeringskansliet-se.cloud	Backup address for ensuring the connection reaches the attacker's server.
drivestoredirect	s:*	Redirects all drives, enabling PyRDP to crawl and exfiltrate the victim's files.
redirectprinters, redirectclipboard, redirectsmartcards, etc.	1	Enables redirection of client devices and resources for exploitation. As an example, PyRDP can read the contents of the clipboard.
remoteapplicationname	AWS Secure Storage Connection Stability Test v24091285697854	Misleads the victim into thinking they are accessing a legitimate application.
remoteapplicationprogram	AWS Secure Storage Connection Stability Test v24091285697854	Specifies the application that will be executed and displayed to the victim during the RDP session.

		This is a critical part of the attack because it allows the attacker to simulate a legitimate application environment.
prompt for credentials	0	Suppresses security prompts, increasing the stealth of the attack.
authentication level	2	Lowers the security of the connection, facilitating exploitation.

Table 1. An example of one of the analyzed RDP configuration files

RDP configuration files like that shown in Table 1 aid the attack by trying to exploit victims by redirecting their RDP sessions to a malicious server. Tools like PyRDP enhance the attack by enabling the interception and manipulation of RDP connections. PyRDP can automatically crawl shared drives redirected by the victim and save their contents locally on the attacker's machine, facilitating seamless data exfiltration. The attack starts by leveraging the full address and alternate full address fields to redirect the victim to a malicious server. Additional fields, such as *remoteapplicationprogram* and *remoteapplicationname*, specify an application to launch, creating a false sense of legitimacy. Upon connection, the malicious server likely uses PyRDP to perform tasks including crawling redirected drives and exfiltrating data.

This attack demonstrates how tools like PyRDP can automate and enhance malicious activities, such as systematically crawling redirected drives to exfiltrate data. Notably, no malware is installed on the victim’s machines per se. Instead, a malicious configuration file with dangerous settings facilitates this attack, making it a stealthier living off the land operation that is likely to evade detection. We believe that Earth Koshchei made use of the final stage of this methodology. Our analysis reproduced and validated 193 proxy servers whose hostnames often suggest the intended target and identified 34 servers that likely served as the rogue RDP backend servers.

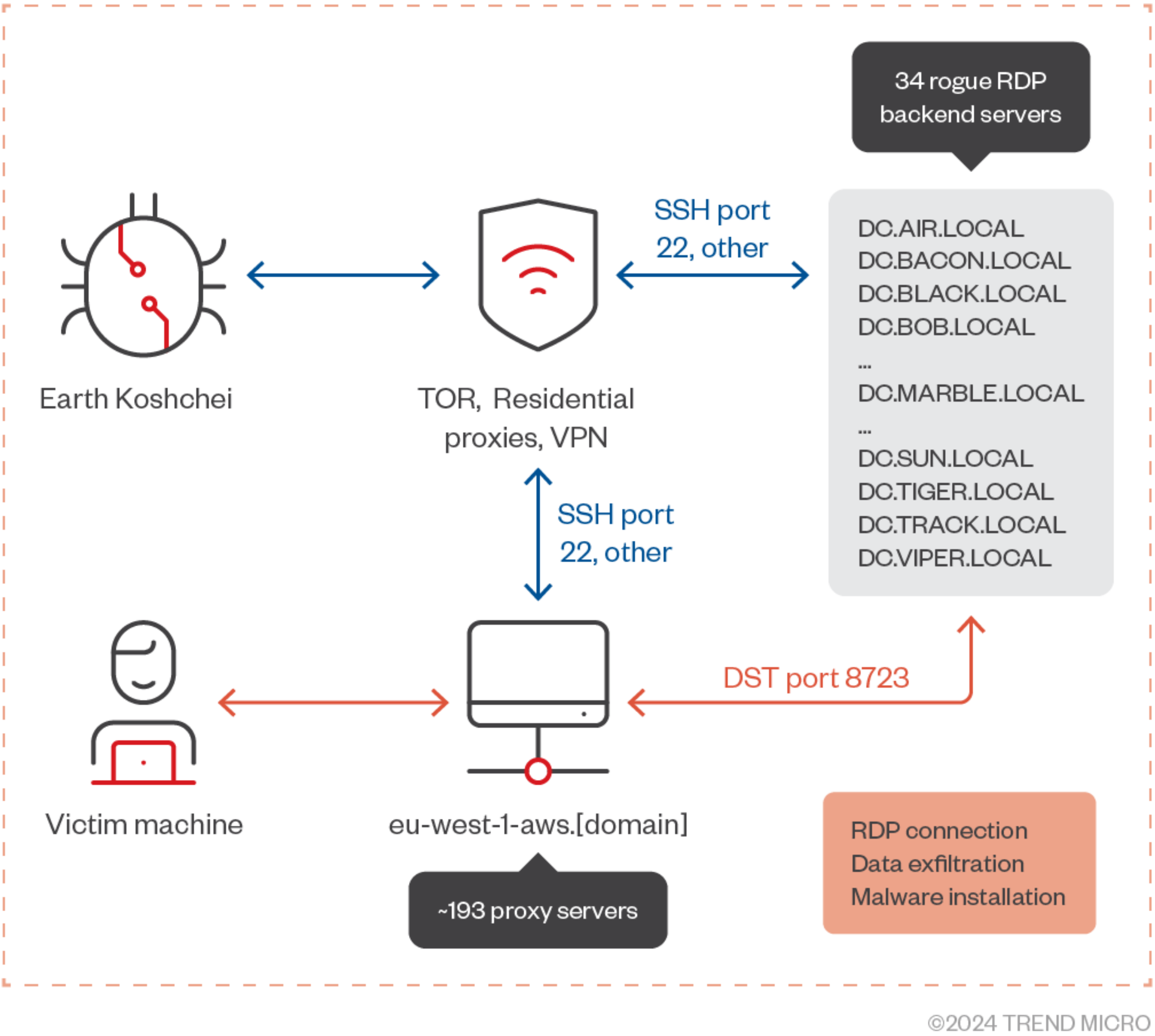


Figure 3. Schema of how Earth Koshchei controls their infrastructure
download

As shown in Figure 3, a victim machine makes an RDP connection to one of the rogue RDP backend servers through connecting to one of the 193 proxy servers. Earth Koshchei controls the proxy servers and the rogue RDP server with SSH over Tor, VPN services and residential proxies.

Anonymization layers

One of the characteristic TTPs of Earth Koshchei is the abundant usage of anonymization layers like commercial VPN services, TOR and residential proxy service providers. The usage of large numbers of (residential) proxies makes defense strategies based on blocking IP address indicators ineffective. The attacker masquerades its malicious traffic in networks that are shared by legitimate users and can spread their attacks over thousands of rapidly changing IP addresses that are used by home users.

These anonymization layers were also used in the recent RDP campaign. We assess with medium confidence that Earth Koshchei had been using TOR exit nodes for weeks to control more than 200 VPS server IP addresses and 34 rogue RDP servers that were set up in the RDP campaign. The spear-phishing emails were sent from at least five legitimate mail servers that looked to be compromised from the outside. We have evidence from our telemetry that Earth Koshchei accessed them through the webmail server by using various residential proxy providers and commercial VPN services.

Earth Koshchei or another actor had likely compromised the email servers weeks before the campaign's peak on October 22. In our telemetry, we counted about 90 unique IP addresses that were used to connect to the compromised email servers to send out the spam. Among the 90 IP addresses were exit nodes from a relatively new commercial peer-to-peer VPN service provider that accepts cryptocurrency payments. Other IP addresses were likely to be exit nodes of a couple of residential proxy service providers.

Timeline

We assess that Earth Koshchei has set up over 200 domain names between August 7 to October 20 (Figures 4 and 5). For 193 of these domain names, we were able to validate that these domains were indeed set up for the RDP campaign. Hence, we assess with medium confidence they were used by Earth Koshchei. There are a couple of dozen other domain names that look to belong to the Earth Koshchei intrusion set, but we did not find evidence these were used.

The domain names were set up in batches and always during weekdays, except for one domain that apparently was aimed to target an organization related to the Netherlands' Ministry of Foreign Affairs. The nature of most of the domain names clearly suggests the intended target (Figure 6), but we have only been able to verify the suggested target with the actual target in a couple of cases. In August 2024, the registered domain names suggested targeting against governments and military in Europe, US, Japan, Ukraine and Australia. At the end of this month, domain names were registered that look to be related to cloud providers and IT companies. Then, in September 2024, there were batches of domain names that appeared to be based on several think thanks and non-profit organizations. There were also several domain names related to online virtual platforms like Zoom, Google Meet, and Microsoft Teams.

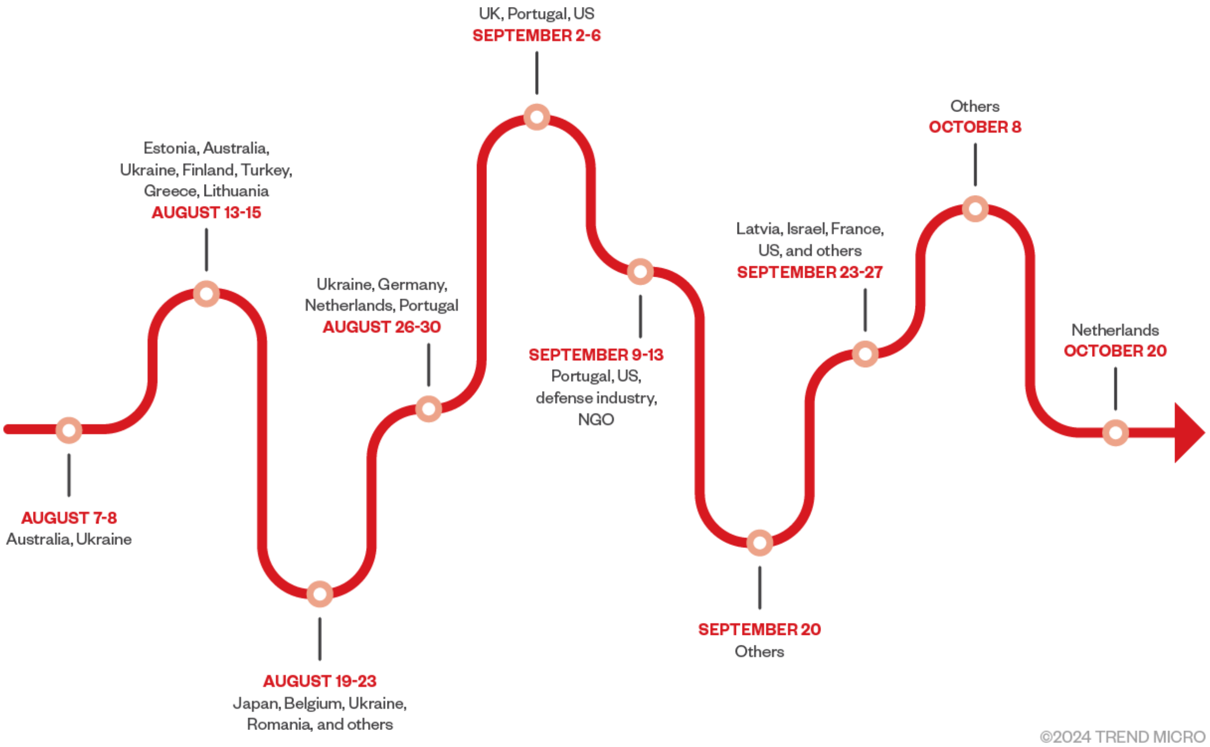

AUGUST 7-8
Australia, Ukraine
Estonia, Australia, Ukraine, Finland, Turkey, Greece, Lithuania
AUGUST 13-15
AUGUST 19-23
Japan, Belgium, Ukraine, Romania, and others
Ukraine, Germany, Netherlands, Portugal
AUGUST 26-30
UK, Portugal, US
SEPTEMBER 2-6
SEPTEMBER 9-13
Portugal, US, defense industry, NGO
SEPTEMBER 20
Others
Latvia, Israel, France, US, and others
SEPTEMBER 23-27
Others
OCTOBER 8
Netherlands
OCTOBER 20
©2024 TREND MICRO

Figure 4. Timeline of domain name registrations (August to October 2024)

download

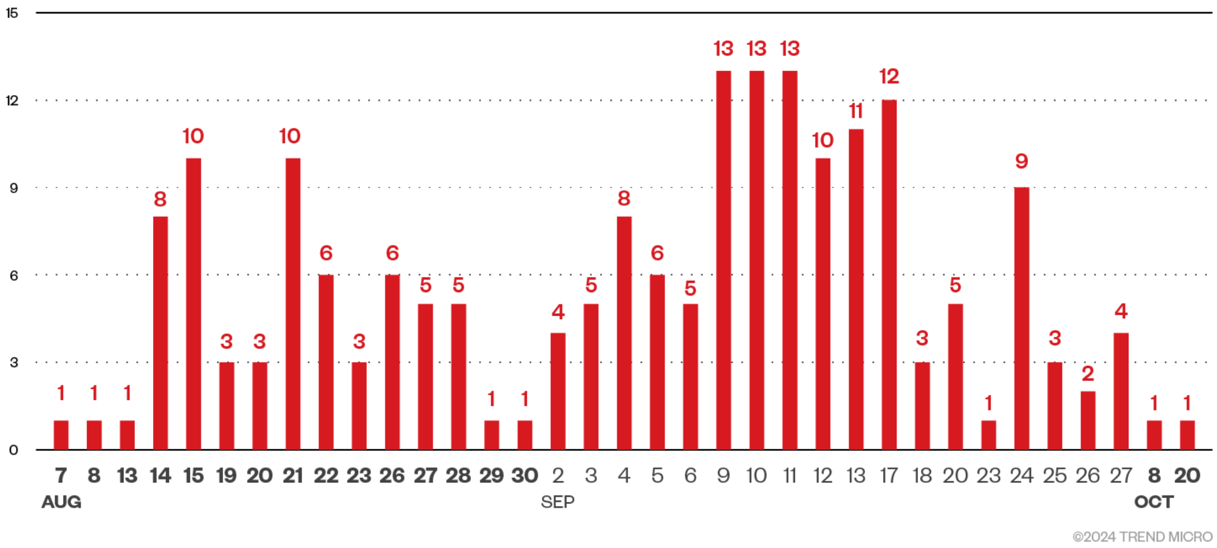


Figure 5. Distribution of domain names that were created over time

download

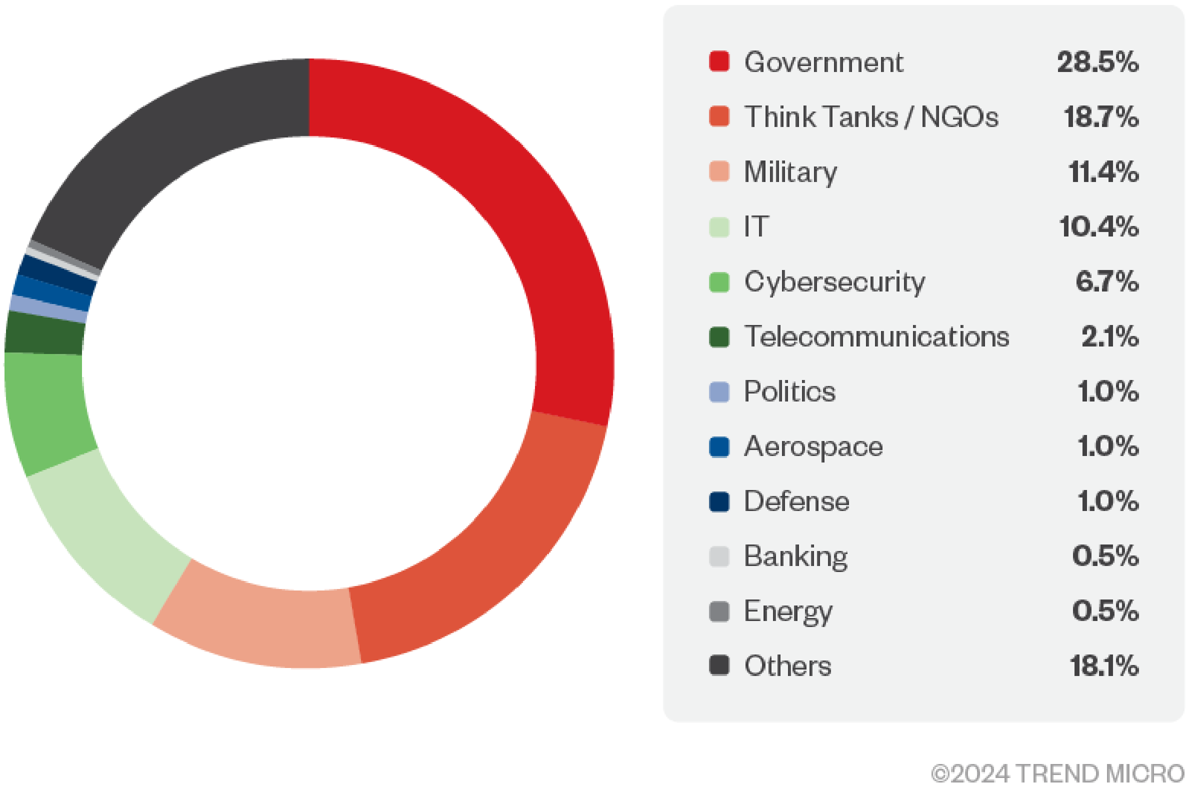


Figure 6. Number of domains per industry

download

The backend rogue RDP servers were most likely set up from September 26 until October 20. We were not able to recover explicit email samples that might have been sent before October 22, but we do think that the rogue RDP servers were used in data exfiltration on October 18 to 21 against targets in the military and a cloud provider. It is plausible that there were other targets before October 22, but we do not have explicit evidence for that.

Attribution

We attribute the RDP campaign to Earth Koshchei with a medium confidence level based on TTPs, victimology, and research from other companies. The TTPs that were used in the rogue RDP campaign are quite typical for Earth Koshchei: The targeting and abundant usage of residential proxy service providers, TOR and commercial VPN services stood out. We have been able to attribute 193 proxy servers and their domain names and 34 rogue RDP servers to Earth Koshchei with a medium confidence level.

Outlook and conclusions

Threat actors like Earth Koshchei show a consistent interest in their targets over the years. The targets include governments, military, defense industry, telecommunications companies, think tanks, cybersecurity companies, academic researchers and IT companies. Earth Koshchei uses new methodologies over time for their espionage campaigns. They not only pay close attention to old and new vulnerabilities that help them in getting initial access, but they also look at the methodologies and tools that red teams develop.

A prime example of this is their usage of rogue RDP servers, most likely inspired by a 2022 blog post from an information security company. This is a perfect example of an APT group utilizing red team toolkits to lessen their work on the attack itself and being able to focus more on targeting organizations with advanced social engineering. It helps them to ensure they can extract the maximum amount of data and information from their targets in the shortest amount of time.

We think that before the massive spear-phishing campaign on October 22, Earth Koshchei had more stealthy campaigns. This is evidenced by traces of data exfiltration through some of their RDP relays. The campaigns probably became less effective over time, so Earth Koshchei did one last scattergun campaign where most of the attacker infrastructure got burned. This makes them a dangerous adversary that will use different methodologies to reach their goals.

Earth Koshchei makes extensive usage of anonymization layers like TOR, VPN and residential proxy services. Using these anonymization layers makes attribution much harder, but not impossible in all cases. We expect that actors like Earth Koshchei will continue with well prepared and innovative attacks against the same targets in the future. Their rogue RDP campaign was of an unusual scale where a lot of infrastructure was used, and the campaign looked well prepared when it comes to social engineering the targets.

Companies that do not block outbound RDP connections to non-trusted servers should do so as soon as possible. One could also block the sending of RDP configuration files over email. Trend Micro detects the rogue RDP configuration files as Trojan.Win32.HUSTLECON.A.

Trend Micro Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Micro customers can access a range of Intelligence Reports and Threat Insights within Trend Micro Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and better prepared for emerging threats. It offers comprehensive information on threat actors, their malicious activities, and the techniques they use. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and respond effectively to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

- Earth Koshchei's Rogue RDP Campaign: Red Team Methods Turned Malicious

Trend Micro Vision One Threat Insights App

- Threat Actor: Earth Koshchei
- Emerging Threats: Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks

Hunting Queries

Trend Micro Vision One Search App

Trend Micro Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Detection of malicious RDP Config file

malName:(*MALCONF* OR *HUSTLECON*) AND eventName:MALWARE_DETECTION

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise (IOC)

The list of indicators of compromise may be found here.

Tags

Latest News | APT & Targeted Attacks | Research