Phishing Campaign Targets Defense and Aerospace Firms Linked to Ukraine Conflict

dti.domaintools.com/phishing-campaign-targets-defense-and-aerospace-firms-linked-to-ukraine-conflict/

March 25, 2025

DomainTools Investigations (DTI) identified a large-scale phishing infrastructure heavily focused on defense and aerospace entities with links to the conflict in Ukraine. The infrastructure comprises a small number of mail servers, each supporting a set of domains designed to spoof that of a specific organization. These domains currently host webmail login pages likely intended to harvest credentials from targeted entities.

This activity is not currently attributed to a specific actor, but available evidence indicates this activity is motivated by cyber espionage, with an emphasis on intelligence collection related to the ongoing conflict in Ukraine.

Detection of Phishing on a Spoofed Ukroboronprom Domain

DTI initially identified a likely phishing page hosted on the domain kroboronprom[.]com a domain spoofing Ukroboronprom, Ukraine’s largest arms manufacturer. The phishing page, located at https[:]//kroboronprom[.]com/sso/login?url=/webmail/?homepage, presents a webmail login prompt. The attackers appear to have built the page using Mailu, an open-source mail server software available on GitHub.

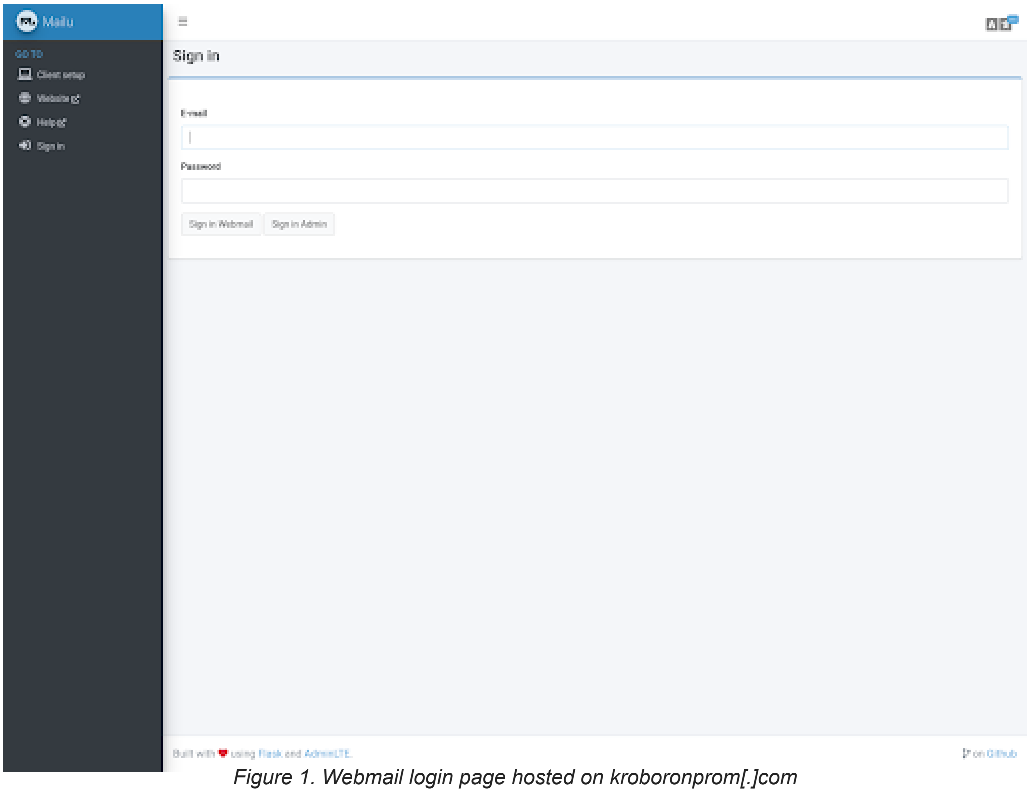


Figure 1. Webmail login page hosted on kroboronprom[.]com

Analysis using DomainTools Iris revealed that the kroboronprom[.]com domain was first seen on December 20, 2024, was hosted on GHOSTnet VPS, and displayed the website title "Mailu-Admin | Mailu." The Iris Pivot Engine identified nine other domains with the same website title, hosted on GHOSTnet VPS, and first seen after December 20, 2024[1].

scooby-doo[.]xyz
lucky-guy[.]space
santa-clause[.]online
yellow-unicorn[.]site
sun-flower[.]space
rainbow-pony[.]buzz
don-quixote[.]quest
rocky-jellyfish[.]biz
lucky-turtle[.]ink

Table 1. Domains Likely Related to kroboronprom[.]com

These domains were all registered using the registrar Spaceship. A second search[2] using the Pivot Engine for domains containing a "-" character, registered via Spaceship, hosted on GHOSTnet VPS IP addresses, and first observed after December 20, 2024 revealed three additional domains:

- space-kitty[.]online
- stupid-buddy[.]mom
- hungry-shark[.]sit

Data from urlscan.io ("urlscan") shows that each of these domains hosts a Mailu webmail login page identical to one seen on kroboronprom[.]com, strongly suggesting they are being used for credential theft.

Iris data showed that, with the exception of scooby-doo[.]xyz, all of these serve as MX domains for mail servers, which support a large set of spoofed domains imitating organizations in the defense, aerospace, and IT sectors. These domains were registered via Spaceship and first observed some time between December 21, 2024 and March 4, 2025. In total, investigation into this activity identified 878 spoofed domains with naming conventions that added or changed a few characters in the targeted entity's legitimate domain.

DTI determined how the actor operationalized this infrastructure. However, the most likely scenario involves phishing emails sent to employees of targeted organizations. The actor likely used spoofed domains in the sender field to make the emails appear as if they originated from within the organization. These emails likely contained malicious links or attachments directing recipients to fake webmail login pages designed to steal credentials.

MX Domain	MX IP Address	Spoofed Domain Entity	Number of Spoofed Domains
hungry-shark[.]site	5.230.38[.]154	Norway-based Defense and Aerospace	75
stupid-buddy[.]mom	5.230.75[.]207	France-based Aerospace	101
space-kitty[.]online	5.230.66[.]98	South Korea-based Defense	56
lucky-turtle[.]ink	5.230.36[.]139	France-based Defense	88
rocky-jellyfish[.]biz	5.230.36[.]138	UK-based Defense	48
don-quixote[.]quest	5.230.253[.]157	Sweden-based Defense and Aerospace	57
rainbow-pony[.]buzz	5.230.68[.]43	France-based Defense and Aerospace	65
sun-flower[.]space	5.230.44[.]151	UK-based Defense and Aerospace	68
yellow-unicorn[.]site	5.230.76[.]174	Italy-based Defense and Aerospace	44
lucky-guy[.]space	5.231.1[.]60	Turkey-based Defense	82
santa-clause[.]online	5.231.1[.]57	United States-based IT	93
kroboronprom[.]com	5.230.45[.]244	Ukraine-based Defense	101

Table 2. Mail servers and the entities they were likely used to target

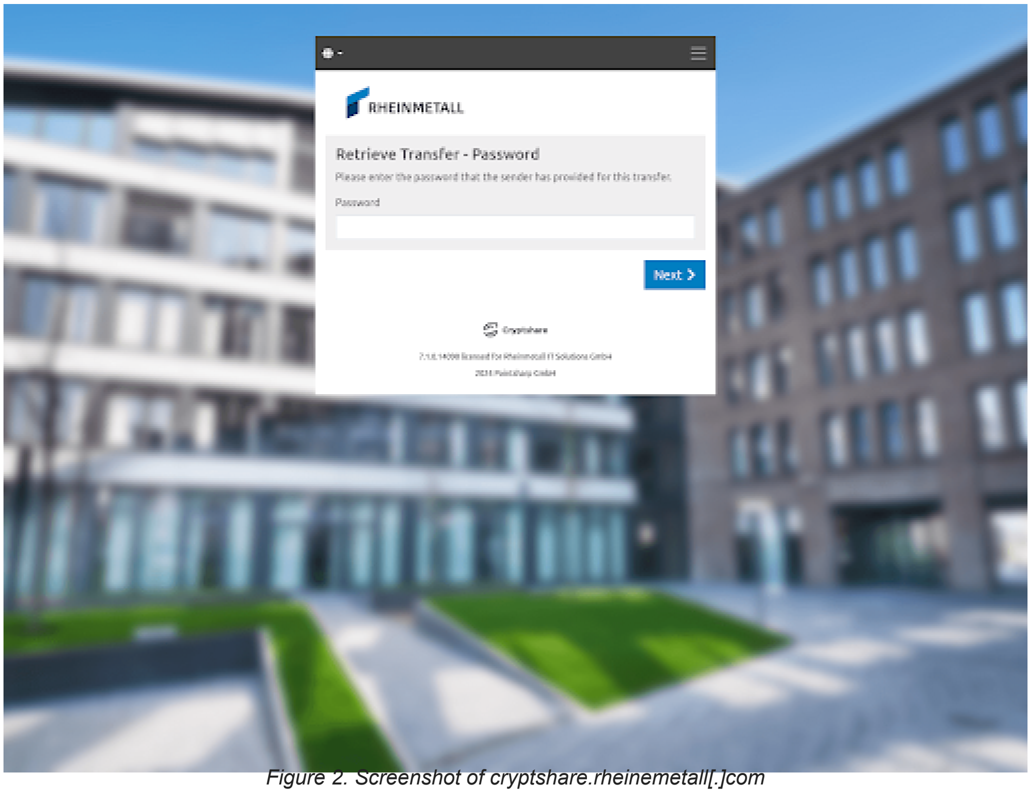
Expanded Domain Analysis: Links to Credential Phishing and Malicious File Distribution

Further analysis of identified infrastructure using urlscan identified four additional domains likely linked to this activity:

- rheinemetall[.]com
- rheinmetall.com[.]de
- ukrtelecom[.]eu
- funky-bober.art

These domains were visually similar to the MX domains identified above and were also hosted on GHOSTnet VPS infrastructure. Another domain, ukrtelcom[.]com, is likely related to this activity based on Whois data overlap with ukrtelecom[.]eu and rheinemetall[.]com. However, at the time of analysis, ukrtelcom[.]com was not hosted on GHOSTnet VPS and did not host a Mailu credential collection page.

In addition to credential phishing, the actor likely used the subdomain cryptshare.rheinemetall[.]com to distribute malicious files. Data from urlscan indicates this subdomain was used to facilitate file distribution between late January and mid-February 2025. Screenshots show the page requesting a password before allowing users to retrieve a file. The subdomain name and password request page refer to Cryptshare, a legitimate secure file retrieval service. DTI cannot confirm how the actor used this subdomain; however, given the available evidence, it was most likely used to deliver malicious files.



Retrieve Transfer - Password

Please enter the password that the sender has provided for this transfer.

Password

7.1.0.14098 licensed for Rheinmetall IT Solutions GmbH

2024 Pointsharp GmbH

Figure 2. Screenshot of cryptshare.rheinemetall[.]com

Assessment of Cyber Espionage Activity Targeting Defense and Aerospace Sectors

There is insufficient evidence to attribute this activity to a known actor; however, the activity likely has a cyber espionage motivation. DTI makes this assessment with moderate confidence based on the tactics, techniques, and procedures (TTPs) and the heavy focus on the defense and aerospace sectors.

The focus on spoofing organizations involved in Ukraine’s defense and telecommunications infrastructure further suggests an intent to gather intelligence related to the conflict in Ukraine. Notably, many of the spoofed defense, aerospace, and IT companies have provided support to Ukraine’s military efforts in its conflict with Russia.

IOCs on GitHub

If the community has any additional input, please let us know.

https://github.com/DomainTools/SecuritySnacks/blob/main/2025/PhishingInfrastructure-UAConflict.csv

Iris Search Hashes

1

U2FsdGVkX1/N26ISOMEKt52j4qVRCFOeOdJm5/SVrHprkuaLnu2BQeUp0P0Kc6qfHvj5jP53SaAxcYJDb48++
Vqi4NintEcAPIkll0UFs8Dqv6g+tIbYEPXAR9Yrlkqv5MIad+FOlQ8f26MzOpo/M7Hqo94HE1H63Jj+B+DEHH
MQ6nNrWIpiEy4XT6Zo2FHo8wSby4ujxE+xC+G9wp5KlAQxnpiW3NjxO6N0NRwt/Evi88HuqJkaBsiChU45YFR
UQ4ssMz6PTRmx0f3r7oWwdg2x+VYe6gewGBmhrSZ+CYh7szWd8XGZ1bkHs3PO/bJoLLkYXugS+pII3U3SHEDx
Sg==

2

U2FsdGVkX1/Oxch4IdGieQH7IfShNh73KLEDd36UhzMQ42084cwIoGKpsWU0GBGPtg8+Z3ONxs1f6kJufq/vn
m2dFC6OYb0EktrRZwhzkyOZDatwnICp9trBVL1Xa1Ep6ZIxAONKhwESx7raSr+qaQv3eTbH263IY49x6aT1i0
6O2C48+ZIFN06/+K8+2JIB3qRu18qYJvxZ21dsy77VMz3XHgA0210bqp5/8BFbwJB4HcnLKKLNcssqA+CdMgi
4IHEoK/dFEBqHjZuPVo11genM2tr89FwcsEMYGfnDc0tZy1O75JMMwVcXc3rugbRLiRehxUSqXrXc9jda0mjM
9IDkmgBYIDw28Cp6jRuUf/I=

Sign Up For DomainTools Investigations’ Newsletter for the Latest Research

Want more from DomainTools Investigations? Be sure to sign up for our monthly newsletter to get the latest research from the team – available on LinkedIn or email.