

Russian APT actor phishes the Baltics and the Balkans



strikerready.com/blog/russian-apt-actor-phishes-the-baltics-and-the-balkans

On December 5th, a Russian APT targeted Transnistria's governing body with a credential phishing email attachment, spoofing the Pridnestrovian Moldavian Republic. The image below shows the email content translated.



Figure 1: translated phish from google translate

Figure 1: translated phish from google translate

The attachment, [Распоряжение № 441пн.pdf .html \(Order No. 441rp.pdf .html\)](#) , shows the decoy content when executed



Figure 2: the decoy, that will be blurred

The html loads the image in a DIV named `bluer`, which is a misspelling of “blur”. The CSS applies a blur filter, as seen below



Figure 3: CSS to blur the background image

Figure 3: CSS to blur the background image

One can see the blur effect when viewing the phish page in a browser



Figure 4: rendered phish box

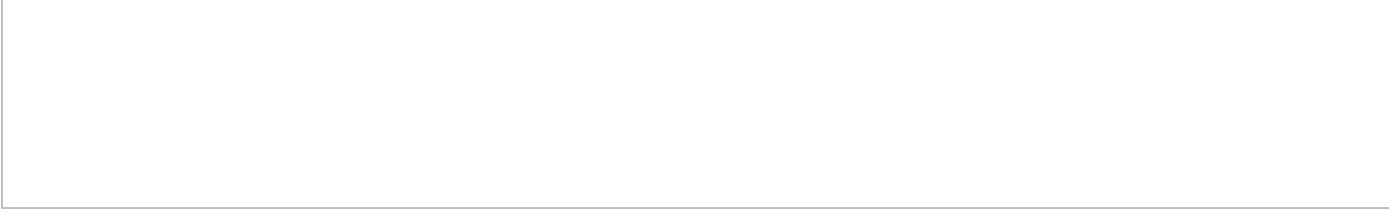


Figure 4: rendered phish box

Upon entering credentials, it checks if the password complies with a complex regex that appears to be [inspired by this blog](#).



Figure 5: checkP function to regex test the password

Figure 5: checkP function to regex test the password

If the password matches the regex, it is POSTed to formcarry.com. However, if the password does not match, it still steals the data, perhaps in an effort to gather secondary passwords that might be valid else where.



Figure 6: send creds to formcarry

Figure 6: send creds to formcarry

This campaign has been active since at least 2023 with spears such as [12th package of sanctions against Russia.pdf.html](#), based on identical regular expressions and javascript logic.

Other notable decoy images from this campaign are below.



Figure 7: other decoy images

Figure 7: other decoy images

There was one phish that did not follow the same pattern, and instead loaded unknown, but suspected malicious code, from an external server, timesyncwindows.com



Figure 8: decoy from an outlier phish, with externally hosted



Figure 8: decoy from an outlier phish, with externally hosted content



Figure 9: assumed malicious content loaded by

Figure 9: assumed malicious content loaded by `script`

Other files from this same campaign are below, along with the target, which is often embedded in the payload

Lure	Assessed Target
Cancellation of personal special economic and other restrictive measures.html	Ukraine DIB
Cyber Threats and NATO Horizon Scanning and Analysis.html	Governments of Bosnia and Herzegovina, Macedonia, Montenegro, Spain
Update of the List of Diplomatic Missions Accredited to EEAS.html	Governments of Ukraine, Lithuania
New Event Scheduling in Outlook on the Web.html	Macedonia Government
NATO SCHOOL Course Catalogue 2024 update.html	Bulgaria Government
12th package of sanctions against Russia.pdf.html	Ukraine DIB
Protected Internal Reporting Regulations.html	Macedonia Government
Secret Report Cyber Threats Security.html	Moldova Government
Распоряжение № 441пн.pdf.html	Moldova Government

Figure 10: Lures from this campaign

Because the phish lures often contain the direct target information, we are not providing the content as we normally do, however the [IOCs are available on our github](#)

Please get in touch at research@strikerready.com if you have question, corrections, or comments

Acknowledgements

The authors would like to thank the reviewers, as well as peer vendors, for their comments and corrections. Please get in touch at research@strikerready.com if you have corrections, would like us to use your group name, or would like to collaborate on research.