Russian Threat Actor Impersonates Aerospace and Defense Companies

Security Awareness Training Blog

Stu Sjouwerman
7 Dec

- Tweet
-

A Russia-linked threat actor tracked as TAG-53 is running phishing campaigns impersonating various defense, aerospace, and logistic companies, according to The Record by Recorded Future. Recorded Future's Insikt Group identified overlaps with a threat actor tracked by other companies as Callisto Group, COLDRIVER, and SEABORGIUM.

"TAG-53 infrastructure was uncovered by analyzing specific combinations of domain registrars, autonomous systems, domain name structures, and related TLS certificates," the researchers write. "Based on this information, it is highly likely that this threat group is continuing its phishing and credential-harvesting operations. While monitoring TAG-53 infrastructure, Insikt Group observed a spoofed Microsoft login page masquerading as a legitimate military weapons and hardware supplier in the US, suggesting that some TAG-53 infrastructure has likely already been operationalized."

Recorded Future isn't sure if the impersonated entities are the specific targets of the operation, but the researchers note that most of these organizations "share a focus around industry verticals that would likely be of interest to Russia-nexus threat groups, especially in light of the war in Ukraine."

"The TAG-53 domain "drive-globalordnance[.]com" includes a spoofed sign-in page for the legitimate company Global Ordnance, a military weapons and hardware supplier in the US," the researchers write. "The spoofed sign-in page…uses Global Ordnance branding and is suspected to be used for follow-on credential harvesting after a target has been phished. It is unclear whether Global Ordnance is the intended target of this attempted credential harvesting operation or whether TAG-53 is using a Global Ordnance-styled domain and spoofed sign-in page to masquerade as a legitimate entity to target victims."

Other impersonated entities included Polish defense company UMO Poland, the nonprofit Commission for International Justice and Accountability (CIJA), US-based satellite communications company Blue Sky Network, logistics company DTGruelle, and Russia's Ministry of Internal Affairs.

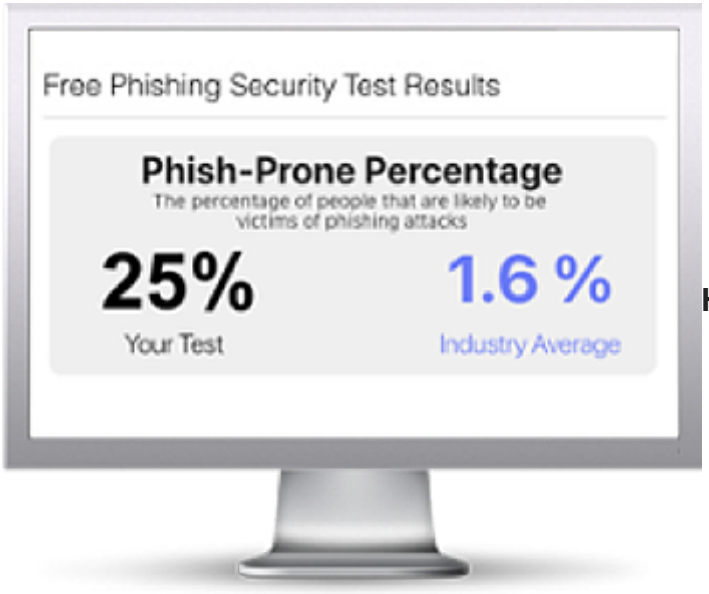
New-school security awareness training can enable your employees to thwart social engineering attacks.

The Record has the story.

Return To KnowBe4 Security Blog

Free Phishing Security Test

Would your users fall for convincing phishing attacks? Take the first step now and find out before bad actors do. Plus, see how you stack up against your peers with phishing Industry Benchmarks. The Phish-prone percentage is usually higher than you expect and is great ammo to get budget.



Here's how it works:

- Immediately start your test for up to 100 users (no need to talk to anyone)
- Select from 20+ languages and customize the phishing test template based on your environment
- Choose the landing page your users see after they click
- Show users which red flags they missed, or a 404 page
- Get a PDF emailed to you in 24 hours with your Phish-prone % and charts to share with management
- See how your organization compares to others in your industry

Go Phishing Now!

PS: Don't like to click on redirected buttons? Cut & Paste this link in your browser:

https://www.knowbe4.com/phishing-security-test-offer

Topics: Phishing

Get the latest about social engineering

Subscribe to CyberheistNews