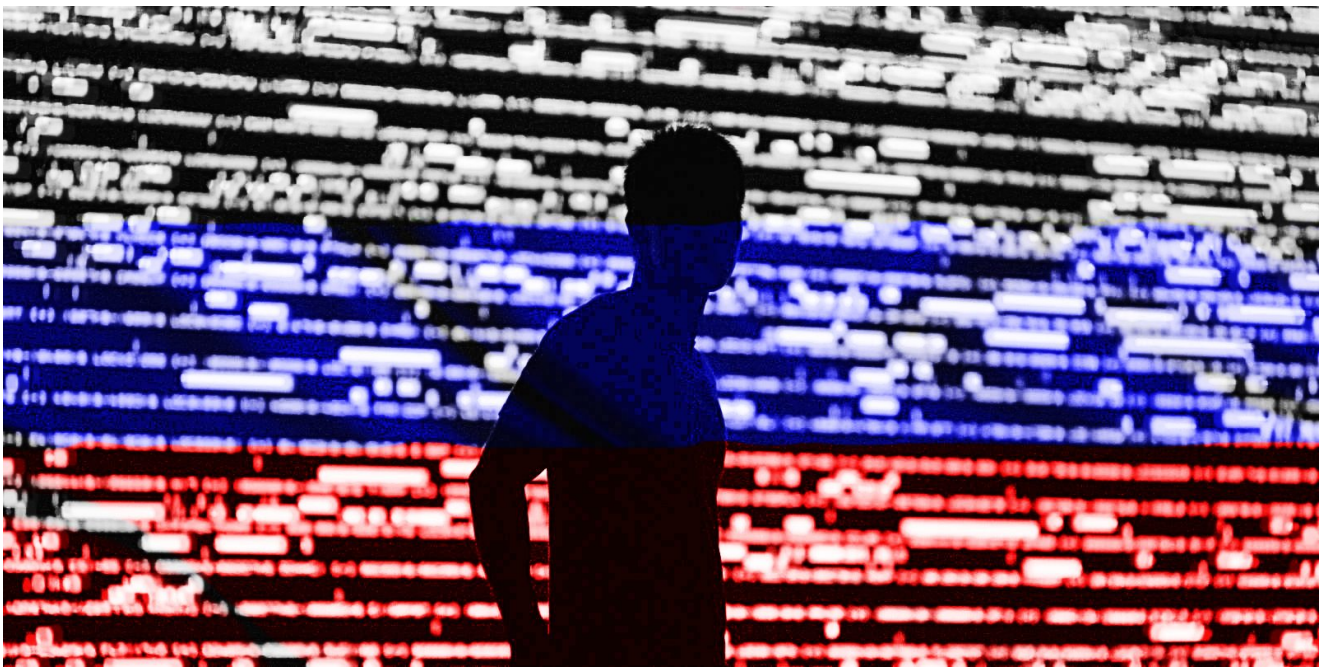
Phishing campaign targets Russian govt dissidents with Cobalt Strike

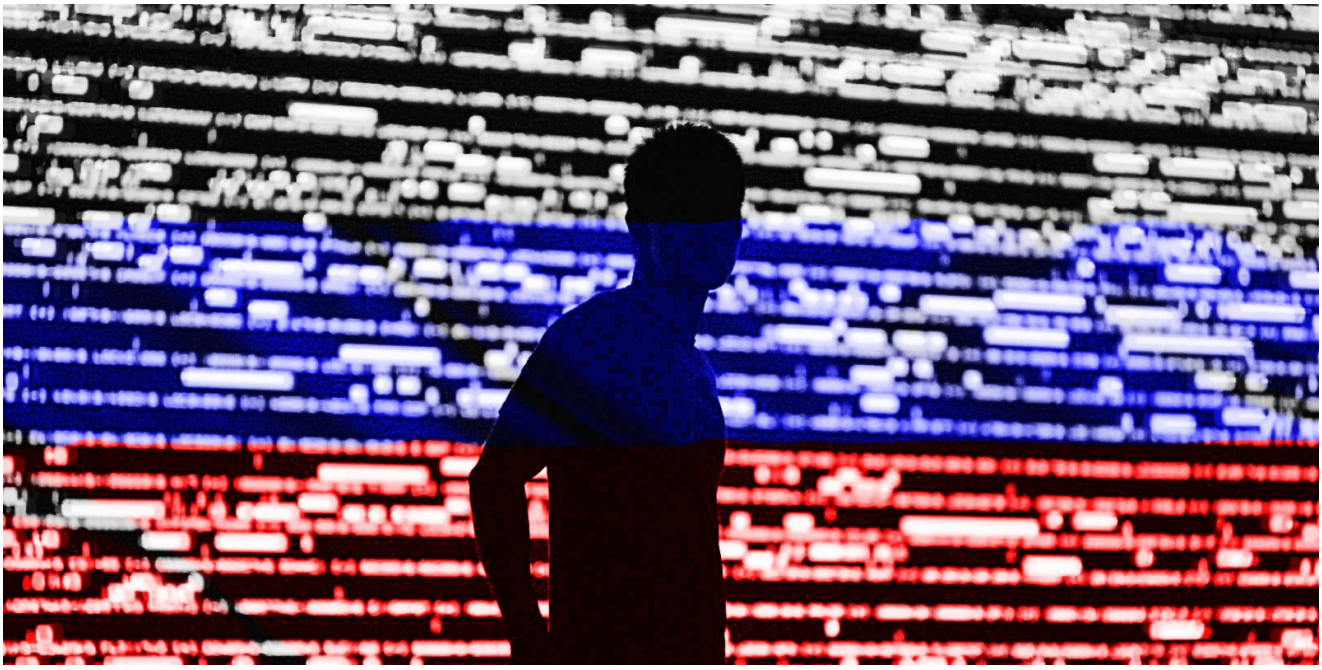
bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/

Bill Toulas



By
Bill Toulas

- March 30, 2022
- 09:05 AM
- 0



A new spear phishing campaign is taking place in Russia targeting dissenters with opposing views to those promoted by the state and national media about the war against Ukraine.

The campaign targets government employees and public servants with emails warning of the software tools and online platforms that are forbidden in the country.

The messages come with a malicious attachment or link embedded in the body that is dropping a Cobalt Strike beacon to the recipient's system, enabling remote operators to conduct espionage on the target.

The campaign's discovery and subsequent reporting come from threat analysts at Malwarebytes Labs, who have managed to sample several of the bait emails.

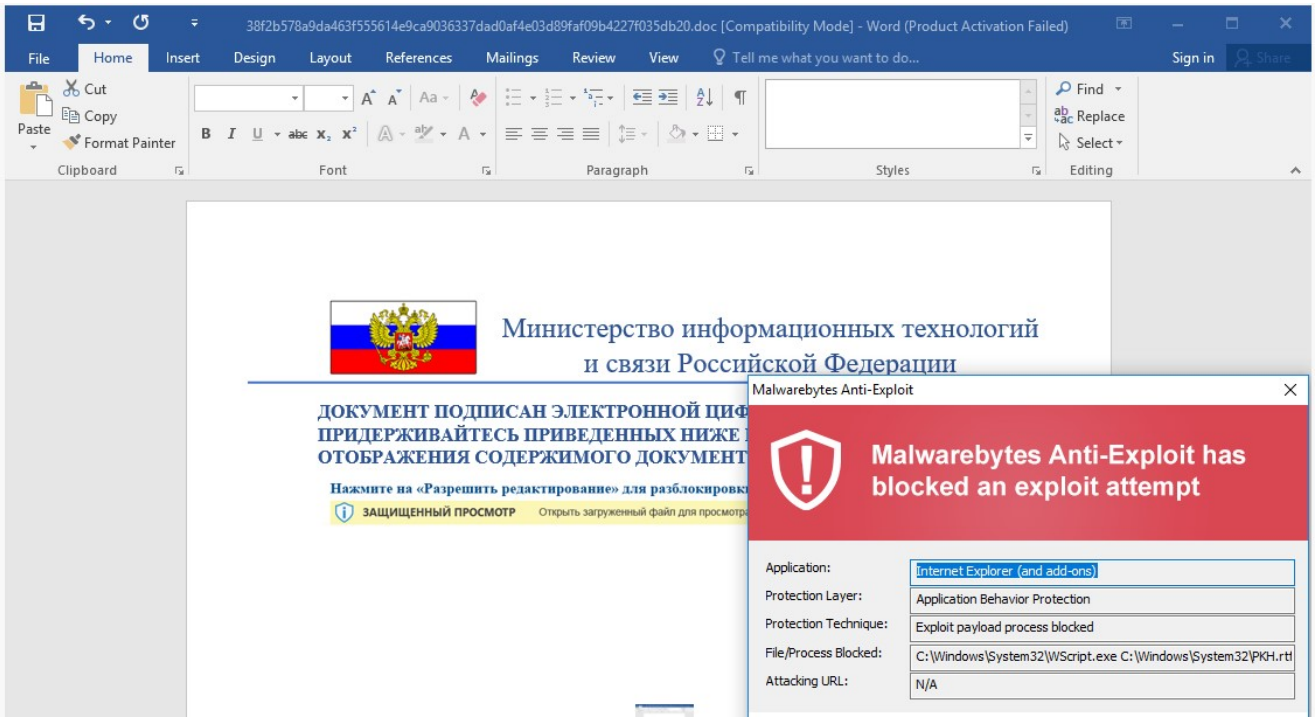
Multiple phishing pathways

The phishing emails pretend to be from a Russian state entity, a ministry, or a federal service, to entice recipients to open the attachment.

The "Ministry of Information Technologies and Communications of the Russian Federation" and the "Ministry of Digital Development, Communications, and mass communications" are the primary two spoofed entities.

The threat actors use three different file types to infect their targets with Cobalt Strike, namely RTF (rich text format) files, archive attachments of documents laced with malicious documents, and download links embedded in the email body.

The case of the RTFs is the most interesting due to involving the exploitation of CVE-2021-40444, a remote code execution flaw in the rendering engine used by Microsoft Office documents.



RTF file triggering the rendering engine exploit *(Malwarebytes)*

As is to be expected, all of the phishing emails are written in Russian, and they seem to have been crafted by native speakers of the language and not machine translated, suggesting that the campaign is endeavor from a Russian-speaking actor.

Apart from Cobalt Strike, Malwarebytes also noticed parallel attempts to deploy a heavily obfuscated PowerShell-based remote access trojan (RAT) with next-stage payload fetching capabilities.

Crackdown on dissidents

The targets of this campaign work mainly in the Russian government and public agencies, including the following entities:

- Portal of authorities of the Chuvash Republic Official Internet portal
- Russian Ministry of Internal Affairs
- ministry of education and science of the Republic of Altai
- Ministry of Education of the Stavropol Territory
- Minister of Education and Science of the Republic of North Ossetia-Alania
- Government of Astrakhan region
- Ministry of Education of the Irkutsk region
- Portal of the state and municipal service Moscow region
- Ministry of science and higher education of the Russian Federation

The above organizations indicate that the phishing actors target individuals who hold key positions and could cause problems to the central government by instigating war-opposing movements.

The so-called "special operation" in Ukraine hasn't unfolded the way Kremlin had envisioned, and western sanctions manifested on a scale way beyond what was accounted for, so this campaign may be the result of the higher government ramping up its alertness against potential coups.

This is a very likely explanation of why Russia-based hackers are interested in conducting espionage against semi-high ranking government officials and ministry employees, but at this time, it's just an assumption.

Malwarebytes has mapped the infrastructure used by the threat actor(s) behind the latest campaign and will continue to monitor the associated activity.

Related Articles:

Russian hackers perform reconnaissance against Austria, Estonia

Ukraine warns of “chemical attack” phishing pushing stealer malware

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Russian hackers compromise embassy emails to target governments

Russian govt impersonators target telcos in phishing attacks

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.