SBA Business Loans
Get the best loan for your business. Apply in minutes.
Lendio

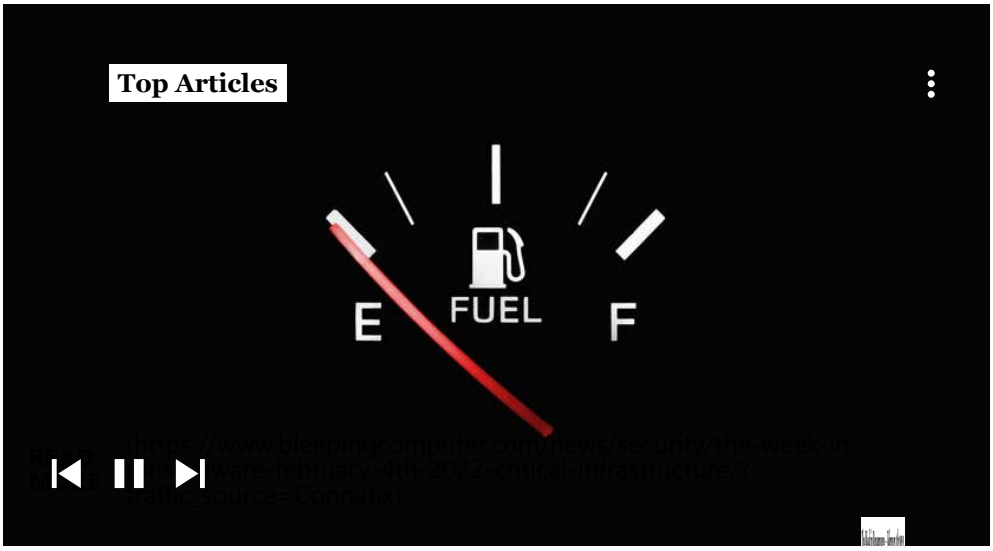
By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

February 4, 2022 03:17 PM **7**

SBA Business Loans
Get the best loan for your business. Apply in minutes.
Lendio

members-of-gamaredon-hacker-group-to-russian-fsb/) to Russia's Federal Security Service (FSB), the country's domestic intelligence service, this hacking group is also tracked as Armageddon, Primitive Bear, and ACTINIUM.

Gamaredon has been active for at least a decade and has been behind thousands of attacks on Ukrainian orgs since 2013.



Security and threat researchers with the Microsoft Threat Intelligence Center (MSTIC) and the Microsoft Digital Security Unit (DSU) said today that Gamaredon's cyber-espionage campaign is being coordinated out of Crimea, confirming SSU's assessment that the Gamaredon hackers are officers of the Crimean FSB who sided with Russia during the 2014 occupation.

"MSTIC has observed ACTINIUM targeting organizations in Ukraine spanning government, military, non-government organizations (NGO), judiciary, law enforcement, and non-profit, with the primary intent of exfiltrating sensitive information, maintaining access, and using acquired access to move laterally into related organizations," Microsoft added (https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/).

"Since October 2021, ACTINIUM has targeted or compromised accounts at organizations critical to emergency response and ensuring the security of Ukrainian territory, as well as organizations that would be involved in coordinating the distribution of international and humanitarian aid to Ukraine in a crisis."

SBA Business Loans
Get the best loan for your business. Apply in minutes.
Lendio

SSU blocks 120 cyberattacks in January

Palo Alto Networks' Unit 42 also issued a report regarding this group's recent activity (https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/) targeting Ukraine and mentioned "an attempt to compromise a Western government entity in Ukraine on Jan. 19, 2022," via a spear-phishing attack pushing a malware downloader.

"In this attempt, rather than emailing the downloader directly to their target, the actors instead leveraged a job search and employment service within Ukraine," Unit 42 said.

"Given the steps and precision delivery involved in this campaign, it appears this may have been a specific, deliberate attempt by Gamaredon to compromise this Western government organization."

The same tactics were described by Symantec's Threat Hunter team (https://www.bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/), who saw Gamaredon distributing macro-laced Word documents in spear-phishing attacks that started in July 2021.

These reports confirm an advisory published by the Ukrainian Computer Emergency Response Team warning of attacks (https://cert.gov.ua/article/18365) against Ukrainian authorities.

One day later, the SSU said it blocked more than 120 cyberattacks (https://ssu.gov.ua/en/novyny/u-sichni-2022-roku-sbu-zablokuvala-ponad-120-kiberatak-na-ukrainski-orhany-vlady) targeting the information systems of state institutions in Ukraine, including brute-force and malware attacks.

"MSTIC assesses that the primary outcome of activities by ACTINIUM is persistent access to networks of perceived value for the purpose of intelligence collection," Microsoft also said today.

SBA Business Loans
Get the best loan for your business. Apply in minutes.
Lendio

Related Articles:

Ukraine links members of Gamaredon hacker group to Russian FSB (https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/)

Russian 'Gamaredon' hackers use 8 new malware payloads in attacks (https://www.bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/)

Canada's foreign affairs ministry hacked, some services down (https://www.bleepingcomputer.com/news/security/canadas-foreign-affairs-ministry-hacked-some-services-down/)

US sanctions former Ukrainian official for helping Russian cyberspies (https://www.bleepingcomputer.com/news/security/us-sanctions-former-ukrainian-official-for-helping-russian-cyberspies/)

Russia charges 8 suspected REvil ransomware gang members (https://www.bleepingcomputer.com/news/security/russia-charges-8-suspected-revil-ransomware-gang-members/)

FSB (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FSB/)

GAMAREDON (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/GAMAREDON/)

RUSSIA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RUSSIA/)

UKRAINE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/UKRAINE/)