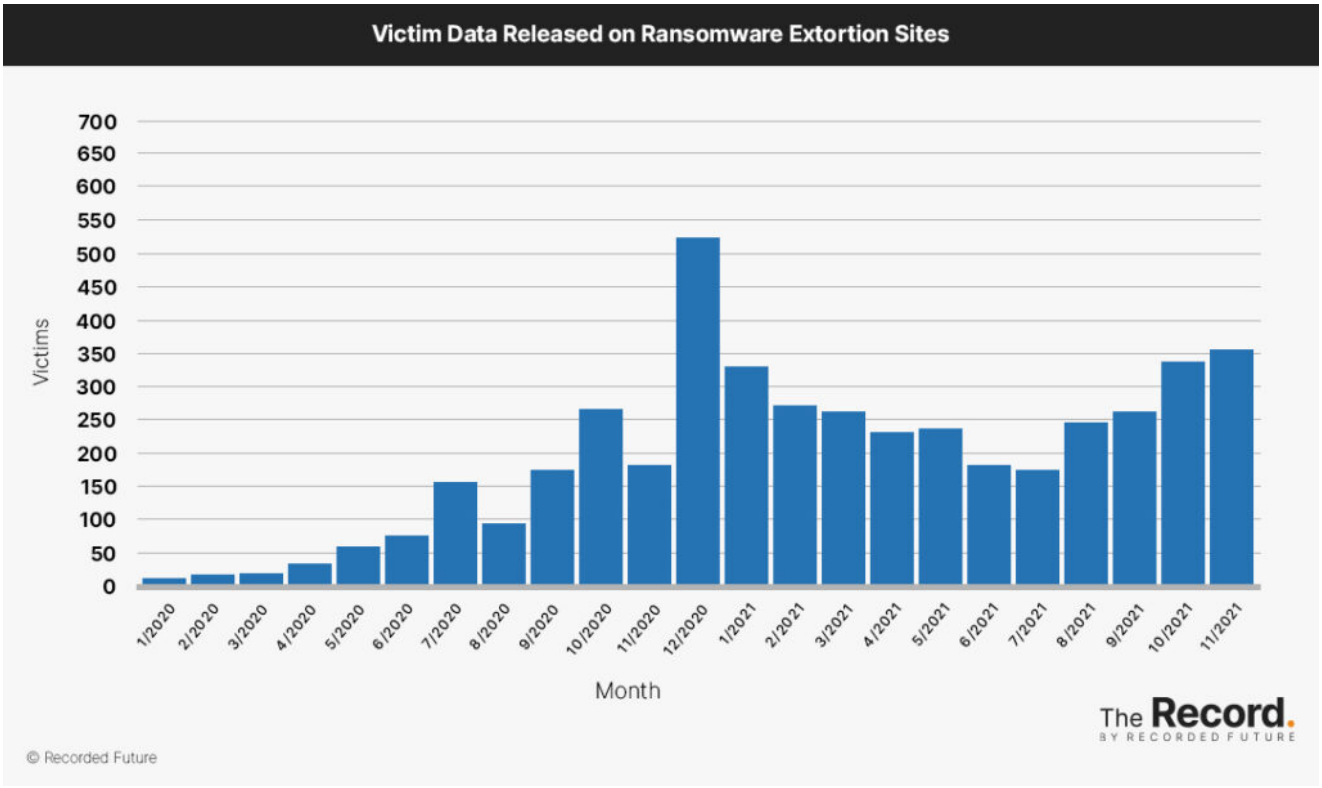
Russian hackers targeted petroleum refining company in NATO state

therecord.media/russian-hackers-targeted-petroleum-refining-company-in-nato-state/

December 20, 2022



Alexander Martin
December 20, 2022

- Cybercrime
- Government
- Nation-state
- News

A hacking group associated with Russia's Federal Security Service (FSB) unsuccessfully attempted to compromise a large petroleum refining company within a NATO member state at the end of August, according to a new report.

The advanced persistent threat group, known as Trident Ursa (also referred to as Gamaredon, Primitive Bear and Shuckworm) is "a specially created structural unit" of the FSB "whose tasks are intelligence and subversive activities against Ukraine in cyberspace," in the analysis of Ukraine's Security Service.

It primarily uses HTML and Word documents as spear phishing lures which, alongside its traditional efforts targeting Ukrainian entities with Ukrainian-language lures, are now also increasingly using English-language lures according to research published Tuesday by Palo Alto Networks' Unit 42.

Unit 42 reported that the hacking group was using these English-language lures to boost its "intelligence collection and network access against Ukrainian and NATO allies."

It found during a review of the group's indicators of compromise (IoCs) that the hackers had unsuccessfully attempted to "compromise a large petroleum refining company within a NATO member nation on August 30," although the company was not identified in the report.

In October, Norway's prime minister warned that Russia posed "a real and serious threat" to the country's oil and gas industry in the wake of suspected sabotage of the Nord Stream I and II pipelines and sanctions against Russian gas imports which left Norway as the largest supplier of gas to Europe.

The majority of recent cyberattacks targeting the oil and gas sector in Europe have appeared to be financially motivated and conducted by ransomware gangs, however the FSB has historically been linked to the Russian cybercriminal underground — in particular in the case of Maksim Yakubets, an alleged cybercriminal who was charged with also stealing classified information and providing it to the Russian authorities.

This has provoked concerns that the ransomware attacks are part of a hybrid campaign coordinated by Russian intelligence, although a Belgian official has downplayed to The Record concerns that these attacks are linked.

Death threats against Ukrainian researchers

Unit 42 also said that an individual "who appeared to be tied to Trident Ursa" used Twitter to threaten a small group of cybersecurity researchers on the platform after they highlighted IoCs linked to the hacking group's activity in the days before the invasion.

The user, who appeared to operate multiple accounts with the username Антон (Cyrillic for Anton), targeted Kyiv-based researcher Mikhail Kasimov among others. On February 26, the user posted Kasimov's full name, his date of birth, and his address alongside an English-language threat: "We are already in the city, there is nowhere to run. You had a chance."

Speaking to The Record on Tuesday, Kasimov described the threat as incidental — occurring solely within the early days of the full-blown invasion without any follow-up since — and noted that the user has not been active since February 26.

Kasimov, who does network IoC detections for the maltrail project, is continuing to share a range of domains related to Gamaredon, and is uploading samples to VirusTotal.

Responding to a question about how his details might have been obtained, Kasimov said: "I suspect, that, if someone wants to get something, he will get it on some day… Perhaps, some citizens database was leaked some year ago…"

In the days before the full-blown invasion of Ukraine, the United States sent a letter to the U.N. warning that the Russian Federation had drawn up lists of Ukrainians who would be targeted either for assassination or imprisonment during what the Russians expected to be

their occupation of the country.

“It is always unpleasant, when someone tries to threat your life anyway… Fortunately, I’m still alive and healthy,” Kasimov said, adding that he had “fortunately” not received any other threats against his life since the posts by Anton.

Tags

- APT
- cybercrime
- FSB
- Gamaredon
- nation-state
- petroleum
- Russia

Alexander Martin is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and is also a fellow at the European Cyber Conflict Research Initiative.