The Russian APT Tool Matrix

By BushidoToken

Published: 2024-09-22 · Archived: 2026-04-06 00:49:32 UTC

Introduction

Based on feedback I have received from fellow CTI researchers, incident responders, and managed detection and response teams around my Ransomware Tool Matrix project, I decided to make another Tool Matrix focused on one hostile state in particular: Russia.

Again, as defenders, we should exploit the fact the tools used by these Russian APT groups are often reused and through proactive defensive work, we can frustrate and even eliminate the ability of certain adversaries to launch intrusions.

Using the Russian APT Tool Matrix comes with its own challenges. While it is undoubtedly useful to have a list of tools commonly used by Russian APTs to hunt, detect, and block, there are some risks, as noted in the repository.

The new repository also contains multiple types of Russian threat groups, this includes adversaries part of the GRU, SVR, and FSB. The alias of each Russian threat group has been chosen by what the author of this repo believes it is most well-known as.

- Russian GRU: Main Intelligence Directorate (Russian Military)

- Russian SVR: Foreign Intelligence Service of the Russian Federation
- Russian FSB: Federal Security Service of the Russian Federation

Also, if you're short on time, you can now listen to this blog as a podcast via YouTube, which I generated using Google's NotebookLM.

Key Findings

Following the collection, extraction, and labelling of all the tools identified as being used by Russian threat groups, some interesting findings were uncovered. These are as follows:

The adversary that used the most scanners was EMBER BEAR, which is affiliated with the GRU. Other GRU threat groups, such as FANCY BEAR and Sandworm, were found often relying on a wide variety offensive security tools (OSTs) to support their intrusions.

Another interesting finding was that Russian threat groups using lots of different tools and platforms for exfiltration was Turla and COZY BEAR. Overall, the Russian threat group with the highest total number different tools used was COZY BEAR, which is affiliated with the SVR.

From extracting all the various tools from several years' worth of threat reports, some general observations about how Russian threat groups used public-available resources to support their campaigns. The thing that stood out most was a large reliance on OSTs across multiple Russian threat groups. Up to 27 different OSTs were recorded. The tools mutually used by the highest number of Russian threat groups are as follows:

- **Mimikatz** is used by COZY BEAR, FANCY BEAR, BERSERK BEAR, Gamaredon, and Turla.
- **Impacket** is used by COZY BEAR, FANCY BEAR, EMBER BEAR, Sandworm, and BERSERK BEAR.
- **PsExec** is used by COZY BEAR, EMBER BEAR, BERSERK BEAR, Gamaredon, and Turla.
- **Metasploit** is used by FANCY BEAR, EMBER BEAR, Sandworm, and Turla.
- **ReGeorg** is used by COZY BEAR, FANCY BEAR, EMBER BEAR, and Sandworm.

If a combination of the above tools are observed during an intrusion, then that intrusion could have been conducted by a Russian state-sponsored threat group. However, using the Ransomware Tool Matrix, we know that four out of the top five tools used by Russian threat groups are also very commonly used by ransomware groups.

The network tunnelling utility ReGeorg is potentially notable for its use by multiple Russian threat groups. ReGeorg is not a well-known tool and it is often used in conjunction with a web shell to turn a compromised server into a proxy. From my collection and extraction of tools from threat reports related to the Ransomware Tool Matrix, I can confirm ReGeorg is used by virtually none of the large ransomware gangs. Therefore, if this specific tool is found during an intrusion, alongside the other top five tools mentioned above, there is arguably an increased chance it was conducted by a Russian threat group.

Russian APT Tool Matrix Project

You can find The Russian APT Tool Matrix in my GitHub repository below:

Source: https://blog.bushidotoken.net/2024/09/the-russian-apt-tool-matrix.html