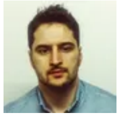
Booz Allen analyzed 200+ Russian hacking operations to better understand their tactics

zdnet.com/article/booz-allen-analyzed-200-russian-hacking-operations-to-better-understand-their-tactics/

Booz Allen: Russia uses its GRU military hackers following predictable patterns based on a public military doctrine.



Written by Catalin Cimpanu, Contributor on March 26, 2020

russian hacker

see also

Booz Allen Hamilton, the largest private contractor for the US intelligence community, has published a comprehensive report this week detailing 15 years (2004 to 2019) of cyber operations carried out by Russia's military hackers.

The report is a rarity in the cyber-security community because it focuses on the bigger picture of how Russia's military uses its hacking units to support its foreign policy all over the globe.

This is in contrast with most other reports from the infosec industry that usually focus their investigations on isolated events, avoiding any political analysis, and rarely attributing attacks back to foreign governments.

Instead, the Booz Allen report takes all the previous reporting on past Russian hacks and puts them in a broader political context, in order to understand why they happened, rather than how, which malware was used, and who pushed what button and when.

The GRU

More specifically, the Booz Allen report focuses on the cyber-operations carried out by the intelligence service attached to Russia's military.

Known as the Main Directorate of the General Staff of the Armed Forces, this intelligence agency is widely known within Russia and abroad by its former acronym, the GRU, derived from its historic name Glávnoye Razvedyvatel'noje Upravléniye (Main Intelligence Directorate, or GRU). The agency's current name is Glávnoye Upravléniye (Main Directorate), or GU, but this term it's rarely used, and the service is still broadly called the GRU.

For context, GRU is different from the Russian government's internal intelligence service, which is known as the FSB, a successor of the infamous KGB. Unlike the FSB, GRU only supports Russia's military operations and the Kremlin's foreign policy.

Over the past 15 years, the GRU has been linked to two very distinct hacking groups. The first is APT28 (aka Fancy Bear) and the second is Sandworm.

Each hacking group is believed to be a different military unit inside Russia's intelligence service, specifically tasked with carrying out cyber operations of various degrees of sophistication, with Sandworm believed to be the GRU's elite division.

GRU attacks can be predicted with Russia's military doctrine

According to the Booz Allen report, the cyber operations conducted by both groups cannot be viewed in isolation. They are almost exclusively conducted in a broader political context.

The GRU being a military-run operation, all actions follow a set of patterns. Booz Allen says it analyzed more than 200 unique cyber incidents publicly attributed to the GRU and found that pattern.

According to the US intelligence contractor, that pattern perfectly fits the principles described in a Russian government document called "The Military Doctrine of the Russian Federation," which the Russian Army publishes at regular intervals.

The last version of this document was published in 2014 and lists 23 security risks to the Russian Federation to which the Russian Army must reply in one form or fashion.

gru-doctrine.png

Image: Booz Allen Hamilton

In a chunky 80-page report, Booz Allen analysts classified and arranged all the 200+ past GRU cyber-attacks into one of these 23 categories, showing how each cyber-attack was Russia's natural defensive mechanism of responding to the changing political environment around it.

The end conclusion of this report is that GRU offensive cyber operations can be predicted.

Companies or governments that find their agendas crossing with the Russian government in a way that Kremlin might interpret as one of the 23 risks listed in its military's response doctrine should anticipate an attack from Russia's famed hacker groups.

"Defending against cyber operations-like those of the GRU-demands understanding not just how these operations occur but, more importantly, why," Booz Allen analysts said this week. "By understanding why adversaries act, defenders can better anticipate when, where, and in what form those actions may occur and take deliberate action to mitigate their risk based on that insight."

We won't list all the 200+ known GRU cyber-attacks from the Booz Allen report in this article as we'll end up with an equally long piece.

However, below we list some international incidents where Russia responded by unleashing its GRU hacking units. We then correlate how a particular cyber-attack could be correlated back to one or more of the 23 principles described in its military doctrine.

We'll focus on the lesser-known incidents and not cover the major incidents.

Montenegro

Russia intervened in the affairs of Montenegro after the country wanted to join NATO. According to its military doctrine, Russia views NATO expansion as #1 on its list of security risks.

GRU operations were crucial in Kremlin's attempts to elect a pro-Russian government and prevent the country from joining NATO.

- Three days before the election GRU operators carried out DDoS attacks to disrupt media sites, the country's largest telecom, an NGO monitoring the election, and government sites in order to disrupt the oncoming election and sow confusion.
- Booz Allen points out that GRU operations also received help from non-military forces, with Russia funneling funds into opposing political groups and also "sought to coordinate with politicians, clergy, NGOs, and media outlets."
- The GRU operation to stop Montenegro from electing a pro-West-friendly politician also included an on-the-ground component. At the time, Montenegrin law enforcement arrested GRU officers and agents who were allegedly planning to attack parliament, assassinate the prime minister, and provoke civil unrest with false-flag attacks on civilians.
- After Montenegro joined NATO, GRU's operations moved back to its hacking units, who continued online with spear-phishing campaigns.

Syria

GRU supported Russia's war efforts in Syria, as the Kremlin tried to preserve a Putin-friendly leader in power. This effort fits with Russia's military doctrine of keeping a stable political climate around it and prevent foreign powers from destabilizing its allies and neighbors (#2 on its military doctrine list).

- Per Booz Allen, "the GRU likely responded to these circumstances [US military intervention in Syria] by using an ISIL hacktivist identity to harass and intimidate US military and law enforcement communities from December 2014 through February 2015."
- GRU operators defaced news media websites in the US to give the impression that ISIL controlled considerable cyber resources.
- GRU operators leaked personal data for US service members. Some of the data was even leaked via hacked social media accounts for the US Military Central Command (CENTCOM).
- GRU operators hacked a Maryland television outlet's text message alert system to send threatening messages to subscribers. Coupled with Russia's military efforts inside Syria, GRU's online efforts appear to have been successful, as the US public's support for a war in Syria diminished and the US eventually withdrew its forces.

Poland

GRU cyber-espionage operations played a role in the Russian government's response to the creation of a major NATO base in Poland. This fits Russia's mandatory response to NATO's ever-increasing presence in the region (#1 on its military doctrine) but also the danger of foreign powers deploying troops near Russia's borders (#3 on its military doctrine).

- Starting with the summer of 2014, GRU was heavily involved in "monitoring of the Polish government and defense sectors."
- This was done via "watering hole" attacks. GRU-linked hackers compromised websites belonging to a Polish government public records website and a Polish defense firm from where they used automated exploits to install a backdoor on visitors' systems.
- Per Booz Allen, the use of a watering hole, as opposed to more targeted spearphishing, suggests desperation to gain maximum visibility around many Polish elements (i.e., policymakers, suppliers).
- When in 2018 Russia proposed to create a similar base in Belarus to counter NATO's Poland base, Belarus declined. The same month, GRU hackers began targeting the Belarus government with spear-phishing operations.

Romania

GRU hackers began targeting Romania after the country increased its military spending and military operations. Just like in Poland's case, Russia responded to a foreign country increasing its military presence in an area of interest -- the Black Sea, in this case (also #3 on its military doctrine).

- In the same month when Romania proposed the creation of a joint military unit with neighboring country Moldova, GRU operators launched spear-phishing attacks against Romania's embassy in Russia in order to closely monitor further developments.
- After Russia annexed Crimea in 2014, Romania placed orders for three submarines and four surface vessels to modernize its navy's presence in the Black Sea. A month later, several spear-phishing operations targeted Romanian entities, with malware samples associated with GRU often being uploaded on the VirusTotal virus-scanning portal from Romania.

Denmark

GRU hacking operations targeted Denmark for years after the country announced it was joining the NATO Missile Defense System.

Here, Russia responded to the US undermining its military deterrence capabilities by deploying an anti-missile system near its border (#4 on its military doctrine).

- On March 15, Russia's ambassador to Denmark warned in a newspaper interview that Denmark joining the "American-controlled missile defense [makes] Danish warships...targets for Russian nuclear missiles."
- Ten days later, GRU launches a two-year effort to hack email accounts for Danish Foreign and Defense Ministry employees.

UK

Russia deployed its military hackers against the UK after the country considered deploying troops in Syria, an obvious move that put it at odds with Russia (#2 and #8 on its military doctrine).

- GRU hackers established preemptive beach-heads at a UK television station on the same month the UK government was pondering sending troops to Syria, in July 2015.
- The TV channel was named Islam Channel, and it was believed GRU would use it to target the UK Islamic community with propaganda.
- Similar attacks on television stations were also seen in France and the US, the UK's partners, all under the guise of an ISIL-aligned hacktivist group called CyberCaliphate.

US

Russia deployed APT28 to meddle in the 2016 US presidential election after the US broke security risk #14 on its military doctrine -- State-sponsored subversive activities targeting Russia -- when the US ran a state-sponsored foreign influence campaign to support President's Putin rival during the 2012 Russian presidential election.

What followed was the DNC hack, APT28 posing as the Guccifer 2.0 hacktivist, DCLeaks, and an army of online trolls and networks of fake news sites targeting the US public.

International Sports Organizations

Russia also deployed its GRU hackers to discredit international sports organizations across the world after Russian athletes were banned from several sporting events.

At the time, it seemed odd that Russian state hackers would go after sporting organizations since this is not the usual target of a state-sponsored hacker group. But per Booz Allen, WADA banning Russian athletes from the Olympics amounted for a public embarrassment of the Russian state, and effectively broke principle #17 in Russia's military doctrine -- which saw the WADA ban as an attack on Russian historical, spiritual, and patriotic values and traditions.

True to its military doctrine, the Russian unleashed its GRU hackers, which led to some of the non-standard state-backed hacking campaigns seen this decade, next to the 2014 Sony hack.

- The GRU hacked the World Anti-Doping Agency (WADA) in 2016 and leaked-via fake proxy hacktivist identities-foreign athletes' therapeutic use exemptions (TUE).
- The goal was to establish a false sense of moral equivalency between Russian athletes who doped and athletes in other countries who were using doping substances for medical reasons. This narrative was heavily pushed by Russian state media, once the GRU leaked TUE files.
- GRU hackers also tried to sabotage and crash the opening ceremony of the 2018 Winter Olympics, two years later, also as a response to Russian athletes still being banned from the Olympics.

Tens of other cases studies are detailed further in the Booz Allen report.

The world's most famous and dangerous APT (state-developed) malware