TechXplore

Russia's shadow war: Vulkan files leak show how Putin's regime weaponizes cyberspace

April 4 2023, by Matthew Sussex

Credit: Pixabay/CC0 Public Domain

Recent revelations about the close partnership between the Kremlin and NTC Vulkan, a Russian cybersecurity consultancy with links to the military, provide some rare insights into how the Putin regime weaponizes cyberspace.

More than 5,000 documents have been leaked by an anonymous whistleblower, angry at Russia's conduct in the war in Ukraine. They purport to reveal details about hacking tools to seize control of vulnerable servers; domestic and international disinformation campaigns; and ways to digitally monitor potential threats to the regime.

Although caution is always necessary before accepting claims about cyber capabilities, it's noteworthy several Western intelligence agencies have confirmed the documents appear genuine.

The leak also corroborates the view of many strategists: that the Russian government regards offensive cyber capabilities as part of a holistic effort to degrade its enemies. This includes the sowing of mistrust via social media, the gathering of kompromat (compromising material), and the ability to target crucial infrastructure.

That list of enemies is a long one, and has grown since Putin's full-scale invasion of Ukraine in February 2022. Naturally, the Kremlin's just-released 2023 Foreign Policy Concept identifies the United States as the "main source of threats" to Russian security.

But Ukraine, every NATO and European Union member, and several other states are identified as "unfriendly countries", including Australia, Japan, Singapore and New Zealand.

War in the shadows

Russia utilizes a range of methods to wage war in cyberspace.

On one end of the spectrum, it uses groups attached to official agencies, such as the GRU (military intelligence) and the FSB (ostensibly domestic intelligence, but also carries out missions overseas).

The GRU's groups include Sandworm and Fancy Bear. Another group, Cozy Bear, is associated with the FSB.

One or more of these groups have been responsible for a series of prominent cyber attacks on a range of targets, including:

- the Pentagon in 2015
- the Ukrainian power grid in 2015
- the 2016 Democratic National Convention
- the 2017 NotPetya ransomware attacks, which targeted Ukraine but spread globally
- German and French elections in 2017 and 2018
- the International Olympic Committee
- US-based NGOs and think tanks
- COVID-19 vaccine data
- the 2021 Republican National Committee
- and a 2022 attempt to cause a power blackout in Ukraine.

At the other end of the spectrum, Russian information operations regularly use armies of bots and trolls, as well as unsuspecting "citizen curators", to spread false narratives.

Doing so is cheap and increases the distance between the attacker and its agents, allowing for plausible deniability.

Like biological warfare, it also weaponises the targets to do the job of spreading the narrative disease for it.

Russian information campaigns operate globally, among nations it considers its friends as well as its adversaries. Russian-weaponised media can be found in Africa, where the Russian Wagner paramilitary organization has been especially active, as well as in South Asia and Australia.

In many respects, Russian information operations mimic Soviet geopolitical doctrine during the Cold War. This focused on courting areas of the world where the West was weakest.

But in the gray space between official agencies, useful idiots and unwitting proxies is an area of increasing emphasis of Russian cyberwar: outsourcing. Some of these, such as Vulkan, retain an aura of respectability as consultancies that do government work as well as contracting to other firms.

They also include the Internet Research Agency in St Petersburg, which was used to coordinate social media attacks on the US Democratic Party during the 2018 mid-term elections, leading to an indictment by the Department of Justice.

Others are organized criminal gangs, like the aptly named "EvilCorp," that use malware to harvest people's banking details or personal information.

The November 2022 breach of Australia's private health insurer Medibank was one example, which exposed patients' sensitive health details such as treatments for drug addiction or HIV.

The Vulkan revelations

The Vulkan leak adds more detail to what we know about Russian methods, tactics and targets in cyberspace. The GRU group Sandworm is identified as having authorized Vulkan to help build "Skan-V," a piece of software that can monitor the internet to detect vulnerable servers to hack.

Another Vulkan project, known as "Fraction," was designed to monitor social media sites for key words to identify regime opponents, both at home and abroad.

An even larger project in which Vulkan seems to have been engaged was "Amezit." This is a tool that would enable operators to seize control of the internet both inside Russia and in other nations, and hijack information flows.

To function, its users need to be able to control physical infrastructure such as mobile phone towers and wireless internet nodes. Amezit can then be used to mimic legitimate sites and social media profiles, scrub content that might be deemed hostile, and replace it with disinformation.

Given the requirement to possess physical infrastructure, it's clear Azemit was designed not solely as a piece of software, but to operate in tandem with the coercive instruments of a state.

This has internal uses as well as external ones. Domestically, it could be used to silence dissent in restive Russian regions. In a war zone, such as Ukraine, it could be used alongside Russia's armed forces to intercept government communications and swap genuine information sources for false ones.

The Vulkan leak also included information on physical objects. Although not a concise target list, its software allowed users to map physical infrastructure. This included airports worldwide, the Swiss Ministry of Foreign Affairs, and the Muhlberg nuclear power plant near Bern.

What's more, the document drop featured mapped clusters of internet servers in the United States. And the Skan-V project identified a site in the US labeled "Fairfield" as a potentially vulnerable point of entry.

If the documents are accurate, Vulkan's work for the Russian government shows how extensive the Kremlin's attempts have been to monitor digital infrastructure, collect information about vulnerabilities, and develop the capacity to hijack it.

Combating Russian cyber attacks

Cyber threats are insidious because they can be used in multiple combinations and aimed at different targets. Hack-and-leak campaigns against influential figures can be mixed with attempts to sabotage vital infrastructure, perform corporate espionage, undermine social cohesion and trust, and push fringe narratives to the political center.

They can be drip-fed into the digital ecosystem. Or, much like the campaign that accompanied Russia's takeover of Crimea in 2014, they can be employed all at once in a cyber-blizzard.

This makes cyber attacks very hard to build resilience against, and even harder to deter. They are a weapon of potentially mass disruption that can result in real casualties. Turning off the power grid in a city, for example, can lead to deaths among people on life support in hospitals, traffic accidents, and exposure to extreme cold in certain regions.

But beyond infrastructure and industry, such attacks also target social pressure points: a states' institutions, ideas and people. This makes them especially useful in attacking democracies, making the open and free exchange of views a potential vulnerability.

As the Vulkan leaks demonstrate, hostile governments have greater ambitions in cyberspace than being able to switch off the lights. They seek to be able to encourage us to question what we believe to be true, and pit us against one another.

Recognizing that will be a crucial step in preventing the poisonous seeds of disinformation from taking root.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Russia's shadow war: Vulkan files leak show how Putin's regime weaponizes cyberspace (2023, April 4) retrieved 23 April 2024 from https://techxplore.com/news/2023-04-russia-shadow-war-vulkan-leak.html