Who is behind APT29? What we know about this nation-state cybercrime group

John Leyden July 23, 2020

John Leyden 23 July 2020 at 12:40 UTC
Updated: 23 September 2021 at 10:20 UTC
Cyber Warfare Cyber-attacks Cybercrime
APT29 has been accused of targeting coronavirus vaccine organizations, but this is not the first time the group has attracted global attention

In a July 2020 report, the UK and its allies publicly blamed cyber-attacks on organizations involved in coronavirus vaccine development on APT29, a hacking group linked to Russian intelligence agencies.

The National Cyber Security Centre (NCSC), part of GCHQ, blamed APT29 for an ongoing campaign of malicious activity “predominantly against government, diplomatic, think-tank, healthcare and energy targets to steal valuable intellectual property”.

Known targets of APT29 include UK, US and Canadian vaccine research and development organizations, according to a joint alert by NCSC and its intelligence partners in the Canadian Communication Security Establishment and the National Security Agency (NSA).

A full assessment (PDF) offers advice to potentially targeted organizations, as well as firing a shot against the bow of Russian intelligence by publicly calling the Kremlin out for what the NCSC's director of operations, Paul Chichester, described as "despicable attacks against those doing vital work to combat the coronavirus pandemic".

But what do we know about this threat group? The Daily Swig takes a deeper look.

What is APT29?

APT29 is a hacking group that western intelligence agencies and various cybersecurity firms have linked to Russian state intelligence agencies.

Hacked security camera footage allowed the Dutch intelligence service AIVD to link APT29 to the Russian Foreign intelligence service (SVR).

Security intelligence firm CrowdStrike attributed APT29 to either the SVR or Russia's Federal Security Service (FSB).

'APT' in this instance stands for 'advanced persistent threat' – security industry shorthand for a state-sponsored threat group.

APT29 has been given various nicknames by cybersecurity firms, including Cozy Bear, CozyDuke, and the Dukes, among others.

What cyber-attacks have been associated with APT29?

As well as espionage around Covid-19 vaccine data, APT29 has been blamed for a number of other high-profile attacks over the last five years, according to analysis from FireEye Mandiant.

These alleged incidents include:

- Attack on the Pentagon in 2015
- Attack on the US Democratic National Committee (DNC) in 2016
- Attack on Dutch government ministries in 2017
- Assault on Covid-19 vaccine development labs (2020)
- Running a supply chain attack that planted a trojan in updates to SolarWinds Orion enterprise software in a wide-ranging assault ultimately affecting 18,000 organizations but chiefly aimed at US federal government agencies (2020)
- Breaching systems of the Republican National Committee (2021)

According to Symantec, APT29 has been attacking diplomatic organizations and governments since at least 2010, if not earlier.

APT29 Cozy Bear was implicated alongside another Kremlin-linked hacker group, Fancy Bear (APT28, widely credited as a unit of the Russian military intelligence directorate, GRU), in the cyber-attacks against the DNC during 2016 US presidential election.

The threat group is known to be interested in foreign intelligence, according to Finnish security firm F-Secure.

"APT29 has traditionally focused on intelligence to inform national and security policy, rather than the theft of intellectual property," Calvin Gan, manager at F-Secure's tactical defense unit, told The Daily Swig.

"However, Covid-19 could be such a major national security priority for Russia that they need all hands on deck."

How is the workload split between APT29 and other groups?

The tradecraft of APT29 is generally credited as more subtle and sophisticated than that of APT28, the even more infamous Kremlin-linked cybercrime group.

Ben Read, senior manager of analysis at Mandiant Threat Intelligence, told The Daily Swig: "APT29 has historically targeted geopolitical intelligence, with a focus on stealing information.

"They have not been linked to the type of disruptive operations that APT28 and Sandworm team have undertaken but have instead operated with much more discretion."

What are the tactics, techniques, and procedures of APT29?

APT29 uses a variety of tactics, techniques, and procedures (TTPs) including spear-phishing and custom malware known as 'WellMess' and 'WellMail'.

According to Mandiant, APT29 is an adaptive and disciplined threat group that hides its activity on a victim's network.

"In the past it has communicated infrequently and in a way that closely resembles legitimate traffic," Mandiant explains.

"By using legitimate popular web services, the group has taken advantage of encrypted SSL connections, making detection even more difficult."

APT29 is one of the "most evolved and capable threat groups", according to Mandiant's analysis:

It deploys new backdoors to fix its own bugs and add features. It monitors network defender activity to maintain control over systems. APT29 has also often used compromised servers for [command and control] communication.

It counters attempts to remediate attacks. It also maintains a fast development cycle for its malware, quickly altering tools to hinder detection. APT29 has been known to switch tactics and approaches (notably between 'smash-and-grab' and 'slow-and-deliberate') depending on the perceived intelligence value and/or infection method of victims, according to an ATT&CK Evaluations assessment by Mitre Corporation.

APT29 is known to employ a vast arsenal of malware toolsets, according to F-Secure:

The Dukes have engaged in apparently biannual large-scale spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations.

These campaigns utilize a smash-and-grab approach involving a fast but noisy break-in followed by the rapid collection and exfiltration of as much data as possible.

If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long-term intelligence gathering.
More details on APT29's alleged tactics can be found in a recent white paper on APT29 by F-Secure (PDF).

Is it possible to defend against APT29?

Patch management and other techniques can help to defend against APT29 and similar attackers.

"APT groups typically update their arsenal fairly quickly and are customized to the target or environment that they are interested in," F-Secure's Gan explained.

"While EDR [endpoint detection and response] is around to spot for suspicious behaviors within the network, it is only one part of the defense strategy.

"There are other processes and technologies that must be in place to minimize loopholes as much as possible. This includes patch management, as we have seen in the recent advisory of how APT29 purportedly gained a foothold through known vulnerabilities."

Tony Cole, CTO at Attivo Networks, added: "It's unfortunate that an actor such as APT29 with such sophisticated capabilities is still able to simply scan targets for existing known vulnerabilities and then compromise with little effort or use phishing emails to obtain their initial set of credentials.

"Organizations must step up their efforts to counter adversaries targeting them."

Read more of the latest cyber-attack news

Cole continued: "Patching is an imperative that must be met. Instrumentation focused on detection and lateral movement inside the network perimeter and across all endpoints is another imperative since prevention often fails regardless of defensive spending."

Charity Wright, a cyber threat intelligence advisor at IntSights and former NSA Chinese espionage expert, told The Daily Swig: "The Russian intelligence services are organized and deliberate about their targeting, missions, and toolsets. They adapt and overcome target defenses and typically go after strategic intelligence, military, and government entities."

She advised: "Organizations should understand what valuable data they have, which state-sponsored groups would be likely to target them either for their proprietary data or to use them as a third party to pivot to their target, and be prepared to defend against those APTs.

"Utilizing a threat intelligence service, creating intelligence requirements, and integrating tactical intelligence into their defense strategy is vital to protecting their assets. I would also encourage them to conduct threat modeling and purple team exercises to prepare for increases in attacks from nation-state cyber threats."

How does Russia respond to the cybercrime accusations?

Russia's basic stance is to acknowledge that cyber-attacks are happening but to deny any responsibility.

In July 2020, Russia's Ambassador to the UK, Andrei Kelin, gave an interview with Deborah Haynes, foreign affairs editor at Sky News, claiming that Russia itself was frequently targeted by cyber-attacks and calling for the creation of a convention on cyber-warfare.

READ MORE Russian national pleads guilty over involvement in $568m cybercrime operation

“We would like to set up a normal order, under the UN auspices, probably a convention, which would provide for easily understandable rules of cooperation,” Kelin said. “Otherwise there will be a cyber chaos.”

When pressed on accusations that Russia’s cyber activities pose threat to the UK, Kelin raised doubts about attribution.

“The cyber world is extremely complicated, but attribution of cyber-attacks to the government of any country is very dubious,” he said.

During the interview, Kelin went on to dismiss the latest, very specific accusation that Russian intelligence agencies as being behind cyber-attacks against vaccine research centers. “Those accusations are about nothing,” he said.

YOU MIGHT ALSO LIKE Declassified: GCHQ celebrates 100 years of secrets well kept

John Leyden

@jleyden