July 17, 2020

Covid-19 vaccines, economies in peril after Russian APT29 attacks

Teri Robinson
Follow @TeriRnNY

Warnings by officials in the U.S., U.K. and Canada that Russia's Cozy Bear, APT29, is actively trying to steal Covid-19 vaccine research by hacking vaccine trials and dropping WellMess and WellMail malware proves at least two things: Russia military intelligence is still going hard against U.S. targets, and the health care industry, particularly during the pandemic, represents an excruciatingly vulnerable soft underbelly for hackers.

"APT29's campaign of malicious activity is ongoing, predominantly against government, diplomatic, think tank, healthcare and energy targets to steal valuable intellectual property," the U.K.'s National Cyber Security Centre (NCSC) noted in an advisory.

Although the warning, backed by advisories from Canada and the U.S., explained that "throughout 2020, APT29 has targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines," Russia's underlying motives remain hazy. The most straightforward assessment would have the

nation-state actors snagging research to beat competitors to the market with a vaccine of its own – striking a blow to the U.S., which has already invested billions in securing massive doses of vaccines before their efficacy and safety have been established in the hopes that widespread immunization will help stabilize the economy by putting an end to devastating lockdowns and restore normalcy.

"For years, China and Russia have stolen research and other types of valuable data to further their own advancements, and it is clear that cybercriminals adapt and change to what is most important to their government," said LogRhythm CSO and Vice President James Carder, pointing to a May warning from the FBI over Chinese hackers attempts to steal U.S. coronavirus vaccine data. "In this case, being the first country to develop a vaccine would result in not only the protection of their people but also a political and economic advantage."

Calling the race to find a vaccine for COVID-19 "every bit as important as the space race was years ago," John Ford, senior security strategist at IronNet and a former healthcare CISO, said, "In addition to national pride, there is a significant and long-lasting economic benefit that will be bestowed upon the winner."

Until these attacks were revealed, "most people would assume this race was between the United States in combination with our allies, and Chna," he said, but now "we have to ask: has Russia entered the race too? Perhaps, but one thing is very clear – this is not a race that the U.S. can afford to lose."

Still, it could be that Cozy Bear, the APT group within the Russian GRU military intelligence organization that hacked the DNC, seeks to sew chaos and discord much the same way that it did during the 2016 presidential election when its efforts dovetailed with Russia's massive influence campaign to sway results in favor of then-candidate Donald Trump.

That APT29 has changed its modus operandi to targeting research organizations for the purpose of intellectual property theft make it difficult to accurately "speculate if there are ulterior motives or if the end game is truly COVID19 related research, said Bill Swearingen, cybersecurity strategist at IronNet.

Noting that "state-sponsored cyberattacks on the home front have become typical international acts of aggression, particularly among Russian hacking groups that are known for trying to sow discord in Western democracies," Paul Martini, CEO and cofounder of iboss, said "Unfortunately, these bad actors are not above leveraging uncertainty and chaos caused by the coronavirus, and by aiming their attacks at research organizations, that are working overtime to save lives, these groups have shown the lengths to which they will go to wreak havoc."

Russia, not surprisingly, has denied the accusations. "We can say one thing — Russia has nothing at all to do with these attempts," the Tass news agency cited Dmitry Peskov, a spokesman for Russian President Vladimir Putin, as saying.

But NSA Cybersecurity Director Anne Neuberger urged that the threat be taken seriously and NSCS advisory details how the group has used "custom malware known as 'WellMess' and 'WellMail' to target a number of organizations globally," including those involved with COVID-19 vaccine development. "WellMess and WellMail have not previously been publicly associated to APT29," the agency said.

The attackers used basic vulnerability scanning against specific IP addresses owned by the research organizations then deployed public exploits, such as CVE-2019-19781 Citrix, CVE-2019-11510 Pulse Secure, CVE-2018-13379 FortiGate, and CVE-2019-9670 Zimbra against those services identified as vulnerable.

Cozy Bear, aka Dukes, also obtained authentication credentials to internet-accessible login pages for the targeted organizations through spearphishing. "Upon gaining access to a system, the group likely drops further tooling and/or seeks to obtain legitimate credentials to the compromised systems in order to maintain persistent access," the NSCS advisory said, explaining the hackers likely use anonymizing services when they use the nicked credentials.

As the warnings about Cozy Bear's latest attacks on Covid-19 vaccine trials emerged, President Trump was uncharacteristically mum on what the revelations mean for the U.S.'s relationship with Russia going forward and how his administration might respond to these attacks.

The president has spent the better part of four years dismissing Russia's interference in 2016 – and the investigations that followed – as nothing more than a hoax perpetuated by his political opponents, cultivating a friendly relationship with Russian President Vladimir Putin, despite warnings from lawmakers and officials on both sides of the aisle that Russia is continuing its cyber assaults on the U.S.

Swearingen said the U.S. can't afford to "simply be on the sidelines" whether the race is to create the first Covid vaccine or to leverage recent exploits for profit. "It would not be surprising if this group were to leverage CVE-2020-1350 which affects all versions of Windows Server with the Domain Name System (DNS) role enabled when exploit code is released," he said.

The Cozy Bear attacks are a painful reminder of the how vulnerable health care and medical institutions are, particularly during a pandemic. "Like many technology sectors, a lack of security when designing devices and systems prevalent in healthcare research environments and poor cyber hygiene creates targets rich for exploitation," according to a report from the Institute for Critical Infrastructure Technology (ICIT). "Significantly improving cybersecurity in healthcare research environments is not easy and will require cooperation from everyone, including doctors, nurses, IT professionals, and device manufacturers."

But it must be done – as quickly as feasible.

"Securing COVID-19 research centers has become crucial," said Carder, who explained that busy researchers are "unlikely to have cybersecurity at top of mind." Organizations, then, must implement

policies and strategies to identify and respond to the uptick of cyberthreats wrought during the pandemic. must make certain that they have the proper policies and strategies in place to identify and respond to the increase in cyberthreats that we have seen throughout the pandemic. Even “basic education on handling email and training on red flags to look out for, such as an email having unnecessarily urgent language or a news that’s a bit too good to be true, can help users who are perhaps not fully attentive to phishing emails,” he said.

Back to Top ↑

Videos

Executive Insight Guidelines

Subscribe

Editorial Calendar

OTHER SC SITES

RiskSec Conference

SC Resource Library

SC Online Events

SC Awards