Lapsus$ Activity Betrays Nation-State Motivation

By Sam Curry

Archived: 2026-04-05 18:37:34 UTC

A new cybercrime group has made headlines recently with a release of evidence they had hacked both Okta and Microsoft. Lapsus$--which emerged only a few months ago—seems reminiscent of early script-kiddie groups motivated by notoriety and claims to be in it for the money.

However, a closer examination of the group's tactics and targets suggests they may have a different agenda because Russia has used mercenaries from the Wagner Group–both in Syria and currently in its invasion of Ukraine–to execute operations they don't want directly traceable to the Kremlin. It is fair to assume they also may engage cyber mercenaries and follow a similar strategy for cyberattacks.

Lapsus$ Hacking Group

Lapsus$ is a relatively new hacker group that is believed to be based in Brazil. A profile by Wired from March 15, 2022 notes that their initial attacks primarily targeted Portuguese-language targets. "In December and January, the group hacked and attempted to extort Brazil's health ministry, the Portuguese media giant Impresa, the South American telecoms Claro and Embratel, and Brazilian car rental company Localiza, among others."

The group is not a ransomware gang. They have focused on data theft and extortion but have not been known to encrypt systems or data. Lapsus$ originally seemed to gain access to victim networks and systems through phishing attacks. They have also been known to use denial-of-service attacks and more mischievous tactics like redirecting a victim's website to an adult entertainment site in their self-proclaimed pursuit of non-state-sponsored profit.

Bloomberg published a story identifying a British teen as the mastermind behind Lapsus$, and police in the United Kingdom subsequently arrested 7 suspects ranging in age from 16 to 21. However, it is still unclear whether those suspects are actually connected to Lapsus$ at all.

The last message published by Lapsus$ on their Telegram account last week stated, "A few of our members has a vacation until 30/3/2022. We might be quiet for some times. Thanks for understand us - we will try to leak stuff ASAP." And, as promised, Lapsus$ returned on March 30 to publish a 70GB torrent file with data allegedly stolen from Globant–a large software development consultancy.

Lapsus$ is also linked to a group called "Recursion Team" in a recent report that claims they were able to obtain sensitive user data from Apple, Meta, and other tech companies by posing as law enforcement officials and using forged "emergency data requests." Recursion Team is no longer active, but cybersecurity researchers believe that some of the individuals associated with Recursion Team moved on to form or join Lapsus$.

It is worth noting that Lapsus$ also claims that the suspects arrested in the United Kingdom are not part of the group and that no members of Lapsus$ have been arrested. Perhaps that is true, or maybe Lapsus$ recruited

minors with the intent to expose them as a distraction if needed. Whether the individuals arrested in the United Kingdom are part of Lapsus$ or not, it seems like Lapsus$ is still going strong and there is still a question about what their motives are.

Me Thinks Thou Dost Protest Too Much

The group has gone out of its way to emphasize that they are financially motivated and that they are not a nation-state threat actor.

Lapsus$ issued a statement in December on its Telegram channel stressing, “Remember: The only goal is money, our reasons are not political.”

The Wired profile points out that Lapsus$ reiterated this after breaching Nvidia in February. The group shared on Telegram, “Please note: We are not state sponsored and we are not in politics AT ALL.”

While it may be true that Lapsus$ is just a group of malicious hackers looking for quick cash, the statements also seem suspect. The very fact that they are so vocal about not being a nation-state actor raises the question of whether they might be just that.

Profit Motive with No Profit

Whatever the group started out as, or whatever it claims to be, the pattern and profile of recent targets indicate a radical change in behavior and personality. There no longer appears to be any profit motive for recent attacks, and there is no logical business model at face value.

A cybercrime gang that is motivated by money would focus on simple, low-cost attacks that have the highest potential for a quick and lucrative return. The reason ransomware is popular is that it enables attackers to generate significant revenue with very little effort and even less chance of being caught and held accountable. They would also not be spending money absent a business model on credentials, as they advertise on Telegram:

Krebsonsecurity.com shared a screenshot of a Lapsus$ post on its Telegram channel soliciting insiders from telecom and tech companies to provide credentials for attacks.

But, Lapsus$ is not using ransomware, and no longer seems to be pursuing profit at all. They have shifted radically from DDoS extortion attacks against companies in Latin America to attacks against large global tech giants—companies like Samsung, Nvidia, Ubisoft, Okta, and Microsoft that millions of companies and government agencies around the world rely on.

Not only are the Lapsus$ attacks not generating revenue as far as we know, but the group is actually investing money in the attacks. Lapsus$ is reportedly bribing employees at target companies or their partners and suppliers to share credentials to facilitate the attacks. This significantly drives up the cost of the attacks, but there is no evidence they are realizing any return on the investment.

That is unless someone else is paying them.

Lapsus$ Business Model

The burning question when it comes to Lapsus$ is, “What is their business model now that they have shifted tactics and targets?”

Either the initial attacks and statements were outright lies or an elaborate ruse, or there is something else going on behind the scenes. It does not make any sense for Lapsus$ to spend money and resources on high-profile attacks that do not yield any profit.

The pattern and current business model lead to two potential conclusions. Either Lapsus$ is engaged in contract work on behalf of a third party, or the group is actually a nation-state threat actor hiding behind a script-kiddie façade.

Either way, the most obvious puppet master is Russia.

From Russia, With Love

Russia spent the first couple of months of this year massing its military strategically along the border with Ukraine —both from Russia and “conducting joint military exercises” with Ukraine’s northern neighbor, Belarus. Despite aggressive efforts to find a diplomatic solution to convince Putin to deescalate, Russia invaded Ukraine at the end of February.

As tensions increased, there was much speculation that Russia would engage in widespread cyberattacks prior to or in conjunction with the launch of the military invasion. However, that didn’t really happen. There were some minor attacks and evidence of malicious wipers planted on some servers in Ukraine, but nothing like the scale or scope of attacks that were expected.

That may be strategic. Russia likely understands that there is an ongoing debate about the line between cyberwar and traditional war, and whether or not a cyberattack warrants a kinetic response. Russia talks big, but Putin and his advisors probably understand that an overt cyberattack from Russia risks escalation that might give nations like the United States and NATO allies justification to respond.

Russia has two notorious world-class APTs. APT-28 is a function of Russia’s military intelligence agency (GRU), and APT-29 is associated with the Foreign Intelligence Service (SVR) and/or the Federal Security Service (FSB). Major cyberattacks and disinformation campaigns, including the hack of the Democratic National Committee, NotPetya, and the SolarWinds hack, have been attributed to these two APTs. So, why is Russia not using these resources more aggressively with regard to the invasion of Ukraine?

One likely answer is that they don’t want to burn their stockpile of zero-days or perhaps even grow it. If APT28 and APT29 use their zero-day exploits, they will lose effectiveness as cybersecurity vendors and the world’s de facto immune system reacts and identifies the IOCs to render them useless. It is fair to assume that Russia has a hoard of dangerous zero-day exploits, but that this may not be the right time to use them. It would make sense to use such exploits in a massive, simultaneous assault on adversary critical infrastructure targets at a future date.

Russia also has access to a number of cybercrime gangs. Groups like Conti, Darkside, and REvil are private entities, but with ties to the Russian intelligence apparatus. Russia allows them to operate in a state-ignored or state-condoned way with attacks that align with Russian state interests but give Putin and the Russian government some degree of plausible deniability.

That arms-length separation may not be enough right now, though. Perhaps Russia is cognizant of the risk that cyberattacks from Russia itself or Russian threat actors believed to be working on behalf of Russia would likely result in a much stronger response from the United States and NATO allies that could escalate the conflict beyond what Russia is comfortable with.

If It Quacks Like a Duck

That is where Lapsus$ comes in. The recent change in tactics and behavior could be an indication that the group has been commissioned as “cyber mercenaries” working on Russia’s behalf. It benefits Russia to have an “independent” cybercrime gang wreak havoc on adversary nations and gain access to source code and valuable intelligence that Russia can use for future cyberattacks, delivery mechanisms, and tools.

The fact that Lapsus$ is spending money to buy credentials to carry out operations implies they are getting the money from somewhere—or they are themselves a nation-state threat actor. Either Russia (or another threat actor aligned with Russia) is paying them, or they lied about being financially motivated in the first place and they’re actually a nation-state threat actor using the Brazil script-kiddie façade as cover. Either way, the tactics, and motives only make sense if there is a nation-state actor involved.

In either case, if it’s true that Lapsus$ is working with or for Russia, then the war in Ukraine has expanded even further beyond the nations’ borders. It’s possible we are only seeing the tip of the iceberg where cyber mercenaries and Russian interests are concerned. The potential exists that we may be at risk of a massive, coordinated attack targeting multiple critical entities simultaneously.

This is all speculation at this point. It is just educated guesses and analysis of evidence and trends to arrive at possible—or probable—conclusions. But, if it walks like a duck and quacks like a duck, it’s probably a Russian threat actor.

About the Author

Sam Curry

Sam Curry is CSO at Cybereason and is a Visiting Fellow at the National Security Institute. Previously, Sam was CTO and CISO for Arbor Networks (NetScout) and was CSO and SVP R&D at MicroStrategy in addition to holding senior security roles at McAfee and CA. He spent 7 years at RSA, the Security Division of EMC as Chief Technologist and SVP of Product. Sam also has over 20 patents in security from his time as a security architect, has been a leader in two successful startups and is a board member of the Cybersecurity Coalition, of SSH Communications and of Sequitur Labs.

All Posts by Sam Curry
