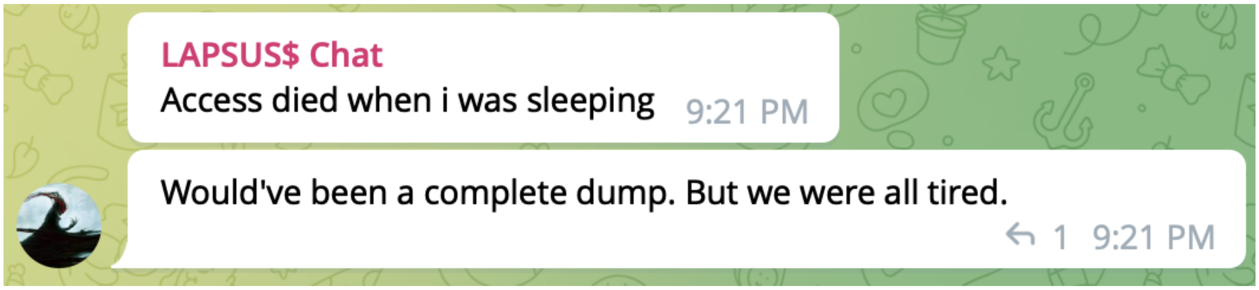
A Closer Look at the LAPSUS$ Data Extortion Group

krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

Microsoft and identity management platform **Okta** both this week disclosed breaches involving **LAPSUS$**, a relatively new cybercrime group that specializes in stealing data from big companies and threatening to publish it unless a ransom demand is paid. Here's a closer look at LAPSUS$, and some of the low-tech but high-impact methods the group uses to gain access to targeted organizations.

First surfacing in December 2021 with an extortion demand on Brazil's Ministry of Health, LAPSUS$ made headlines more recently for posting screenshots of internal tools tied to a number of major corporations, including **NVIDIA, Samsung, and Vodafone.**

On Tuesday, LAPSUS$ announced via its Telegram channel it was releasing source code stolen from Microsoft. In a blog post published Mar. 22, Microsoft said it interrupted the LAPSUS$ group's source code download before it could finish, and that it was able to do so because LAPSUS$ publicly discussed their illicit access on their Telegram channel before the download could complete.



LAPSUS$ Chat
Access died when i was sleeping 9:21 PM

Would've been a complete dump. But we were all tired. 1 9:21 PM

One of the LAPSUS$ group members admitted on their Telegram channel that the Microsoft source code download had been interrupted.

"This public disclosure escalated our action allowing our team to intervene and interrupt the actor mid-operation, limiting broader impact," Microsoft wrote. "No customer code or data was involved in the observed activities. Our investigation has found a single account had been compromised, granting limited access. Microsoft does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk."

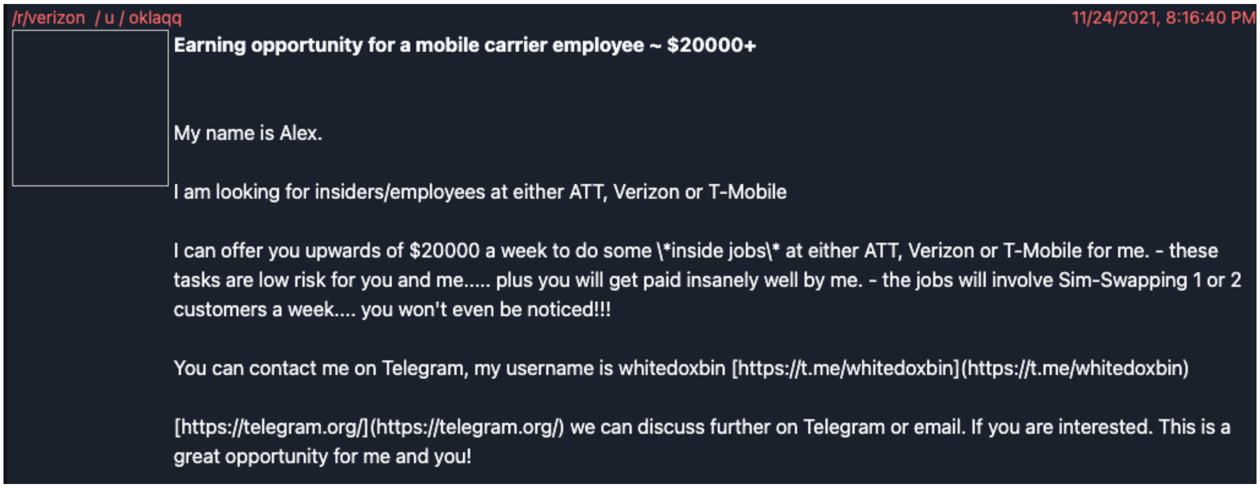
While it may be tempting to dismiss LAPSUS$ as an immature and fame-seeking group, their tactics should make anyone in charge of corporate security sit up and take notice. Microsoft says LAPSUS$ — which it boringly calls "**DEV-0537**" — mostly gains illicit access to targets via "social engineering." This involves bribing or tricking employees at the target organization or at its myriad partners, such as customer support call centers and help desks.

“Microsoft found instances where the group successfully gained access to target organizations through recruited employees (or employees of their suppliers or business partners),” Microsoft wrote. The post continues:

> “DEV-0537 advertised that they wanted to buy credentials for their targets to entice employees or contractors to take part in its operation. For a fee, the willing accomplice must provide their credentials and approve the MFA prompt or have the user install AnyDesk or other remote management software on a corporate workstation allowing the actor to take control of an authenticated system. Such a tactic was just one of the ways DEV-0537 took advantage of the security access and business relationships their target organizations have with their service providers and supply chains.”

The LAPSUS$ Telegram channel has grown to more than 45,000 subscribers, and Microsoft points to an ad LAPSUS$ posted there offering to recruit insiders at major mobile phone providers, large software and gaming companies, hosting firms and call centers.

Sources tell KrebsOnSecurity that LAPSUS$ has been recruiting insiders via multiple social media platforms since at least November 2021. One of the core LAPSUS$ members who used the nicknames “Oklaqq” and “WhiteDoxbin” posted recruitment messages to Reddit last year, offering employees at AT&T, T-Mobile and Verizon up to $20,000 a week to perform “inside jobs.”



/r/verizon / u / oklaqq

11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

My name is Alex.

I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!

LAPSUS$ leader Oklaqq a.k.a. “WhiteDoxbin” offering to pay $20,000 a week to corrupt employees at major mobile providers.

Many of LAPSUS$’s recruitment ads are written in both English and Portuguese. According to cyber intelligence firm Flashpoint, the bulk of the group’s victims (15 of them) have been in Latin America and Portugal.

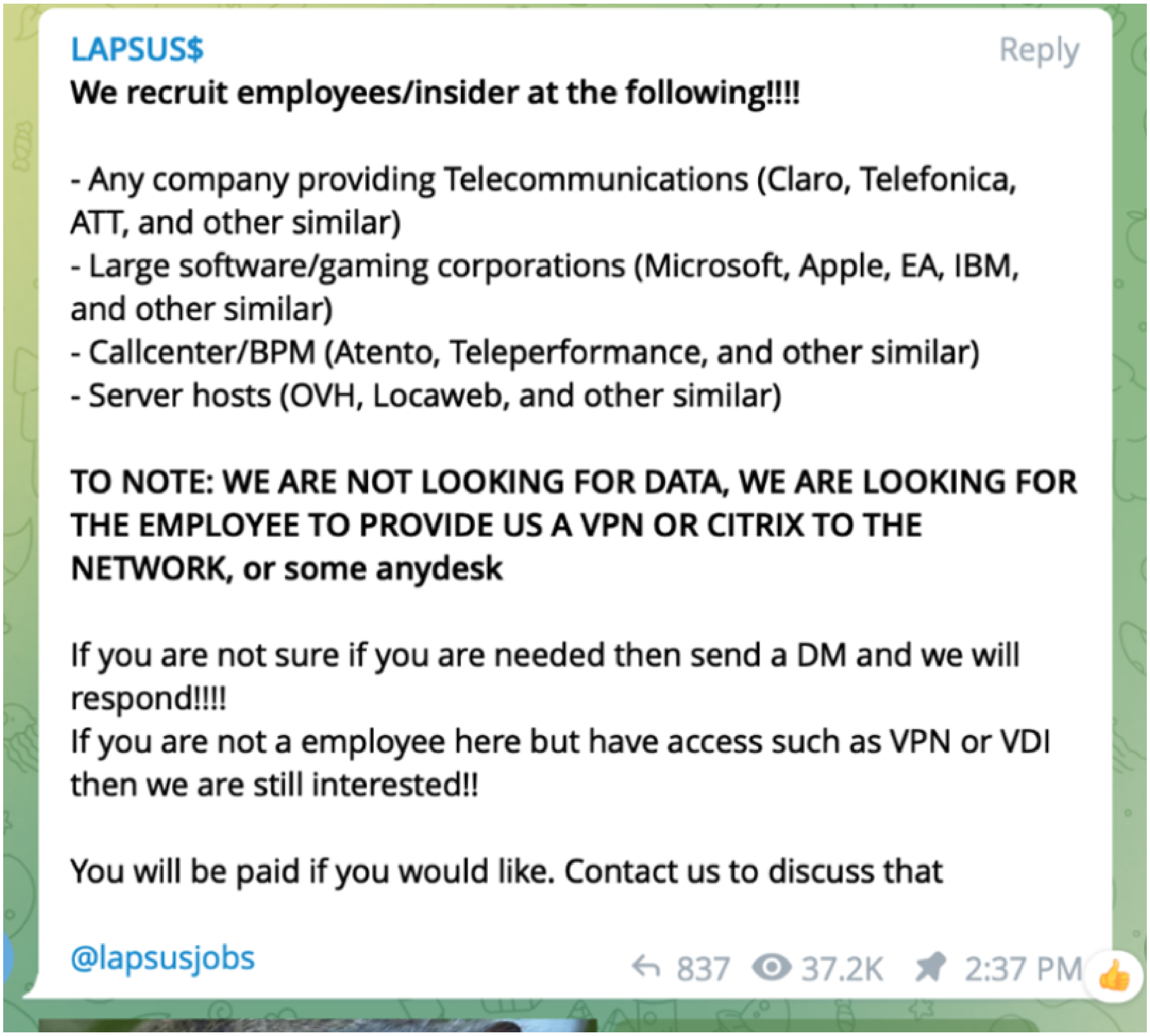
“LAPSUS$ currently does not operate a clearnet or darknet leak site or traditional social media accounts—it operates solely via Telegram and email,” Flashpoint wrote in an analysis of the group. “LAPSUS$ appears to be highly sophisticated, carrying out increasingly high-profile data breaches. The group has claimed it is not state-sponsored. The individuals behind the group are likely experienced and have demonstrated in-depth technical knowledge and abilities."

Microsoft said LAPSUS$ has been known to target the personal email accounts of employees at organizations they wish to hack, knowing that most employees these days use some sort of VPN to remotely access their employer's network.

"In some cases, [LAPSUS$] first targeted and compromised an individual's personal or private (non-work-related) accounts giving them access to then look for additional credentials that could be used to gain access to corporate systems," Microsoft wrote. "Given that employees typically use these personal accounts or numbers as their second-factor authentication or password recovery, the group would often use this access to reset passwords and complete account recovery actions."

In other cases, Microsoft said, LAPSUS$ has been seen calling a target organization's help desk and attempting to convince support personnel to reset a privileged account's credentials.

"The group used the previously gathered information (for example, profile pictures) and had a native-English-sounding caller speak with the help desk personnel to enhance their social engineering lure," Microsoft explained. "Observed actions have included DEV-0537 answering common recovery prompts such as "first street you lived on" or "mother's maiden name" to convince help desk personnel of authenticity. Since many organizations outsource their help desk support, this tactic attempts to exploit those supply chain relationships, especially where organizations give their help desk personnel the ability to elevate privileges."



LAPSUS$

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

837 37.2K 2:37 PM

LAPSUS$ recruiting insiders via its Telegram channel.

SIM-SWAPPING PAST SECURITY

Microsoft said LAPSUS$ also has used "SIM swapping" to gain access to key accounts at target organizations. In a fraudulent SIM swap, the attackers bribe or trick mobile company employees into transferring a target's mobile phone number to their device. From there, the attackers can intercept any one-time passwords sent to the victim via SMS or phone call. They can also then reset the password for any online account that allows password resets via a link sent over SMS.

"Their tactics include phone-based social engineering; SIM-swapping to facilitate account takeover; accessing personal email accounts of employees at target organizations; paying employees, suppliers, or business partners of target organizations for access to credentials and multifactor authentication (MFA) approval; and intruding in the ongoing crisis-communication calls of their targets," Microsoft wrote.

Allison Nixon is chief research officer at Unit 221B, a cybersecurity consultancy based in New York that closely tracks cybercriminals involved in SIM-swapping. Working with researchers at security firm **Palo Alto Networks**, Nixon has been tracking individual members of LAPSUS$ prior to their forming the group, and says the social engineering techniques adopted by the group have long been abused to target employees and contractors working for the major mobile phone companies.

“LAPSUS$ may be the first to make it extremely obvious to the rest of the world that there are a lot of soft targets that are not telcos,” Nixon said. “The world is full of targets that are not used to being targeted this way.”

Microsoft says LAPSUS$ also has been known to gain access to victim organizations by deploying the “Redline” password-stealing malware, searching public code repositories for exposed passwords, and purchasing credentials and session tokens from criminal forums.

That last bit is interesting because Nixon said it appears at least one member of LAPSUS$ also was involved in the intrusion at game maker **Electronic Arts** (EA) last year, in which extortionists demanded payment in exchange for a promise not to publish 780 GB worth of source code. In an interview with *Motherboard*, the hackers claimed to have gained access to EA’s data after purchasing authentication cookies for an EA Slack channel from a dark web marketplace called Genesis.

“The hackers said they used the authentication cookies to mimic an already-logged-in EA employee’s account and access EA’s Slack channel and then trick an EA IT support staffer into granting them access to the company’s internal network,” wrote **Catalin Cimpanu** for *The Record*.

Why is Nixon convinced LAPSUS$ was behind the EA attack? The “WhiteDoxbin/Oklaqq” identity referenced in the first insider recruitment screenshot above appears to be the group’s leader, and it has used multiple nicknames across many Telegram channels. However, Telegram lumps all aliases for an account into the same Telegram ID number.

Back in May 2021, WhiteDoxbin’s Telegram ID was used to create an account on a Telegram-based service for launching distributed denial-of-service (DDoS) attacks, where they introduced themself as “**@breachbase**.” News of EA’s hack last year was first posted to the cybercriminal underground by the user “Breachbase” on the English-language hacker community **RaidForums**, which was recently seized by the FBI.

WHO IS LAPSUS$?

Nixon said WhiteDoxbin — LAPSUS$’s apparent ringleader — is the same individual who last year purchased the **Doxbin**, a long-running, text-based website where anyone can post the personal information of a target, or find personal data on hundreds of thousands who have already been “doxed.”

Apparently, Doxbin's new owner failed to keep the site functioning smoothly, because top Doxbin members had no problems telling WhiteDoxbin how unhappy they were with his stewardship.

"He wasn't a good administrator, and couldn't keep the website running properly," Nixon said. "The Doxbin community was pretty upset, so they started targeting him and harassing him."

Nixon said that in January 2022, WhiteDoxbin reluctantly agreed to relinquish control over Doxbin, selling the forum back to its previous owner at a considerable loss. However, just before giving up the forum, WhiteDoxbin leaked the entire Doxbin data set (including private doxes that had remained unpublished on the site as drafts) to the public via Telegram.

The Doxbin community responded ferociously, posting on WhiteDoxbin perhaps the most thorough dox the community had ever produced, including videos supposedly shot at night outside his home in the United Kingdom.

According to the denizens of Doxbin, WhiteDoxbin started out in the business of buying and selling zero-day vulnerabilities, security flaws in popular software and hardware that even the makers of those products don't yet know about.

"[He] slowly began making money to further expand his exploit collection," reads his Doxbin entry. "After a few years his net worth accumulated to well over 300BTC (close to $14 mil)."

WhiteDoxbin's Breachbase identity on RaidForums at one point in 2020 said they had a budget of $100,000 in bitcoin with which to buy zero-day flaws in Github, Gitlab, Twitter, Snapchat, Cisco VPN, Pulse VPN and other remote access or collaboration tools.

"My budget is $100000 in BTC," Breachbase told Raidforums in October 2020. "Person who directs me to someone will get $10000 BTC. Reply to thread if you know anyone or anywhere selling this stuff. NOTE: The 0day must have high/critical impact."

KrebsOnSecurity is not publishing WhiteDoxbin's alleged real name because he is a minor (currently aged 17), and because this person has not officially been accused of a crime. Also, the Doxbin entry for this individual includes personal information on his family members.

Nixon said that prior to launching LAPSUS$, WhiteDoxbin was a founding member of a cybercriminal group calling itself the "Recursion Team." According to the group's now-defunct website, they mostly specialized in SIM swapping targets of interest and participating in "swatting" attacks, wherein fake bomb threats, hostage situations and other violent scenarios are phoned in to police as part of a scheme to trick them into visiting potentially deadly force on a target's address.

“The team is made up of Cyber-enthusiasts who major in skills including security penetration, software development, and botting,” reads the now-defunct Recursion Team website. “We plan to have a bright future, and we hope you do too!”

Update, March 24, 11:11 a.m. ET: The **BBC** is quoting City of London Police as saying seven people between the ages of 16 and 21 have been arrested in connection with an investigation into a hacking group. All have been released under investigation.