Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code

Published: 2022-04-22 · Archived: 2026-04-05 21:23:39 UTC

KrebsOnSecurity recently reviewed a copy of the private chat messages between members of the **LAPSUS$** cybercrime group in the week leading up to the arrest of its most active members last month. The logs show LAPSUS$ breached **T-Mobile** multiple times in March, stealing source code for a range of company projects. T-Mobile says no customer or government information was stolen in the intrusion.

LAPSUS$ is known for stealing data and then demanding a ransom not to publish or sell it. But the leaked chats indicate this mercenary activity was of little interest to the tyrannical teenage leader of LAPSUS$, whose obsession with stealing and leaking proprietary computer source code from the world's largest tech companies ultimately led to the group's undoing.

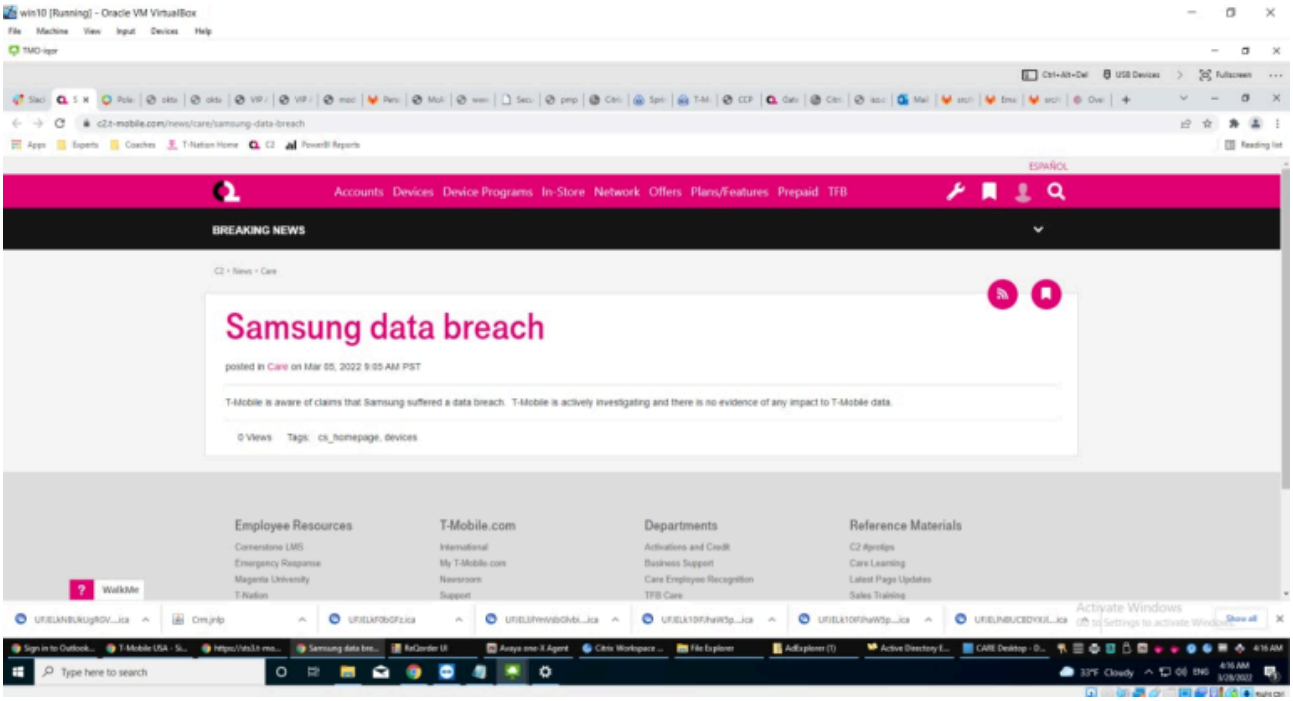
From its inception in December 2021 until its implosion late last month, LAPSUS$ operated openly on its **Telegram** chat channel, which quickly grew to more than 40,000 followers after the group started using it to leak huge volumes of sensitive data stolen from victim corporations.

But LAPSUS$ also used private Telegram channels that were restricted to the core seven members of the group. KrebsOnSecurity recently received a week's worth of these private conversations between LAPSUS$ members as they plotted their final attacks late last month.

The candid conversations show LAPSUS$ frequently obtained the initial access to targeted organizations by purchasing it from sites like **Russian Market**, which sell access to remotely compromised systems, as well as any credentials stored on those systems.

The logs indicate LAPSUS$ had exactly zero problems buying, stealing or sweet-talking their way into employee accounts at companies they wanted to hack. The bigger challenge for LAPSUS$ was the subject mentioned by "Lapsus Jobs" in the screenshot above: Device enrollment. In most cases, this involved social engineering employees at the targeted firm into adding one of their computers or mobiles to the list of devices allowed to authenticate with the company's virtual private network (VPN).

The messages show LAPSUS$ members continuously targeted **T-Mobile** employees, whose access to internal company tools could give them everything they needed to conduct hassle-free "SIM swaps" — reassigning a target's mobile phone number to a device they controlled. These unauthorized sim swaps allow an attacker to intercept a target's text messages and phone calls, including any links sent via SMS for password resets, or one-time codes sent for multi-factor authentication.

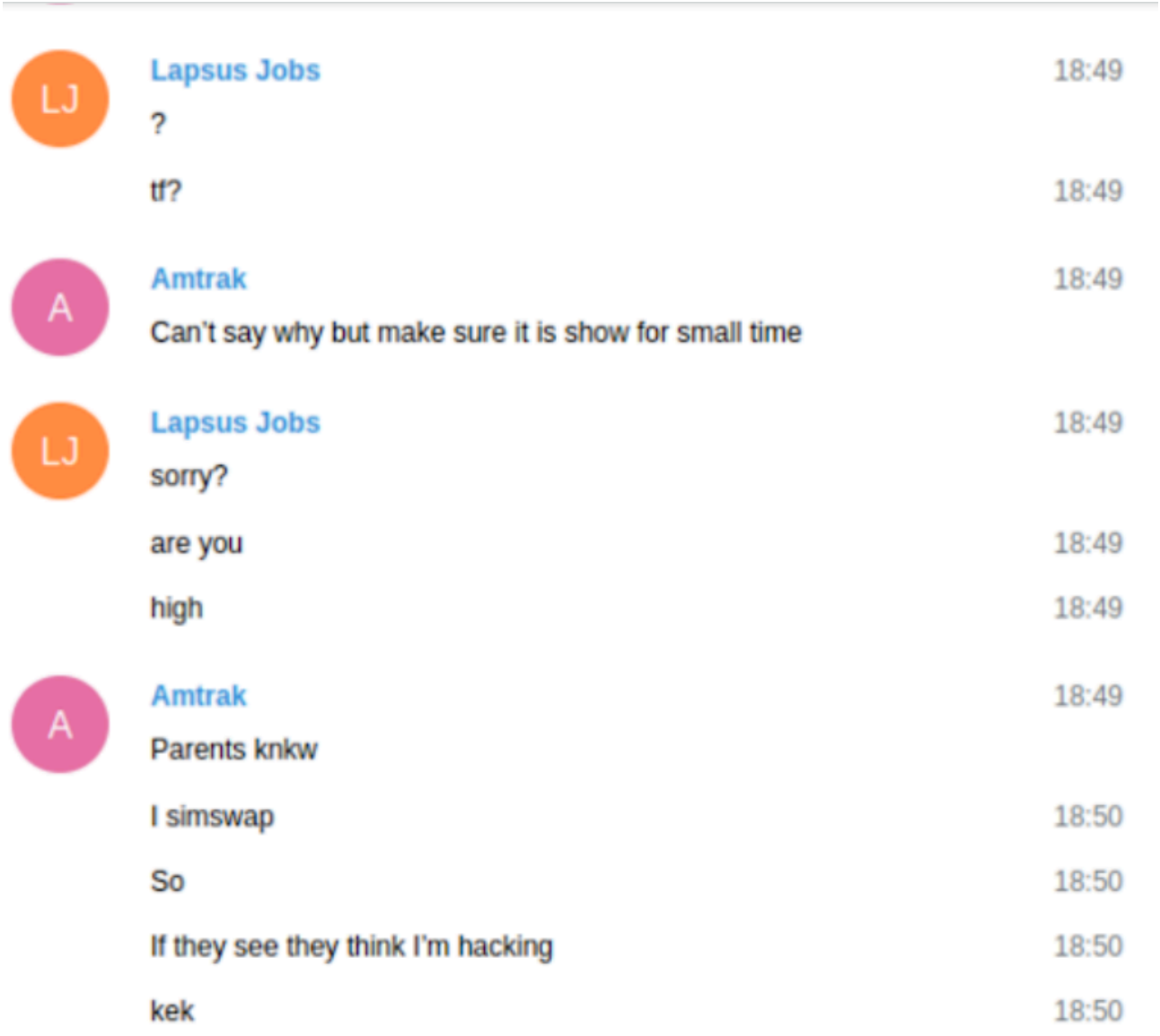


The LAPSUS$ group had a laugh at this screenshot posted by their leader, White, which shows him reading a T-Mobile news alert about their hack into Samsung. White is viewing the page via a T-Mobile employee's virtual machine.

In one chat, the LAPSUS$ leader — a 17-year-old from the U.K. who goes by the nicknames "**White**," "**WhiteDoxbin**" and "**Oklaqq**" — is sharing his screen with another LAPSUS$ member who used the handles "**Amtrak**" and "**Asyntax**."

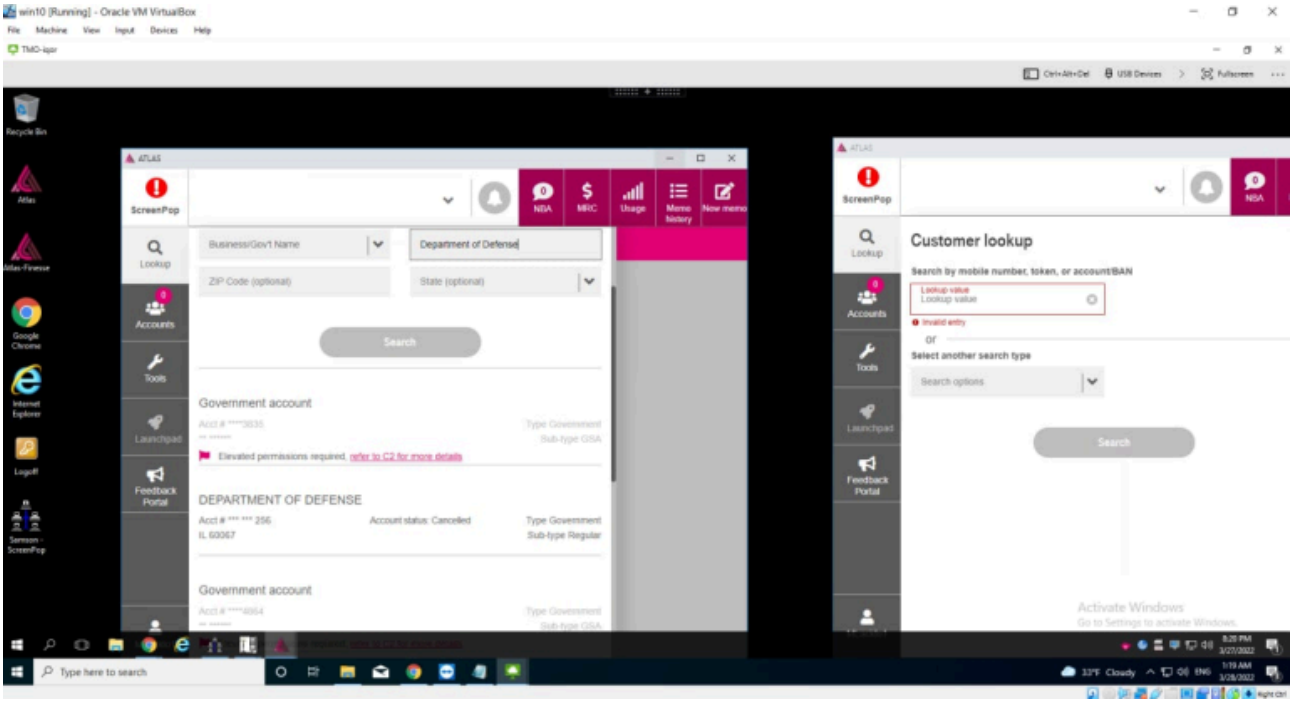
The two were exploring T-Mobile's internal systems, and Amtrak asked White to obscure the T-Mobile logo on his screen. In these chats, the user "**Lapsus Jobs**" is White. Amtrak explains this odd request by saying their parents are aware Amtrak was previously involved in SIM swapping.

"Parents know I simswap," Amtrak said. "So, if they see [that] they think I'm hacking."



The messages reveal that each time LAPSUS$ was cut off from a T-Mobile employee's account — either because the employee tried to log in or change their password — they would just find or buy another set of T-Mobile VPN credentials. T-Mobile currently has approximately 75,000 employees worldwide.

On March 19, 2022, the logs and accompanying screenshots show LAPSUS$ had gained access to **Atlas**, a powerful internal T-Mobile tool for managing customer accounts.

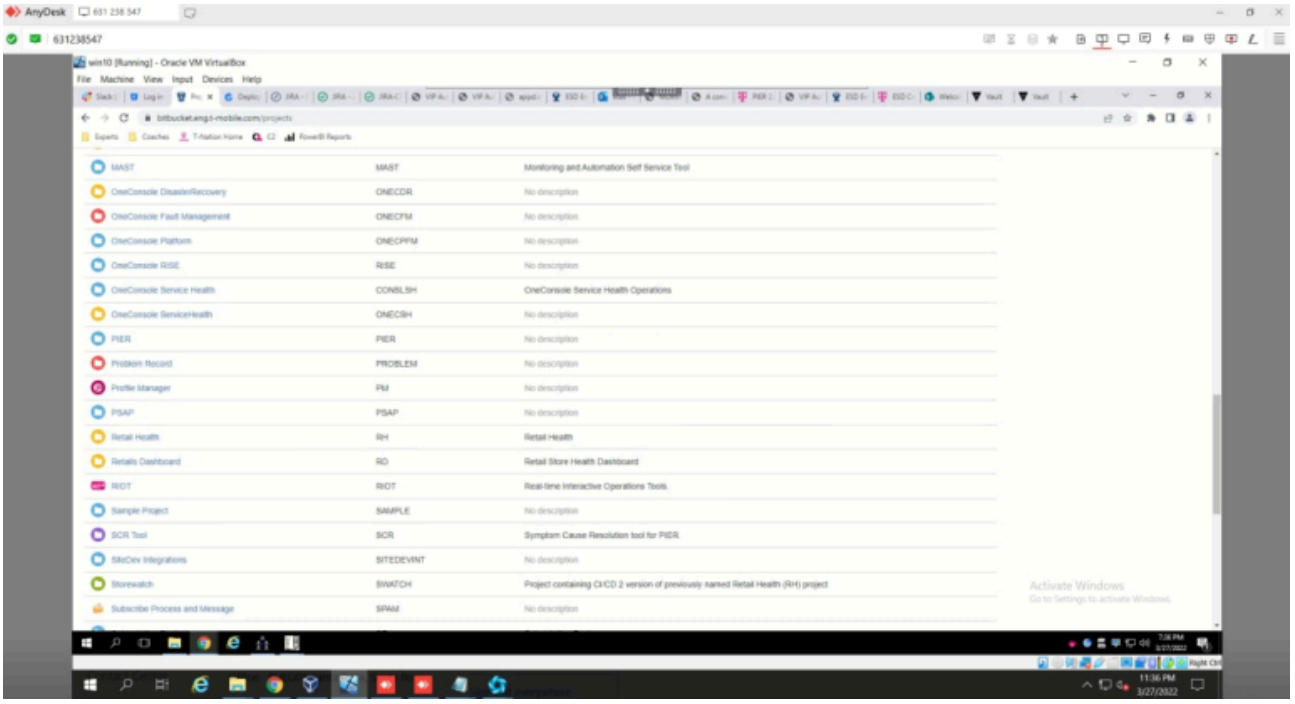


LAPSUS$ leader White/Lapsus Jobs looking up the Department of Defense in T-Mobile's internal Atlas system.

After gaining access to Atlas, White proceeded to look up T-Mobile accounts associated with the **FBI** and **Department of Defense** (see image above). Fortunately, those accounts were listed as requiring additional verification procedures before any changes could be processed.

Faced with increasingly vocal pleadings from other LAPSUS$ members not to burn their access to Atlas and other tools by trying to SIM swap government accounts, White unilaterally decided to terminate the VPN connection permitting access to T-Mobile's network.

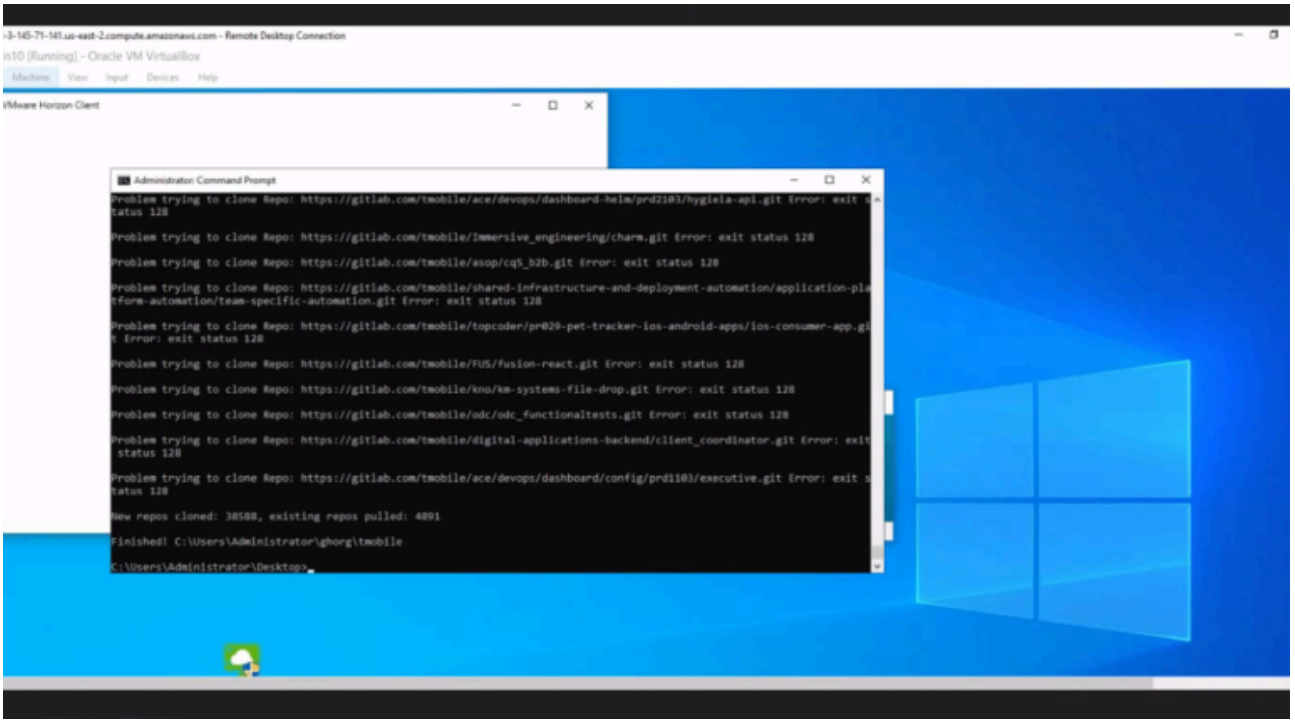
The other LAPSUS$ members desperately wanted to SIM swap some wealthy targets for money. Amtrak throws a fit, saying "I worked really hard for this!" White calls the Atlas access trash and then kills the VPN connection anyway, saying he wanted to focus on using their illicit T-Mobile access to steal source code.



A screenshot taken by LAPSUS$ inside T-Mobile's source code repository at Bitbucket.

Perhaps to mollify his furious teammates, White changed the subject and told them he'd gained access to T-Mobile's **Slack** and **Bitbucket** accounts. He said he'd figured out how to upload files to the virtual machine he had access to at T-Mobile.

Roughly 12 hours later, White posts a screenshot in their private chat showing his automated script had downloaded more than 30,000 source code repositories from T-Mobile.



White showing a screenshot of a script that he said downloaded all available T-Mobile source code.

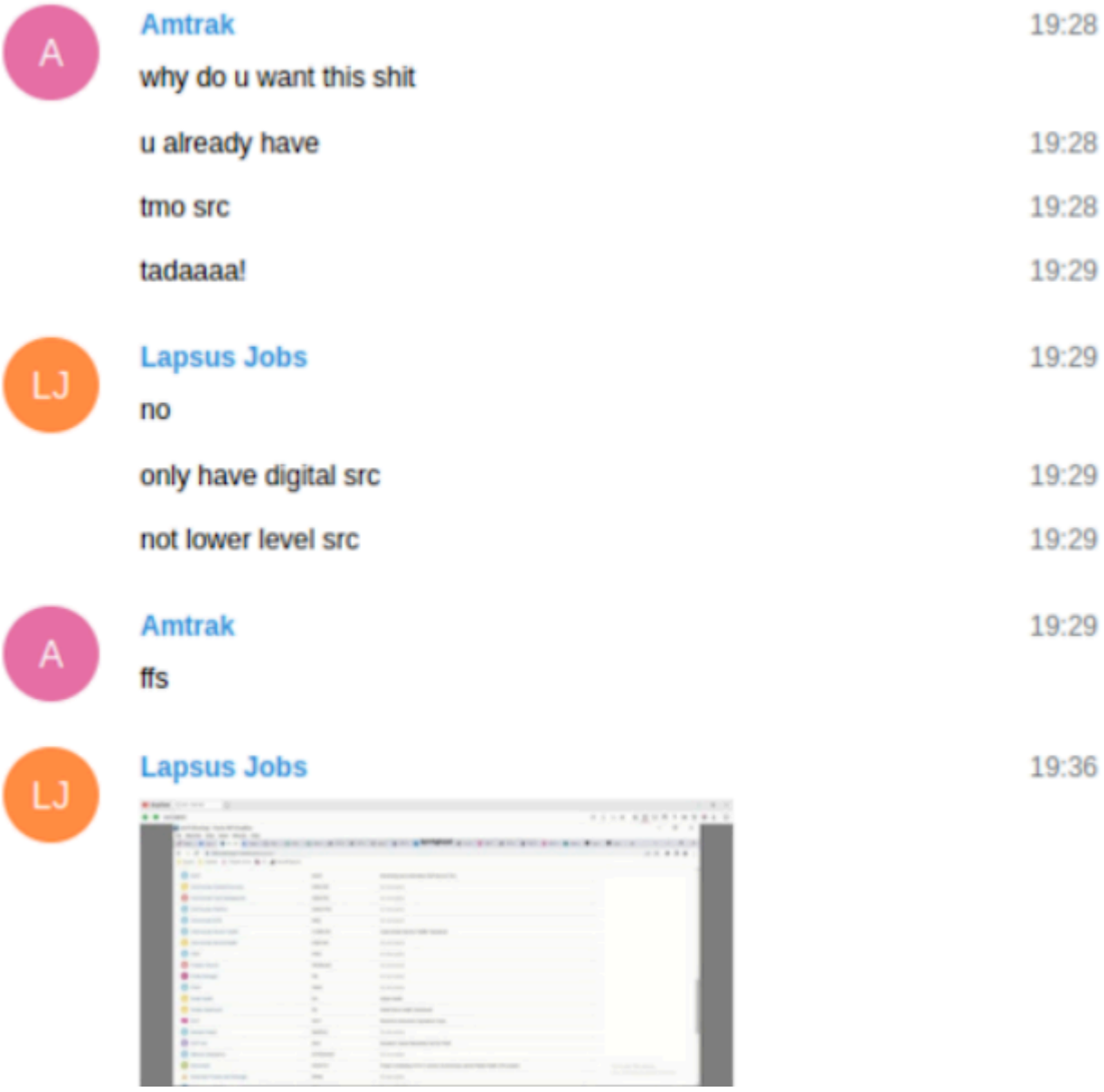
In response to questions from KrebsOnSecurity, T-Mobile issued the following statement:

“Several weeks ago, our monitoring tools detected a bad actor using stolen credentials to access internal systems that house operational tools software. The systems accessed contained no customer or government information or other similarly sensitive information, and we have no evidence that the intruder was able to obtain anything of value. Our systems and processes worked as designed, the intrusion was rapidly shut down and closed off, and the compromised credentials used were rendered obsolete.”

CONSIDER THE SOURCE

It is not clear why LAPSUS$ was so fixated on stealing source code. Perhaps LAPSUS$ thought they could find in the source clues about security weaknesses that could be used to further hack these companies and their customers. Maybe the group already had buyers lined up for specific source code that they were then hired to procure. Or maybe it was all one big Capture the Flag competition, with source code being the flag. The leaked chats don’t exactly explain this fixation.

But it seems likely that the group routinely tried to steal and then delete any source code it could find on victim systems. That way, it could turn around and demand a payment to restore the deleted data.



In one conversation in late March, a LAPSUS$ member posts screenshots and other data indicating they'd gained remote administrative access to a multi-billion dollar company. But White is seemingly unimpressed, dismissing the illicit access as not worth the group's time because there was no source code to be had.

LAPSUS$ first surfaced in December 2021, when it hacked into Brazil's Ministry of Health and deleted more than 50 terabytes of data stored on the ministry's hacked servers. The deleted data included information related to the ministry's efforts to track and fight the COVID-19 pandemic in Brazil, which has suffered a disproportionate 13 percent of the world's COVID-19 fatalities. LAPSUS$'s next 15 victims were based either in Latin America or Portugal, according to cyber threat intelligence firm Flashpoint.

By February 2022, LAPSUS$ had pivoted to targeting high-tech firms based in the United States. On Feb. 26, LAPSUS$ broke into graphics and computing chip maker **NVIDIA**. The group said it stole more than a terabyte of NVIDIA data, including source code and employee credentials.

Dan Goodin at *Ars Technica* wrote about LAPSUS$'s unusual extortion demand against NVIDIA: The group pledged to publish the stolen code unless NVIDIA agreed to make the drivers for its video cards open-source. According to these chats, NVIDIA responded by connecting to the computer the attackers were using, and then encrypting the stolen data.

Like many high-tech firms whose value is closely tied to their intellectual property, NVIDIA relies on a number of technologies designed to prevent data leaks or theft. According to LAPSUS$, among those is a requirement that only devices which have been approved or issued by the company can be used to access its virtual private network (VPN).

These so-called **Mobile Device Management** (MDM) systems retrieve information about the underlying hardware and software powering the system requesting access, and then relay that information along with any login credentials.

In a typical MDM setup, a company will issue employees a laptop or smartphone that has been pre-programmed with a data profile, VPN and other software that allows the employer to track, monitor, troubleshoot or even wipe device data in the event of theft, loss, or a detected breach.

MDM tools also can be used to encrypt or retrieve data from connected systems, and this was purportedly the functionality NVIDIA used to claw back the information stolen by LAPSUS$.

"Access to NVIDIA employee VPN requires the PC to be enrolled in MDM," LAPSUS$ wrote in a post on their public Telegram channel. "With this they were able to connect to a [virtual machine] that we use. Yes, they successfully encrypted the data. However, we have a backup and it's safe from scum!!!"

NVIDIA declined to comment for this story.

On March 7, consumer electronics giant **Samsung** confirmed what LAPSUS$ had bragged on its Telegram channel: That the group had stolen and leaked nearly 200 GB of source code and other internal company data.

The chats reveal that LAPSUS$ stole a great deal more source code than they bragged about online. One of White's curious fascinations was SASCAR, Brazil's leading fleet management and freight security company. White had bought and talked his way into SASCAR's systems, and had stolen many gigabytes worth of source code for the company's fleet tracking software.

It was bad enough that LAPSUS$ had just relieved this company of valuable intellectual property: The chats show that for several days White taunted SASCAR employees who were responding to the then-unfolding breach, at first by defacing the company's website with porn.

The messages show White maintained access to the company's internal systems for at least 24 hours after that, even sitting in on the company's incident response communications where the security team discussed how to evict their tormentors.

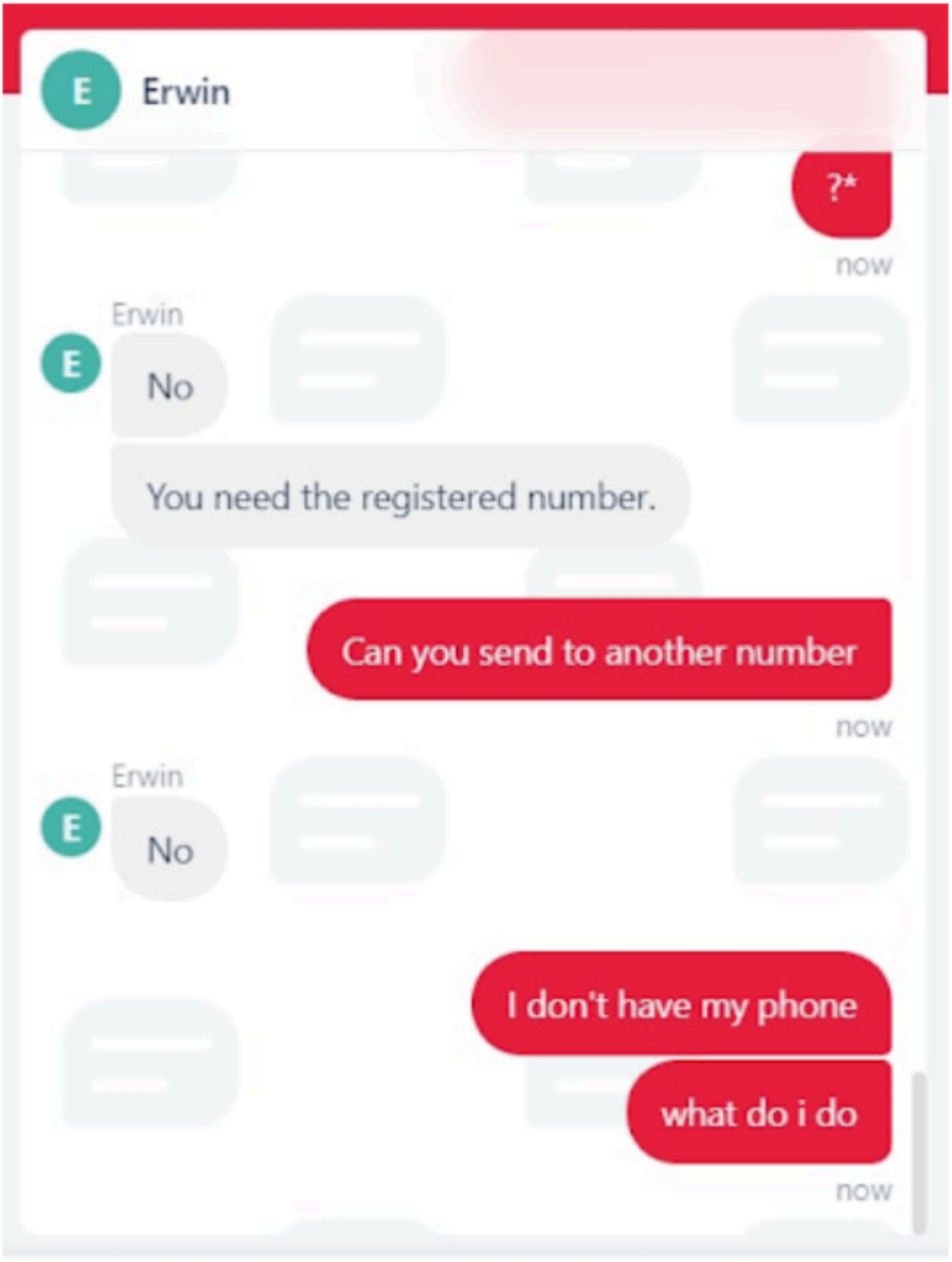
SASCAR is owned by tire industry giant Michelin, which did not respond to requests for comment.

ENROLLMENT

The leaked LAPSUS$ internal chats show the group spent a great deal of time trying to bypass multi-factor authentication for the credentials they'd stolen. By the time these leaked chat logs were recorded, LAPSUS$ had spent days relentlessly picking on another target that relied on MDM to restrict employee logins: **Iqor**, a customer support outsourcing company based in St. Petersburg, Fla.

LAPSUS$ apparently had no trouble using Russian Market to purchase access to Iqor employee systems. "I will buy login when on sale, Russians stock it every 3-4 days," Amtrak wrote regarding Iqor credentials for sale in the bot shops.

The real trouble for LAPSUS$ came when the group tried to evade Iqor's MDM systems by social engineering Iqor employees into removing multi-factor authentication on Iqor accounts they'd purchased previously. The chats show that time and again Iqor's employees simply refused requests to modify multi-factor authentication settings on the targeted accounts, or make any changes unless the requests were coming from authorized devices.



One of several IQOR support engineers who told LAPSUS$ no over and over again.

After many days of trying, LAPSUS$ ultimately gave up on Iqor. On Mar. 22, LAPSUS$ announced it hacked **Microsoft**, and began leaking 37 gigabytes worth of Microsoft source code.

Like NVIDIA, Microsoft was able to stanch some of the bleeding, cutting off LAPSUS$'s illicit access while the group was in the process of downloading all of the available source code repositories alphabetically (the group publicized their access to Microsoft at the same time they were downloading the software giant's source code). As

a result, LAPSUS$ was only able to leak the source for Microsoft products at the beginning of the code repository, including Azure, Bing and Cortana.

BETRAYAL

LAPSUS$ leader White drew attention to himself prior to the creation of LAPSUS$ last year when he purchased a website called **Doxbin**, a long-running and highly toxic online community that is used to "dox" or post deeply personal information on people.

Based on the feedback posted by Doxbin members, White was not a particularly attentive administrator. Longtime members soon took to harassing him about various components of the site falling into disrepair. That pestering eventually prompted White to sell Doxbin back to its previous owner at a considerable loss. But before doing so, White leaked the Doxbin user database.

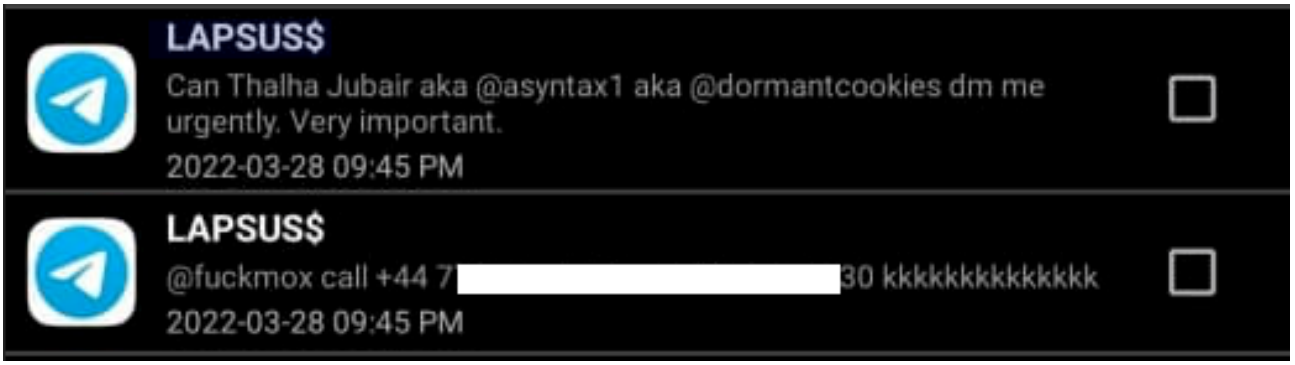
White's leak triggered a swift counterpunch from Doxbin's staff, which naturally responded by posting on White perhaps the most thorough dox the forum had ever produced — including videos filmed just outside his home where he lives with his parents in the United Kingdom.

The past and current owner of the Doxbin — an established cybercriminal who goes by the handle "**KT**" — is the same person who leaked these private LAPSUS$ Telegram chat logs to KrebsOnSecurity.

In early April, multiple news outlets reported that U.K. police had arrested seven people aged 15-21 in connection with the LAPSUS$ investigation. But it seems clear from reading these leaked Telegram chats that individual members of LAPSUS$ were detained and questioned at different times over the course of several months.

In his chats with other LAPSUS$ members during the last week in March, White maintained that he was arrested 1-2 months prior in connection with an intrusion against a victim referred to only by the initials "BT." White also appeared unconcerned when Amtrak admits that the City of London police found LAPSUS$ Telegram chat conversations on his mobile phone.

Perhaps to demonstrate his indifference (or maybe just to screw with Amtrak), White responds by leaking Amtrak's real name and phone number to the group's public Telegram channel. In an ALL CAPS invective of disbelief at the sudden betrayal, Amtrak relates how various people started calling their home and threatening their parents as a result, and how White effectively outed them to law enforcement and the rest of the world as a LAPSUS$ member.



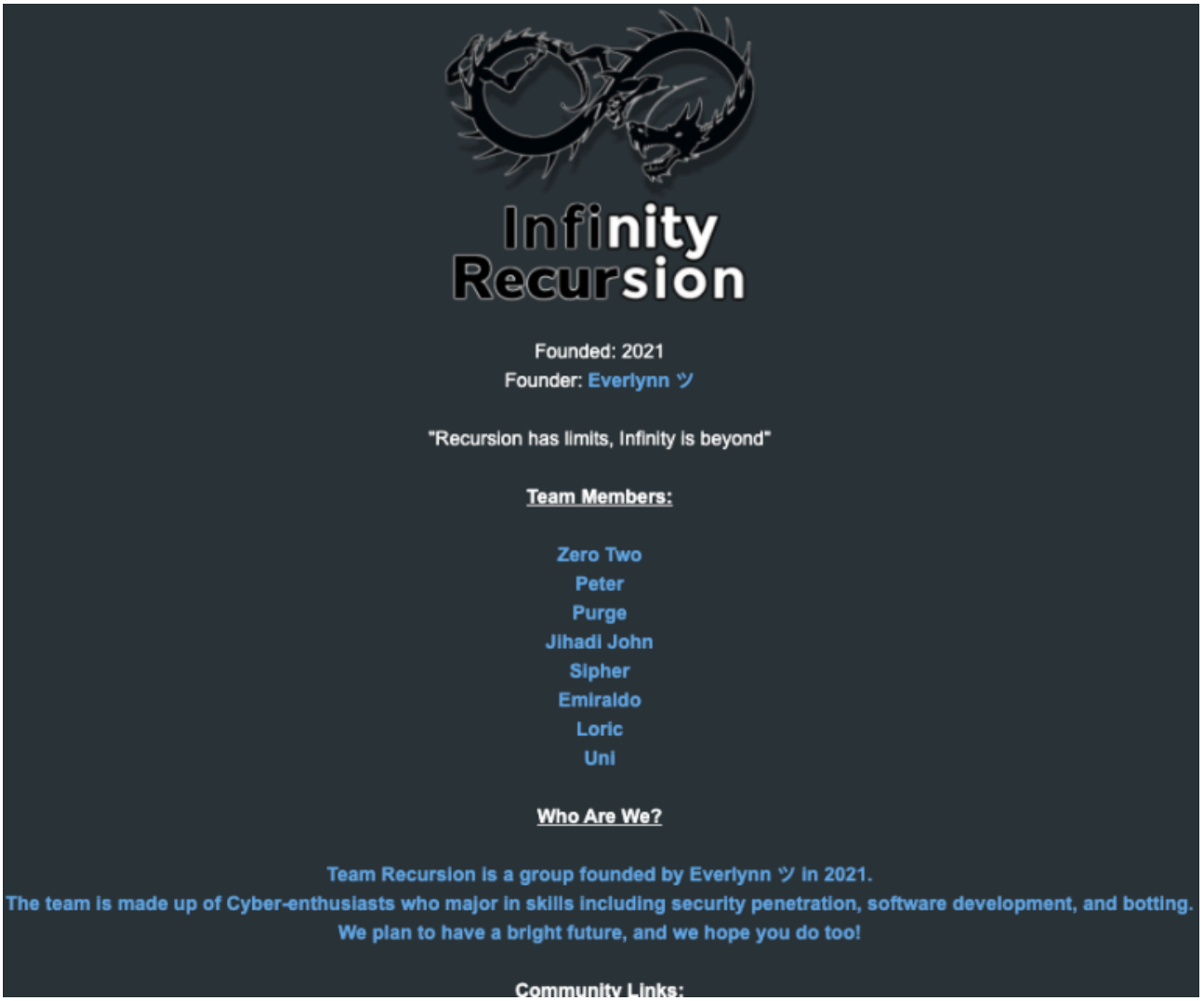
The vast majority of noteworthy activity documented in these private chats takes place between White and Amtrak, but it doesn't seem that White counted Amtrak or any of his fellow LAPSUS$ members as friends or confidants. On the contrary, White generally behaved horribly toward everyone in the group, and he particularly seemed to enjoy abusing Amtrak (who somehow always came back for more).

"**Mox**," one of the LAPSUS$ members who shows up throughout these leaked chats, helped the group in their unsuccessful attempts to enroll their mobile devices with an airline in the Middle East to which they had purchased access. Audio recordings leaked from the group's private Telegram channel include a call wherein Mox can be heard speaking fluently in Arabic and impersonating an airline employee.

At one point, Mox's first name briefly shows up in a video he made and shared with the group, and Mox mentions that he lives in the United States. White then begins trying to find and leak Mox's real-life identity.

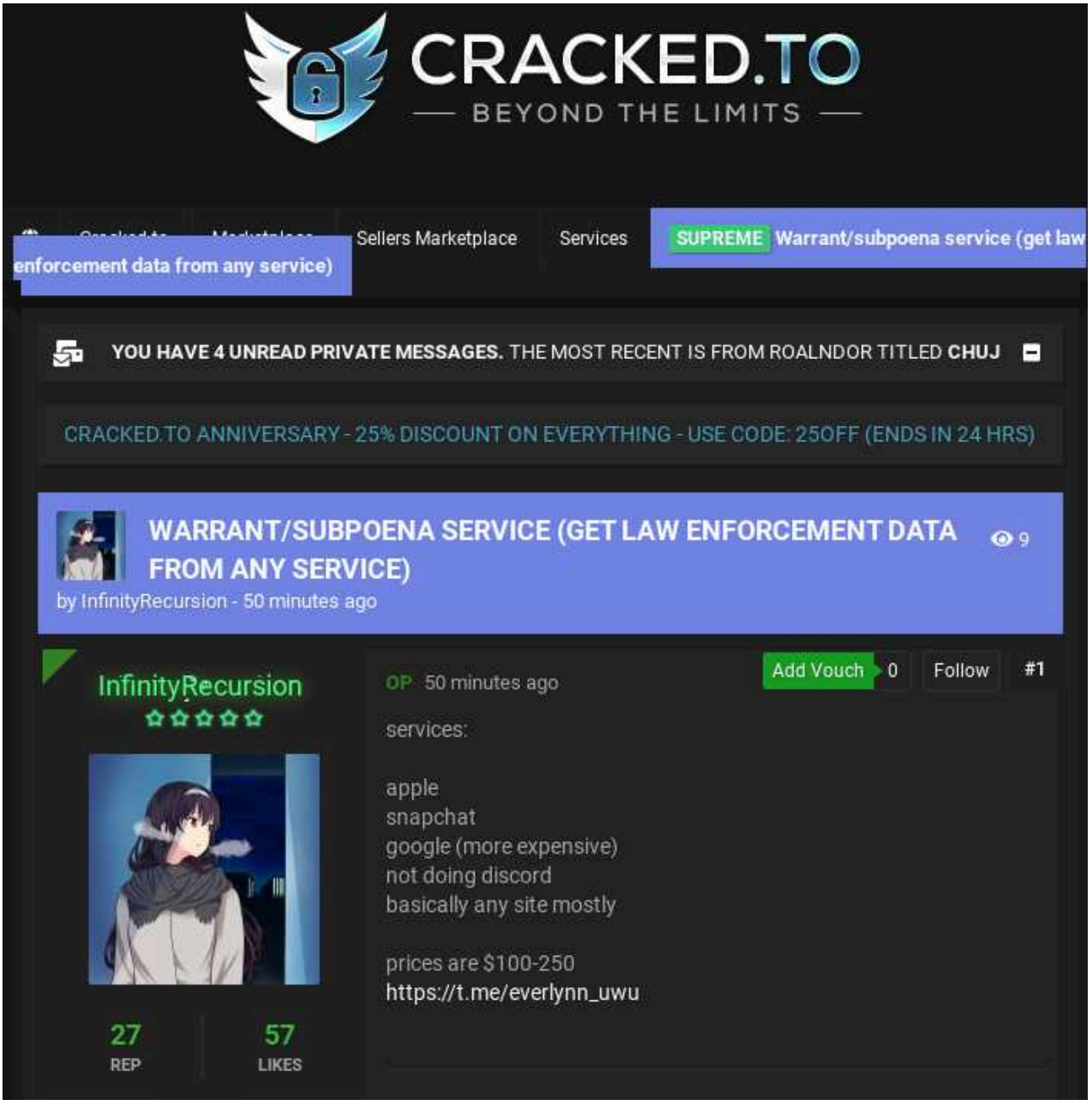
When Mox declares he's so scared he wants to delete his iCloud account, White suggests he can get Mox's real name, precise location and other information by making a fraudulent "emergency data request" (EDR) to **Apple**, in which they use a hacked police department email account to request emergency access to subscriber information under the claim that the request can't wait for a warrant because someone's life is on the line.

White was no stranger to fake EDRs. White was a founding member of a cybercriminal group called "Recursion Team," which existed between 2020 and 2021. This group 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 roster of the now-defunct “Infinity Recursion” hacking team, from which some members of LAPSUS$ hail.

The Recursion Team was founded by a then 14-year-old from the United Kingdom who used the handle “**Everlynn**.” On April 5, 2021, Everlynn posted a new sales thread to the cybercrime forum cracked[.]to titled, “Warrant/subpoena service (get law enforcement data from any service).” The price: $100 to $250 per request.

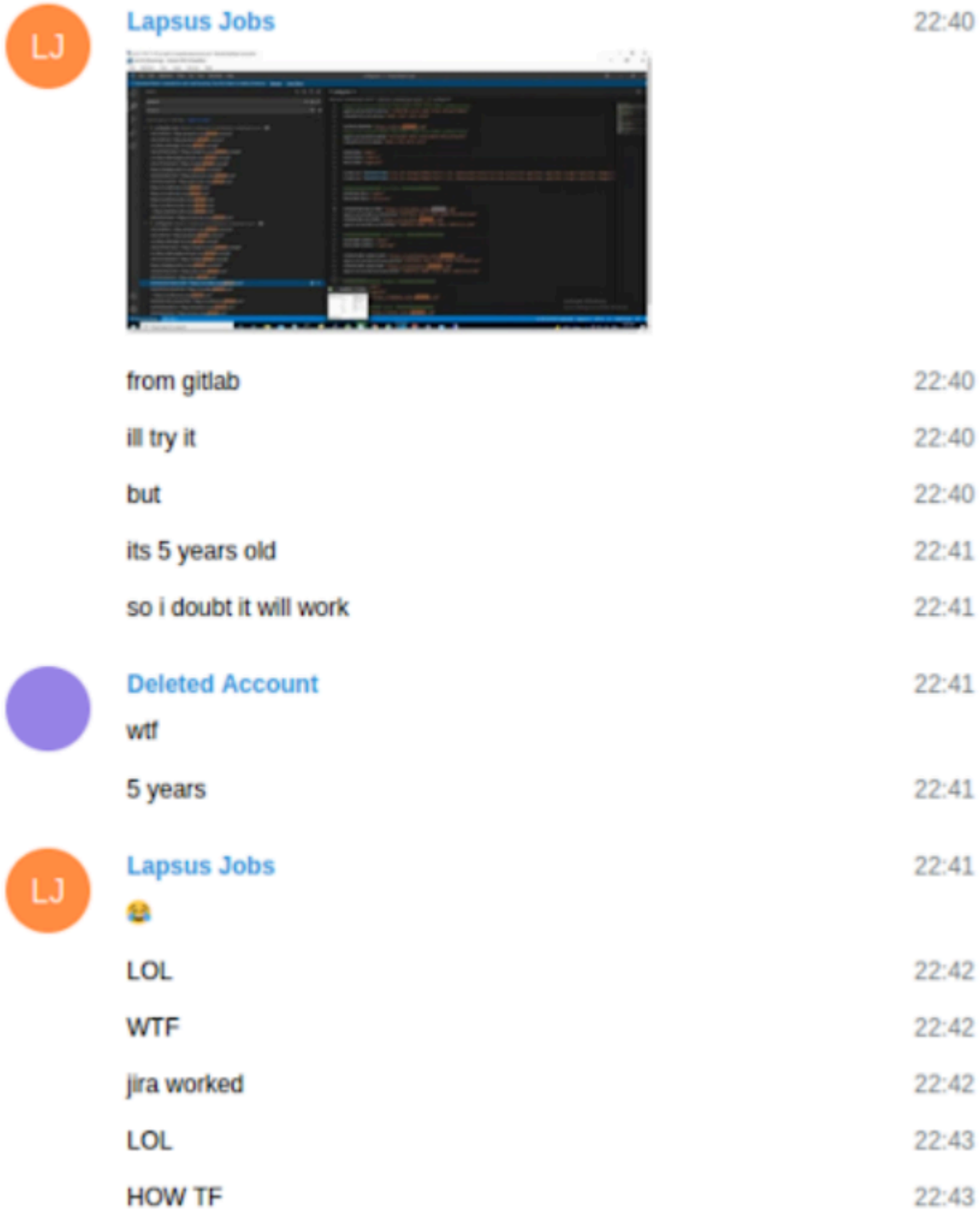


Everlynn advertising a warrant/subpoena service based on fake EDRs.

Bringing this full circle, it appears Amtrak/Asyntax is the same person as Everlynn. As part of the Recursion Team, White used the alias "**Peter**." Several LAPSUS$ members quizzed White and Amtrak about whether authorities asked about Recursion Team during questioning. In several discussion threads, White's "Lapsus Jobs" alias on Telegram answers "yes?" or "I'm here" when another member addresses him by Peter.

White dismissed his public doxing of both Amtrak and Mox as their fault for being sloppy with operational security, or by claiming that everyone already knew their real identities. Incredibly, just a few minutes after doxing Amtrak, White nonchalantly asks them for help in stealing source code from yet another victim firm — as if nothing had just happened between them. Amtrak seems soothed by this invitation, and agrees to help.

On Mar. 30, software consultancy giant **Globant** was forced to acknowledge a hack after [LAPSUS$ published 70 gigabytes of data stolen from the company](), including customers' source code. While the Globant hack has been widely reported for weeks, the cause of the breach remained hidden in these chat logs: A stolen five-year-old access token for Globant's network that still worked.



LAPSUS$ members marvel at a 5-year-old stolen authentication cookie still working when they use it against Globant to steal source code.

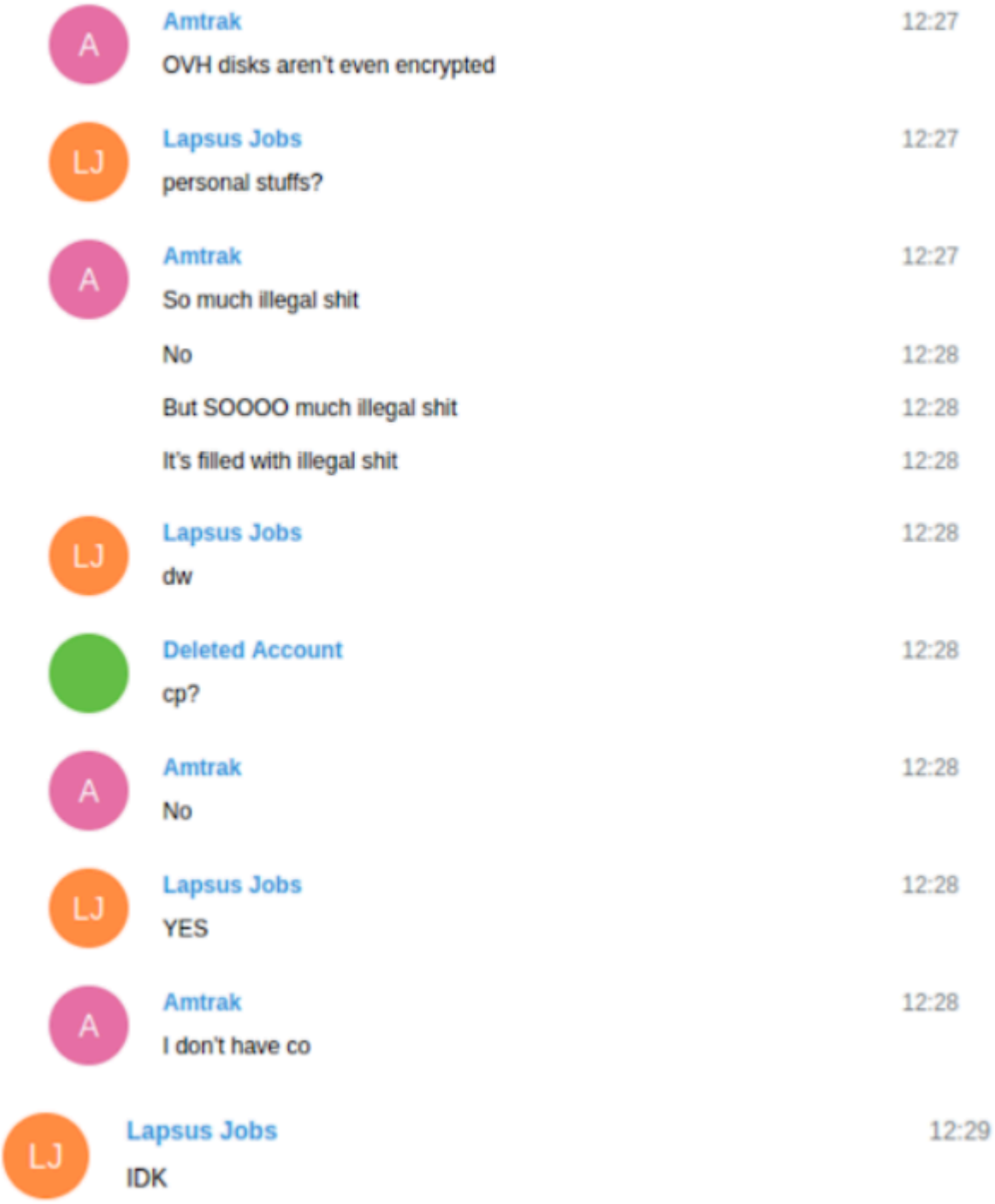
Globant lists a number of high-profile customers on its website, including the U.K. Metropolitan Police, software house Autodesk and gaming giant **Electronic Arts**. In March, KrebsOnSecurity showed how White was connected to the theft of 780 GB worth of source code from Electronic Arts last summer.

In that attack, the intruders reportedly gained access to EA's data after purchasing authentication cookies for an EA Slack channel from the dark web marketplace "Genesis," which offers more or less the same wares as the Russian Market.

One remarkable aspect of LAPSUS$ was that its members apparently decided not to personally download or store any data they stole from companies they hacked. They were all so paranoid of police raiding their homes that they assiduously kept everything "in the cloud." That way, when investigators searched their devices, they would find no traces of the stolen information.

But this strategy ultimately backfired: Shortly before the private LAPSUS$ chat was terminated, the group learned it had just lost access to the Amazon AWS server it was using to store months of source code booty and other stolen data.

"RIP FBI seized my server," Amtrak wrote. "So much illegal shit. It's filled with illegal shit."



White shrugs it off with the dismissive comment, "U can't do anything about ur server seized." Then Amtrak replies that *they never made a backup of the server*.

"FFS, THAT AWS HAD TMO SRC [T-Mobile source] code!" White yelled back.

The two then make a mad scramble to hack back into T-Mobile and re-download the stolen source code. But that effort ultimately failed after T-Mobile's systems revoked the access token they were using to raid the company's source code stash.

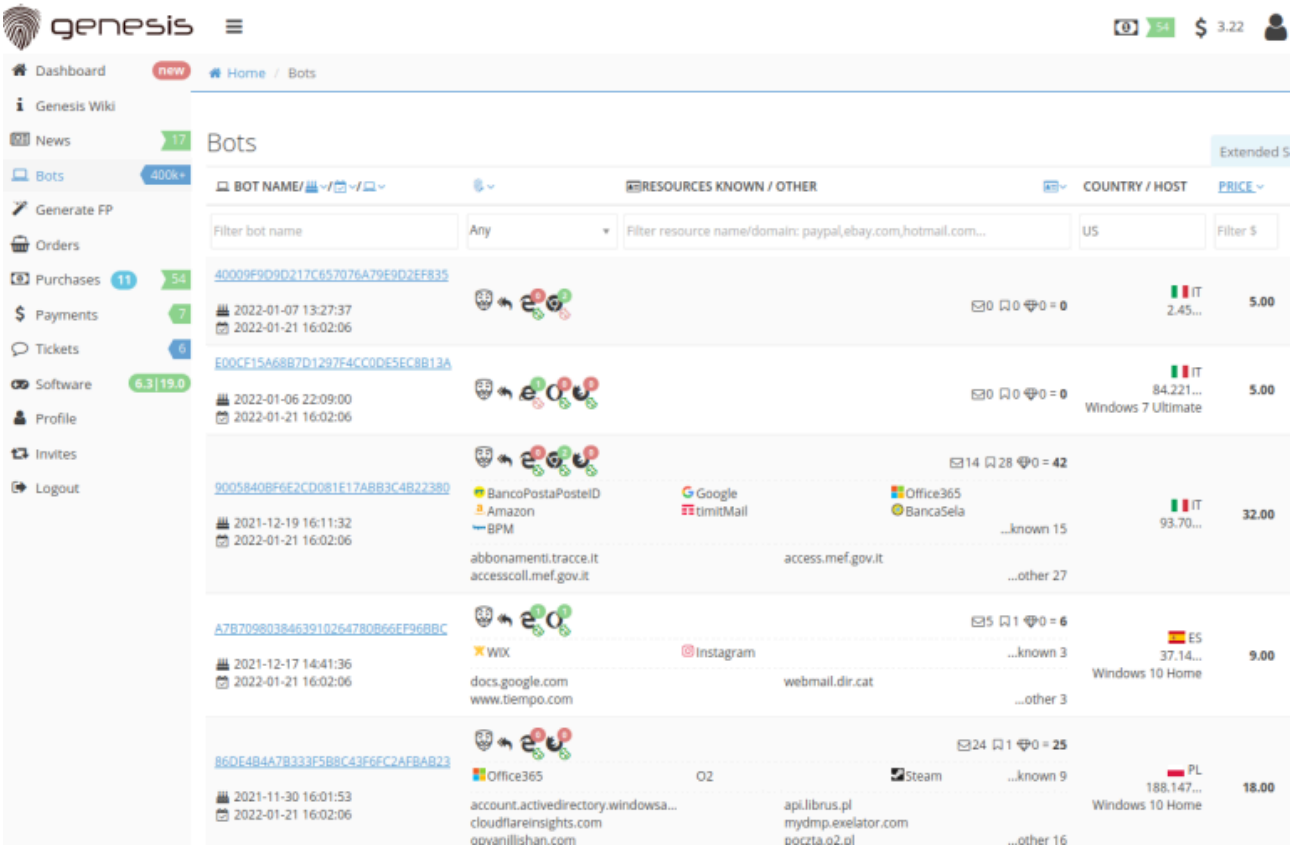
"How they noticed?" Amtrak asked White.

“Gitlab auto-revoked, likely,” White replied. “Cloning 30k repos four times in 24 hours isn’t very normal.”

Ah, the irony of a criminal hacking group that specializes in stealing and deleting data having their stolen data deleted.

It’s remarkable how often LAPSUS$ was able to pay a few dollars to buy access to some hacked machine at a company they wanted to break into, and then successfully parlay that into the theft of source code and other sensitive information.

What’s even more remarkable is that anyone can access dark web bot shops like Russian Market and Genesis, which means larger companies probably should be paying someone to regularly scrape these criminal bot services, even buying back their own employee credentials to take those vulnerable systems off the market. Because that’s probably the simplest and cheapest incident response money can buy.



The Genesis bot shop.

Source: https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/