Threat Brief: Lapsus$ Group

unit42.paloaltonetworks.com/lapsus-group/

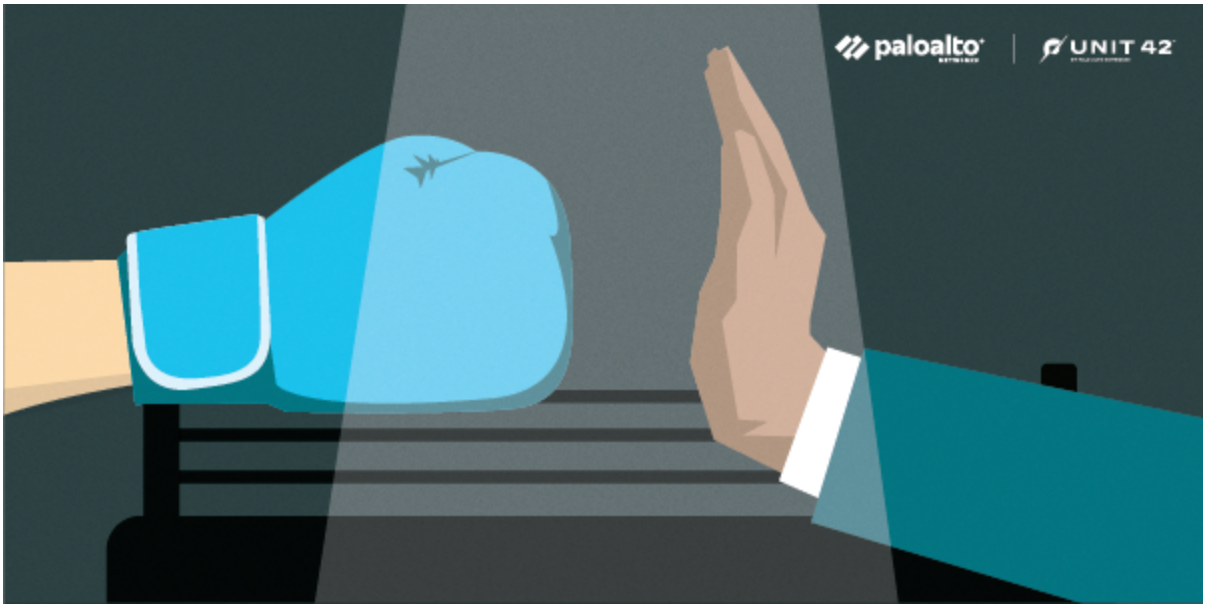
Unit 42 March 24, 2022

By Unit 42

March 24, 2022 at 12:15 PM

Category: Threat Brief

Tags: data exfiltration, Lapsus$



This post is also available in: 日本語 (Japanese)

Executive Summary

The Lapsus$ Group threat actor has grown in just a few months from launching a handful of destructive attacks to stealing and publishing source code of multiple top-tier technology companies.

Though sometimes called a ransomware group in reports, Lapsus$ is notable for not deploying ransomware in extortion attempts. In today's environment, threat actors favor using ransomware to encrypt data and systems and often extort victims for significant amounts of cryptocurrency in exchange for decryption keys, sometimes turning up the pressure with the threat of publishing stolen data. Lapsus$, however, is unusual in its approach – for this group, notoriety most often appears to be the goal, rather than financial gain.

Unit 42 has helped organizations respond to multiple Lapsus$ attacks. The Lapsus$ Group doesn't employ malware in breached victim environments, doesn't encrypt data and in most cases, doesn't actually employ extortion. They focus on using a combination of stolen credentials and social engineering to gain access to victims. We've also seen them solicit employees on Telegram for their login credentials at specific companies in industries including: telecom, software, gaming, hosting providers and call centers.

However, the group's attacks and leaking of stolen data even without extortion can be very damaging. In addition, we've seen destructive Lapsus$ attacks where the actors got access to an organization's cloud environment, wiped systems and destroyed over a thousand virtual machines.

Although there are no public indicators of compromise (IoCs), and no tactics, techniques and procedures (TTPs) that are unique to Lapsus$ Group, here we will summarize what is known of this threat actor to better enable defenders in understanding and mitigating this threat.

Related Unit 42 Topics Threat Briefs, Threat Assessments

Table of Contents

Early Targets of Lapsus$

We first observed the "Lapsus$" handle mid-2021, but the first attack activity quoting that handle was in August 2021, with some U.K. mobile phone customers reporting receiving threatening texts (Figure 1).

We are LAPSUS$, remember our name, we have your userdata. we have EE's, BT and Orange source code. If EE pay us 4 millions USD in XMR before the 20th august, we will delete everything from our servers. XMRADDR: 42qLW1FiEDQKjeoSAFQRXaVpSUxB8fTYJ2Zeah8dcDTYDEjCb71iCR76ctGMysAB4nj3MTTCE5GuJMsC1eLuwKdu7v6FKf3

Figure 1. Early Lapsus$ activity.

In December 2021, the Ministry of Health of Brazil fell victim to an attack claimed by Lapsus$ (Figure 2). This included the soon-to-be de rigueur data exfiltration and deletion technique, and also redirection of some DNS records. This was followed in short order by attacks on South American telecoms providers Claro and Embratel, Brazilian state-owned postal service “Correios,” and Portuguese media giant Impresa. This initial focus has led to speculation that Lapsus$ Group may be Brazilian, although we understand the choice of targets to have been influenced by extended team members rather than the team leadership.

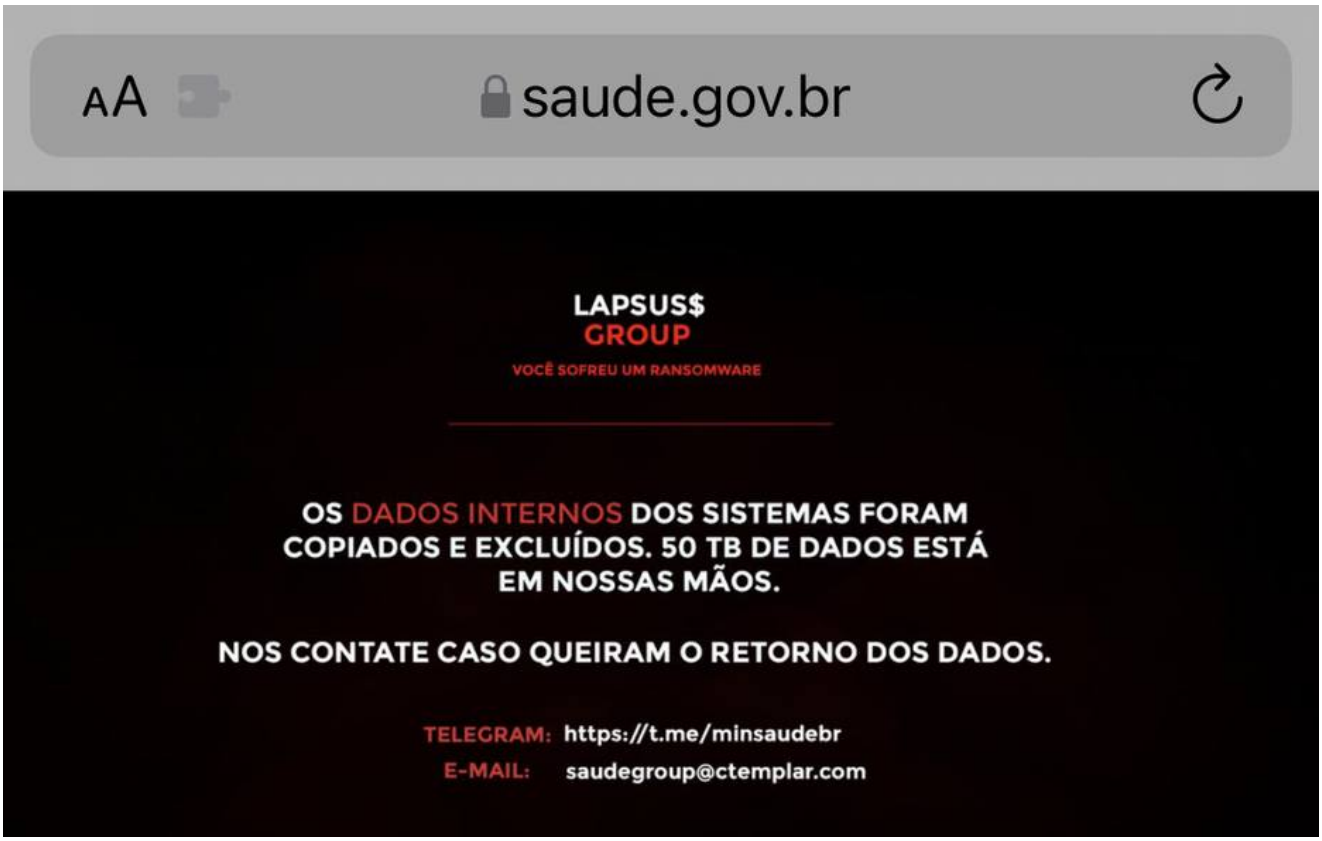


Figure 2. Ministry of Health of Brazil defacement.

Evolution of Targeted Organizations

Apart from Argentinian eCommerce provider Mercado Libre / Mercado Pago, subsequent victimology has departed South America and pivoted to focus on the high-tech sector.

Recent public victims have included:

- Nvidia
- Samsung
- Ubisoft
- Vodafone
- Microsoft
- LG
- Okta

It should be understood that in addition there are likely any number of other victims, targeted by attacks not known in the public sphere. It is likely that some victims are not the intended end-target, but are rather breached in order to gain access to their customers, or for example, to help bypass multi-factor authentication (MFA). To this end, we are aware of this actor's involvement in vishing, SIM-swapping and soliciting third parties at providers for insider access. For example, in the "proof" of the Okta breach posted on the Lapsus$ Group's Telegram channel, the actor states: "… our focus was ONLY on okta customers" (Figure 3).

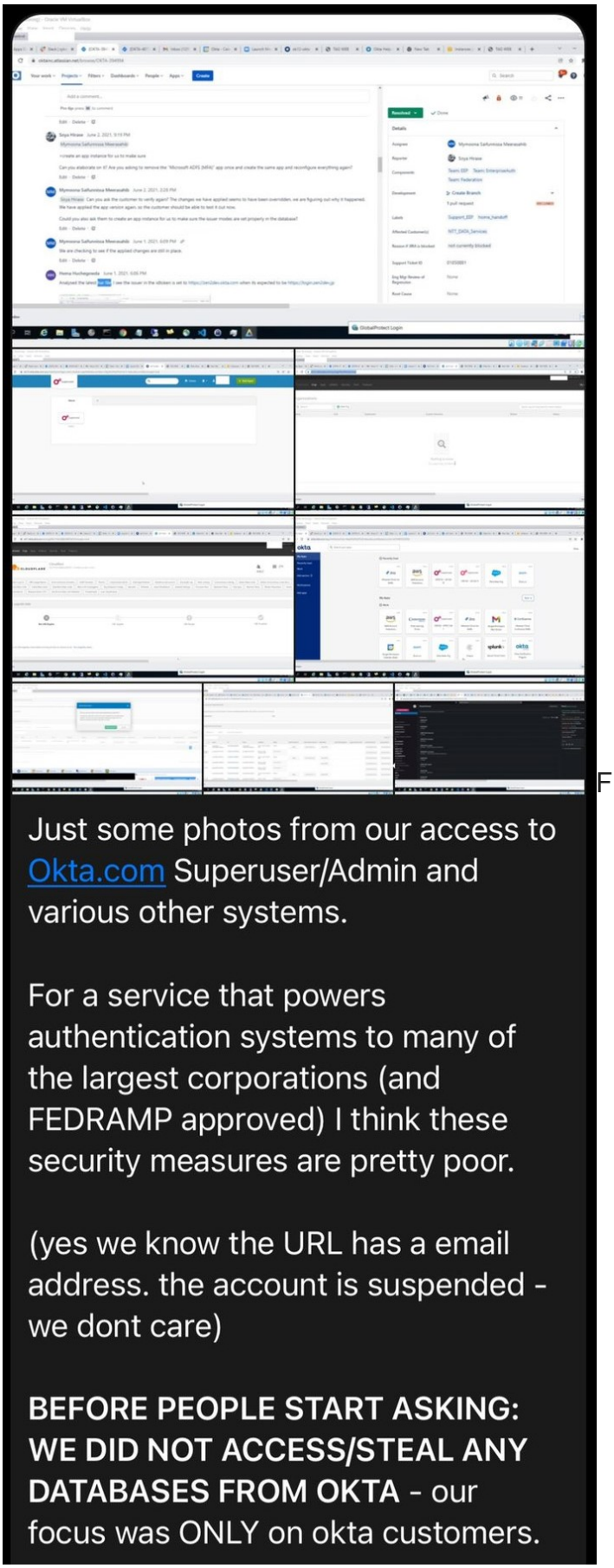


Figure 3. Okta breach evidence posted on the Lapsus$ Group's Telegram channel.

Several of the Lapsus$ Group's attacks involved the theft and publication of source code. In the case of Nvidia, it was observed as a non-financial extortion attempt. In other cases, for example that of Microsoft, there was simply publication without extortion, again supporting the understanding that the primary motivation of this actor is notoriety rather than financial gain.

However, as notoriety and success cause this group to grow, we should expect to see diversity of membership reflected in a diversity of victimology, TTPs and action-on-objective motivations.

Mitigation Actions

Owing to the diversity of techniques used, and the lack of use of malware, there is no single defense against or detection of Lapsus$ attacks specifically.

A hallmark of this group is the diversity of techniques used both for initial access and action-on-objective. Credentials are harvested from dumps, purchased or spear-phished. When employed, various techniques to bypass MFA are observed – from social engineering, through SIM-swapping and even compromising MFA/telecoms providers.

Zero Trust network architecture and strong security hygiene are the best defenses against this type of threat actor. If Lapsus$ has purchased credentials for a network, they can effectively operate as an insider threat, taking advantage of the same privileges the employee has inside the network.

Focus on general information security best practices: MFA, access controls and network segmentation. Ensure your organization has the ability to detect anomalous activity, including activity that involves trusted third parties in your environments, and protect against non-technical techniques such as vishing and SIM-swapping. Patching of internal systems that might support lateral movement and privilege escalation should be prioritized, as well as against known public exploits that these actors might employ.

Although the commodity malware RedLine Stealer has been implicated for credential harvesting in some attacks, it's unclear if this is first- or third-party, and it cannot be used as a definitive indicator of Lapsus$-specific activity.

Conclusion

Lapsus$ Group has made headlines recently for high-profile attacks, with an apparent goal of gaining notoriety. They claim in some cases to have targeted organizations with the specific goal of gaining access to customers.

While referred to as a ransomware group in many reports, the Lapsus$ Group is more accurately called an attack group. Most notably, their focus to date does not appear to have been on extortion and financial gain. Even without extortion, the group's attacks and leaks of stolen information can be damaging.

Because the group uses a diversity of techniques for attacks, no single technique can protect against Lapsus$ or detect its attacks. Because of this, we recommend that organizations focus on observing general information security best practices as described in the Mitigation Actions section above.

Unit 42, together with researchers at Unit 221b, identified the primary actor behind the Lapsus$ Group moniker in 2021, and have been assisting law enforcement in their efforts to prosecute this group.

If you think you may be subject to an active attack or have an urgent matter, get in touch with the Unit 42 Incident Response team or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Palo Alto Networks will update this Threat Brief with new information and recommendations as they become available.

Additional Resources

DEV-0537 criminal actor targeting organizations for data exfiltration and destruction
A Closer Look at the LAPSUS$ Data Extortion Group
Lapsus$ Telegram channel: t[.]me/minsaudebr
Email address associated with Lapsus$ Group: saudegroup[at]ctemplar[.]com

Updated March 25, 2022, at 8:30 a.m. PT.