Meet Lapsus$: An Unusual Group in the Cyber Extortion Business

digitalshadows.com/blog-and-research/meet-lapsus-an-unusual-group-in-the-cyber-extortion-business/

March 17, 2022

In December 2021, a new cyber threat group began attracting the security community's attention, after conducting several high-profile extortion attacks against organizations operating in Latin America and then move on to global targets like Samsung and NVIDIA. In the early stages of their operations, the Lapsus$ threat group compromised and attempted to extort the Brazilian Ministry of Health, South American telecommunications organizations, and Portuguese media corporations.

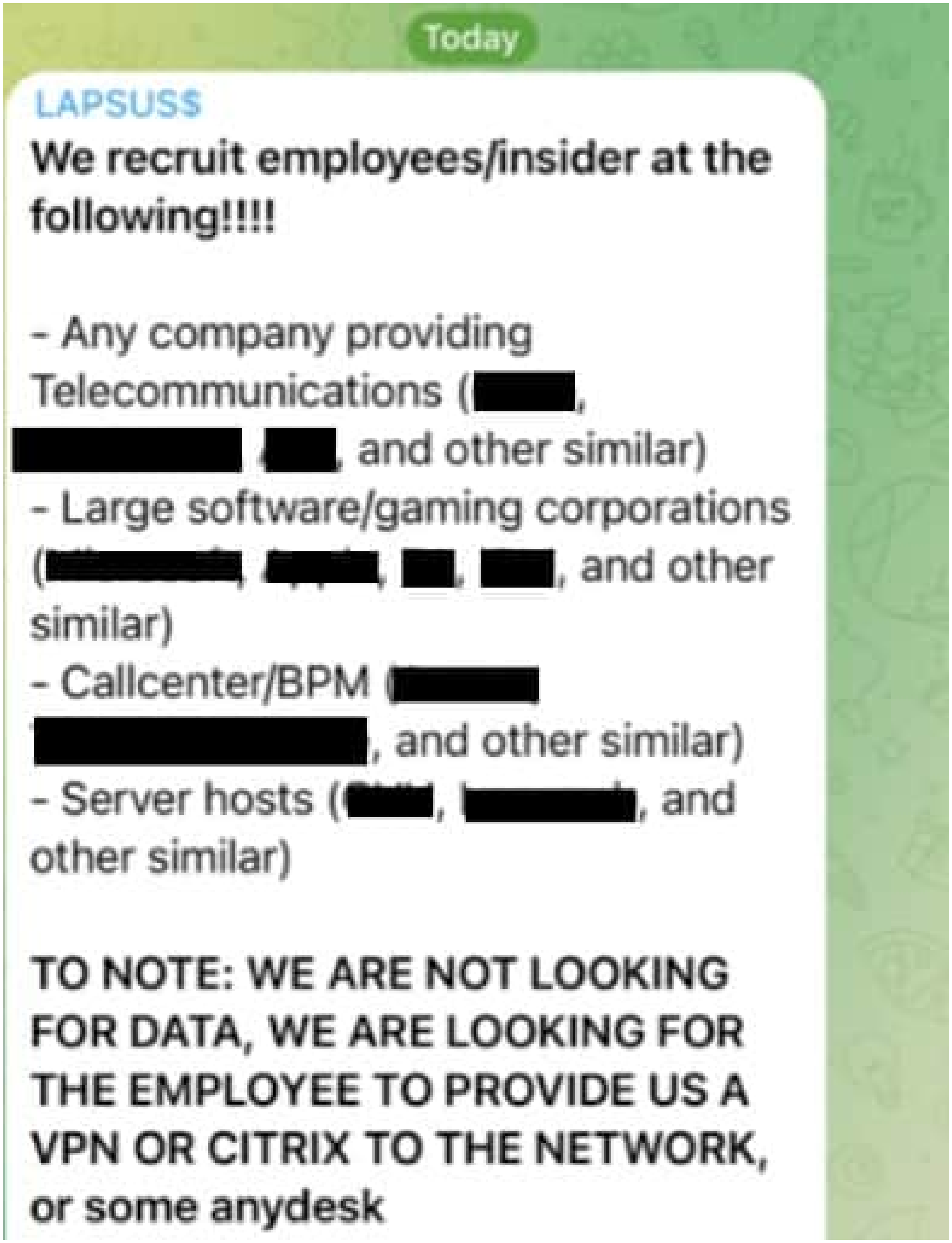
What makes Lapsus$ stand out is its peculiar way of conducting business. Although some researchers have labeled Lapsus$ as a ransomware group, there's still no evidence that they have ever deployed ransomware malware onto their targets' systems. On top of that, Lapsus$ has been using an innovative technique to communicate with the public, preferring a private Telegram channel instead of the more traditional data leak sites.

Lapsus$ currently represents an interesting case study of how cybercriminals innovate their techniques to adapt to an ever-changing threat landscape. So, without further ado, let's dive into the observed modus operandi of this threat group to better comprehend how you can increase your robustness against their attacks.

How does Lapsus$ conduct its operations?

Given the relatively short lifespan of Lapsus$, details are still emerging on how this threat group gains access to and later compromises its victims. Reporting on Lapsus$'s initial operations indicated that the group had exploited public-facing Remote Desktop Protocol (RDP) protocols and phishing emails to gain initial access; it is also realistically possible that this group bought access from Initial Access Brokers to conduct some of its operations. Based on what we observed, Lapsus$ likely uses a combination of methods to gain initial access to targeted systems.

On 10 March 2022, the Photon Intelligence Team independently observed the Lapsus$ operators publishing a message on their Telegram channel to recruit malicious insiders who can provide Virtual Private Network (VPN), Virtual Desktop Infrastructure (VDI), or Citrix credentials to organizations operating in the telecommunications and technology sectors. The message offered an unspecified amount of payment in an unknown currency. As such, it is possible that Lapsus$ may have gained initial access to their targets by using malicious insiders working in those companies.



LAPSUS$

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

- Any company providing Telecommunications ([redacted], [redacted], [redacted], and other similar)
- Large software/gaming corporations ([redacted], [redacted], [redacted], [redacted], and other similar)
- Callcenter/BPM ([redacted] [redacted], and other similar)
- Server hosts ([redacted], [redacted], 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

Lapsus$'s Telegram message (named organizations have been redacted)

At the time of writing, it is still uncertain how this group operates within compromised organizations, once it gains initial access. Based on similar cyber extortion operations, it is realistically possible that this group might attempt to escalate privileges or move laterally in a network to access high-value targets. Once valuable information has been located, Lapsus$ reportedly begins exfiltrating that data.

Lapsus$ then announces the identity of its victims via the group's dedicated data leak channel on Telegram – the same one used for most public-facing announcements. Using Telegram for these communications is a marked departure from the usual methods used by other cyber extortion-focused threat groups, like ransomware actors. It is likely that Lapsus$ decided to abuse a legitimate tool like Telegram for its operations to broaden the potential audience of its messages and reduce the chances of being disrupted by denial of service attacks. Lapsus$ also runs polls on its data leak channel, providing members with the ability to decide whose data should be breached next. Among cyber extortion groups, few also involve their followers or the public in such a direct manner.

How to mitigate the threat posed by groups like Lapsus$

According to the observed operations and Lapsus$'s own messages in its Telegram channel, the Photon Intelligence Team assesses that the group's primary motivation is soliciting ransoms from victims. When Lapsus$ compromised technology giant NVIDIA, it requested the firm remove the Lite Hash rate (LHR) from graphics cards as part of its extortion demands. This request was reportedly intended to facilitate a more conducive environment for cryptocurrency mining. Although this focus on cryptocurrency mining suggests that the group may ultimately be financially driven, Lapsus$ has certainly taken a different approach to other groups in soliciting financial rewards; it is realistically possible that the group's targeting is determined by another, unknown, motivation.

Given the latest brazen high-profile operations, including technology and telecommunications giants like NVIDIA and Samsung, it is likely that this group will be emboldened to conduct even riskier and more profitable operations. This ambition to hit highly visible targets also hints at this group's intention to expand its reputation and credibility in the cybercriminal environment.

To defend against groups like Lapsus$, organizations should prioritize strengthening their defenses to hinder these groups' attempts to gain initial access into their environments. Useful mitigation techniques include:

- Secure remote working tools like VPN and RDP by using strong passwords, enabling multi-factor authentication (MFA), and restricting access to a limited number of users.
- Provide timely and up-to-date training to your employees to increase your defending chances against social engineering campaigns, such as phishing and vishing attacks.
- Monitor your employees' morale and intentions when possible; taking the time to listen and act on their grievances can greatly reduce the risk of insider threats.

In summary, Lapsus$ appears to be a technically-sophisticated threat group with great ambitions to target high-profile organizations. This group's activity will likely continue in the coming weeks and months. If you want a deeper dive into how this group operates, get a customized demo of SearchLight.