Brazen, Unsophisticated and Illogical: Understanding the LAPSUS$ Extortion Group

By Claire Tills

Published: 2022-07-20 · Archived: 2026-04-05 21:29:30 UTC

Having gained the industry's attention in the first months of 2022, the LAPSUS$ extortion group has largely gone quiet. What can we learn from this extortion group's story and tactics?

In early 2022, the LAPSUS$ group broke onto the scene with flashy and disruptive attacks. While occasionally lumped in with ransomware groups, LAPSUS$ is an extortion group. What differentiates it from established, professional ransomware groups and what lessons can organizations learn from its tactics to improve their defenses?

The LAPSUS$ group made a considerable splash at the beginning of 2022, but has fallen to ripples among the bigger waves caused by more established groups like Conti. LAPSUS$'s brief tenure as a leader of cybersecurity news cycles was marred by idiosyncrasies and apparent mistakes.

Source: Tenable Research, July 2022

Ransomware or extortion?

I noted that LAPSUS$ is an extortion, not ransomware, group. For these purposes, I am being intentionally specific with the definition of ransomware. While some cases of extortion involve stealing data and "ransoming"

it back to organizations, ransomware specifically refers to incidents when data-encrypting malware (ransomware) is deployed and access to those systems is ransomed back to target organizations.

Over the years, ransomware groups have adopted diverse extortion tactics. To learn about those tactics and other key features of the ransomware ecosystem, read Tenable's report. Extortion groups like LAPSUS$ focus on opportunistic data theft and threats to publicly release the stolen data. Occasionally, these groups will also delete the original data.

With that distinction established, let's examine one of the recent prominent names in extortion: the LAPSUS$ group.

Who is the LAPSUS$ group?

While there are other groups that perform extortion-only attacks, the LAPSUS$ group broke onto the scene in a big way at the end of 2021 and brought this type of threat group to the forefront.

LAPSUS$'s official career began in December 2021 with attacks against companies in South America and continued into January with targets in South America and Portugal, likely related to the location of some group members. (While the initial breach of Sitel and subsequent compromise of Okta occurred at the end of January, it wasn't publicized for another two months.) In the following months, LAPSUS$ expanded its targets to multinational technology companies. This brought the group to the attention of the cybersecurity community at large.

The LAPSUS$ group solely operates through a private Telegram group and doesn't manage a dark web leak site like other threat groups, limiting the data available for analysis. Nonetheless, many security analysts, researchers and reporters have examined the information available and developed insights into the group's characteristics and tactics.

Common themes among these analyses include:

- Lower maturity tactics and behaviors
- Priority for clout and notoriety
- Primarily focused on monetary goals

The theorized goals of money and fame are supported by the group's transition from targeting companies in South America to companies with much larger areas of influence, "large scale international technology companies," as Flashpoint research puts it. Targeting these companies theoretically could earn cybercriminals higher payouts, and it absolutely earned the group notoriety.

As many analysts have pointed out, it is difficult to attribute a singular, monolithic goal — or even confidently discount goals — to such a "loose collective." LAPSUS$ has vehemently asserted that it is not politically motivated or state sponsored and its actions appear consistent with this assertion.

If ransomware groups like Conti are well-organized operations reminiscent of criminal enterprises depicted in TV shows and films such as Boardwalk Empire or the Godfather — complete with customer service and human resources — LAPSUS$ comes off more like the teams in Point Break or Bottle Rocket. Many analysts have

referred to its behavior as immature and impulsive, comparing it to the stereotypical "teenager in the basement," the script kiddies.

While it's hard to identify individual members of any cybercrime group, researchers and law enforcement have traced LAPSUS$ operations to a few teenagers in Brazil and the U.K. These identifications, subsequent arrests and apparent silence from the group, seem to align with analysis stating the group is made of "talented but inexperienced" actors who are "reckless and disruptive." These traits are based on the observed tactics and behaviors of the group, so let's examine those in some detail.

How does LAPSUS$ operate?

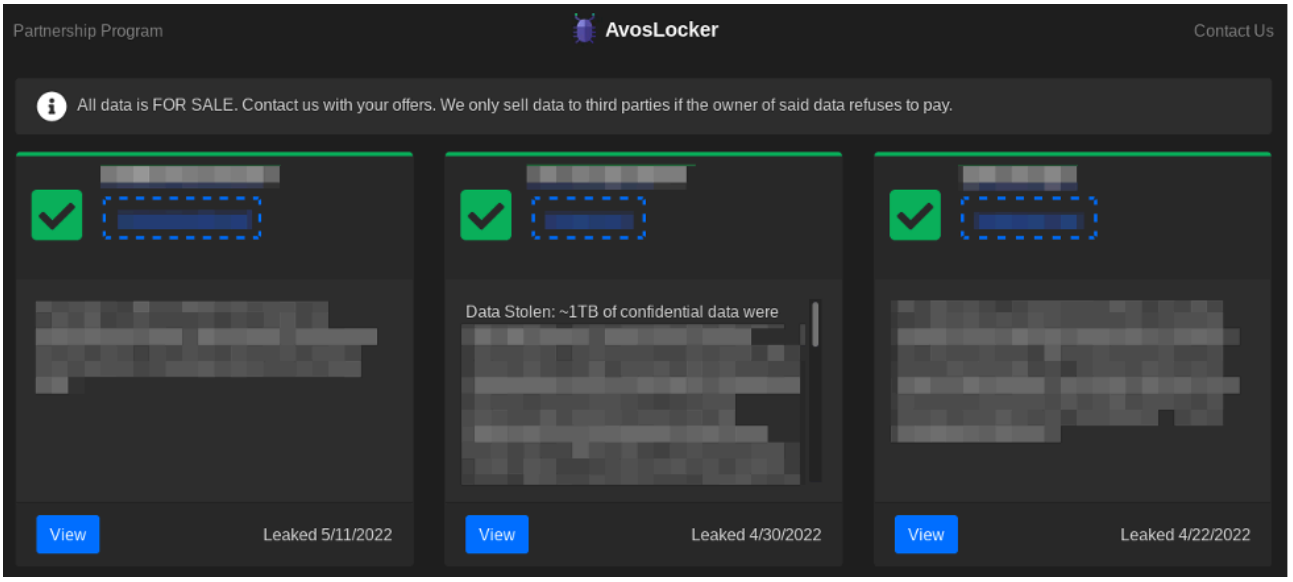
The LAPSUS$ group, maybe short lived given the latest developments, still showed a trajectory of maturity. This trajectory has not been linear, which further supports the loose collective nature of the group. Over time, the LAPSUS$ group has made opportunistic shifts in tactics and priorities for its attacks — moving from traditional customer and client data theft to theft of proprietary information and source code.

In terms of tactics, early attacks featured distributed denial of service (DDoS) and website vandalism. But, as early as January 21, the LAPSUS$ group was already engaged in the multi-stage breach that eventually led to the incident at Okta. Throughout that maturation process, the LAPSUS$ group heavily relied on tried-and-true tactics like purchasing credential dumps, social engineering help desks and spamming multifactor authentication (MFA) prompts to achieve initial access to target organizations.

According to reports from Microsoft and the NCC Group, the former from its own breach by the group, these are some key tactics, techniques and procedures of the LAPSUS$ group:

- Initial access via purchased or publicly available credential repositories, password stealers and paying employees for access
- Circumventing MFA through spamming prompts or contacting help desk
- Accessing internet-facing applications like virtual private networks, Microsoft SharePoint, virtual desktops etc. to collect further credentials and access sensitive information
- Elevating privileges by exploiting unpatched vulnerabilities in Jira, GitLab, and Confluence and enumerating users with Active Directory Explorer
- Exfiltrating data via NordVPN or free file drop services and then deleting resources
- Using access to the target's cloud environments to build attack infrastructure and remove all other global administrators

As I've noted above, the LAPSUS$ group differs from other threat groups in the extortion and ransomware spaces in a key way: it does not operate a leak website. The group solely uses its Telegram channel to announce victims, often soliciting input from the broader community on which organization's data to release next. Compared with the polished, standardized sites of ransomware groups (like AvosLocker, LockBit 2.0, Conti etc.), these practices come off as disorganized and immature.



AvosLocker leak website, Image Source: Tenable, May 2022

On the surface, the move to stealing source code and proprietary information could be seen as a strategy to motivate and elicit higher extortion payments, but the LAPSUS$ group has also used these thefts in strange ways. With the Nvidia data, LAPSUS$ also leaked a code-signing certificate that allowed malware authors to freely use this certificate to smuggle their wares into target environments as legitimately signed programs from Nvidia. LAPSUS$ was able to pilfer valuable information from Nvidia, but wasn't interested in or capable of capitalizing on it for its own benefit. The group didn't appear to have a strong sense of what data had value. The data stolen from Microsoft "does not lead to elevation of risk" and Samsung did not "anticipate any impact to [its] business or customers."

In fact, LAPSUS$ didn't always effectively communicate extortion demands to victims, occasionally disagreed publicly on how to leak data and made "unreasonable and illogical" demands. With Nvidia, LAPSUS$ demanded functional changes to Nvidia chips that could not reasonably be accomplished. It seems this demand was a longer-term monetary strategy to increase capacity to mine cryptocurrency, albeit an ill-conceived one.

What has LAPSUS$ accomplished?

Even though earlier attacks by the LAPSUS$ group didn't gain the level of attention its later attacks received, some were quite disruptive and quickly placed the group on defenders' radar screens, particularly in the regions hardest hit by those early attacks. The group managed to disrupt several telecommunications and media companies in Latin America and Europe, as well as Brazil's Ministry of Health.

It wasn't until the attack against Nvidia, in late February, that LAPSUS$ really broke into the broader limelight. With this breach, LAPSUS$ stepped out onto the global stage and started a brief tear through major technology companies, doing so with perhaps more flair than function.

Even though the breaches at Samsung, Microsoft and Okta did not have the technical impact we all fear from an incident at companies of that caliber, the disruption was still considerable. The incident at Okta in particular threw

the cybersecurity industry into a furor while it was being investigated and disclosed. While these major incidents were occurring, the group continued targeting smaller organizations in Latin America and Europe.

Characterized by erratic behavior and outlandish demands that cannot be met — at one point, the group even accused a target of hacking back — the LAPSUS$ group's tenure at the forefront of the cybersecurity newscycle was chaotic. It's hard to say how much money the LAPSUS$ group has earned from its enterprise, but it cannot be denied that the group gained notoriety, for better or worse. Three months since the peak of LAPSUS$ attacks and the arrests, the group remains largely inactive.

How organizations should respond

The LAPSUS$ group's primary tactics are focused on social engineering and recruiting insiders. In its report on the group's activities, NCC Group has provided indicators of compromise for LAPSUS$ attacks. Organizations should adopt the following guidance to defend against attacks from LAPSUS$ and other extortion groups.

- Reevaluate help desk policies and social engineering awareness
- Strengthen MFA: avoid SMS-based MFA; ensure strong password use; leverage passwordless authentication
- Use robust authentication options for internet-facing applications like OAuth and security assertion markup language
- Find and patch known-exploited vulnerabilities that could allow attackers to move laterally in your systems, elevate privileges and exfiltrate sensitive data
- Bolster cloud security posture: improve risk detections, strengthen access configurations

In its analysis of the incident targeting its own systems, Okta points to its adoption of zero trust as a key defense mechanism. The additional authentication steps required to access sensitive applications and data prevented the LAPSUS$ group from achieving access that could have had catastrophic impact on Okta and its customers.

Extortion groups like LAPSUS$ don't target Active Directory with the same motivations as traditional ransomware groups, but still seek to compromise AD targets for the sake of pivoting their access to higher-privileged users. Proper AD configuration and monitoring are as critical for stopping extortion as they are for stopping ransomware. Additionally, these extortion groups are very likely to target cloud environments. The LAPSUS$ group has been observed targeting cloud infrastructure, deleting resources and locking out legitimate users.

Like their ransomware counterparts, these extortion groups still rely on legacy vulnerabilities that organizations have left unpatched. At the RSA Conference in June 2022, NSA Cybersecurity Director Rob Joyce said that addressing these known exploited vulnerabilities "needs to be the base" of cybersecurity efforts. Tenable customers can use our Ransomware Ecosystem scan template, dashboards (Tenable.io, Tenable.sc) and reports to assess their environments for vulnerabilities known to be targeted by ransomware groups, many of which are also exploited by extortion groups.

The future of extortion groups

LAPSUS$ is not the only name in extortion. In the wake of Conti shutting down, some of its affiliates have been observed engaging in similar attacks. U.S. government agencies have also warned of another extortion group, Karakurt, which moved from merely operating a leak website for other's data to engaging in data theft and extortion operations on its own behalf.

As the LAPSUS$ group's activities were waning, the RansomHouse group has been rising in prominence. Like LAPSUS$, it has been categorized by some as a ransomware group, but it does not encrypt data on target networks. Many of its tactics are similar to that of the LAPSUS$ group's; RansomHouse even advertised its activities on the LAPSUS$ Telegram channel.

Just like ransomware, extortion attacks aren't going anywhere until they are made too complicated or costly to conduct. Organizations should evaluate what defenses they have in place against the tactics used, how they can be hardened and whether their response playbooks effectively account for these incidents. While it may feel easy to downplay the threat groups like LAPSUS$ because of their brazen, unsophisticated and illogical tactics, their disruption of major international technology companies reminds us that even unsophisticated tactics can have serious impact.

Get more information

- Report: A Look Inside The Ransomware Ecosystem
- ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware – How Tenable Can Help

Claire Tills

Claire Tills is a senior research engineer with Tenable's Security Response Team. Previously, she was product marketing manager for Nessus and Tenable Research. Before joining Tenable, Claire worked for the FS-ISAC upon receiving a Master’s degree in communication, with a focus on information security.
