Dataminr

NEWCOM Authorized Partner



How Scattered LAPSUS$ Hunters Illustrates the Evolution of Cybercrime

The emergence of Scattered LAPSUS$ Hunters (SLH), a new alliance of members of The Com, shows the vast evolution of the cybercrime industry as they have launched their own Ransomware-as-a-Service (RaaS), ShinySp1d3r. Organizations need to monitor dark web activity and watch for insider threats to defend against these business-like, AI-enhanced cybercriminals.

In recent years, few cybercrime collectives have made more headlines than The Com. This collection of cybercriminals, typically made up of 18-30 year olds based in the U.S. or other English speaking countries, has had a number of sub-groups that identify themselves with a number of names such as LAPSUS$, Scattered Spider, UNC6040, and more recently ShinyHunters. Each of these names carries with it memories of highly publicized data breaches such as Twilio, MGM and Caesars resorts, Marks & Spencer, and an attack that granted the actors downstream access to dozens of organizations' Salesforce instances.

Now, in their most recent development, a number of these individuals have created their own alliance—calling themselves "Scattered LAPSUS$ Hunters" or SLH. Combining these three names, which are associated with these highly visible data breaches, gives the alliance a level of clout and credibility in both the attacker and defender communities. And while this alliance seems to be executing the exact same playbook against Gainsight as they did against Salesforce, there's one very significant development: they're using this publicity to showcase their own Ransomware-as-a-Service (RaaS) platform called ShinySp1d3r.

Author

Jeanette Miller-Osborn, Field Cyber Intelligence Officer

NOVEMBER 25, 2025



Ransom message for ShinySp1d3r

To learn more, contact **NEWCOM**
781.826.7989 | sales@newcomglobal.com
NEWCOMGlobal.com

NEWCOM

How Did We Get Here?

The way that this group has evolved over the last few years is representative of the broader evolution of the global threat landscape. Cybersecurity teams now have to worry about a much broader set of threat actors with access to commoditized tools and AI that help them build highly convincing campaigns, which have proven to be highly effective in breaching some of the largest enterprise organizations in the world.

The reality is that cybercrime groups now organize themselves like businesses—adhering to seniority levels, hiring people based on their skill sets, offering competitive compensation, and re-investing their earnings into research and development to become even more capable. Over time, that R&D seems to have been more focused on advances to their typical playbooks, such as building more capable social engineering kits.

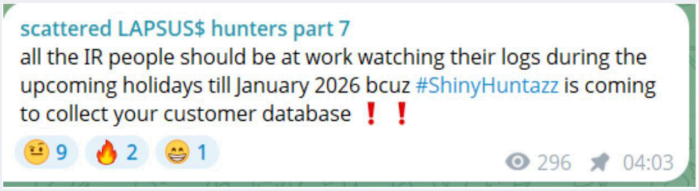
But with the release of ShinySp1d3r, we're seeing a very concerning advancement in what these groups are capable of creating. Typically, members of The Com would team up with an outside ransomware vendor, like ALPHV/Black Cat or DragonForce, to encrypt a target's infrastructure and extort them for a large ransom. However, ShinySp1d3r now enables them to both execute their own ransomware attacks and offer it as a service to other cybercrime groups that don't have the ability to build their own. This opens up a massive amount of opportunity for SLH to increase their revenue and influence, while smaller groups can leverage their services to inflict even more damage on organizations.

What Can be Done?

Modern cybercrime groups like SLH move quickly and are very good at getting highly personal when targeting potential victims. A significant part of their playbook is social engineering, which is a tactic that AI has massively simplified for threat actors. However, they also frequently discuss what they're going to do in open forums such as Telegram. While there's a lot of posturing in those forums, there's also a lot to be aware of if you're trying to keep your people and your organization safe.

Gather the earliest intelligence possible

While most security operations center (SOC) teams operate under the assumption that their organization could be targeted at any moment, the earliest signals often appear in conversations on dark web forums, Telegram channels, and other disparate sources. Learning when a company appears in that chatter can give security teams precious minutes or hours of time to get ahead of the attack.



A public Telegram post forewarning incident response teams of holiday activity

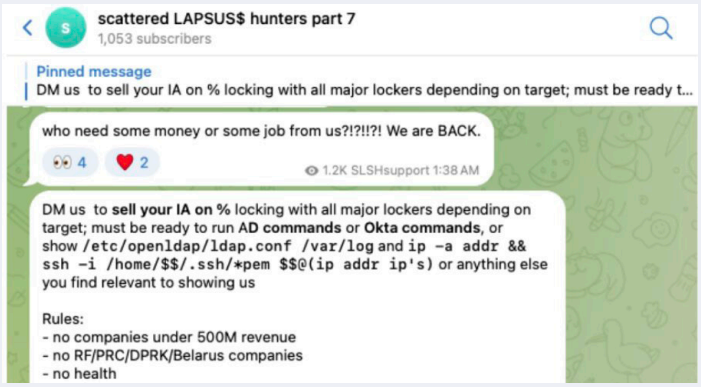
Even if a team's specific organization isn't mentioned, it can also be helpful to know if a group is targeting peer or third-party organizations, has taken interest in a certain industry, or is intending to exploit a vulnerability in a widely used solution.

Leverage AI to make sense of the chatter

AI has presented a unique opportunity to get ahead of the inevitable. As your teams gather intelligence from countless data sources, it's impossible for them to comb through each data point to uncover threats or correlate signals of malicious activity. In addition to initial alerts, a purpose-built AI platform can provide live context around an incident, adapt dynamically to the latest intelligence, and even align potential impact to your own internal systems.

Monitor insider user and systems activity

Modern threat actors like Scattered LAPSUS$ Hunters are actively advertising for company insiders who can grant them direct access to internal systems. While everyone would like to believe that an employee would never give up access for financial gain, it's impossible to know whether external factors such as personal debts or a sick family member could influence an individual to help the actors out.



SLH attempting to recruit company insiders

In this particular case, the actor is not just asking for a legitimate set of login credentials, but rather direct access via a VPN or VDI solution. If this is indicative of a growing trend, then it's just as important to know where your internal systems are connecting and what traffic is moving in and out of your network.



Dataminr Pulse for Cyber Risk

Learn how Dataminr Pulse for Cyber Risk provides early, actionable intelligence for SOC teams.

REQUEST DEMO

@ 2025 Dataminr. All rights reserved