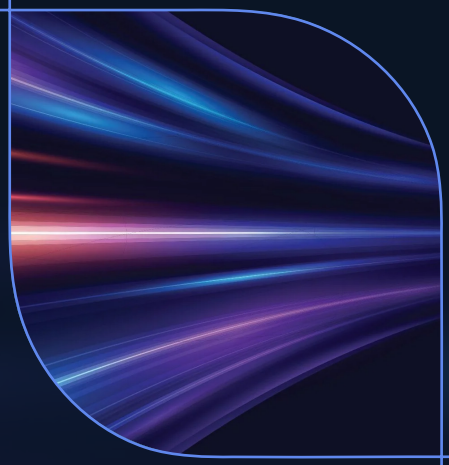
Dataminr NEWCOM Authorized Partner

Cybercrime Evolution from Data Encryption to Exfiltration



Cybercrime operations have shifted focus from encrypting to stealing data, driven by a combination of speed and efficiency. The result for defenders and others is a landscape that is more difficult to defend but lacking immediate risk of operational disruption. Understanding how adversaries are pursuing data exfiltration and extortion is critical to positioning organizations to defend against such actions.

Cybercrime or "ecrime" remains a scourge for individuals, companies, and public sector institutions. The last available estimate of cybercrime costs to the broader economy by the FBI placed them at over $16 billion, a 33% increase from 2023. That ecrime is an issue for organizations is given; the nature of that threat, however, remains in flux.

Typical thoughts on ecrime focus on either business email compromise (BEC) activity, where adversaries leverage communications to elicit fraudulent payments from victims, or traditional ransomware activity, where threat actors compromise a network then proceed to encrypt files to hold that network hostage. While other facets of ecrime exist, including support mechanisms such as initial access brokers and credential and identity theft campaigns ("infostealers"), these two tend to dominate discussions in ultimate impact to individuals and organizations.

To look at ransomware more closely, such activity includes multiple implementations to prompt victim payment. Encrypting victim files is the most straightforward and longest-running version of such activity, but beginning around 2019 various threat actors began to engage in "double extortion" ransomware. In these incidents, data is exfiltrated from victim networks prior to encryption, with victims facing two forms of extortion: recovery of files within the internal network, and maintaining the confidentiality of information from possible leak or exposure by the threat actors.

Author

Joe Slowik, Director, Cybersecurity Alerting Strategy

DECEMBER 2, 2025

Encryption to Exfiltration

Soon after the introduction of double-extortion ransomware, new types of ransomware-like campaigns emerged that eschewed file encryption entirely in favor of focusing purely on the data exfiltration and leak threat. For example, the notorious cl0p threat actor is associated with multiple campaigns where vulnerabilities in managed file transfer (MFT) solutions or similar file sharing portals were exploited to gain access to data for rapid exfiltration. More recently, groups such as Everest and Coinbase Cartel have moved away from traditional ransomware toward compromising external file sharing services, such as FTP servers, to exfiltrate information from entities such as Collins Aerospace and Svenska Kraftnat.

In examining these incidents, several commonalities appear that are of concern for defenders and organizations:

- Activity often focuses on externally-accessible, rapidly-exploited (via vulnerabilities or valid credentials) services.
- Threat actors typically limit their operation to rapid data exfiltration from the compromised asset while avoiding further victim penetration, despite accessed systems providing the opportunity to do so.
- The activity in question leverages public pressure through leak sites and similar to (attempt to) force victims to pay a ransom for not disclosing (if not exactly deleting) compromised information.

Such events are interesting in that they are significantly more "efficient" than traditional ransomware activity, and can scale very rapidly in cases of vulnerable applications such as MFT services. For traditional ransomware operations, threat actors must breach the victim environment, typically gain some form of domain-wide execution or similar, seed a ransomware payload throughout the network, and trigger execution. While such activity can range from days to hours depending on the entity and how aggressive they are in operations, pure exfiltration activity from external-facing assets can take a matter of hours or minutes to achieve. When paired with a successful exploit and the ability to rapidly scan for external-facing vulnerable servers, threat actors can quickly compromise dozens if not hundreds of systems while automating exfiltration actions.

Defensive Challenges

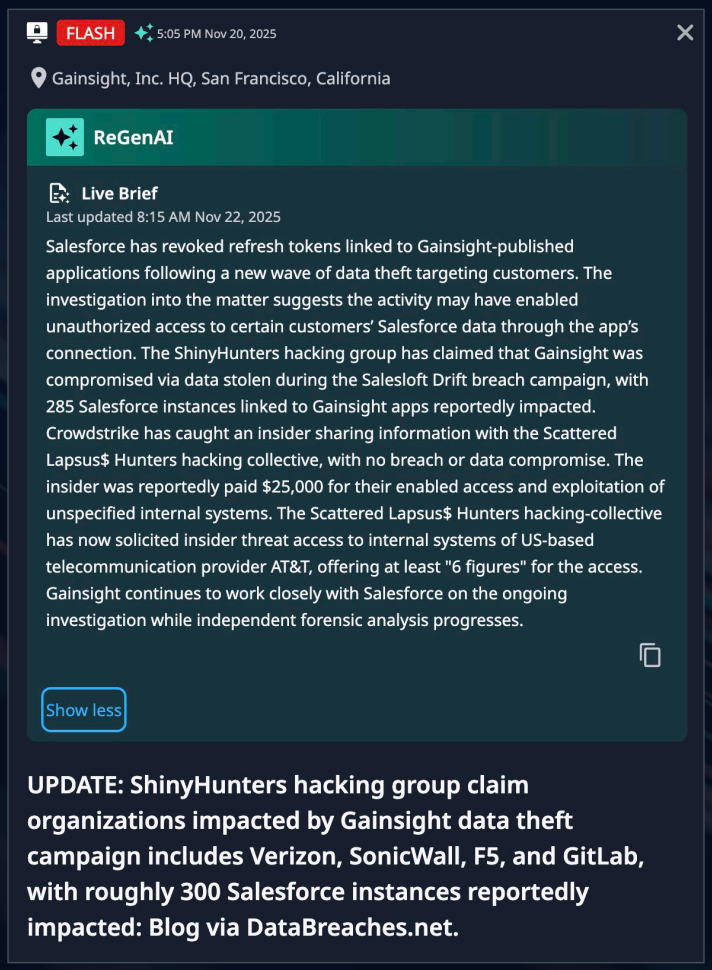
Arguably the most concerning and critical element of the above transition is the significant reduction in potential detection or disruption points for defenders. While traditional ransomware entities can move quickly from initial access to full domain compromise, these actions still require a number of discrete steps for success with multiple opportunities to identify or defeat such activity before the adversary achieves their objectives.

Conversely, pure data exfiltration from vulnerable systems or from systems for which legitimate credentials exist features few if any touchpoints for defenders to take advantage of prior to data loss. The result is a faster, more efficient mechanism for threat actors that evades many (if not most) traditional security controls.

Given the above benefits, it is no surprise to observe that entities ranging from cl0p to various permutations of Scattered Spider, Shiny Hunters, Lapsus$, and more recent combinations of these groups engage in such activity with enthusiasm (while at times also engaging in more traditional ransomware activity). Such entities have leveraged vulnerabilities in software or software relationships such as in Salesforce (via Salesloft Drift integrations and more recently Gainsight connections), Oracle E-Business suite, as well as historical campaigns targeting Fortra GoAnywhere MFT.

This comes in addition to more traditional replay of stolen credentials against single-factor file storage and transfer instances, such as public-facing FTP servers. The result has been claims of significant data exfiltration from organizations as varied as major health services, critical infrastructure entities and contracting organizations, and entertainment companies.

Learn More: Scattered Spider is Wreaking Cyber Havoc. Here's How to Stay Ahead.



Example alert of ShinyHunters leveraging third-party application for data theft

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

NEWCOM

Orienting Defense to Non-Traditional Attacks

Combating or defeating such activity goes beyond traditional IT defenses and security mechanisms. However organizations can employ several strategies to mitigate or reduce risk:

- Organizations must reduce attack surface and deploy preventative mechanisms. These can range from eliminating single-factor authentication from all external-facing services to ensuring rapid deployment of patches to external applications such as file transfer applications.
- In the case of zero day exploitation, organizations must move to reduce exposed services through design architecture or leveraging services such as VPNs to control access to such applications.
- Organizations must work to detect anomalous data flows from file transfer services—while easy to say, this is challenging to implement since such services by design serve large amounts of data for download or transfer. A combination of baselining and leveraging technical solutions such as network flow anomaly detection and monitoring could meet this, but requires significant investment.
- Organizations must maintain situational awareness on threat actor operations to identify shifts in behavior such as moves to favor data exfiltration to spur and justify countermeasures and controls.

In addition to the above, a note of caution is also warranted. Ecrime actors can also claim compromise when no such activity may in fact exist, or exfiltrated data is publicly available or otherwise non-sensitive. However, making such a determination is often difficult to impossible for most organizations absent robust monitoring and awareness of what data is stored where within their environment. Thus, degrees of both cyber hygiene (to control where data is stored and knowing these locations) and monitoring (to identify when and from where information is exfiltrated) is necessary to vet threat actor claims.

While the shift in adversary activity towards pure data exfiltration for extortion purposes is concerning and raises many challenges, it is not impossible to address. Understanding how adversaries achieve this objective, through both compromised credentials and various types of vulnerabilities, can allow organizations to implement mitigations to reduce the scope of such activity if not eliminate it entirely from defended environments.



How Scattered LAPSUS$ Hunters Illustrates the Evolution of Cybercrime

For more about the evolving cybersecurity threat landscape, read our blog on How Scattered LAPSUS$ Hunters Illustrates the Evolution of Cybercrime.

READ NOW

@ 2025 Dataminr. All rights reserved