



| Flash |

Play Ransomware Increases Activity

F-2023-11-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware

November 22, 2023

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on November 22, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Play Ransomware Increases Activity

› Key Findings

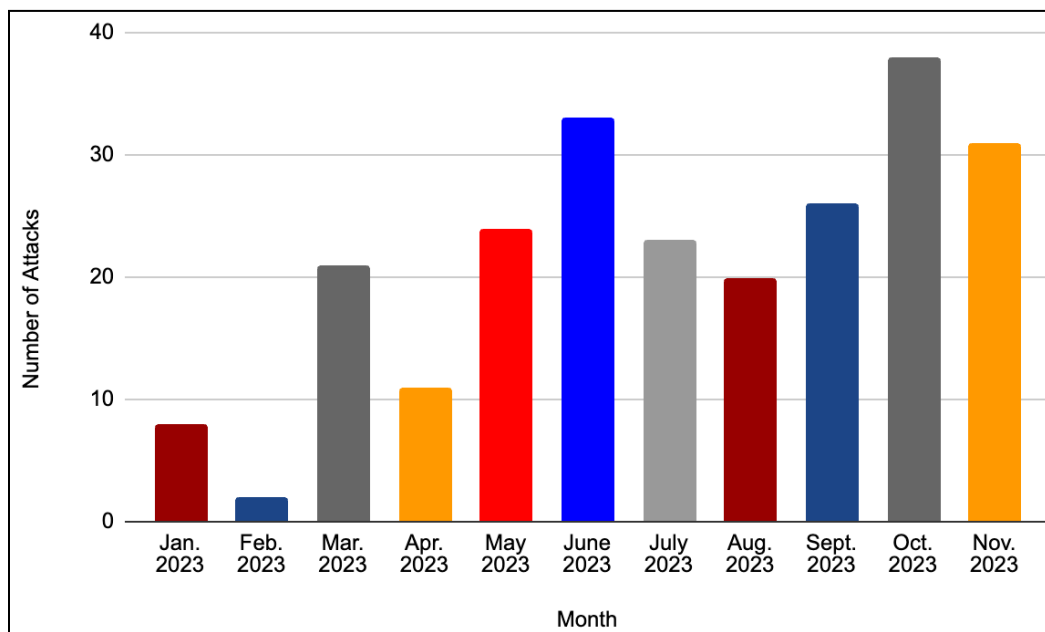
- Financially-motivated ransomware collective Play has increased the cadence of its operational activity in Q4 2023, having been responsible for approximately 14 percent of all ransomware and digital extortion (R&DE) activity observed by ZeroFox in October.
- Play is increasingly targeting organizations based in North America, which comprised 74 percent of all victims in October 2023. This is in stark contrast to just 35 percent of victims being from this region between Q2 2022 and Q3 2023.¹
- There is a roughly even chance that this increased operational tempo is due in part to a recent shift by Play to an as-a-service model, whereby affiliates are able to purchase the software or lease it via a subscription-based model. This would see associated activity increase, particularly if the services are made available to threat groups and individuals of lower sophistication.

| Details

The financially motivated ransomware collective Play (also known as PlayCrypt) has increased its operational activity in Q4 2023. The strain, actively deployed since as early

¹ ZeroFox Intelligence Internal Collections

as June 2022, recorded its highest number of victims in October 2023—responsible for approximately 14 percent of all R&DE activity in the month and second only to LockBit. This trend has continued into November, with attacks set to be even higher.²



Number of observed Play Ransomware attacks so far in 2023.

Source: ZeroFox Intelligence Internal Collections

Play operators leverage various initial intrusion vectors to gain network access, including illicitly obtained credentials, exploitation of internet-facing applications, exploitation of external remote services, and phishing emails with malicious attachments. Privilege escalation and lateral movement then enable the accessing of sensitive victim information, which is exfiltrated and then encrypted before being held to ransom (double-extortion).³ Play was reportedly among the first strains to demonstrate intermittent encrypting in an effort to decrease attack speeds, encrypting small, targeted parts of the files' content which still renders the data unrecoverable.⁴

² ZeroFox Intelligence Internal Collections

³

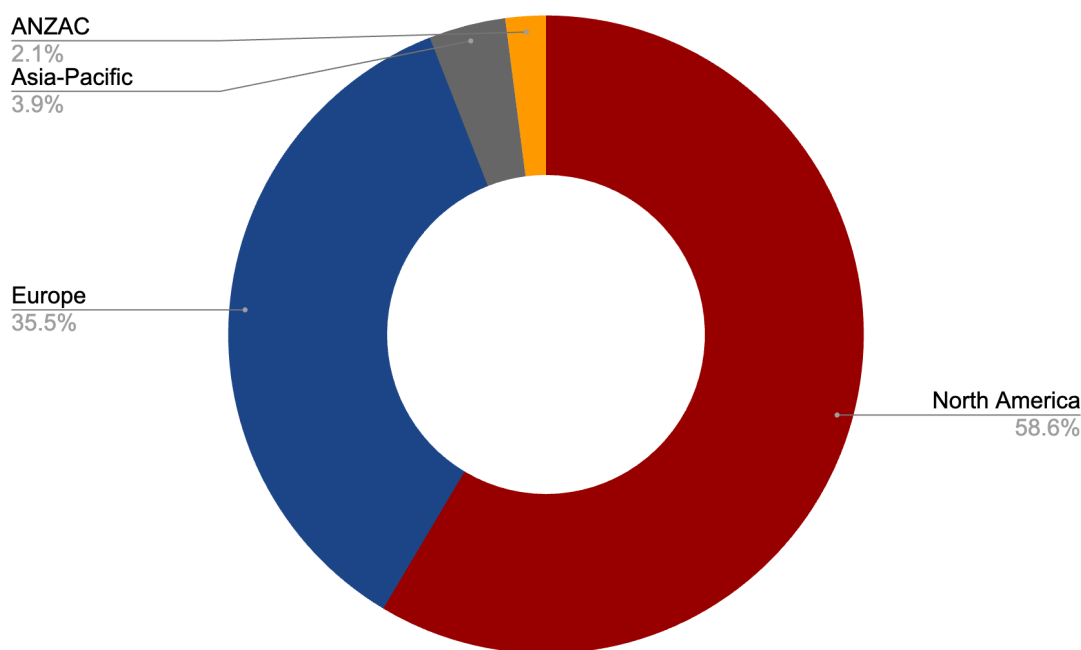
[hXXps://adlumin\[.\]com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/](https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/)

⁴

[hXXps://www.bleepingcomputer\[.\]com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/](https://www.bleepingcomputer.com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/)

Post-launch, Play was primarily leveraged to target victims in Europe, Asia-Pacific, and Latin America, together accounting for over 90 percent of victims during 2022.

In 2023, Play targeting has shifted significantly towards North American targets—which have accounted for 74 percent of victims since October—and away from all other regions. This is very likely due to, in part, the abundance of lucrative potential targets in North America owing to its significant digital infrastructure. Within all regions, the manufacturing and construction industries are the most heavily targeted.⁵



Play Ransomware Victim Locations in 2023

Source: ZeroFox Intelligence Internal Collections

Recent reporting alludes to the observed indicators of compromise (IoCs) associated with Play activity being notably similar across attacks, often lacking any of the variation that would be expected between deployments.⁶ This includes the same password being used in the creation of high-privileged accounts and many of the same attack commands being observed.

- There is a roughly even chance that the continuity between attacks is due to a recent shift by Play towards an as-a-Service (RaaS) model, which would lead to

⁵ ZeroFox Intelligence Internal Collections

⁶ [hXXps://thehackernews\[.\]com/2023/11/play-ransomware-goes-commercial-now.html](https://thehackernews[.]com/2023/11/play-ransomware-goes-commercial-now.html)

the ransomware being leveraged by both sophisticated threat groups and lower capability actors. Some affiliates would likely be supplied with step-by-step instructions as a part of the service, leading to many of the reported similarities observed in recent attacks.⁷



Play ransom note, including contact information

Source: Original-Network.com

Play has previously been observed leveraging its own custom-made software, including Grixba-a .NET infostealer, and a tool that allows the copying of files prior to encryption, before they can be locked by the operating system.⁸ The shift to a RaaS model is likely a financially-motivated move seeking to increase growth and profitability and benefit from the marketing of effective and established malware strains.

- RaaS offerings have almost certainly been proliferating in deep and dark web (DDW) marketplaces during 2023, as both new and established collectives offer competing prices, increasingly customizable malware, different levels of initial access, and varying customer support commitments. These flourishing marketplaces are very likely a contributing factor to the significant upward trajectory in R&DE attacks observed during 2023, as well as the increasing activity observed from smaller threat groups such as NoESCAPE, Lost Trust, Cactus, and Ransomed.

⁷

[hXXps://adlumin\[.\]com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/](https://adlumin[.]com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/)

⁸

[hXXps://symantec-enterprise-blogs.security\[.\]com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy](https://symantec-enterprise-blogs.security[.]com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy)

- RaaS proliferation almost certainly lowers entry barriers to would-be threat actors who may otherwise lack the sophistication. It also very likely decreases the time within which the group can establish proficiency and begin conducting attacks.

| Recommendations

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of R&DE threats and their associated tactics, techniques, and procedures (TTPs) and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%