Lumma Stealer actively deployed in multiple campaigns

intrinsec.com/lumma_stealer_actively_deployed_in_multiple_campaigns/

Equipe CTI 17 octobre 2023

LummaC2 Stealer

Key findings

In this report are presented:

Lumma Stealer, also known as LummaC2 Stealer, is a malware-as-a-service sold through Telegram and Russian-speaking cybercrime forums. In this report, the following will be addressed:

- The presence of Lumma in Russian-speaking forums and Telegram.
- Code analysis of different campaigns distributing Lumma stealer using various techniques.
- The infrastructure associated with Lumma stealer, including the old and new versions of C2 panels.A trail, that we uncovered, which indicates a potential use of Lumma by a Russian intrusion set.

Intrinsec's CTI services

Organisations are facing a rise in the sophistication of threat actors and intrusion sets. To address these evolving threats, it is now necessary to take a proactive approach in the detection and analysis of any element deemed malicious. Such a hands-on approach allows companies to anticipate, or at least react as quickly as possible to the compromises they face.

For this report, shared with our clients in July 2023, Intrinsec relied on its Cyber Threat Intelligence service, which provides its customers with high value-added, contextualized and actionable intelligence to understand and contain cyber threats. Our CTI team consolidates data & information gathered from our security monitoring services (SOC, MDR …), our incident response team (CERT-Intrinsec) and custom cyber intelligence generated by our analysts using custom heuristics, honeypots, hunting, reverse-engineering & pivots.

Intrinsec also offers various services around Cyber Threat Intelligence:

- Risk anticipation: which can be leveraged to continuously adapt the detection & response capabilities of our clients' existing tools (EDR, XDR, SIEM, …) through:
  - **an operational feed of IOCs based on our exclusive activities.**
  - **threat intel notes & reports, TIP-compliant.**

- Digital risk monitoring:
  - **data leak detection & remediation**
  - **external asset security monitoring (EASM)**
  - **brand protection**

For more information, go to www.intrinsec.com/en/cyber-threat-intelligence/.

Continue reading


INTRINSEC
Cyber Threat Intelligence
Various actors actively deploying
Lumma Stealer in multiple campaigns
Follow us for more Cyber Threat Intelligence content
www.intrinsec.com
www.intrinsec.com/blog
@Intrinsec
@Intrinsec

N'hésitez pas à nous contacter

Laissez-nous un message décrivant vos besoins en sécurité, ou bien contactez-nous si vous souhaitez avoir des informations concernant nos activités. Nous vous répondrons dans les meilleurs délais.

N’oubliez pas de renseigner votre adresse e-mail ou téléphone afin que nous puissions vous recontacter rapidement.

Découvrez nos expertises