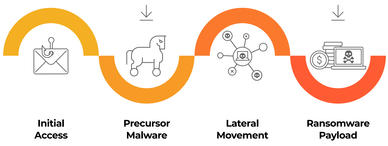
2023 Ransomware Flashcard

black hat

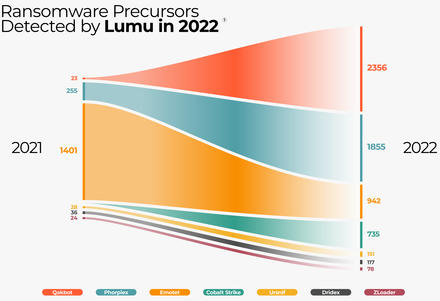
Ransomware Is Not Laying Low in 2023

Ransomware continues to ramp up in 2023. Whereas Ransomware Groups used to avoid publicity in the wake of the Colonial Pipeline attack, threat actors now openly broadcast their ransom demands. CL0P Ransomware, in particular, is foregoing private ransomware notes, in favor of publishing ransoms on their CL0P leaks website, relying on media and the information security community to spread its message.

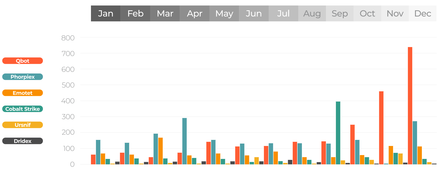
Ransomware **Precursor Activity**



Ransomware Precursors Detected by **Lumu in 2022** [1]



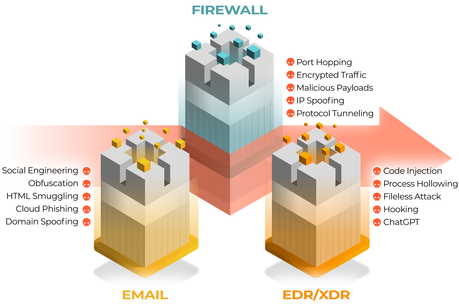
Top Ransomware Precursors by **Month** [1]



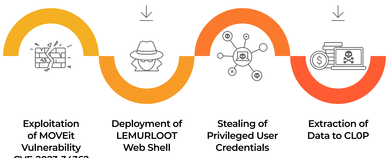
Ransomware Groups: Which Precursors do they use? [1]

Precursor	Ransomware Group
Qbot	Egregor, ProLock, MegaCortex, Black Basta, Royal, Conti
Phorpiex	Avaddon, Nemty, Knot, BitRansomware, DSoftCrypt/ReadMe, GandCrab, Pony, REvil
Emotet	Ryuk, Conti, ALPHV/BlackCat
Cobalt Strike	Crysis/Dharma, DJVU/STOP
Ursnif	Egregor
Dridex	DoppelPaymer, BitPaymer

How **Ransomware** Is **Evading** the Triad of Cyber Defenses



Attack in Focus: How CL0P Exploits MOVEit [2]



Network Visibility Is Essential to Detect Breaches in Time

Ransomware groups continue to successfully bypass defenses and are only growing bolder. Precursor malware doesn't need much to take hold on the network. All it takes is a vulnerability found by the bad guy first or an employee to mistakenly click on one malicious email.

A layered approach to cybersecurity requires investment in both prevention and detection. But we've seen time and time again that eventually defenses will get bypassed. But the silver lining is that ransomware groups need to use the network to achieve their aims. With network visibility, you can detect, understand, and stop malicious behavior in your network before the ransomware payload is delivered.

Stay Ahead of Ransomware
Try Lumu Free

Open a Lumu Free Account

www.lumu.io

Sources:

1. Precursor malware associated with Ransomware deployment detected by Lumu in 2022. In 2022 Lumu processed 1.307 billion records, up from 430.4 billion in 2021.
2. ArsTechnica: Mass exploitation of critical MOVEit flaw is ransacking orgs big and small: https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/2/

LUMU