>> Ransomware V.2023

>> CaaS (Cybercrime as a Service) and the explosive growth of RaaS (Ransomware as a Service)

The market for ‘Cybercrime as a Service’ is now comparable in its sophistication and range of available products to the SaaS market.

Relatively unsophisticated criminals can buy advanced ransomware services – on the dark web – with commercial terms copied from legitimate marketplaces, including monthly subscription and profit-sharing affiliate arrangements. And as with SaaS, the attractions of flexibility and scalability have contributed to a boom in ransomware deployment. Fortinet, for example, recently identified over 10,000 new ransomware variants in the first half of 2022; nearly twice as many as in the same period of 2021. This growth – largely driven by RaaS – may be expected to continue next year.

CaaS offerings also support the ransomware industry in other ways: ‘Initial Access Brokers’ provide AaaS (Access as a Service), specialising in acquirement of credentials and cookies that enable an attacker to infiltrate devices and networks. Reconnaissance as a Service assists with targeted attacks. We may also see in 2023 the emergence of Money Laundering as a Service, which will provide automated services to cycle ransom funds through exchanges and mixers.

>> Ransomware 2.0

Now that many organisations back up their data to a segregated location, encryption alone is a far less effective method for extortion, and some ransomware operators have abandoned it altogether.

Most groups do still encrypt files, but also exfiltrate them beforehand for later release via the dark web (double extortion) – in fact causing a data breach. Further pressure may be applied by going after individual victims of the attack whose credentials have been revealed or even launching DDoS attacks against the organisation’s website. The objective is always to exert as much pressure as possible, to try to force the hand of the victim.

When files are encrypted, the process can be fast. Analysis by Splunk revealed that LockBit malware is able to encrypt 50GB of data in just over 4 minutes.

Kiowa
INFORMATION SECURITY

robin.long@kiowa.tech

>> Targeted attacks

’Big game hunting’ will continue, although the geographical focus may shift from the US towards Europe, due to the increasingly aggressive American political stance regarding ransomware.

Targeted attacks on high-value objectives are characterised by the amount of time spent on reconnaissance and planning. Also:

- Very carefully crafted spear-phishing attacks targeting admin users

- Bribery of employees to gather credentials and carry out other ‘inside jobs’ such as sim-swapping

- Skilled lateral movement in search of specific, high value information such as personal data and sensitive intellectual property

- Attacks on backups by encryption of small pieces of data over a long period, so that backup files are slowly and discretely corrupted

- Use of cutting edge hacking techniques, such as deployment of C2 frameworks like Cobalt Strike, zero-day exploits purchased on the dark web and attacks on MFA

>> Following data to the cloud

Ransomware groups are well aware of the ongoing migration of sensitive data to the cloud. They also know that the fact that many organisations are struggling to stay on top of increasingly complicated cloud infrastructure often leads to vulnerabilities.

Watch out next year for ransomware attacks that leverage misconfiguration of cloud resources and vulnerable and neglected APIs. Although, note also that these will be data breaches rather than encryption attacks.

Attackers are likely also to step up their interest in the Managed & Cloud Service Providers (MSP, CSP) that secure companies’ data.

Kiowa
INFORMATION SECURITY

Ransomware V.2023 <<

robin.long@kiowa.tech