Cyber Threat Advisory

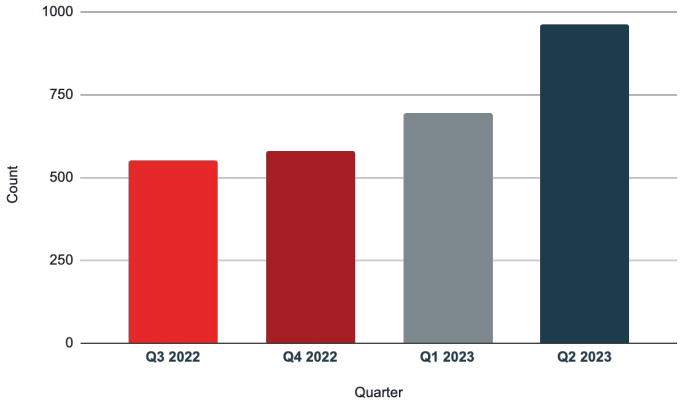
June 22, 2023 F-2023-06-22a

ZEROFOX Intelligence

Ransomware & Digital Extortion Incidents Surging In Q2 2023

- The number of ransomware and digital extortion (R&DE) incidents recorded so far this quarter is almost 40% higher than in Q1 2023. This is expected to increase for the remainder of Q2 2023, not least as Clop continues to name victims from the successful exploitation of CVE-2023-34362 affecting MOVEit Transfer software. This bucks a trend in recent years of fewer attacks in mid-year months when compared with the rest of the year.
- The threat has increased to almost all sectors and geographies; despite raw numbers increasing, the proportion of attacks targeting each sector remains broadly consistent with Q1 2023. Deployment of well-known strains has increased, as well as new strains like 8Base, Akira, CrossLock and CryptNet. This supports the hypothesis that the increased threat is likely to be sustained, rather than a temporary spike.
- 8Base, identified as early as May 2023, is the most prolific new strain in Q2 2023, conducting 92 attacks including 72 in June to date. Victims—predominantly small-medium size businesses—are dispersed geographically and are primarily from the finance, manufacturing and technology sectors. There has been a growing trend so far this year in attacks from newer, less established threat collectives.
- Recent successes have very likely emboldened threat actors, with attacks leveraging vulnerabilities in third-party service software having considerable downstream impact. Russia-based threat actors are likely able to conduct R&DE attacks more freely, with mitigated risk of punitive punishment, reduced disruption to operations compared with the initial stages of Russia's invasion of Ukraine, and the ease of exfiltrating data and extorting victims, rather than deploying ransomware. ZeroFox Intelligence anticipates the R&DE threat will remain heightened in coming months.

Total Ransomware & Digital Extortion Incidents By Quarter



Source: ZeroFox Intelligence

Ransomware & Digital Extortion Incidents By Strain

	Q4 2022	Q1 2023	Q2 2023
LockBit	138	198 (+44%) ↑	223 (+13%) ↑
ALPHV	64	78 (+22%) ↑	122 (+56%) ↑
Royal	67	61 (-9%) ↓	52 (-15%) ↓
Vice Society	29	33 (+14%) ↑	12 (-64%) ↓
Black Basta	38	48 (+26%) ↑	53 (+10%) ↑
Play	26	31 (+19%) ↑	50 (+61%) ↑

Source: ZeroFox Intelligence

Recommendations

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new R&DE targets.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise and metadata related to R&DE.
- Should your organization be impacted by this type of cyber event, engage with ZeroFox for support through our DarkOps and Incident Response teams by utilizing the RFI button in the ZeroFox platform.