

Data theft extortion grows in popularity as revenue-generating attack

Could these types of attacks soon become more popular than ransomware?

BACKGROUND

Data theft extortion is a tactic in which cybercriminals access, steal and threaten to release victims' files or other data without using any encryption mechanisms. The adversary promises to not release the data—such as by publishing it or selling it to others—if the victim pays the requested ransom. But in these cases, the actors never use ransomware. Data theft extortion is becoming increasingly popular among threat actors and was [Cisco Talos Incident Response's top threat they observed](#) in Q2 2023.

TACTICS

- Tactics, techniques, and procedures (TTPs) in data theft extortion operations highly resemble those in pre-ransomware activity, making predicting the threat actor's final operational objective more difficult.
- Data theft extortion actors are very persistent in their communications with victims, often escalating the frequency and tone of their correspondence, including through emails and phone calls, when demands are not met.
- The actors behind these attacks often have well-known and high-visibility leak sites where they threaten to publish the stolen data if the ransom demands aren't met. These disclosures often lead to negative press coverage for the targeted company, and any leaked data could be sold to other threat actors and used in follow-on attacks and scams.

OUTLOOK

- Data theft extortion was the top observed threat in Q2 2023, accounting for 30 percent of the threats seen, according to Talos IR's latest [quarterly trends report](#).

- The rise in data theft extortion incidents compared to previous quarters is consistent with public reporting on a growing number of groups stealing data and extorting victims without deploying ransomware.
- Actors' growing reliance on data theft extortion is likely a result of consistent industry and government efforts to thwart ransomware attacks.

AFFECTED INDUSTRIES/GROUPS

- Data theft extortion actors are opportunistic, targeting victims they assess will quickly and easily yield lucrative payouts. Some have engaged in "big game hunting," in which actors specifically target highly profitable companies and/or entities with particularly high-value data or assets.
- Based on recent high-profile attacks, companies from all industries and varying in size could be targets of these attacks.

COVERAGE

- All organizations should enforce multi-factor authentication (MFA), such as [Cisco Duo](#), across their environments.
 - Attackers used a technique called "MFA bombing" in up to 40 percent of Talos data theft extortion to gain initial access and to obtain deeper access once additional credentials were found.
- Several [Cisco Talos Incident Response proactive services](#), such as tabletop exercises and penetration tests, can make sure your organization has appropriate backups in place, quality log retention policies and appropriate incident response plans.