Talos
Cisco Security Research

Examining Maze after its big year

Although the threat actor says it's going silent, the ransomware is still top-of-mind

BACKGROUND

Maze ransomware has only been around for about a year and a half. But in that time, it's made plenty of noise, infecting some high-profile victims and becoming one of the most widely distributed ransomware families. In early November, the actors behind Maze said they were ceasing operations – though their level of activity continues to be scrutinized. Given that there's always a chance Maze could return or rebrand, Talos still believes all organizations should be prepared to face this threat.

CAPABILITIES

- Maze is typically distributed via exploit kits or phishing emails containing weaponized Microsoft Word or Excel documents.
- The threat actors have also been known to exploit other high-profile vulnerabilities.
- Uses Cobalt Strike beacons and creates local administrator accounts to establish persistence before leveraging compromised credentials to escalate privileges and move laterally.
- Maze also exfiltrates the data and threatens to leak it if the victims don't pay the ransom.
- Maze teamed up with other ransomware actors to share tactics and victim information, but the group's future is unknown following Maze's shutdown announcement.

INTELLIGENCE

- Talos and Cisco Talos Incident Response (CTIR) researchers have observed Maze using a range of network reconnaissance methods to prepare for an attack.
- Actors use Cobalt Strike beacons to collect network, host, filesystem, and domain related information, which Talos researchers can later examine.
- Maze actors frequently interacted with technology and security reporters, resulting in public reports that revealed additional information about the group's actions.

RESPONSE

- Talos researchers and incident responders work together on Maze-related incidents by conducting telemetry analysis and providing real-time intelligence support.
- Talos also conducts regular open-source research on activity involving Maze.
- CTIR continues to respond to Maze-related incidents, helping victims mitigate attacks and collecting first-hand data that aids in future research.
- All findings are crucial for Talos analysts writing expansive coverage for ClamAV®, SNORT®, OSQuery and Fireamp.

AFFECTED INDUSTRIES/GROUPS

- There have been more than 100 victims spanning nearly every industry sector, including manufacturing, legal, financial services, construction, health care, technology, retail and government.
- Victims have been primarily based in North America, but threat actors have also targeted entities in South America, Europe, Asia and Australia.
- Anyone with an email inbox is subjected to spam emails that may contain Maze or other types of malware.

COVERAGE

- Cisco AMP for Endpoints deploys coverage into users' environments, preventing the adversaries from deploying the ransomware binaries and associated malware.
- There are numerous ClamAV and SNORT signatures that protect users from many of Maze's malicious activities.
- Cisco NGFW and Stealthwatch detect any changes in customers' network and monitor outbound and inbound traffic patterns that may point to a malware infection.
- Email security products such as Cisco Secure Email and SpamCop can protect users from receiving spam with malicious attachments that may contain Maze.

talos-external@cisco.com | talosintelligence.com