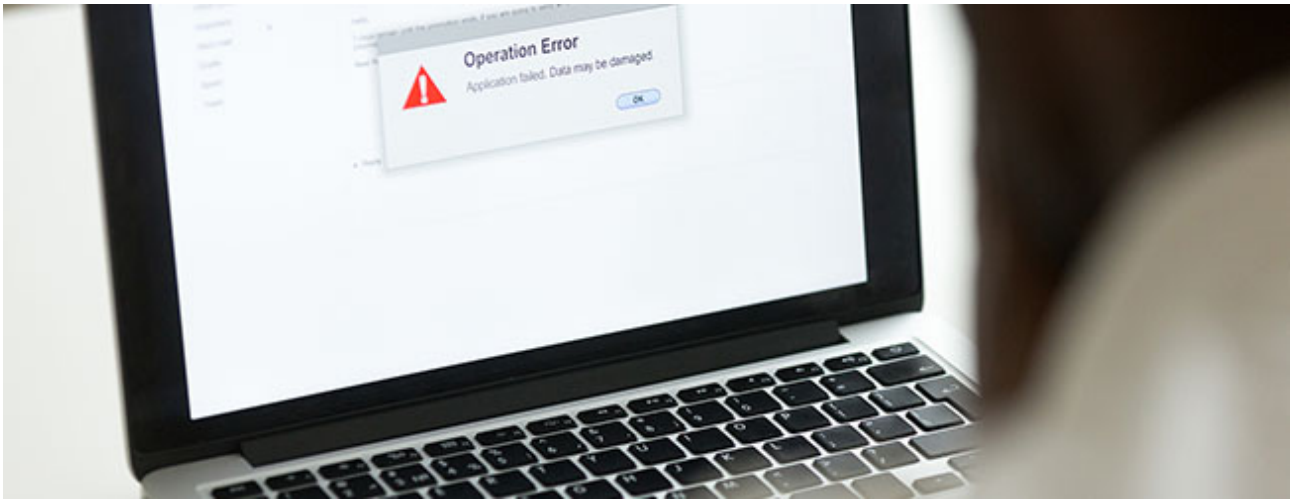
A Deep Dive Into the Latest Maze Ransomware TTPs

By Laurie Iacono

Published: 2020-05-05 · Archived: 2026-04-06 03:20:29 UTC



With the recent attack on a Fortune 500 IT service provider, Maze ransomware is back in the news. Kroll incident response (IR) practitioners worked on multiple Maze ransomware cases during the first quarter of 2020 and have new insights on the tactics, techniques and procedures (TTPs) of these actors and why organizations should revisit their IR plans.

In our work with one client, Kroll had access to a discussion with Maze actors that revealed some of their inner workings. Coupled with the new FAQ document that Maze recently posted on their "shaming" site, it becomes apparent these threat actors are leaving nothing to chance when pressuring victims to pay up quickly. Organizations should heed some of the claims and threatened reprisals for nonpayment as they provide direction for updates to existing incident response plans in the event of such attacks. Consider a few of their claims and threats:

- Once in a system, Maze ransomware actors continuously download anywhere from 100gb to 1tb of data specifically focusing on proprietary or sensitive data that can be used as the basis for regulatory action, lawsuits or ultimately maximize pressure to pay the ransom.
- Actors use tools such as credential-harvesting malware Mimikatz and network reconnaissance software Advanced IP Scanner to facilitate lateral movement throughout the network.
- They actively look for and leverage known vulnerabilities, such as the Pulse VPN CVE-2019-11510 alert, to compromise targets.
- If the victim doesn't pay the ransom, the threat actors will immediately send a prepared press release to the media in addition to releasing the information on their "shaming" site. If the victim is a publicly traded company, the actors will also send the release to the stock exchange where the victim's stock is listed.
- Maze claims that credentials harvested from non-paying victims will be used for attacks against the victims' partners and clients.

Representative Maze Attack Scenarios

As these examples of recent Kroll case work show, no industry sector is safe and actors hunt for data that can inflict the most reputational and regulatory damage.

- A healthcare client learned that Maze threat actors sent emails directly to their patients threatening to expose their personal health data.
- Maze operators told a mortgage company they had 24 hours to pay the ransom or Maze would release their data. The client reported that about two weeks prior, their email system had gone down and were told by their IT vendor that they had a virus. In retrospect, the client believed their server was breached in this incident.
- A realty company started seeing viruses hit their domain environment and a remote access tool was placed by a new user account as a database administrator. The client could restore from backups and did not pay the ransom. Maze posted their data on their shaming site about three weeks after the attack.
- An insurance broker was alerted of a server failure early one morning, but the servers were restored later that day. The client's initial investigation showed that actors had logged into the server with elevated privileges using the chief operating officer's credentials and pushing a password change. Two days later, files were encrypted and they received a ransom note threatening to release their data.

According to Coveware, a ransomware recovery first responder, Maze initial ransomware demands are close to USD 2.3 million, second only to those demanded for Ryuk ransomware. The average final ransom amount is closer to USD 1 mn after negotiation, indicating a roughly 55% discount through negotiation.

Incident Response Planning for Ransomware and PR Attacks

Kroll has shared numerous best practices on how to avoid becoming a victim of ransomware. Likewise, we have described what to do first if an attack does succeed.

A new concern for organizations, however, is that the Maze ransomware operators have intensely compressed the decision making process. Organizations in the past could somewhat control how and when to disclose the details of a suspected data breach. In many cases, organizations need time to ascertain the true extent of a reportable data breach and implement support mechanisms to meet the needs of affected consumers.

Now, with ransomware actors reaching out directly to an organization's customers, the media and regulatory agencies, victim organizations must be prepared to act decisively and immediately.

- Organizations should explicitly build their IR plans with ransomware-specific policies and procedures. Additionally, the organization should have already established its stance on paying or negotiating ransoms, as well as authorized decision makers for the process.
- To get a true sense of the pressure and gaps that could arise in a ransomware attack, organizations should also include ransomware scenarios in their IR plan tabletop exercises.

Are You Ready for Ransomware?

As Kroll's casework has proved, every organization can be a target for ransomware cybercriminals. Kroll has developed a Ransomware Preparedness Assessment that can help your organization better understand your unique vulnerabilities and how to avoid or mitigate ransomware harms. Call us today to learn more.
