FBI Warns of Maze Ransomware Focusing on U.S. Companies

By Ionut Ilascu

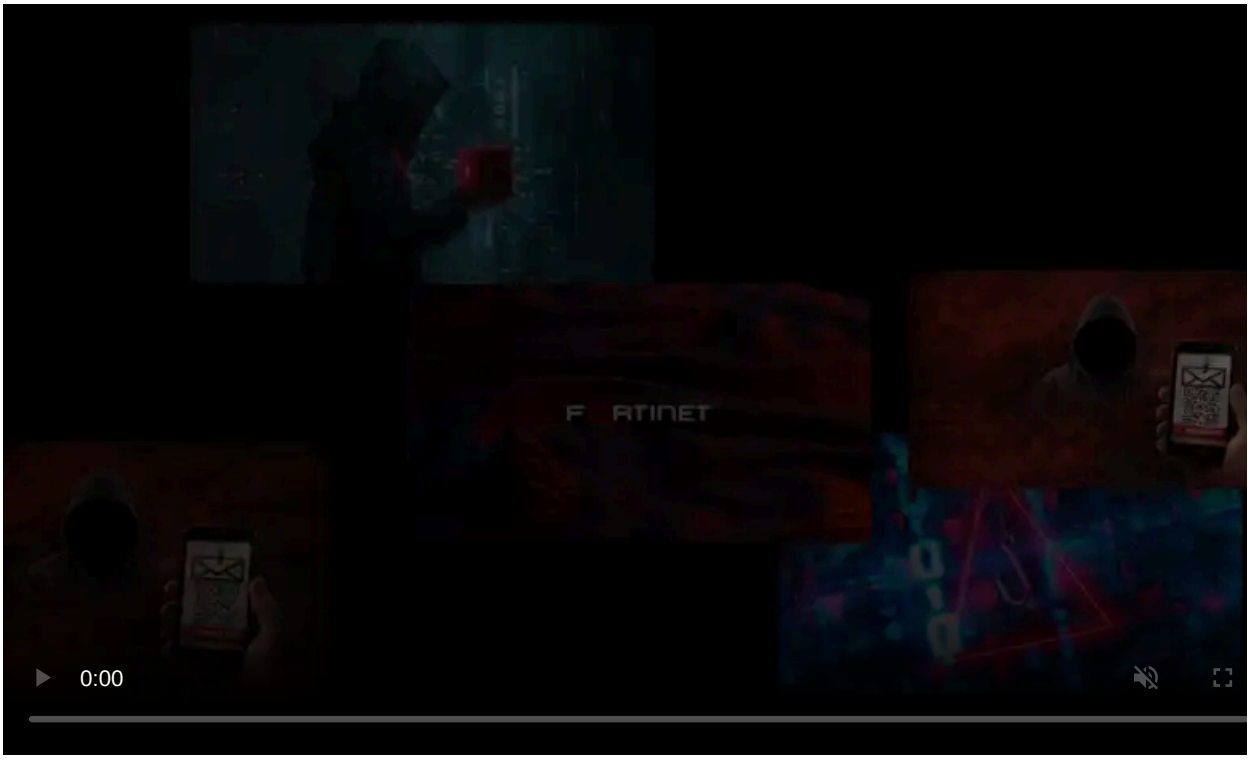
Published: 2020-01-03 · Archived: 2026-04-05 20:18:42 UTC

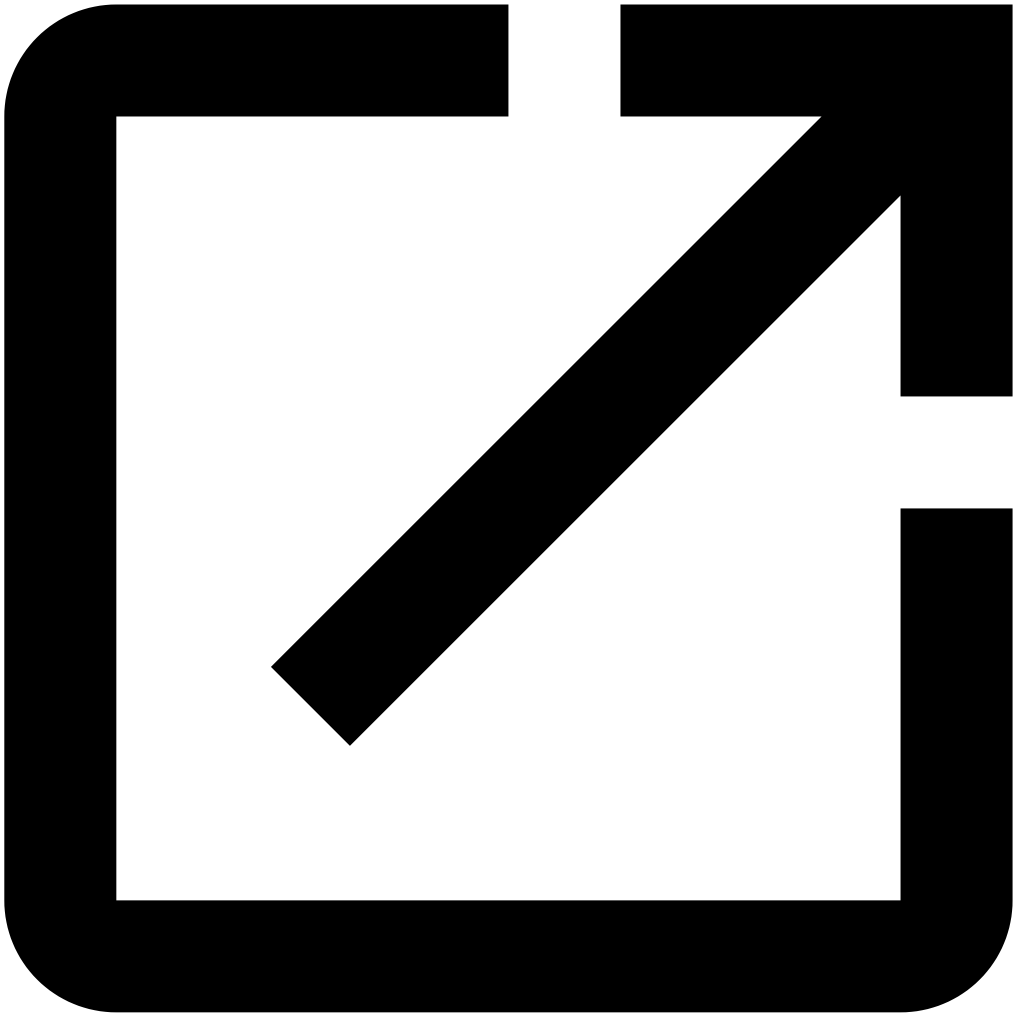
Organizations in the private sector received an alert from the F.B.I. about operators of the Maze ransomware focusing on companies in the U.S. to encrypt information on their systems after stealing it first.

The warning came less than a week after the Bureau warned about the LockerGoga and MegaCortex ransomware threats infecting corporate systems.

The many tricks of Maze ransomware

On December 23, the F.B.I. shared with private businesses a Flash Alert seen by BleepingComputer to increase awareness about Maze ransomware's increased targeting of institutions in the U.S.


F RTINET
0:00



The warning is marked TLP: Green, meaning that it is not shareable via public distribution channels, and contains technical details to help organizations avoid falling victim to this threat.

Maze has been operating since early 2019 at a global level but the "FBI first observed Maze ransomware activity against US victims in November 2019."

Following a network breach, the threat actor first exfiltrates, or steals, company files before encrypting computers and network shares. The actors then demand a victim-specific ransom in exchange for the decryption key.

The stolen data serves as leverage to force victims to pay the ransom, under the promise that it would be destroyed once the attackers get the money.

Maze operators in the past have released data from victims that did not pay them. Two recent examples are the City of Pensacola and Southwire, a manufacturer of cables and wires.

According to the F.B.I. alert, the threat actors behind Maze ransomware use several methods to breach a network, which include fake cryptocurrency sites and malspam campaigns that impersonate government agencies and security vendors.

The malware was also seen distributed by exploit kits like Fallout in May 2019, and Spelevo in October 2019 exploiting unpatched vulnerabilities in Internet Explorer and Adobe Flash (CVE-2018-8174, CVE-2018-15982, and CVE-2018-4878).

"As of late November 2019, malicious cyber actors posing as government agencies or security vendors deployed Maze through phishing emails containing a macro-enabled Word document attachment. When the embedded macro was executed, Maze was downloaded and executed to infect the victim machine" - Federal Bureau of Investigation

The F.B.I. does not recommend paying the ransom since this action does not guarantee the recovery of the encrypted files or the destruction of the stolen data; it would only encourage the threat actors to attack other organizations.

FBI wants the IoCs from victims

Providing indicators of compromise (IoCs) from cyber attacks as soon as possible can help law enforcement in ongoing investigations. The name of the victim is not required in such cases but time is of essence; IoCs should be reported as soon as possible because their value in the investigation decreases at a fast rate.

The agency encourages victims to contact local field offices immediately after the discovery of a ransomware incident and provide the following information:

- Recovered executable file
- Copies of the file or other documents suspected to be related to Maze
- Complete phishing email file with headers
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- Network and Host-Based Log files
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount and whether or not the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)
- Tor sites used to contact the attackers
- Names of any other malware identified on your system
- Copies of any communications with attackers
- Document use of the domains used for communication
- Identification of website or forum where data was leaked

Recommended mitigations

Organizations can lower the chances of falling victim to a ransomware attack by working with up-to-date software, using multi-factor authentication and strong passwords, and by separating the more important systems from the wider access network.

Furthermore, recovering from ransomware is easier and less expensive when a proper routing exists for creating backups offline and the integrity of the process is constantly under scrutiny.

If the attack already happened, the F.B.I. recommends the following mitigation steps:

- Execute a network-wide password reset
- Scan system backups for registry persistence
- Scan system backups for other malware infections, particularly IcedID banking Trojan, Trickbot, and/or Emotet
- Audit logs for unexpected network traffic and mitigate as needed

---

Source: https://www.bleepingcomputer.com/news/security/fbi-warns-of-maze-ransomware-focusing-on-us-companies/