# Business giant Xerox allegedly suffers Maze Ransomware attack

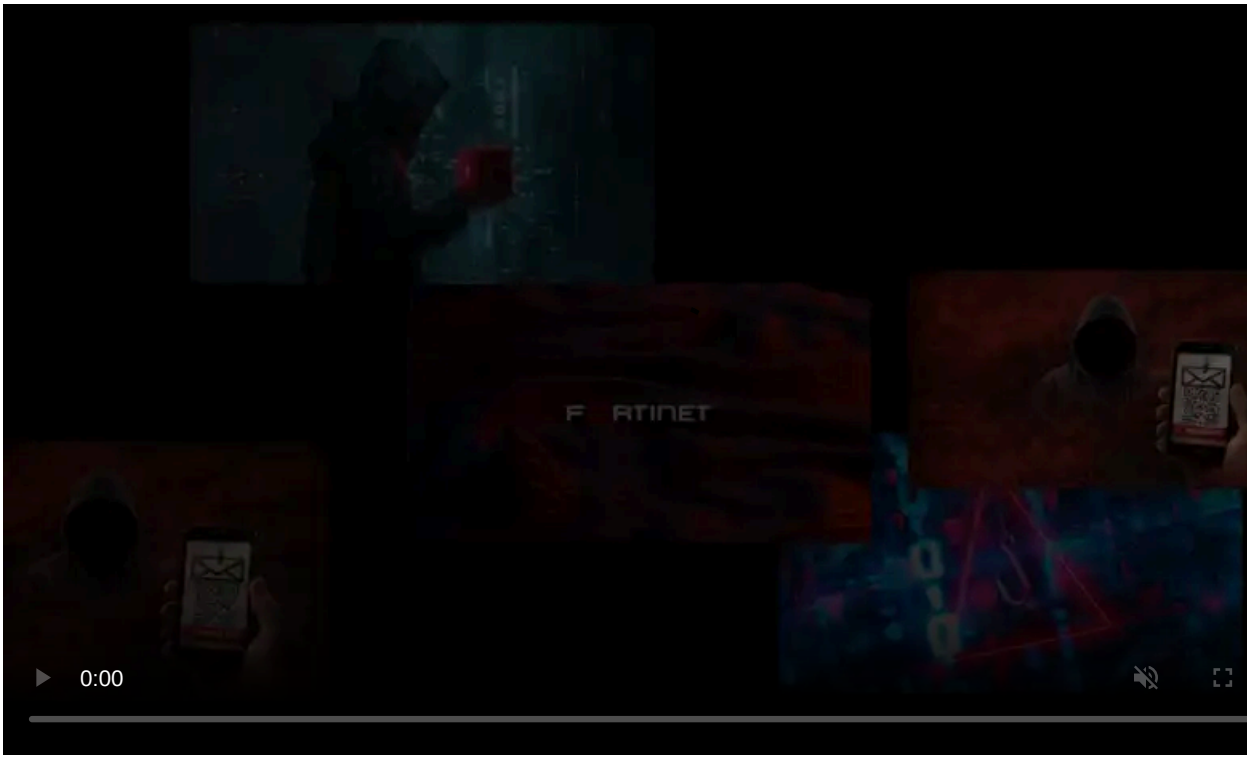
By Ionut Ilascu

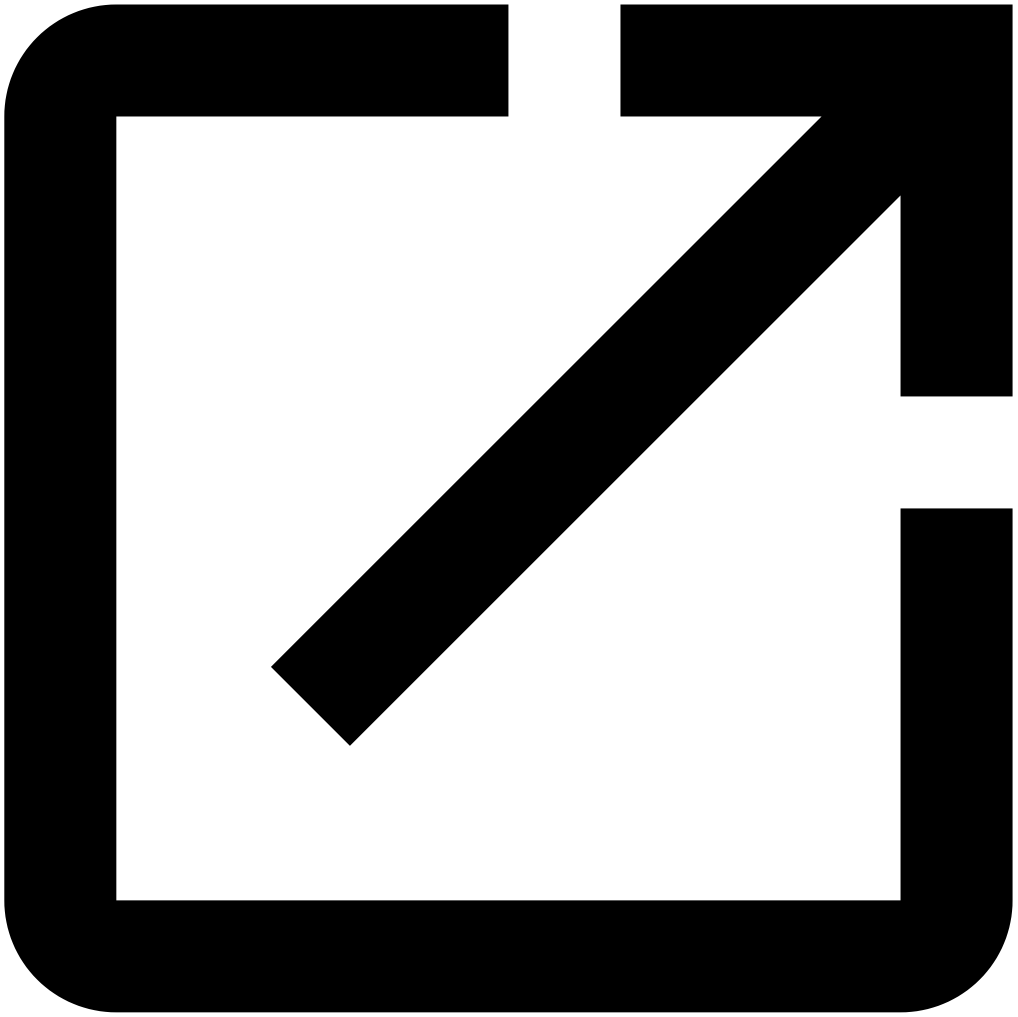
Published: 2020-06-30 · Archived: 2026-04-05 21:11:33 UTC

Maze ransomware operators have updated their list of victims adding Xerox Corporation to the roster. It appears that the encryption routine had completed on June 25.

The company has yet to confirm or deny a cyberattack on its network but screenshots from the attacker show that computers on at least one Xerox domain have been encrypted.

Xerox Corporation is a huge business present in at least 160 countries. It registered over $1.8 billion in revenue in Q1 2020 and has 27,000 employees across the globe. It's part of the Fortune 500 list, currently ranking at 347, with a revenue of over $9 billion last year.


F RTINET
0:00



### Threat to publish over 100GB of data

On June 24, for a brief while, Maze's leak site showed Xerox among the victims of this ransomware group. We contacted Xerox at the time but did not receive an answer.

The attackers told BleepingComputer that they had compromised the company's network but added them too early.

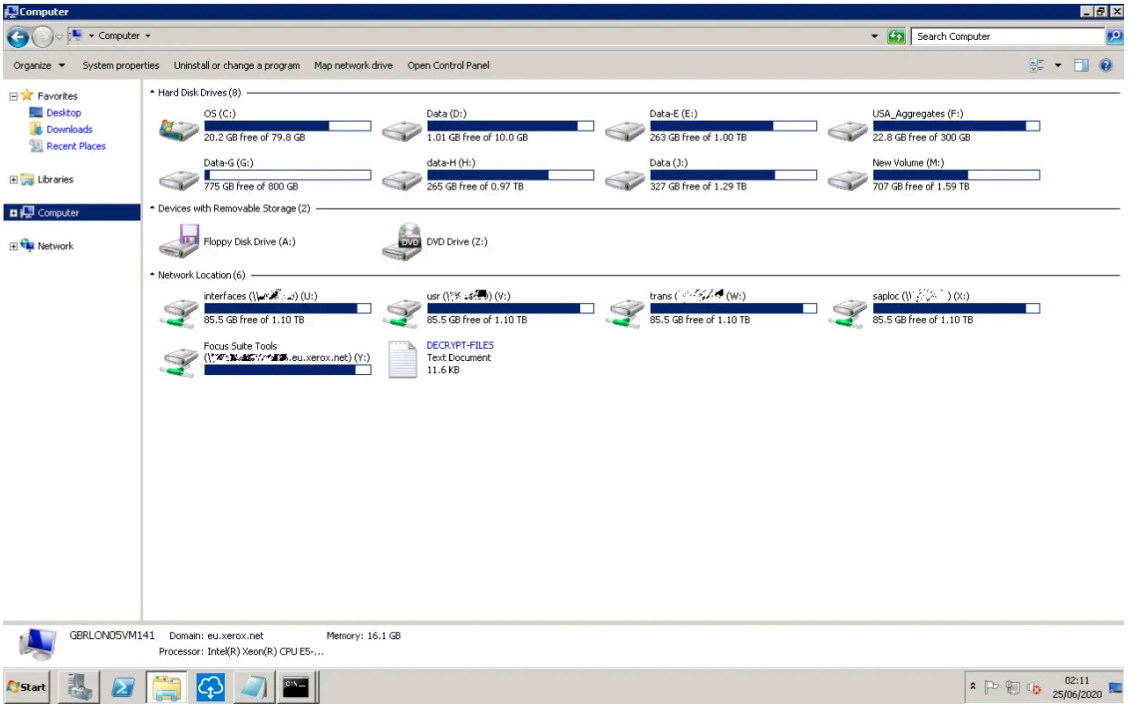
Just like previous posts from Maze, the one for Xerox lacks any details about the attack except for proof of the breach and of encrypting the company's systems.

According to the attacker, they have stolen more than 100GB of files from Xerox and are determined to share it all if the company chooses not to engage in negotiations for a ransom payment.

"After the payment the data will be removed from our disks and decryptor will be given to you, so you can restore all your files," reads the ransom note.

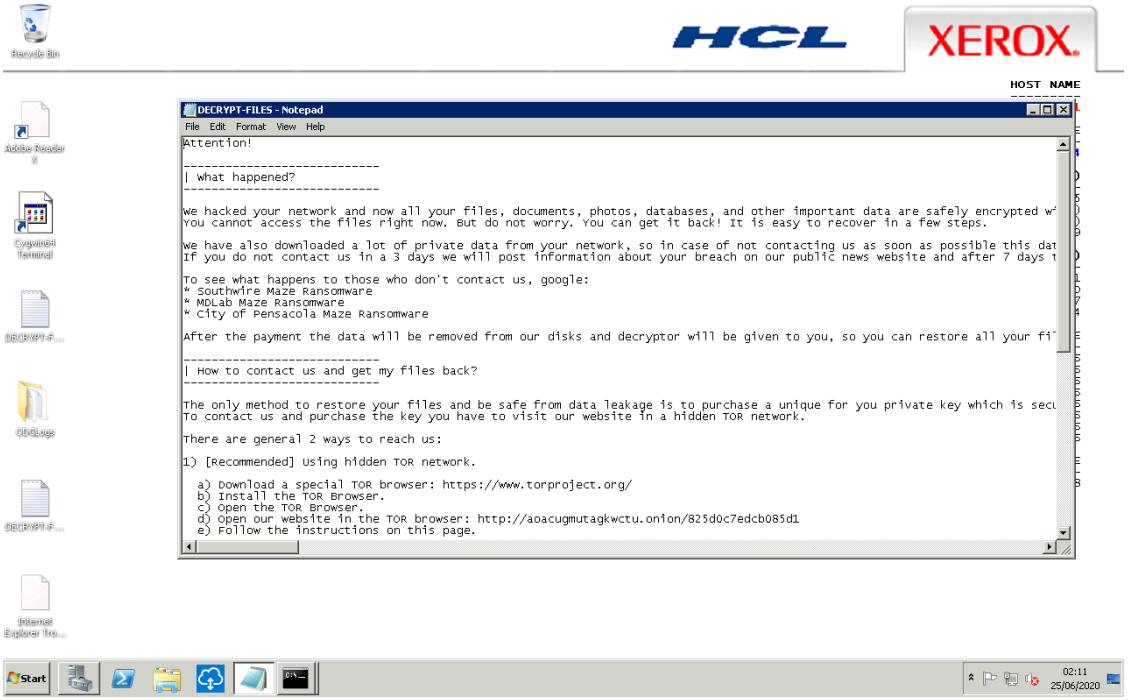
Maze published a set of 10 screenshots, showing directory listings from June 24 and 25, network shares, and the ransom note that is dropped after the encryption routine completes.

Specifically, one image shows that hosts on "eu.xerox.net," managed by Xerox Corporation, were compromised. Systems on other domains might also be impacted.




While the domain reveals that Maze ransomware breached a Xerox branch in Europe, the names of the hosts hint that it's the one in London.

Another screenshot of a desktop screen with the Xerox brand name shows the ransom note dropped by the attacker, who threatened to publish information from the breach if the company did not contact them in three days.




Maze ransomware affiliates have been breaching big companies left and right. Some of the more recent attacks claimed by this group include LG Electronics, chip maker MaxLinear, IT giant Cognizant, and business services company Conduent.

Ransomware infections typically leverage exposed remote desktop services and then gain access to domain admin accounts. From there, they can pivot to valuable hosts. Vulnerabilities in systems that face the public web are also an entry point for these attackers.

Starting last year, ransomware groups began to steal data from the victim network and threaten to publish it unless the ransom is paid.

## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---