Maze Ransomware:Is Posting Data Couterproductive?

Ransomware incidents dominated INFOSEC news in 2019. Penetration methods continued to evolve, attacks became more targeted and ransom demands continued to rise. A major shift in attacker tactics happened in early December when the group behind the Maze ransomware variant started to exfiltrate their victim's data along with encrypting their files. It was disclosed during active ransom negotiations with the Maze actors that the data that is being exfiltrated from victim networks is being analyzed by Maze actors to determine the price for the ransom demand. The Maze group also created a web page and began to publish data of the victims who refused to pay the ransom.

Maze victims could now be extorted in two different ways, forcing clients to deal with a double-pronged issue - data loss on the one hand and data leakage on the other. This makes restoration from backups a lot less appealing as attackers now are leveraging the data extortion component to apply pressure to victims to pay the ransom demands (even if they have valid backups) to stop further data leakage.

It didn't take long for a few other ransomware variants, like REvil/Sodinokibi, DopplePaymer, Pysa/Mespinoza, Ako, Clop, Lockbit, Nefilm, Nemty, Netwalker, Ragnar, Sekhmet, Snatch, and Zeppelin, to follow Maze off the bridge and start accessing and exfiltrating their victim's data as well. All groups believed that having their victim's data may increase their chances of the ransom being paid but, in reality, this strategy will most likely do quite the opposite.

For every organization that is experiencing a ransomware event, the overall incident response price tag consists of several components:

- Initial triage and containment efforts to ensure that the attackers no longer have access to systems and networks
Legal assessment to identify all applicable obligations under state and federal laws and regulations
Forensic evidence collection and preservation
Recovery of data and systems (note: this can occur either by paying the ransom, restoring from backups, or rebuilding systems and data from scratch)
Digital forensics investigation

And, if the results of the forensics investigation do not rule out data access or exfiltration by the attacker:

- Collection and data mining of compromised data to identify all PII/PCI/PHI records (eDiscovery
- Legal review of results
- Notifications of individuals and organizations whose data was compromised;
- DarkWeb search and monitoring services to proactively detect if compromised data would get posted on hacker forums or undergroundmarkets.

Prior to December 2019, data access and/or exfiltration for the majority of ransomware incidents were ruled out based upon the results of digital forensics investigations. Because of that, the chances of victims being required to pay hefty fees for eDiscovery and notification services were fairly low. Currently, since more and more ransomware groups have been adopting

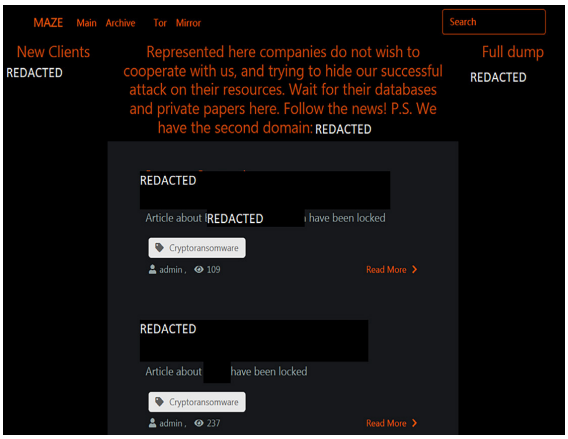
the tactic of stealing sensitive data, victims have to assume that, as a part of incident response costs, they'll have to pay for eDiscovery and notification services as well.

At the end of the day, whether to pay or not to pay a ransom is a business decision for every company. By stealing sensitive data, ransomware groups automatically trigger additional mandatory expenses for their victims. This money will be going to companies that specialize in eDiscovery / breach notifications and not the ransomware groups. Even if victims of ransomware attacks have cyber insurance policies, a large portion of their coverage limits will be eaten away by those additional expenses, leaving less money on the table for potential ransom payments.

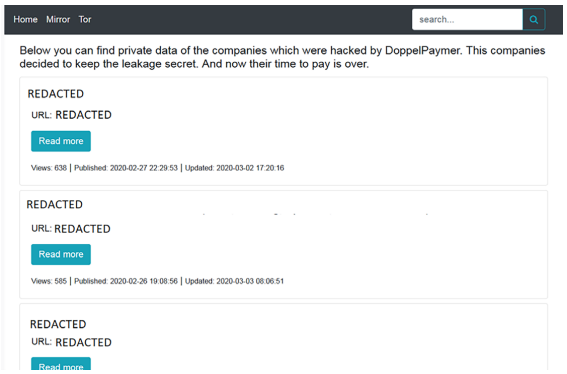
It might be a good time for ransomware groups to reconsider their strategy and climb back up on that bridge.

Some screen shots of sites where ransomware groups publish victims' data:

Maze



Dopplepaymer



Sodinokibi

Mespinoza