Double Extortion: An Emerging Ransomware Attack Pattern

Traditionally in Ransomware Attacks, cybercriminals deployed ransomware into the corporate network and encrypted all files and databases, locking the victims out of their own files. In order to get back to Business-as-usual, victims normally ended up paying attackers' ransom demand, hoping they would deliver the decryption keys. Had the victims refused to pay, their data and files would be destroyed.

As if that wasn't threatful enough, cybercriminals have come up with another tactic to inflict more pain on ransomware victims by adding an additional stage into their attacks – exfiltrating a copy of the data before encrypting and threatening the victim to publish it on their website or sell them to third parties, unless ransom demands are met. This evolution of ransomware attacks is referred as Double Extortion as it is a combination of a ransomware attack and a data breach.

Double Extortion, the most recent incarnation of ransomware attack, first emerged in late 2019 by the Maze Operators but has become quite prevalent in 2020. Researchers have found that many ransomware attack groups, such as Maze, REvil, DoppelPaymer etc., now boast of a dedicated website in which they list the names of non-cooperative victims and publish a sample of stolen data to put additional pressure on their victims. For instance, in the November 2019 attack against the Allied Universal, a large American security staffing company, the threat actors published 700 MB worth of stolen files including contracts, medical records (only 10% of the stolen information) when the company refused to pay 300 Bitcoin ($2.3 Million) ransom.

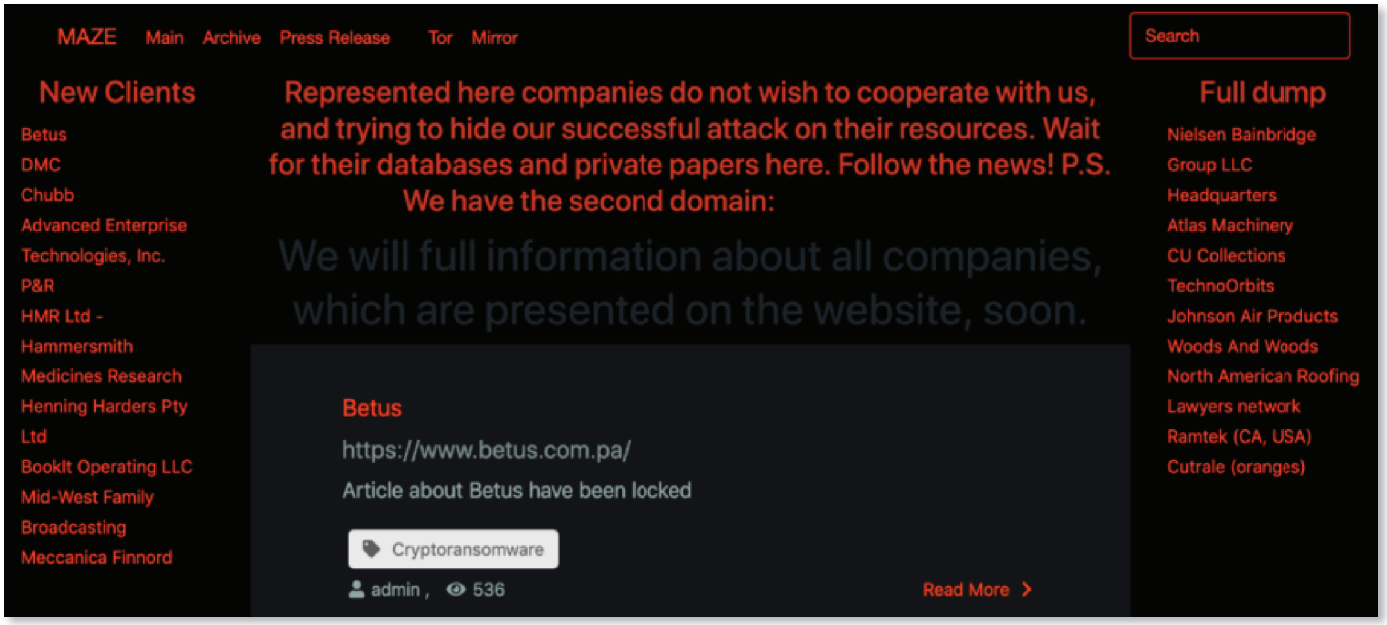


Fig1: Compromised data listed on Maze web page (Source: https://threatpost.com/double-extortion-ransomware-attacks-spike/154818/)

Trends observed in the year 2020

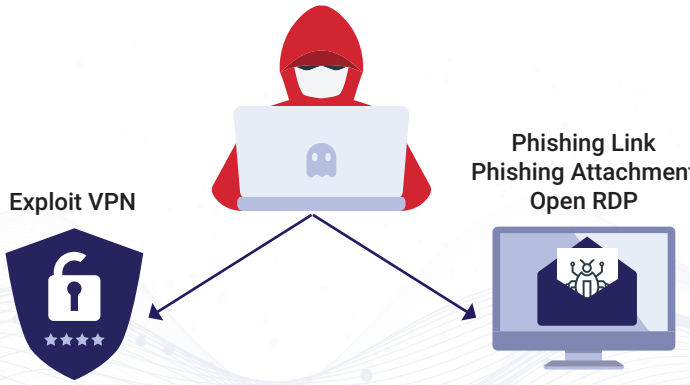
Cybercriminals from ransomware families haven't stopped to capitalize on the helplessness of various companies amidst the ongoing pandemic. Researchers issued cautions and urged various companies, especially in the healthcare sector, to be aware of the ransomware attacks as many cybercriminals would use the concerns surrounding the pandemic as bait to target high profile companies. But, amidst these concerns, the Maze Group pledged publicly that it wouldn't attack healthcare sector or medical institutions during the coronavirus outbreak by issuing this statement:

Fig2: Maze's statement issued on 18th March (Source: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus)

What shouldn't come as a surprise is that the promises made by the ransomware gangs were fake. Despite pledging publicly that they wouldn't attack in the midst of pandemic, cybercriminals continued with their campaigns, proving that they're interested only in money. On 14th March 2020, the IT team of Hammersmith Medicines Research, a London-based healthcare provider that was working with the British government to test COVID-19 vaccines, discovered a severe attack. After the company refused to pay a ransom, the Maze Group published personal details of thousands of former patients.[1]

Post this, researchers have seen an exponential increase in cyber-attacks with COVID19 themed phishing and malware campaigns. Attackers have been seen to target employees working from home by:

1. By exploiting known vulnerabilities such as open RDP and VPN connections.
2. By Phishing Campaigns (using Spear Phishing Attachments or URLs)



[1] https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

A closer look at the attack phases in COVID19 Campaigns

As is evident from the trends described above, cybercriminals continued to play cat-and-mouse with cyber sleuths and security experts during COVID19 with newer tactics. Understanding the need to stay proactive, Threat Intel Team at ColorTokens studied all the instances of Double extortion in 2020 and found these attack phases:

1. Infection - With the failure of automated detection controls, firewall, proxy, antivirus solutions and intrusion detection system allow the traffic. With the help of phishing document and URL, malware and ransomware are installed

2. Staging - To obtain the encryption key, primary C2 communications are made. At this point, various systems changes are made, and persistence is established. The attacker now "owns" the system

5. Pay Day – Ask victim to pay the amount before the given deadline

4. Exfiltration & Encryption - Exfiltration Local file encryption can occur in minutes; however, network file encryption can take many hours as data on network file shares are copied down and encrypted locally. Then, the encrypted files are uploaded, exfiltrated and the original files are deleted. This process takes a lot of time.

3. Scanning – Firstly, the malware scans the local computer to find files to encrypt. It also scans for data stored in the cloud, which is synced via folders and appears as local data. This can take seconds to minutes. Then, it looks for file shares. This can take hours depending on how many shares you have on your network. The goal is to investigate what data is available and determine which level of permissions the compromised user has (e.g., list, write, delete).

General measures to stay ahead of threat actors

With all the financial cost and reputational damage Double Extortion attacks entail, preventing them in the first place is better than mitigating their effects afterwards. Hence, we recommend these precautionary measures to stay ahead of evolving attack vectors:

Patch Management

Patch the Operating System and the Software your company uses, since cyber criminals seek for vulnerabilities to use in their advantage

Privileged Access Management

Based on the principle of Zero Trust and least privileges, a good account management can minimize the potential impact of a successful ransomware attack

Disable MS Office Macros

The modus operandi of the Maze group heavily relies on the execution of malicious documents sent through phishing e-mail. Thus, Macros and the editing mode should not be enabled by default

Browse Securely

Block ad pop-ups, avoid installing extensions and update your browser to avoid becoming the next victim of maze ransomware

Check for unusual behavior

Pay attention to alerts and any anomalies observed in user behavior

ColorTokens Solutions proactively stop Double Extortion attempts

Based on Zero Trust Architecture, ColorTokens' solutions – Xshield & Xprotect- defend organizations against the most sophisticated ransomware attacks. The various attacks phases and ColorTokens' approach to blocking them are described below:

Infection

Xshield detects amount of data infiltrated from the Phishing domain/ IP in Bytes which determines the malware, Ransomware or other payload downloads.

Xprotect detects and prevents bad reputed hash-based file and abnormal behavior-based process execution also helps in understanding the process chain which helps in understanding the anatomy of the threat

Staging

Xshield identify the C2 communication using inbuilt Threat Intelligence feature along with sent and received bytes information which helps in understanding commands sent and received

Xprotect identify and prevent persistence techniques such as unknown/malicious process creating tasks scheduler and other system file modifications using ring rules

Scanning

Xprotect detects and blocks usages of scanning related commands and processes based on Threat Intelligence information and process behavior

Xshield detects and show the Cloud Storage connections and scan related connections

Xshield identify the SMB, FTP or other file sharing related service communications across the network including the duration and the bytes transfer information

Exfiltration & encryption

Xprotect detects and prevent suspicious and malicious command execution using inbuilt ring rule features.

Xshield identify the data aggregation through the connections which includes bytes information, duration, service used and unauthorized connections based on Micro Segmentation.

Xshield identify the connections to file sharing, C&C, Online storage sites including the amount of data being sent.

LEARN MORE

Click to read more about our solutions

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com