Unmasking Ransomware Using Stylometric Analysis: Shadow, 8BASE, Rancoz

blog.bushidotoken.net/2023/05/unmasking-ransomware-using-stylometric.html

BushidoToken

I recently came across a cool GitHub repo from Zscaler's ThreatLabz team (see here) which contains a whole array of ransom notes from known and new ransomware families. I imagine that Zscaler has some sort of malware hunting capability (potentially LiveHunt YARA rules in VirusTotal) and they manually check for ransom notes uploaded to VT containing strings

such as ".onion" to find new and interesting ransomware families. However they actually do it, this is a handy repo for the community to use.

Three new ransom notes that Zscaler shared that caught my eye belonged to Shadow, 8BASE, and Rancoz. Tracking new ransomware families can be an interesting task because so many new groups are appearing, it is hard to tell which ones are worth paying attention to of the literal hundreds of variants out there launching attacks. These three stick out, however, due to the presence of the ".onion" Tor link inside their ransom notes though because that means they have setup custom infrastructure for advanced cyber extortion, such as negotiation portals, decryption sites, or a data leak site (DLS) to post stolen data if the victim refuses to pay.

Figure 1: An original Seinfeld meme

Cybercrime intelligence analysts who investigate new ransomware groups should know that it's important to make note when new groups appear and try to see if there are any connections to known threat actors. This helps with intelligence collection efforts and can help analysts decide whether investigating these groups should be a priority. There is only a limited amount of time and a limited amount of resources and, unfortunately, so so many ransomware groups. Using the ransom notes we can try to identify similarities to other known ransomware families.

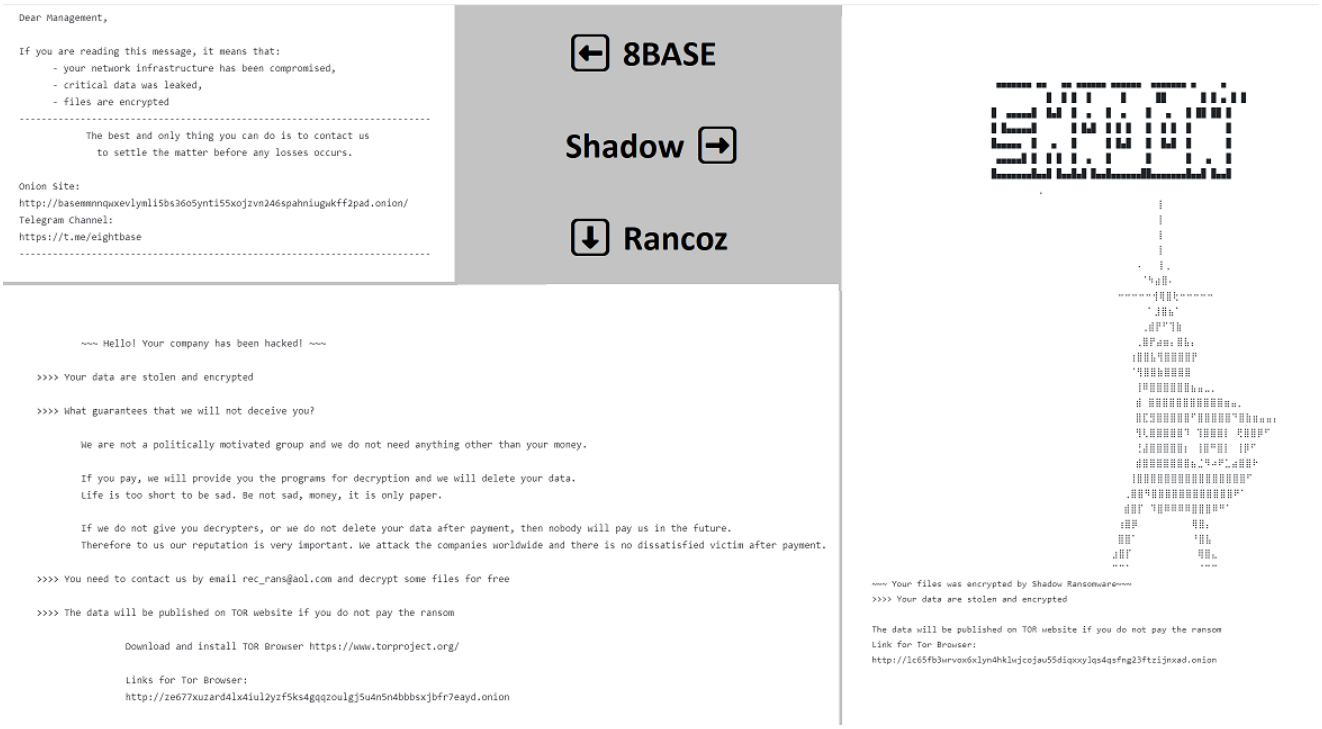

Figure 2: Ransom Notes

What is Stylometry and Stylometric Analysis?

Stylometry is the application of the study of linguistic style, usually to written language but it can also be applied to code and ransom notes. It has also been applied successfully to music, paintings, and chess. We can evaluate an author's style through manual comparisons as well as the application of statistical analysis to a body of their work. Stylometry is often used to attribute authorship to anonymous or disputed documents. To unmask these ransomware group for who they really are, I used a mixture of the text comparison site copyleaks.com and by doing it manually.

Shadow

Analysis of Shadow's ransom note, although with some original elements, there are numerous similarities between it an LockBit3.0's ransom note. We can say with fairly strong accuracy that this is a reskin of the leaked LockBit3.0 (aka LockBitBlack) builder. There are multiple similarities in the notes that tie these two together. The wide availability of the leaked builder also makes this overlap a very likely scenario. The Shadow ransom note is available

in Zscaler's GitHub repo (see here). The LockBit3.0 ransom note is available from PCRisk (see here).

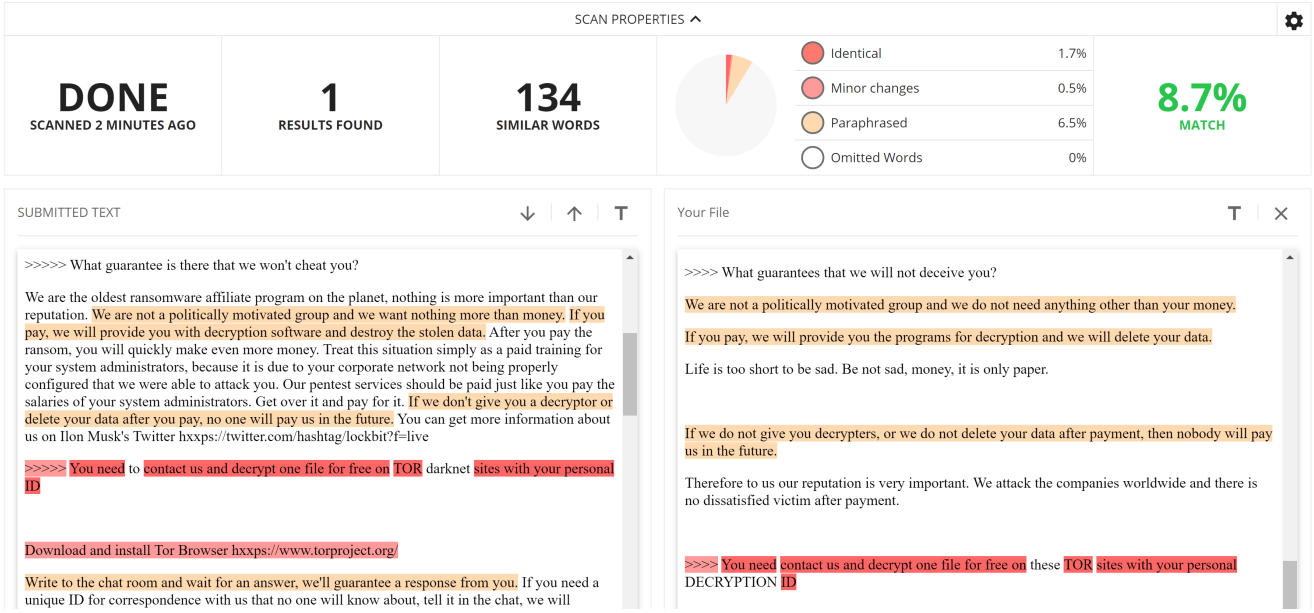

Figure 3: Comparison between Shadow and LockBit3.0 ransom notes

8BASE

When I examined the 8BASE ransom note it also looked familiar. It turned out that it share a ton of similarities to a ransom note from the leaked builder of Babuk ransomware. Again, due to the availability of the Babuk ransomware builder and numerous ransomware groups that use it, this is also a likely scenario. The 8BASE ransom note is available in Zscaler's GitHub repo (see here). The ransom note of the DarkAngel's variant of Babuk ESXi is available from PCRisk (see here).

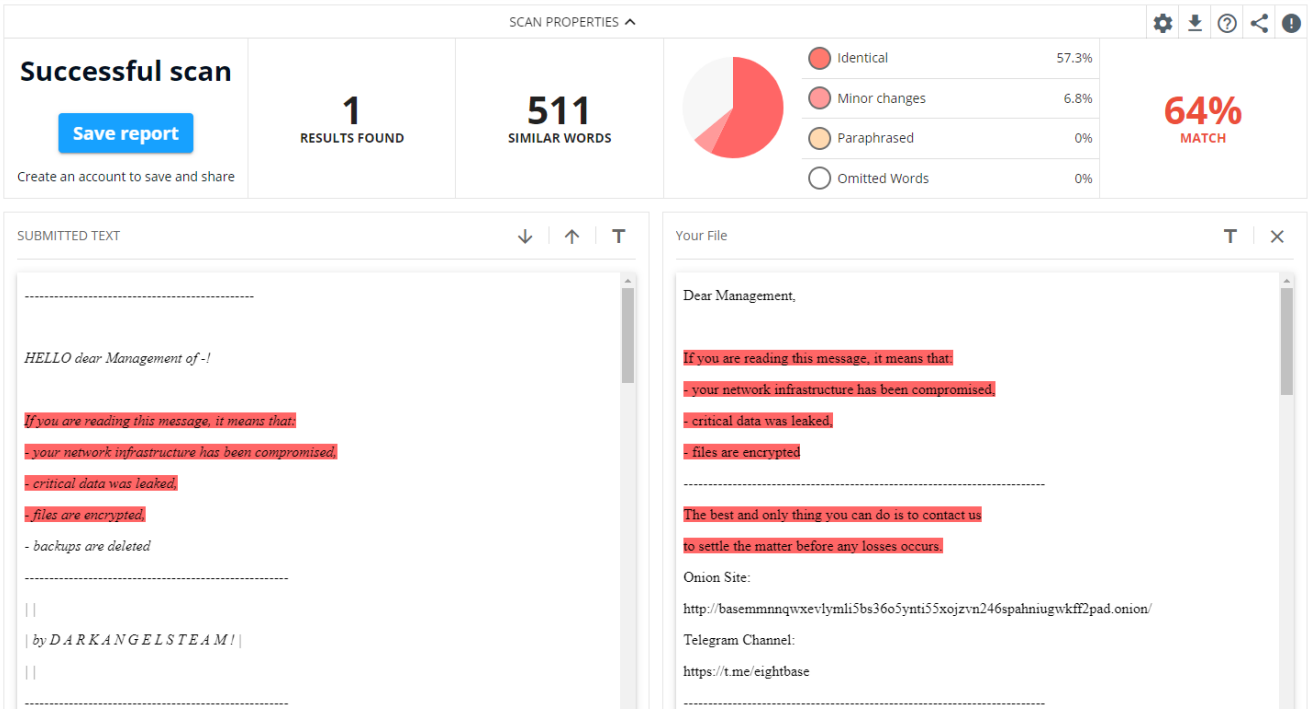

Figure 4: Comparison of 8BASE and Babuk ESXi ransom notes

Rancoz

Rancoz seemed to be a little bit more interesting as Cyble analyzed Rancoz (see here) and shared some technical insights. Twitter researcher @F_kZ_ also highlighted the similarities between the Rancoz and 0mega data leak sites (see here). However, neither mentioned that the ransom note is practically identical to the LockBit3.0 note. The Rancoz ransom note is available in Zscaler GitHub repo (see here)

Figure 5: Comparison of Rancoz and LockBit 3.0 ransom notes

Conclusion

Ransomware research is pretty straight forward these days. These types of cybercriminals prefer templated attacks, reusing tried and trust TTPs. Now, they do not even need to code their own ransomware or partner with RaaS groups. There are multiple freely available leaked builders ready for them to use instantly.

LockBit and Babuk provide low skilled and few resourced the immediate ability to attack and ransom large organizations. There have already been dozens of variants of these two families. Shadow, 8BASE, and Rancoz are also not likely to be the last.

My advice is to keep an eye on these threat actors as eventually they may begin to retool and evolve. While they are still inexperienced is the best time to try and track them down. Any tips you have to do that are best sent to law enforcement, as well as groups like The Ransomware Task Force and NoMoreRansom.

Detecting and Fingerprinting Infostealer Malware-as-a-Service platforms

Brute Ratel cracked and shared across the Cybercriminal Underground

The Continuity of Conti