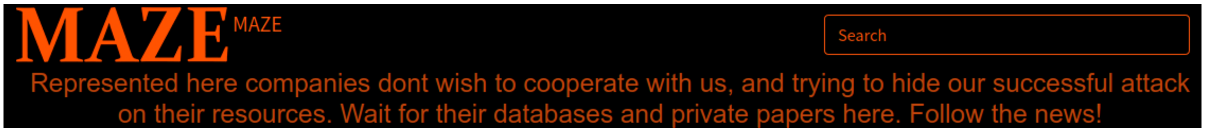
Ransomware Gangs Now Outing Victim Businesses That Don’t Pay Up

krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

As if the scourge of ransomware wasn’t bad enough already: Several prominent purveyors of ransomware have signaled they plan to start publishing data stolen from victims who refuse to pay up. To make matters worse, one ransomware gang has now created a public Web site identifying recent victim companies that have chosen to rebuild their operations instead of quietly acquiescing to their tormentors.



Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!

The message displayed at the top of the Maze Ransomware public shaming site.

Less than 48 hours ago, the cybercriminals behind the Maze Ransomware strain erected a Web site on the public Internet, and it currently lists the company names and corresponding Web sites for eight victims of their malware that have declined to pay a ransom demand.

“Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources,” the site explains in broken English. “Wait for their databases and private papers here. Follow the news!”

KrebsOnSecurity was able to verify that at least one of the companies listed on the site indeed recently suffered from a Maze ransomware infestation that has not yet been reported in the news media.

The information disclosed for each Maze victim includes the initial date of infection, several stolen Microsoft Office, text and PDF files, the total volume of files allegedly exfiltrated from victims (measured in Gigabytes), as well as the IP addresses and machine names of the servers infected by Maze.

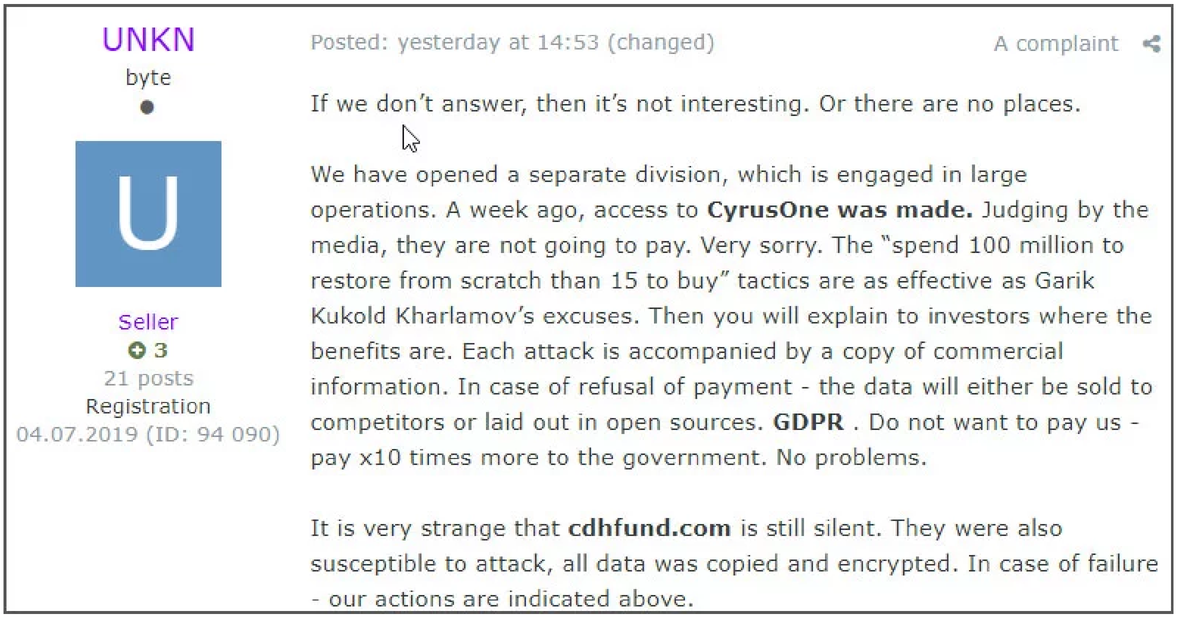
As shocking as this new development may be to some, it’s not like the bad guys haven’t warned us this was coming.

“For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data would be publicly released,” said **Lawrence Abrams**, founder of the computer security blog and victim assistance site BleepingComputer.com. “While it has been a well-known secret that ransomware actors snoop through victim’s data, and in many cases steal it before the data is encrypted, they never actually carried out their threats of releasing it.”

Abrams said that changed at the end of last month, when the crooks behind Maze Ransomware threatened Allied Universal that if they did not pay the ransom, they would release their files. When they did not receive a payment, they released 700MB worth of data on a hacking forum.

“Ransomware attacks are now data breaches,” Abrams said. “During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company’s files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out. Now that ransomware operators are releasing victim’s data, this will need to change and companies will have to treat these attacks like data breaches.”

The move by Maze Ransomware comes just days after the cybercriminals responsible for managing the “Sodinokibi/rEvil” ransomware empire posted on a popular dark Web forum that they also plan to start using stolen files and data as public leverage to get victims to pay ransoms.



UNKN
byte

Seller
3
21 posts
Registration
04.07.2019 (ID: 94 090)

Posted: yesterday at 14:53 (changed)

If we don’t answer, then it’s not interesting. Or there are no places.

We have opened a separate division, which is engaged in large operations. A week ago, access to **CyrusOne was made.** Judging by the media, they are not going to pay. Very sorry. The "spend 100 million to restore from scratch than 15 to buy" tactics are as effective as Garik Kukold Kharlamov’s excuses. Then you will explain to investors where the benefits are. Each attack is accompanied by a copy of commercial information. In case of refusal of payment - the data will either be sold to competitors or laid out in open sources. **GDPR** . Do not want to pay us - pay x10 times more to the government. No problems.

It is very strange that **cdhfund.com** is still silent. They were also susceptible to attack, all data was copied and encrypted. In case of failure - our actions are indicated above.

Forum post by REvil operator

The leader of the Sodinokibi/rEvil ransomware gang promising to name and shame victims publicly in a recent cybercrime forum post. Image: BleepingComputer.

This is especially ghastly news for companies that may already face steep fines and other penalties for failing to report breaches and safeguard their customers’ data. For example, healthcare providers are required to report ransomware incidents to the U.S. Department of Health and Human Services, which often documents breaches involving lost or stolen healthcare data on its own site.

While these victims may be able to avoid reporting ransomware incidents if they can show forensic evidence demonstrating that patient data was never taken or accessed, sites like the one that Maze Ransomware has now erected could soon dramatically complicate these incidents.