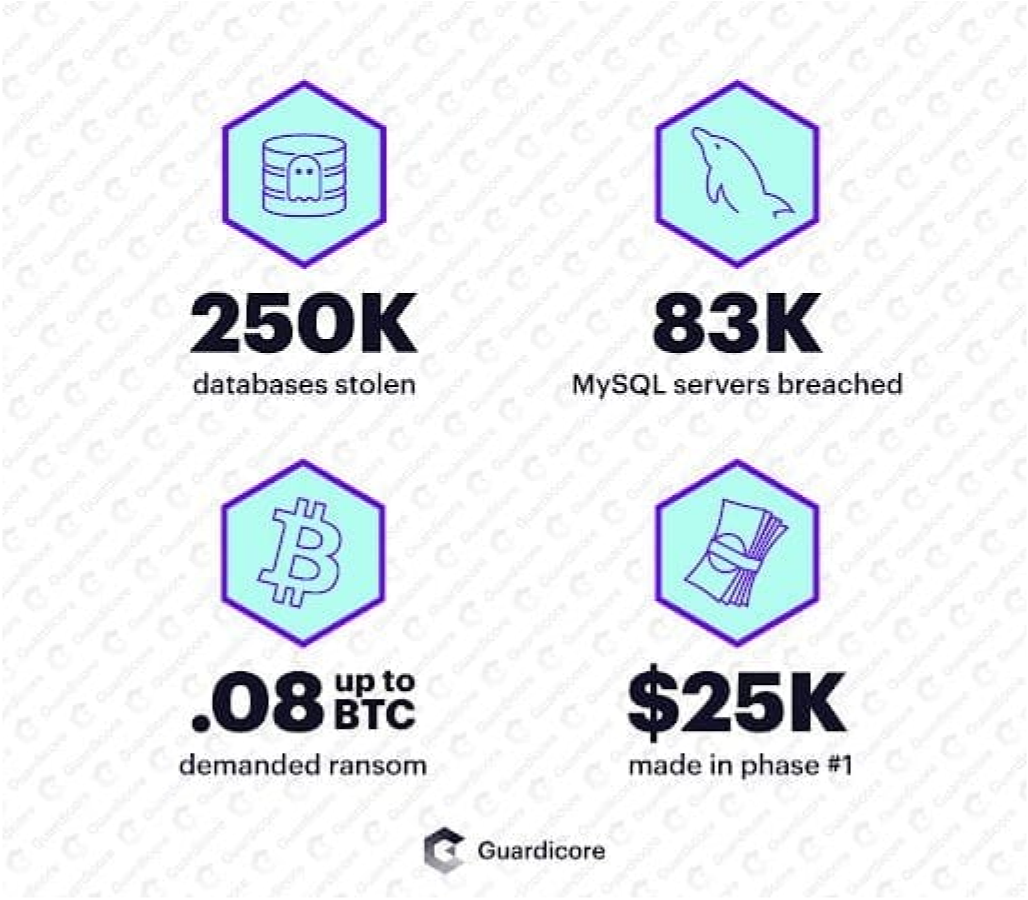
PLEASE_READ_ME: The Opportunistic Ransomware Devastating MySQL Servers

guardicore.com/labs/please-read-me-opportunistic-ransomware-devastating-mysql-servers/

By Ophir Harpaz

Executive Summary

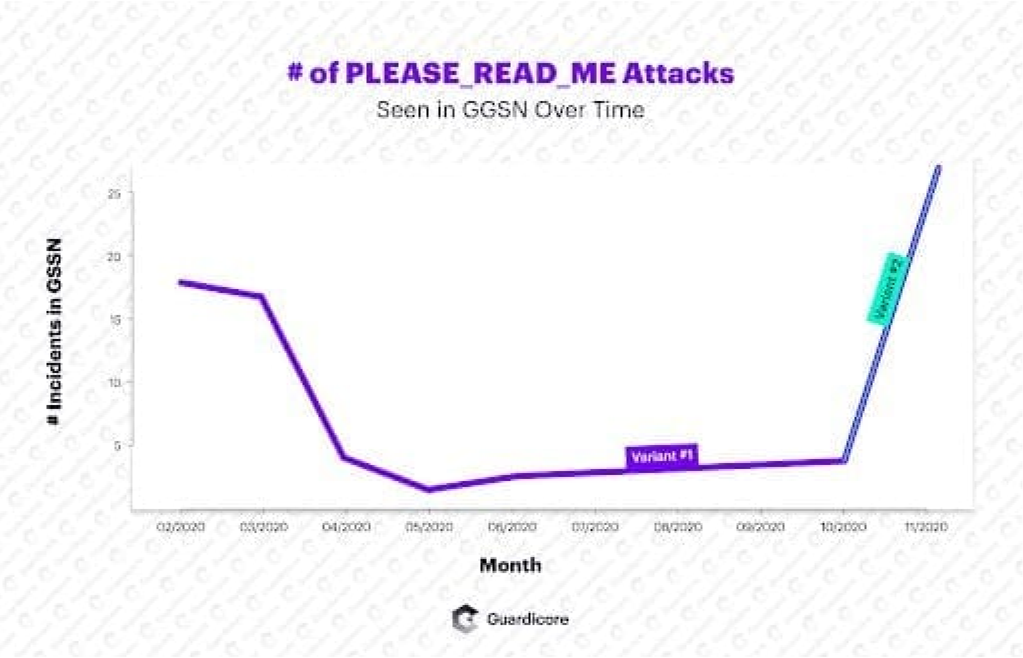
- PLEASE_READ_ME is an active ransomware campaign targeting MySQL database servers and dates back to at least as early as January 2020.
- The attack chain is extremely simple and exploits weak credentials on internet-facing MySQL servers. There are close to 5M internet-facing MySQL servers worldwide.
- The attackers leave a backdoor user on the database for persistence, allowing them to re-access the network.
  Guardicore Labs have witnessed two variants of the campaign, detailed in this post.
- 250,000 databases are offered for sale in the attackers' dashboard, from 83,000 successfully-breached victims.
- Monetization of the campaign has evolved into a double extortion attempt – publishing and offering data for sale to pressure victims into paying ransom.
- Indicators of Compromise are available at Guardicore Labs campaigns repository.



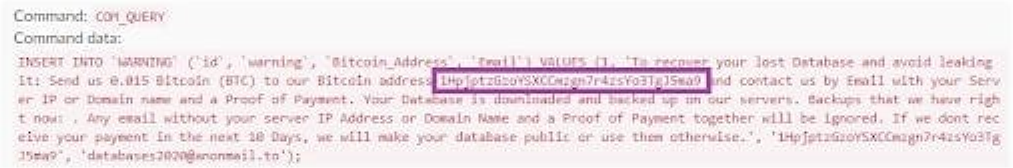
Ready to protect your data center against ransomware and other active threats? Find out how to get started.

An Evolving Ransomware Campaign

The first attack on Guardicore Global Sensors Network (GGSN) was captured on January 24, 2020. Since then, a total of 92 attacks have been reported by our sensors, showing a sharp rise in their number since October. The attacks originate from 11 different IP addresses, most of which are from Ireland and the UK. What drove us to closely monitor this threat is its use of double extortion, where stolen data is published and offered for sale as a means to pressure victims into paying the ransom.



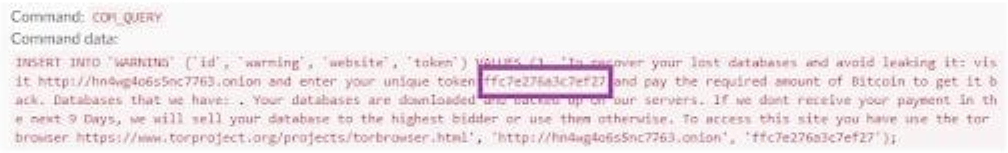
Guardicore Labs observed two different variants during the lifetime of this campaign. In the first, which lasted from January till the end of November, the attackers left a ransom note with their wallet address, the amount of Bitcoin to pay and an email address for technical support. 10 days were given for victims to perform payment. Since Bitcoin wallets were specified explicitly in ransom notes, we could explore the wallets and the amount of BTC transferred to each of them. We found that a total of 1.2867640900000001 BTC had been transferred to these wallets, equivalent to 24,906 USD. Guardicore Sensors captured 63 attacks of this type, coming from 4 different IP addresses.



```
Command: COM_QUERY
Command data:
INSERT INTO `WARNING` (`id`, `warning`, `Bitcoin_Address`, `Email`) VALUES (1, 'To recover your lost Database and avoid leaking
It: Send us 0.015 Bitcoin (BTC) to our Bitcoin address 1HpJptzGzoYSXCCmzgn7r4zsYo3TgJ5ma9 and contact us by Email with your Serv
er IP or Domain name and a Proof of Payment. Your Database is downloaded and backed up on our servers. Backups that we have righ
t now: . Any email without your server IP Address or Domain Name and a Proof of Payment together will be ignored. If we dont rec
eive your payment in the next 10 Days, we will make your database public or use them otherwise.', '1HpJptzGzoYSXCCmzgn7r4zsYo3Tg
J5ma9', 'databases2020@anonmail.to');
```

The second phase started on October 3rd and lasted till the end of November, and marked an evolution of the campaign. Payment is no longer done directly to a Bitcoin wallet, and no email communications are needed. Instead, the attackers put up a website in the TOR network where payment can be made. Victims are identified using unique alphanumeric tokens they receive in the ransom note.

The website is a good example of a double extortion mechanism – it contains all leaked databases for which ransom was not paid. The website lists 250k different databases from 83k MySQL servers, with 7TB of stolen data. Up till now, GGSN captured 29 incidents of this variant, originating from 7 different IP addresses.



```
Command: COM_QUERY
Command data:
INSERT INTO `WARNING` (`id`, `warning`, `website`, `token`) VALUES (1, 'To recover your lost databases and avoid leaking it: vis
it http://hn4wg4o6s5nc7763.onion and enter your unique token ffc7e276a3c7ef27 and pay the required amount of Bitcoin to get it b
ack. Databases that we have: . Your databases are downloaded and backed up on our servers. If we dont receive your payment in th
e next 9 Days, we will sell your database to the highest bidder or use them otherwise. To access this site you have use the tor
browser https://www.torproject.org/projects/torbrowser.html', 'http://hn4wg4o6s5nc7763.onion', 'ffc7e276a3c7ef27');
```

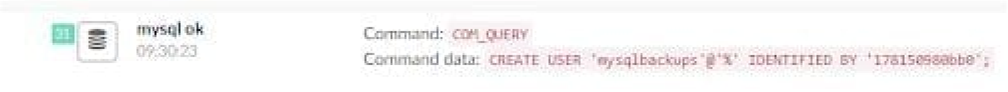
This phase marks an evolution of the campaign in several ways.

- First, the mapping between a victim and their stolen database is now done automatically, with a unique token, and does not involve searching through IPs and domains to find the stolen database.
- In addition, the “repository” of all stolen databases is managed in one place and is public – victims can see their databases on the list and be pressured into paying the ransom.
- Last, the website creates a smoother experience for the victim and even builds more trust between the victim and the attackers, as the details of the database are provided.

Attack Chain

The attack starts with a password brute-force on the MySQL service. Once successful, the attacker runs a sequence of queries in the database, gathering data on existing tables and users. By the end of execution, the victim’s data is gone – it’s archived in a zipped file which is sent to the attackers’ servers and then deleted from the database. A ransom note is left in a table named WARNING, demanding a ransom payment of up to 0.08 BTC.

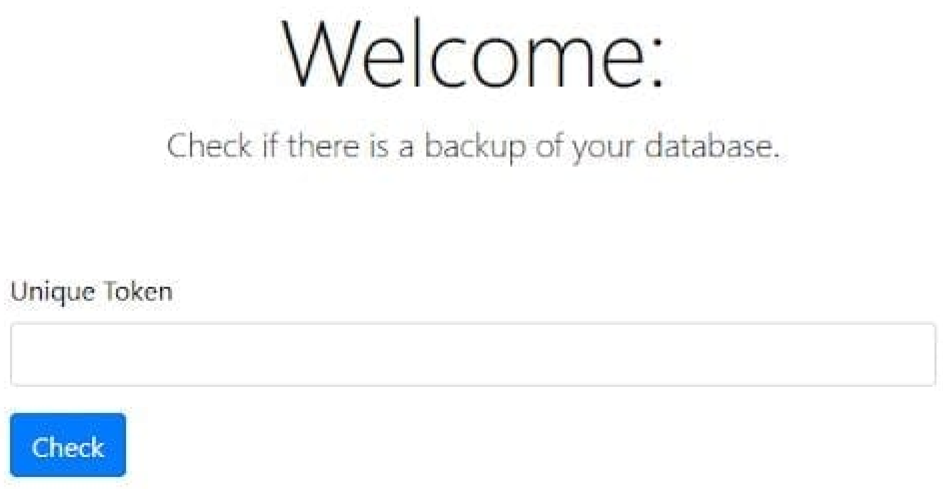
INSERT INTO `WARNING` (`id`, `warning`, `website`, `token`) VALUES (1, ‘To recover your lost databases and avoid leaking it: visit https://hn4wg4o6s5nc7763.onion and enter your unique token ffc7e276a3c7ef27 and pay the required amount of Bitcoin to get it back. Databases that we have: . Your databases are downloaded and backed up on our servers. If we don’t receive your payment in the next 9 Days, we will sell your database to the highest bidder or use them otherwise. To access this site you have use the tor browser https://www.torproject.org/projects/torbrowser.html’, ‘https://hn4wg4o6s5nc7763.onion’, ‘ffc7e276a3c7ef27’);
Additionally, a backdoor user mysqlbackups’@’%’ is added to the database for persistence, providing the attackers with future access to the compromised server.



```
mysql ok        Command: COM_QUERY
09:30:23        Command data: CREATE USER 'mysqlbackups'@'%' IDENTIFIED BY '1781509800bb0';
```

Leak Site Offers Databases for Purchase

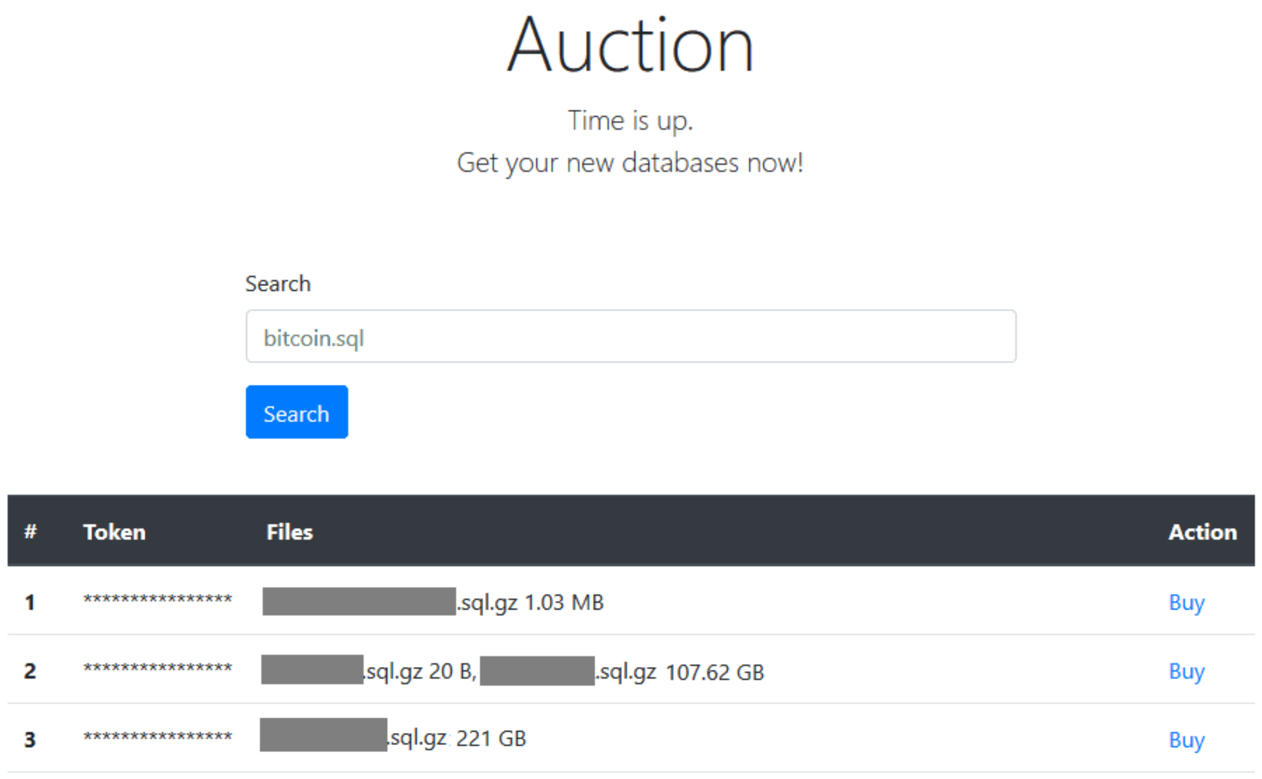
The .onion domain – hn4wg4o6s5nc7763.onion – leads to a full-fledged dashboard where victims can provide their token and make the payment. The .onion top-level domain is used to distinguish services hosted in the TOR network. Such websites can only be accessed from the TOR browser, and guarantee that both their operators and the client-side users remain anonymous. Choosing to use an .onion domain makes it harder to trace the attackers and where their infrastructure is hosted.



Welcome:

Check if there is a backup of your database.

All stolen databases are offered for sale in a section in the website titled Auction, all having a uniform price of 0.03 Bitcoin. A table on this page lists all stolen databases per token, along with their sizes. By crawling the auction pages, Guardicore Labs found nearly 83k unique tokens. Restoring data will cost a victim 0.03 BTC, which equals (at the time of writing) around $520.



Auction

Time is up.
Get your new databases now!

Search: bitcoin.sql

#	Token	Files	Action
1	****************	[redacted].sql.gz 1.03 MB	Buy
2	****************	[redacted].sql.gz 20 B, [redacted].sql.gz 107.62 GB	Buy
3	****************	[redacted].sql.gz 221 GB	Buy

Ransomware Attacks Come in Different Forms

Some ransomware campaigns are highly targeted; they are planned ahead for months and are executed flawlessly. Those campaigns are advanced, persistent threats (APTs). They breach the network, perform silent and careful lateral movement to infect multiple assets, encrypt valuable data and demand ransom for restoration.

Others campaigns are opportunistic in nature. These campaigns are usually automatic, meaning they are executed from a script rather than by a human being. Intelligence gathering or reconnaissance are not part of the process. This characteristic allows such campaigns to scale significantly and potentially infect important servers that are mistakenly connected to the internet.

Attack campaigns of this sort are untargeted. They have no interest in the victim's identity or size, and result in a much larger scale than that available for targeted attacks. Think of it as "Factory Ransomware" – the attackers run the attack, making less money per victim but factoring the number of infected machines.

PLEASE_READ_ME is a great example of the latter type:

1. It is untargeted: it attempts to infect any of the 5 million MySQL servers which are internet-facing.
2. It is transient – it does not spend time in the network besides that required for the actual attack. With no lateral movement involved, the attack begins and ends inside the MySQL database itself and does not try to escape it.
3. It is simple. There are no binary payloads involved in the attack chain, making the attack "malwareless". Only a simple script which breaks in the database, steals information and leaves a message.

The PLEASE_READ_ME operators are trying to up their game by using double extortion in scale. Factoring their operation will render the campaign more scalable and profitable. Guardicore Labs provides an IOCs repository and will keep monitoring this campaign to help organizations protect against it.

Ready to protect your data center against ransomware and other active threats? Find out how to get started.

Experienced a Breach? Contact Us:
Email: labs@guardicore.com
Call:
US: +1 415-200-1993
UK: +44 118 310 0896