ASEC (AhnLab Security Emergency-response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.’s homepage (www.ahnlab.com).

Contents

Malware Statistics in Q3 2022
InfoStealer Takes Up the Largest Portion of Malware in Q3 at 55.1% 03

Statistics on Malware Targeting MS-SQL Servers in Q3 2022
Which Malware Most Frequently Attacked MS-SQL Servers in Q3? 11
ASEC analysis team leverages the automatic analysis system called “RAPIT” to categorize, analyze and respond to malware collected from various environments. The first part of the report will categorize and provide statistics on known malware collected during Q3 2022. As a note, a group of malware in the statistics are executable files.

In general, attackers distribute malware via spam mail or web browsers, and they seek to weaponize vulnerabilities for a victorious campaign. Our collected malware was either reported by our customers or detected while performing malicious behaviors in the environment where AhnLab products were deployed.

Known malware refer to the ones sold by developers or designed with cracked builders, and they have been steadily distributed over the years. Some operators develop and deliver malware themselves, mostly banking malware.

The report categorizes malware by types, such as ransomware or backdoor, and provides detailed statistics on each one of them. In addition, it examines the distribution method and notable features.

**Malware Statistics in Q3 2022**

According to our analysis on malware collected in Q3 2022, InfoStealer(55.1%) marked the highest rate followed by Downloader(22.6%), Backdoor(16.4%), Ransomware(4.7%), Banking malware(0.8%), and CoinMiner(0.4%).
InfoStealer literally steals the victim’s assets such as crypto wallet address, file, or account information saved in programs like web browsers or email clients. Backdoor, which comes with RAT (Remote Administration Tool), installs other forms of malware and launches malicious actions such as keylogging or taking screenshots by receiving a command from the operator.

Banking malware also pilfers user information as InfoStealer does. However, it can further collect information such as online banking account credentials by using the technique called “form grabbing” which hijacks the data entered by the user in web browsers.

As for the Downloader, its ultimate objective is to install additional malware. Ransomware is already well known for encrypting files to achieve financial gain, and CoinMiner surreptitiously carries out crypto mining and consumes the victim’s computational power.

**Malware Details by Type in Q3 2022**
The following is detailed information on a group of malware collected in Q3 2022.

1. **InfoStealer**
AgentTesla, Formbook, and Lokibot mostly make up InfoStealer, which accounts for the largest portion out of all malware types. AgentTesla is usually distributed as spam mail
attachments, and it steals account credentials saved in web browsers, emails, and FTP clients.

Formbook, Lokibot, and SnakeKeylogger are also prominent information-stealing malware spread via spam mail. Unlike others prevalent for years, SnakeKeylogger was first identified in 2021 and has been dominant so far. Alike AgentTesla, SnakeKeylogger mainly uses SMTP when stealing information, but also supports HTTP and FTP. RedLine is a common malware disguised as commercial software cracks. It carries out malicious behaviors by receiving commands from the attacker, and like other InfoStealers, it is also equipped with features to steal the victim's information.

In addition, there are ColdStealer, Vidar, and Cryptbot distributed via malicious websites disguised as download pages for cracks and keygens of commercial software. First spotted in 2022, ColdStealer has constantly been prevalent until these days. Vidar is also the one preferred by attackers for years. The Vidar developer is continuously adding features along with the version updates, and the malware now abuses the gaming platform to obtain the C2 server address.
2. Downloader

The most infamous malware among downloaders, GuLoader downloads and executes additional malware. While it was packed with Visual Basic language to evade detection, it is now delivered as an NSIS installer. Once known as CloudEye, the malware is now called GuLoader for using Google Drive in its download address. For reference, the malware also uses other URLs including Microsoft One Drive.

BeamWinHTTP is spread via malware masquerading as a PUP installer. Once executed, it installs Garbage Cleaner (PUP malware) and downloads other malware such as InfoStealer. SmokeLoader is delivered via malicious websites disguised as download pages for commercial software cracks or keygens. Upon the operator’s configuration, it deploys other malware like Stop Ransomware or modules to steal user credentials.

3. Backdoor

First off, Backdoor contains the RAT (Remote Administration Tool) malware. Remcos, the most popular one among its peers, is a commercial RAT adored by threat actors, and it is usually distributed as spam mail attachments. It has recently been utilized with Cobalt Strike in malicious campaigns targeting vulnerable MS-SQL servers.
Another RAT malware, NanoCore also propagates itself via spam mail. It has been beloved by threat actors for almost ten years ever since the crack version of the builder was released. This is the same story for AveMaria which has been continuously updated by the developer just like Remcos.

njRAT is a well-known RAT malware disguised as adult games or illegal crack programs on Torrent. Despite losing its popularity, threat actors continuously look for njRAT as it is easy to design with publicly available builders. AsyncRAT is also an easy-to-get RAT malware published on GitHub and is widely used in malicious campaigns.

![Figure 4. Backdoor statistics by type](image)

4. Ransomware

For ransomware distributed as executables, Stop Ransomware, deployed by other malware such as SmokeLoader, has been prevalent. Unlike other typical ransomware, Stop Ransomware conducts encryption after installing information-stealing malware like Vidar.
and gathering user information.

In Korea, the LockBit Ransomware has been distributed as spam mail attachments by disguising them as job applications; it has recently been updated to v3.0. The attachments utilize fake icons and names luring unsuspected victims into execution. Mallox and GlobeImposter are prominent ransomware that aim at vulnerable MS-SQL servers with weak credentials.

![Figure 5. Ransomware statistics by type](image)

5. Banking Malware

Emotet is one of the most well-known banking malware. It momentarily disappeared due to international law enforcement action, but it had become active again last year. However, its distribution rate is dwindling again in recent days.

Emotet is usually installed with malicious Excel files attached to spam mail, and these files contain the image prompting users to enable macro by clicking the 'Enable Content' button. Afterward, it deploys other malicious programs via infostealing and banking-related modules or steals user credentials.
Qakbot is also a prominent banking malware which shares a similar distribution method with Emotet. It is worth noting that Qakbot recently propagates itself via the ISO attachment in spam mail instead of an Excel file.

Lastly, IntelRapid is a typical ClipBanker malware that modifies the crypto wallet address to a malicious address when it is copied by the victim. It is usually installed by other malware like CryptBot.

![Figure 6. Banking malware statistics by type](image)

6. CoinMiner

A representative CoinMiner, Glupteba was thriving for years, but it has been experiencing a rapid decline since 1Q 2022 as Google, in cooperation with the hosting company, prevented the botnet infrastructure. Glupteba lures victims into installing fake cracks or keygens of commercial software downloaded from malicious web pages. Then, it launches malicious behaviors like information theft and ultimately mines Monero with impairing the victim’s system performance.

Vollgar is a CoinMiner targeting MS-SQL servers with vulnerable account credential settings.
In summary, most malware covered in the Q3 2022 statistics are distributed via either spam mail attachments or malicious web pages, luring victims into downloading cracks or keygens for commercial software. Threat actors also breach environments, particularly MS-SQL servers, with vulnerable settings.

Here are key takeaways. First, users should not execute the attachment from suspicious emails or download files from file-sharing websites; we always recommend downloading the file or using the content from authorized websites.

Administrators must make their passwords unguessable and change them regularly to protect database servers from malicious campaigns. Plus, keep V3 and other software up-to-date to reduce vulnerabilities and prevent malware.
AhnLab has been leveraging our “ASD(AhnLab Smart Defense)” infrastructure to categorize, analyze and respond to attacks targeting vulnerable MS-SQL servers. Based on the logs collected in Q3 2022, the second part of the report will examine the current state of damage to MS-SQL servers as well as related statistics. The malware will be categorized by types such as CoinMiner, Backdoor, Trojan, and Ransomware. Then, there will be detailed statistics provided for known malware.

Attacks Against MS-SQL Servers

Figure 1 below visualizes the frequency of MS-SQL server attacks that we have identified from Q1 to Q3 2022.
The "State of Damage" in Figure 1 indicates the number of systems breached by attackers. These systems have a record of malware installation after attackers got control of the servers. Threat actors are likely to compromise vulnerable servers that are not updated, configured, and managed properly. If they achieve access to the system with an administrator account, it becomes easy for them to get control of these servers.

The "Number of Attacks" basically shows how many times the operators attacked the servers. These vulnerable MS-SQL servers are generally breached by multiple attackers and malware, which means that infection logs can be overlapped.

**Categorization of Malware Used in Attacks Against MS-SQL Servers**

We categorized malware used in attacks against MS-SQL servers in Figure 2.

![Figure 2. Statistics on malware used in attacks against MS-SQL servers by type](image)

As seen in Figure 2, there were various types of malware aiming at MS-SQL servers. Let's take a closer look at each one of them.
1. Backdoor

We categorized malware that launches malicious behaviors by receiving a command from C2 as Backdoor. Most of them were RAT malware such as Remcos RAT or Gh0st RAT while we found some others like CobaltStrike or Meterpreter, originally intended for a penetration test. Recently, threat actors often install normal remote-control applications like AnyDesk instead of malware.

Remcos RAT is the most frequently detected one not just as a Backdoor but as a malware. It is usually installed by means of spam mail but recent cases reveal that it is also found in MS-SQL servers. It runs PowerShell commands during the installation process. Despite large numbers of cases, the malware seems to be utilized by the same operator.

Gh0st RAT is a remote access tool employed by multiple threat actors. Its source code is public, so there are multiple variants targeting vulnerable MS-SQL servers. For example, there was a variant called “Gh0stCrince” spotted attacking MS-SQL servers.

CobaltStrike and Meterpreter are commercial penetration test tools, often used as a
medium to take control of the internal system. When operators attack vulnerable MS-SQL servers, they deploy CobaltStrike for initial access while they tend to use malware in other cases.

2. CoinMiner

![Figure 4. Statistics on CoinMiner by type](image)

Vollgar, PurpleFox, LoveMiner, and MyKings are four prominent CoinMiners. They share the objective to mine Monero and tend to be distributed to systems with account credential flaws.

As for LoveMiner, it is deployed in MS-SQL server in form of CLR assemblies by executables or downloader malware. Unlike LoveMiner without any feature other than mining, others have their own characteristics. For instance, MyKings or PurpleFox can compromise systems by additionally installing a scanning module after the initial infection. When the malware propagates itself, it targets not only vulnerable MS-SQL servers but also unpatched systems by exploiting SMB vulnerabilities.
3. Trojan

CLR assembly shell malware accounts for most of the Trojans. In terms of compromising MS-SQL servers, there are various methods to execute OS commands besides the `xp_cmdshell` command, and one of them is using CLR assemblies. It was originally designed to provide extended features on SQL servers, but threat actors began abusing it by adding malicious features. CLR assembly type of downloader is also utilized by LoveMiner.

CLR Shell launches malicious behaviors by receiving commands from threat actors; it is similar to web shells of a web server. In order to install additional modules, LemonDuck directly runs the `xp_cmdshell` command or deploys CLR Shell to leverage its command.

There are different types of malware categorized as Trojan, and the major type is the one adding the user account on the affected system before activating RDP to enable future access. There are also multiple proxyware-type malware providing internet bandwidth, installed in targeted systems.

AhnLab has previously published an analysis report on the activities of ShadowForce
which have been detected since 2013. ShadowForce is still active, and the attackers target and infiltrate vulnerable MS-SQL servers to install not only Backdoor or reverse shell but a variety of malware, including privilege escalation tools.

4. HackTool
Attackers employ a variety of tools to achieve further objectives even after gaining control over the affected system. For example, there are privilege escalation or proxy tools. According to our ASD logs, Sweet Potato and Juicy Potato are the most popular tools while there are some others exploiting privilege escalation vulnerabilities.

5. Ransomware

![Figure 6. Sweet Potato malware](image)

![Figure 7. Statistics on ransomware by type](image)
Currently, there are two types of ransomware spotted targeting vulnerable MS-SQL: Mallox and GlobeImposter. Mallox has been detected since 2021, and it is likely that the attackers only target vulnerable MS-SQL servers as no other cases have been reported.

On the other hand, the variants of GlobeImposter have been constantly identified since February 2017 along with several attack cases. There was a case that its sibling was distributed via spam mail in September 2017. Lockis Ransomware, one of its variants, was also spotted recently.

Downloader is currently unidentified, but it is likely to have downloaded Remcos RAT or CobaltStrike. In April 2022, the RedLine InfoStealer malware was downloaded aside from Remcos RAT and CobaltStrike.

Downloader malware is developed with .NET, and they download packed binaries from an external environment and execute them in memory.

In terms of techniques, brute force and dictionary attack are commonly used to compromise MS-SQL database servers with weak account credentials. Furthermore, threat actors can always employ various methods to compromise unpatched systems.

Here are key takeaways. Administrators should make the passwords unguessable and
change them regularly to protect database servers from malicious campaigns. The server should always be up-to-date to be secured from vulnerability exploitation. Also, all access to public-facing database servers should be under control by using a security product such as a firewall.