

MSSQL, meet Maggie

By DCSO CyTec Blog

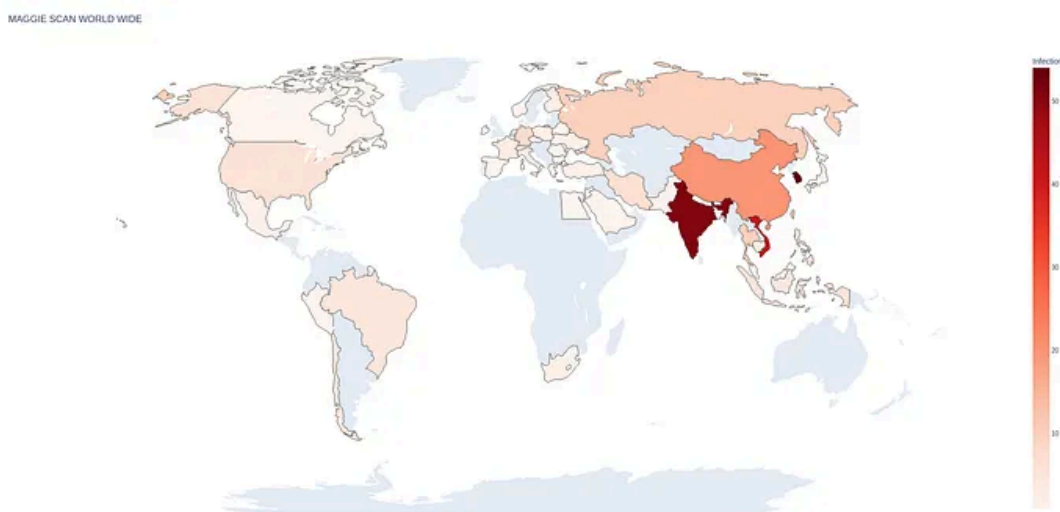
Published: 2022-11-08 · Archived: 2026-04-05 21:52:09 UTC



6 min read

Oct 4, 2022

Press enter or click to view image in full size



Heatmap of Maggie backdoor user by country

Continuing our monitoring of signed binaries, *DCSO CyTec* recently found a novel backdoor malware targeting Microsoft SQL servers.

The malware comes in form of an “Extended Stored Procedure” DLL, a special type of extension used by Microsoft SQL servers. Once loaded into a server by an attacker, it is controlled solely using SQL queries and offers a variety of functionality to run commands, interact with files and function as a network bridge head into the environment of the infected server.

In addition, the backdoor has capabilities to bruteforce logins to other MSSQL servers while adding a special hardcoded backdoor user in the case of successfully bruteforcing admin logins. **Based on this finding, we identified over 250 servers affected worldwide, with a clear focus on the Asia-Pacific region.**

Based on artifacts found in the malware, *DCSO CyTec* calls this novel threat “Maggie”.

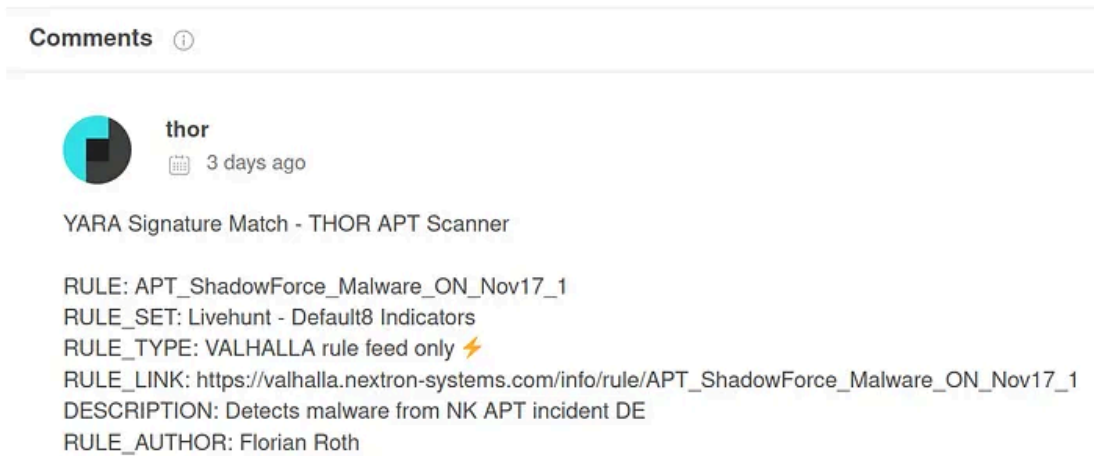
In our follow-up post "[Tracking down Maggie](#)" we also provide practical tips on how to detect Maggie in your environment.

Blog authored by [Johann Aydinbas](#) and [Axel Wauer](#)

Discovery

While looking for new threats, [a file caught our attention](#). Detected as `APT_ShadowForce_Malware_ON_Nov17_1` by THOR and with a matching AV detection by AhnLab-V3 as `Trojan/Win.ShadowForce.R472810` we decided to take a closer look.

Press enter or click to view image in full size



THOR detection on VirusTotal

The DLL file is signed by `DEEPSOFT Co., Ltd.` on 2022-04-12. According to its export directory, the file calls itself `sqlmaggieAntiVirus_64.dll` and only offers a single export called `maggie`.

Press enter or click to view image in full size

```

:000000018003A5F8 ; Export Address Table for sqlmaggieAntiVirus_64.dll
:000000018003A5F8 ;
:000000018003A5F8 off_18003A5F8 dd rva maggie ; DATA XREF: .rdata:00000001
:000000018003A5FC ;

```

DLL export in IDA

Extended Stored Procedures

Closer inspection revealed this DLL to be an `Extended Stored Procedure`.

[Extended Stored Procedures](#) are a way to offer extended functionality to SQL queries for use in an MSSQL server, similar to the infamous [xp_cmdshell](#) stored procedure, which allows SQL queries to run shell commands.

ESPs are common DLL files using a simplistic API. When executed, ESPs are passed a handle to the client connection which allows them to fetch user-supplied arguments (via [srv_paramdata](#)) and return unstructured data to the caller (via [srv_sendmsg](#)).

Maggie utilizes this message-passing interface to implement a fully functional backdoor controlled only using SQL queries.

In order to install *Maggie*, an attacker has to be able to place an ESP file in a directory accessible by the MSSQL server, and has to have valid credentials to load the *Maggie* ESP into the server. It is unclear how an actual attack with *Maggie* is performed in the real-world.

After manually loading *Maggie* with

```
sp_addextendedproc maggie, '<path to DLL>';
```

an authenticated user could start to issue commands to the backdoor via SQL queries, e.g. to call the `whoami` shell command:

```
$ exec maggie 'Exec whoami';  
MSSQL Procedure 04/08/2022  
Execute Command: Exec whoami  
Executing whoami Successfully  
nt service\mssqlserver
```

Commands

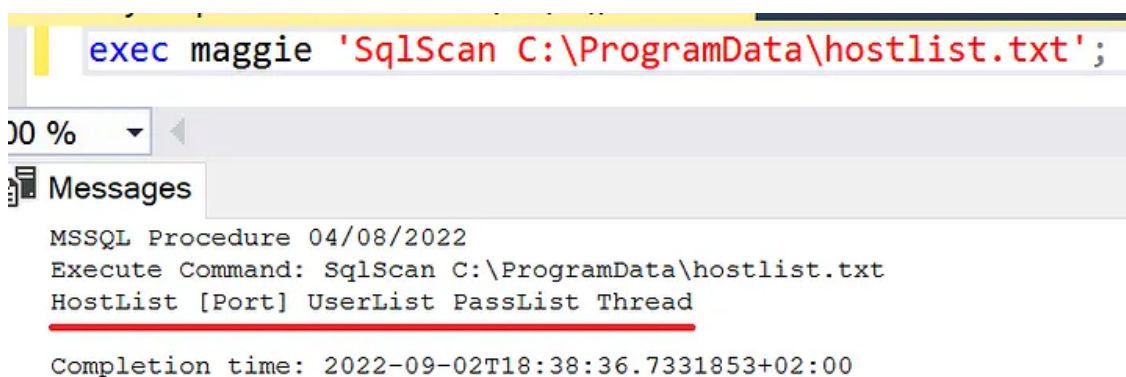
Once installed, *Maggie* offers a variety of commands to query for system information, interact with files and folders, execute programs as well as various network-related functionality like enabling TermService, running a Socks5 proxy server or setting up port forwarding to make *Maggie* act as a bridge head into the server's network environment.

The full list of commands we have identified:

List of commands available in *Maggie*

Commands can take multiple arguments, separated by spaces. For some commands, *Maggie* even includes usage instructions:

Press enter or click to view image in full size



Usage instructions for SqlScan command

Maggie as a network bridge head

Maggie contains functionality for simple TCP redirection, allowing it to function as a network bridge head from the Internet to any IP address reachable by the infected MSSQL server.

When enabled, *Maggie* redirects any incoming connection (on any port the MSSQL server is listening on) to a previously set IP and port, if the source IP address matches a user-specified IP mask. The implementation enables port reuse, making the redirection transparent to authorized users, while any other connecting IP is able to use the server without any interference or knowledge of *Maggie*.

For this to work, `StartHook` instructs *Maggie* to install network API hooks for the following functions:

- `accept`
- `AcceptEx`
- `WSAAccept`
- `setsockopt`
- `CreateIoCompletionPort`

allowing *Maggie* to intercept connections before reaching the underlying services.

Get DCSO CyTec Blog's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The redirection setup can be controlled using the `SetClientData` command with

```
SetClientData <allowed IP mask> <destination IP> <destination port>
```

in order to enable redirection for the given IP mask (can end with '*' wildcard) to the specified IP and port.

Once finished, an attacker can simply disable the IP redirection feature using `StopHook` again.

In addition, *Maggie* contains SOCKS5 proxy functionality for more complex network operations.

Press enter or click to view image in full size

Length	Type	Summary
0000001C	C	Socks5 Stopped Successfully
00000017	C	Socks5 Stopped Failure
00000015	C	Socks5 Isn't Running
00000016	C	Socks5 Thread Failure
0000001C	C	Socks5 Running Successfully
00000019	C	Socks5 Thread Successful
00000017	C	Socks5 Already Running

Debug messages for SOCKS5 functionality

The unknown Exploit commands

Maggie's command list includes four commands that suggest exploit usage:

```
Exploit AddUser  
Exploit Run  
Exploit Clone  
Exploit TS
```

It appears that the actual implementation of all four exploit commands depends on a DLL not included with Maggie directly. Instead, the caller provides a DLL name as well as an additional parameter when calling each function. We therefore assume the caller manually uploads the exploit DLL prior to issuing any exploit commands.

Maggie would then load the user-specified DLL, look for an export named either `StartPrinter` or `ProcessCommand` (depending on the exact command used) and pass the user-supplied argument.

We were not able to dig up any potential candidate DLLs Maggie might be referencing during our research so it's unclear what specific exploit may be utilized here.

SQL bruteforcing and the curious Maggie backdoor user

Maggie's command set also includes two commands that allow it to bruteforce logins to other MSSQL servers:

```
SqlScan  
WinSockScan
```

To start a bruteforce scan, the controller would have to specify a host, user and password list file previously uploaded to the infected server, as well as an optional thread count. Maggie then creates every combination of (host,user,pass) and attempts to log in via SQL using ODBC, or a reimplemention only using basic socket functions in the case of `WinSockScan`.

Successful logins are written to a hardcoded log file, which can be in one of two locations:

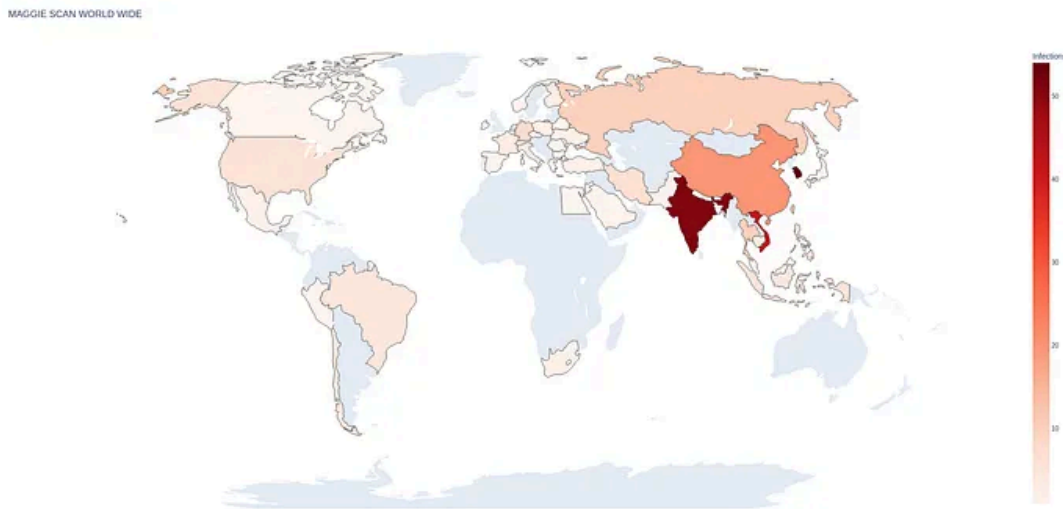
```
C:\ProgramData\succes.dat  
<MAGGIE_LOCATION>\succes.dat
```

Maggie then tries to determine if the bruteforced login has admin rights. In case it successfully bruteforced an admin user, *Maggie* proceeds with adding a hardcoded backdoor user.

Based on this finding, *DCSO CyTec* conducted a scan on publicly reachable MSSQL servers in order to determine how prevalent the identified backdoor user is.

Out of approximately 600,000 scanned servers worldwide, we identified 285 servers infected with *Maggie*'s backdoor user, spread over 42 countries.

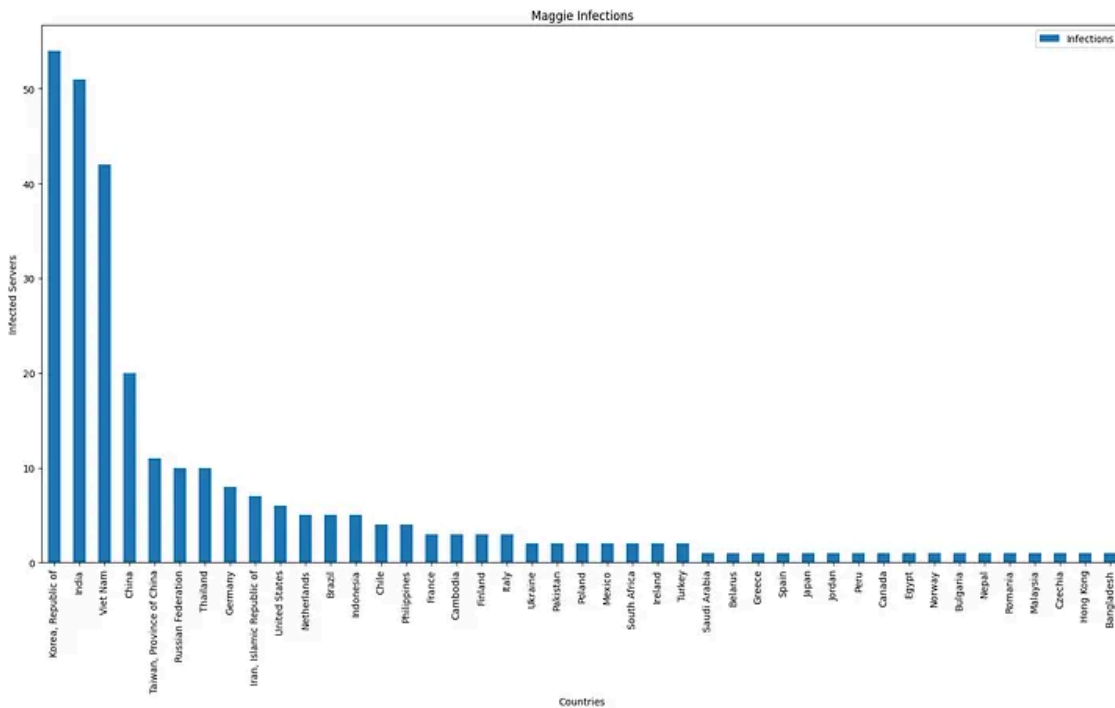
Press enter or click to view image in full size



Heatmap of backdoor user by country

The distribution shows a clear focus on the Asia-Pacific region, with South Korea, India and Vietnam as top 3 followed by China and Taiwan in the fourth and fifth place. Other countries appear to be incidental.

Press enter or click to view image in full size



Prevalence of backdoor user by country

A logical next step would be to see if and how the affected servers are being utilized, which however goes beyond the scope of our analysis.

IoCs

As usual, you can find below IoCs in the form of a MISP event [on our GitHub](#).

Maggie ESP DLLs

```
f29a311d62c54bbb01f675db9864f4ab0b3483e6cfd15a745d4943029dcd14  
a375ae44c8ecb158895356d1519fe374dc99c4c6b13f826529c71fb1d47095c3  
eb7b33b436d034b2992c4f40082ba48c744d546daa3b49be8564f2c509bd80e9  
854bb57bbd22b64679b3574724fafd7f9de23f5f71365b1dd8757286cec87430RAR SFX with Maggie  
4311c24670172957b4b0fb7ca9898451878faeb5dcec75f7920f1f7ad339d958  
d0bc30c940b525e7307eca0df85f1d97060ccd4df5761c952811673bc21bc794ITW URLs
```

<http://58.180.56.28/sql64.dll>

<http://106.251.252.83/sql64.dll>

<http://183.111.148.147/sql64.dll>

<http://xw.xxuz.com/VV61599.exe>

<http://58.180.56.28/vv61599.exe> Hardcoded User-Agent

Mozilla/4.0 (compatible) File paths

C:\ProgramData\Success.dat

Success.dat

Failure.dat

AccessControl.Dat

MITRE ATT&CK

T1110	Brute Force
T1090	Connection Proxy

Source: https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01