

Medium Q Search





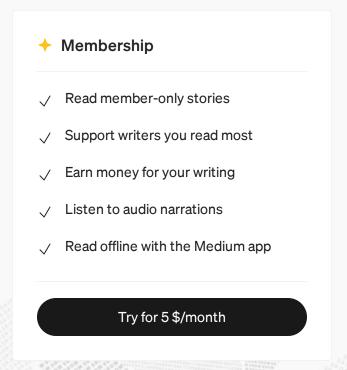


MSSQL, meet Maggie



Medium





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.

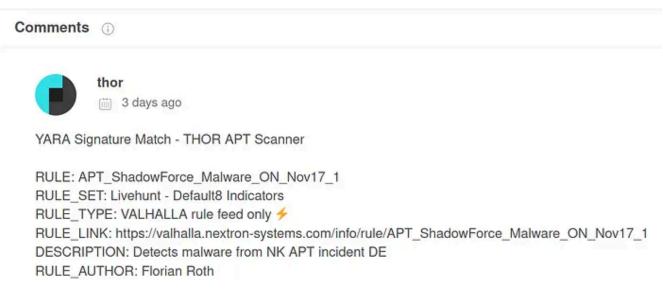
In addition, the backdoor has capabilities to bruteforce logins to other MSSQL servers while adding a special hardcoded backdoor user in the case of successfully bruteforcing admin logins. Based on this finding, we identified over 250 corvers affected worldwide, with a clear focus on the

Medium

Sign up to discover human stories that deepen your understanding of the world.

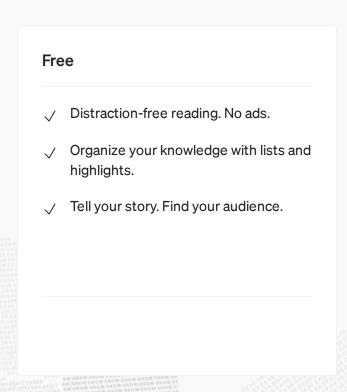
Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

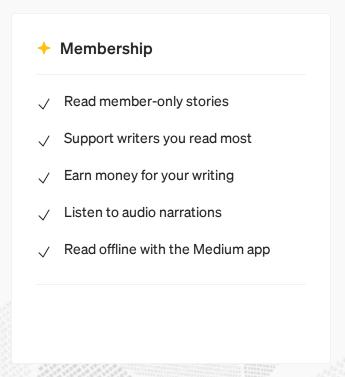
→ Membership
 ✓ Read member-only stories
 ✓ Support writers you read most
 ✓ Earn money for your writing
 ✓ Listen to audio narrations
 ✓ Read offline with the Medium app



THOR detection on VirusTotal

Medium





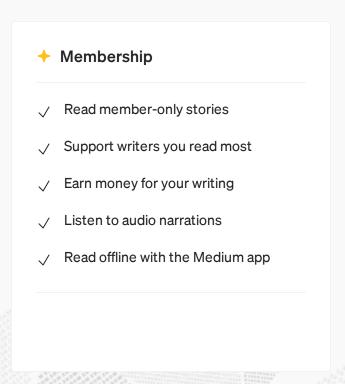
ESPs are common DLL files using a simplistic API. When executed, ESPs are passed a handle to the client connection which allows them to fetch user-supplied arguments (via srv_paramdata) and return unstructured data to the caller (via srv_sendmsg).

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

Medium

Sign up to discover human stories that deepen your understanding of the world.

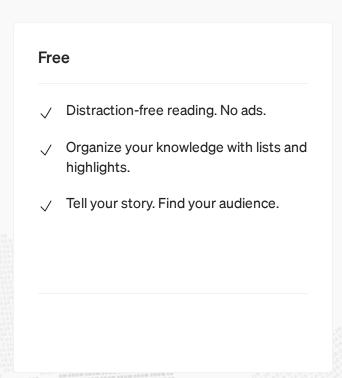


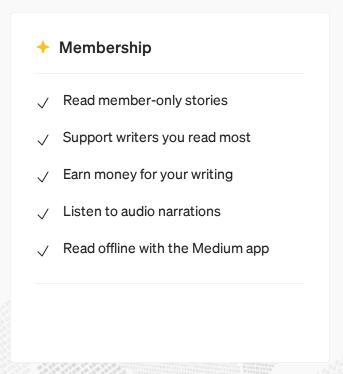
Commands

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:

Medium





Medium

Sign up to discover human stories that deepen your understanding of the world.



Usage instructions for SqlScan command

Medium

Sign up to discover human stories that deepen your understanding of the world.

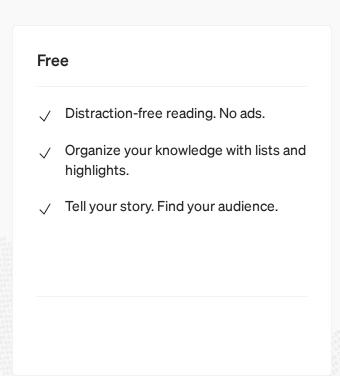


- WSAAccept
- setsockopt
- CreateIoCompletionPort

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

The redirection setup can be controlled using the SetClientData command

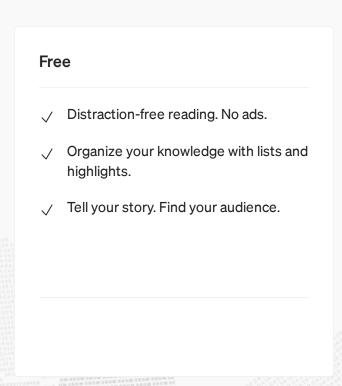
Medium





Debug messages for SOCKS5 functionality

Medium



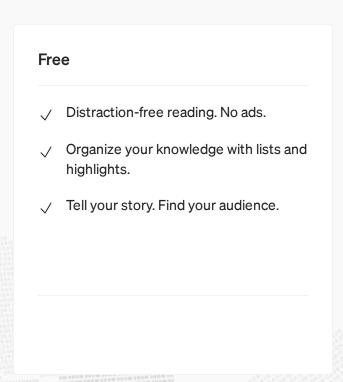


We were not able to dig up any potential candidate DLLs *Maggie* might be referencing during our research so it's unclear what specific exploit may be utilized here.

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:

Medium





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

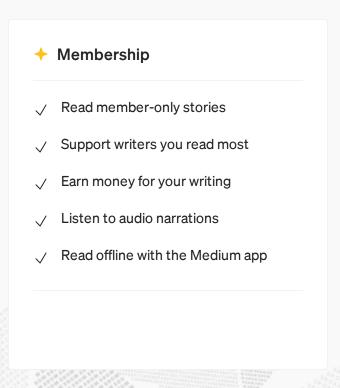
Medium

Sign up to discover human stories that deepen your understanding of the world.



Medium

Sign up to discover human stories that deepen your understanding of the world.



RAR SFX with Maggie

4311c24670172957b4b0fb7ca9898451878faeb5dcec75f7920f1f7ad339d958 d0bc30c940b525e7307eca0df85f1d97060ccd4df5761c952811673bc21bc794

ITW 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

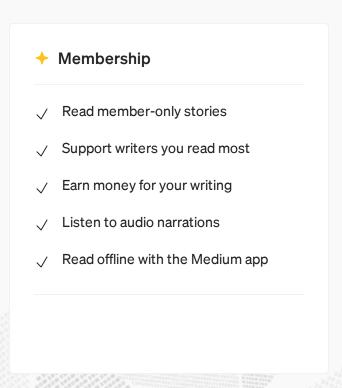
Mozilla/4.0 (compatible)

File paths

C:\ProgramData\Success.dat
Success.dat

Medium

Sign up to discover human stories that deepen your understanding of the world.





Follow

243 Followers

We are DCSO, the Berlin-based German cybersecurity company. On this blog, we share our technical research.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

→ Membership
 ✓ Read member-only stories
 ✓ Support writers you read most
 ✓ Earn money for your writing
 ✓ Listen to audio narrations
 ✓ Read offline with the Medium app