


Open in app ↗

Sign up Sign in

Medium Search

Write 

MSSQL, meet Maggie

 DCSO CyTec Blog · Follow
6 min read · Oct 4, 2022



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.

Sign up for free

✦ 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

Try for 5 \$/month

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

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

Comments ⓘ



thor



3 days ago

YARA Signature Match - THOR APT Scanner

RULE: APT_ShadowForce_Malware_ON_Nov17_1

RULE_SET: Livehunt - Default8 Indicators

RULE_TYPE: VALHALLA rule feed only ⚡

RULE_LINK: https://valhalla.nextron-systems.com/info/rule/APT_ShadowForce_Malware_ON_Nov17_1

DESCRIPTION: Detects malware from NK APT incident DE

RULE_AUTHOR: Florian Roth

THOR detection on VirusTotal

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

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

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

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

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

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

Usage instructions for SqlScan command

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

- WSAAccept
- setsockopt
- CreateIoCompletionPort

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

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

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

Debug messages for SOCKS5 functionality

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

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

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

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

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

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

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.

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



Written by DCSO CyTec Blog

243 Followers

Follow

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