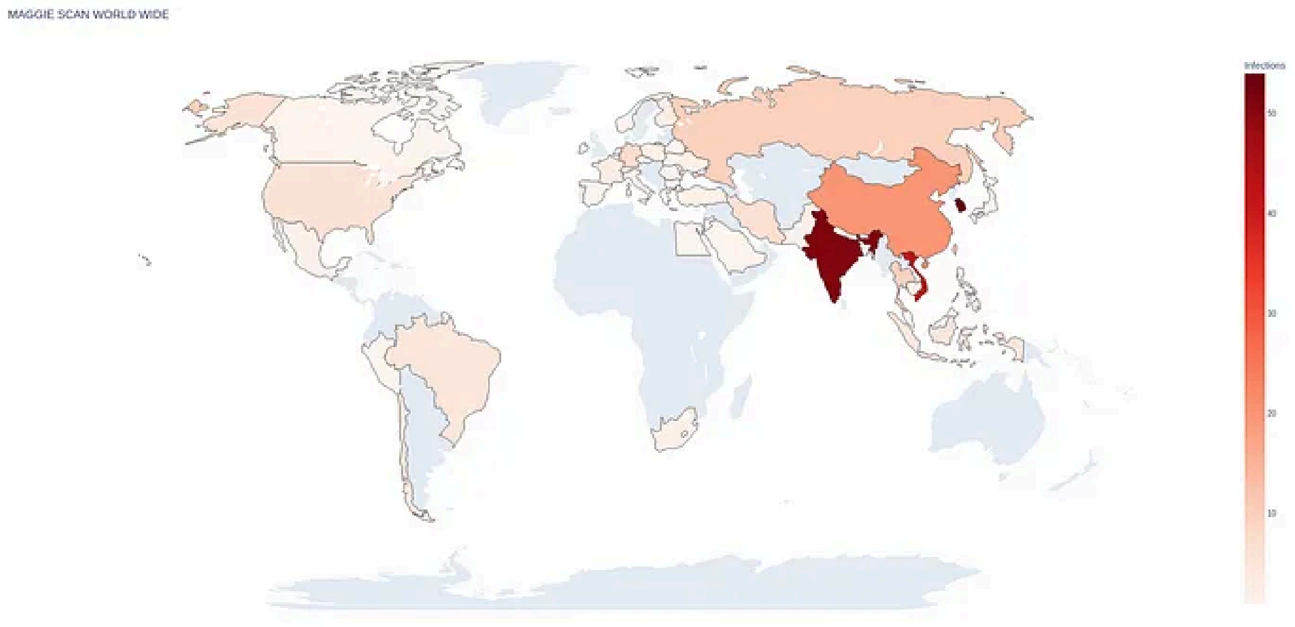
MSSQL, meet Maggie

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

26 1



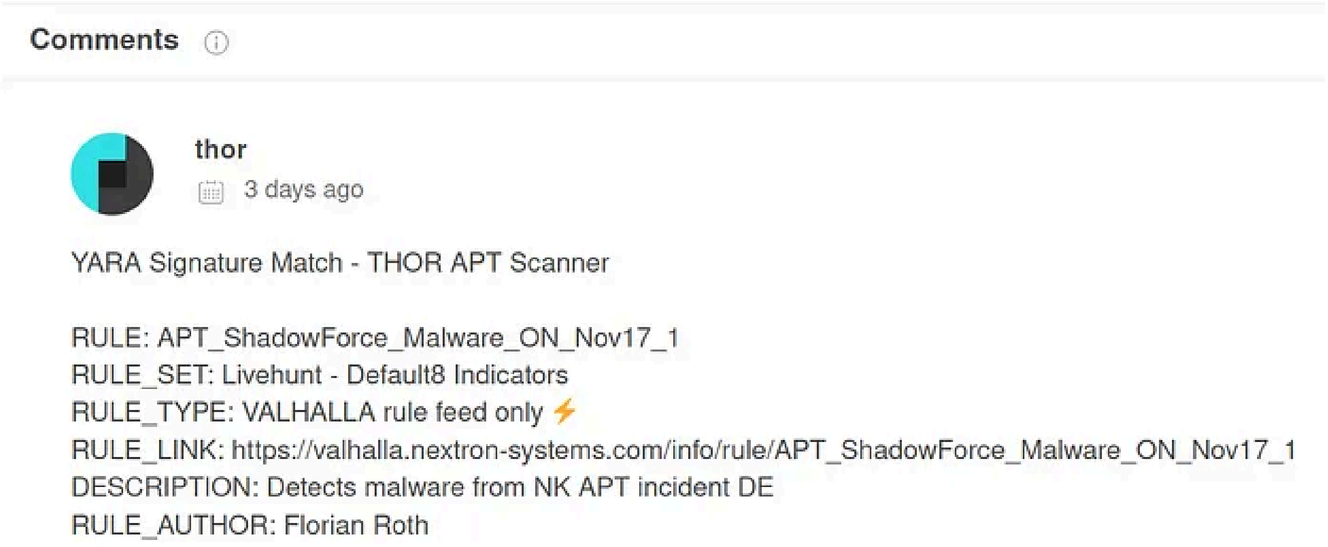
Heatmap of Maggie backdoor user by country

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

Discovery

W `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.



Comments

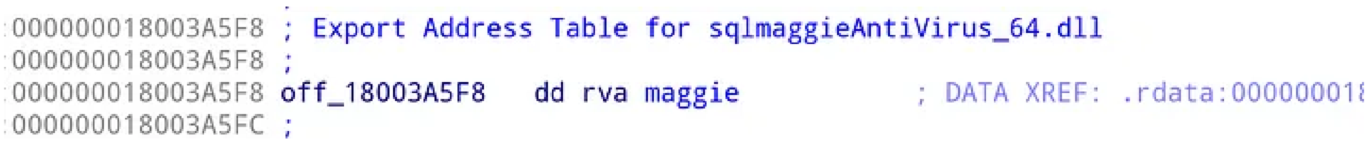
thor
3 days ago

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

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` .



```
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

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:

Commands can take multiple arguments, separated by spaces. For some co

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:

in order to enable redirection for the given IP mask (can end with '*'
wi

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.

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

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 reimplementation 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\success.dat
<MAGGIE_LOCATION>\success.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.

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
f29a311d62c54bbb01f675db9864f4ab0b3483e6cfdd15a745d4943029dcdf14
a375ae44c8ecb158895356d1519fe374dc99c4c6b13f826529c71fb1d47095c3
eb7b33b436d034b2992c4f40082ba48c744d546daa3b49be8564f2c509bd80e9
854bb57bbd22b64679b3574724fafd7f9de23f5f71365b1dd8757286cec87430

RAR SFX with Maggie
```

Malware Analysis Cybersecurity Reverse Engineering Maggie Backdoor

26 1

Written by DCSO CyTec Blog

Follow

243 Followers

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

More from DCSO CyTec Blog

See all from DCSO CyTec Blog

Recommended from Medium

theUnknown

Malware Reverse Engineering Basics. Part 1.

This is the beginning of the series of my brief notes on reverse engineering and assembly.

Jul 11 24

Motasem Hamdan

Using Python to Solve Computational Problems |…

Introduction

Sep 25

RED TEAM

Malware Development Part 8 : Reverse Shell Via Dll Hijacking

“From DLL to Shell: A Step-by-Step Guide to Reverse Shell via DLL Hijacking”

✦ Jun 22 147

Aardvark Infinity in Aardvark Infinity

Dragon

Description: A formidable C# tool designed for advanced Active Directory (AD)...

✦ Sep 28

See more recommendations

Help Status About Careers Press Blog Privacy Terms Text to speech Teams