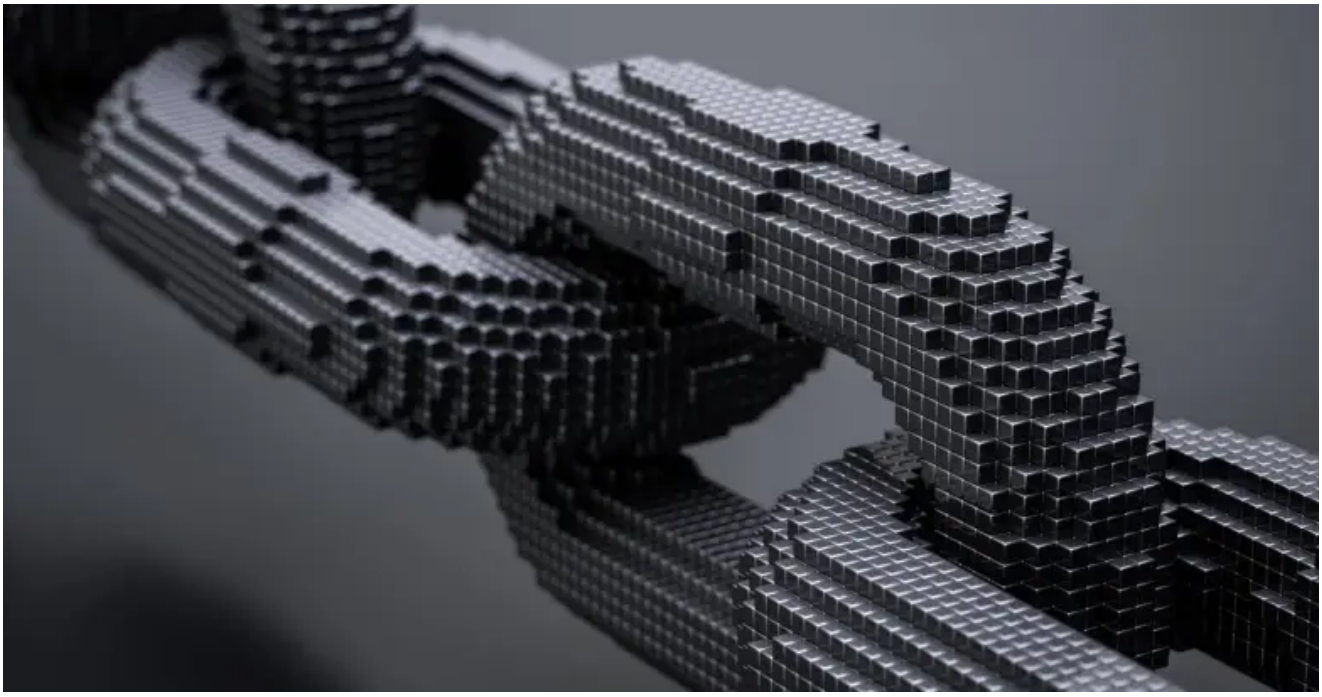
Glupteba – the malware that gets secret messages from the Bitcoin blockchain

nakedsecurity.sophos.com/2020/06/24/glupteba-the-bot-that-gets-secret-messages-from-the-bitcoin-blockchain/

By Paul Ducklin 24 Jun 2020



Here's a SophosLabs technical paper that should tick all your jargon boxes!

Our experts have deconstructed a strain of malware called **Glupteba** that uses just about every cybercrime trick you've heard of, and probably several more besides.

Like a lot of malware these days. Glupteba is what's known a zombie or bot (short for *software robot*) that can be controlled from afar by the crooks who wrote it.

But it's more than just a remote control tool for criminals, because Glupteba also includes a range of components that let it serve as all of the following:

- **A rootkit.** Glupteba includes a variety of Windows kernel drivers that can hide the existence of specific files and processes. Kernel rootkits are unusual these days because they're complex to write and often draw unnecessary attention to themselves. However, if loaded successfully, rootkits can help cybersecurity threats lie low by keeping malware files off the radar of security tools and stopping them from showing up in security logs.

- **A security suppresor.** Glupteba has a module that does its best to turn Windows Defender off, and then regularly checks to make sure it hasn't turned itself back on. It also looks for a laundry list of other security tools, including anti-virus software and system monitoring programs, killing them off so they can no longer search for and report anomalies.
- **A virus.** Glupteba uses two different variants of the ETERNALBLUE exploit to distribute itself automatically across your own network, and anyone else's it can find by reaching out from your computer. That makes it an old-school, self-spreading computer virus (or more specifically a worm) rather than just a standalone piece of malware.
- **A router attack tool.** Glupteba bundles in various exploits against popular home and small business routers, using your computer as a jumping off point to attack other people. It uses one of these attacks to open up unpatched routers to act as network proxies that the crooks can use as "jumping off" points for future attacks. This leaves the unfortunate victim looking like an attacker themselves and showing up as an apparent source of cybercriminal activity.
- **A browser stealer.** Glupteba goes after local data files from four different browsers – Chrome, Firefox, Yandex and Opera – and uploads them to the crooks. Browser files often contain sensitive information such as URL history, authentication cookies, login details and even passwords that can't be accessed by code such as JavaScript running inside the browser. So crooks love to attack your browser from outside, where the browser isn't in control.
- **A cryptojacker.** Along with everything else it does, Glupteba can act as a secretive management tool for two different cryptomining tools. Cryptominers are legal if you use them with the explicit permission of the person paying the electricity bills to run the computers you're using (and cryptomining can consume a lot of power). Here, the crooks get you to pay their power bills and take the cryptocoins for themselves.

There's more – much more

But that's not all.

The most interesting feature that we learned about in the report (and we think you'll be fascinated too) is how Glupteba uses the Bitcoin blockchain as a communication channel for receiving updated configuration information.

As you probably know, zombies or bots aren't much use to the crooks if they can't call home to get their next wave of instructions.

Glupteba has a long list of built-in malicious commands that the crooks can trigger, including the self-explanatory `update-data` and `upload-file` commands that are detailed in the report. But it also includes, as with most bots, generic commands to `download` and `run` new malware, meaning that even if you know everything about Glupteba itself, you can't predict what it might morph into next because the crooks can update the running malware at will.

The current command-and-control servers used by the crooks, known as C2 servers or C&Cs, might get found out and blocked or killed off at any moment, so zombie malware often includes a method for using an otherwise innocent source of data for updates.

After all, to tell a bot to switch from one C&C server to another, you typically don't need to send out much more than new domain name or IP number, and there are lots of public messaging systems that make it easy to share short snippets of data like that.

For example, bots have used services such as Twitter, Reddit, Pastebin and other public websites as temporary storage for secret messages, in the same way that spies from the Cold War era might have communicated using the "Personals" section in a print newspaper.

Bring on the blockchain

Glupteba uses the fact that the Bitcoin transactions are recorded on the Bitcoin blockchain, which is a public record of transactions available from a multitude of sources that are unexceptionably accessible from most networks.

Bitcoin "transactions" don't actually have to be about money – they can include a field called `RETURN`, also known as `OP_RETURN`, that is effectively a comment of up to 80 characters.

Let's start with a list of all the Bitcoin transaction hashes (lightly redacted) associated with one of the Bitcoin wallets used as a covert source of messages by Glupteba.

The wallet ID shown here was extracted from the malware by SophosLabs.

The command line program `bx` below is a popular and useful Bitcoin blockchain explorer tool:

```
$ bx fetch-history 15y7......qNHXRtu5wzBpXdY5mT4RZNC6 | awk '$1 == "hash" { print $2
}'
dfef43552fc953ff14ca7b7bb........b79e8409b5638d4f83b1c5cec0abc3d
98987c05277c97b06edfc030c........07e74334c203075ec27b44b3cc458bf
717da8bea87d02ef62b1806cf........7e01f0267718f0351f9ae1592e02703
20b37b655133491b94a8021ab........0266d15331a14caf10570b6623a86e4
fa9cd0622535cf6c9ff449510........c5d526d5794d9d98ba5d6469a97be2c
0d83cbc74a12a9f130fcead23........d5d56cf769c6c0a4cf1cebbf9e97e4a
a7fb3bb04b82922923e8359f8........3db69bd2863ec88b98f9c69a37212ad
52ee10617c1fc3e25922b146a........7daefdc3c3d5421b0387a737e46b396
f29cbbb96de80dbc7e5236c98........3da6f8118bb356f537ce0317f7ab10c
6a3a720ab97511528309fbf64........f37bc25d95d45d3408540174daad786
8bf7acc56aab4b87d73a85b46........1486f0a764fd0a5f13e2d79e0a14625
3bd54c0832cc411f5299064e4........c11ab05c1a4aff62fa323c068e88945
1e1c0249bb22d1fcfb596e4fb........df7ab3bf627e25a2fe9530eb3dce476
51899ffeadf5d0d605d5122c3........5b82baa15a4fa6b203abf59731c158f
8a7c43d0bbf01cdf3bb28de48........6e339a063251fce30cb83ae50c2096a
55e8fe62bcc41ec465c3f1f28........f5d82443a15a30d88fefc3f55ad2f29
```

If we fetch the details of each of these transactions, we can see which ones include `OP_RETURN` data.

Here's a transaction dump for one that does, truncated to save space:

```
$ bx fetch-tx 55e8fe62bcc41ec465c3f1f28........f5d82443a15a30d88fefc3f55ad2f29
{
    hash 98987c05277c97b06......1ce207e74334c203075ec27b44b3cc458bf
    inputs
    {
        input
        {
[ . . . . . . . . . ]
        output
        {
            script "return
[18fe788a52d7aa57808d801d0f8f7cd39e1a......9f986b877befce0c2f558f0c1a9844833ac702cb3eb

[ . . . . . . . . . ]
            value 0
        }
    }
[ . . . . . . . . . ]
```

The bytes in the `OP_RETURN` data shown above are the secret message.

To decrypt it, you need a 256-bit AES decryption key that's coded into the the Glupteba malware program (you can find the keys in the SophosLabs paper), and you need to know that the data returned in the blockchain consists of:

```
First 12 bytes   = AES-256-GCM initialisation vector
Last 16 bytes    = AES-256-GCM authentication tag
Bytes in between = Encrypted message (bytes from 0f8f7cd3... to ...877befce)
```

Decrypt the data from the blockcode to reverse the AES-256-GCM encryption, and you'll reveal the hidden message.

This sort of "hiding in plain sight" is often referred to as steganography.

Here's some pseudocode to give you the idea:

```
   > cipher = newcipher('AES-256-GCM')
   > cipher.key = d8727a0e...d66503cf               // extracted by SophosLabs
   > cipher.iv  = 18fe788a52d7aa57808d801d          // GCM mode needs an IV
   > cipher.tag = 0c2f558f0c1a9844833ac702cb3eba6e  // GCM mode needs a message hash
   > plain = cipher:decrypt(0f8f7cd39e1a......9f986b877befce)
   > print('secret message is: ',plain)

   secret message is: venoco___ol.com              // see report for full IoC list
                                                   // this is a new C&C server to
move to
```

And that's how Glupteba hides its command-and-control server names in plain sight!

READ REPORT NOW ▶

How bad is it?

The bad news about Glupteba is that its many self-protection components mean that it has many tricks available to stop itself showing up in your security logs.

The good news is that this complexity makes the malware less reliable, and ironically more prone to triggering security alarms at some point.

Indeed, some of the low-level programming tricks it uses, including the kernel-level rootkits, not only don't work on recent versions of Windows, but also often draw attention to themselves by the way they misbehave, up to and including crashing your computer with a giveaway blue screen of death.

Also, Glupteba relies on numerous exploits that were patched many months or years ago – including the attacks it uses against routers – so a patched system is much less likely to get infected in the first place.

Lastly, the main delivery mechanism we're aware of so far that brings infections of Glupteba into a network (assuming you are patched against ETERNALBLUE and can't get infected by its viral component), seems to be via "software cracks" on well-known piracy sites.

Like this one:

This crack didn't lead to Adobe Illustrator.
It led to a Glupteba infection.

What to do?

- **Patch early, patch often.** That includes your operating system, the apps you use, and any devices such as routers and file storage servers on your own network.
- **Use a decent anti-virus with built-in web filtering.** Most malware, including zombie malware, arrives as a series of downloads. Even if you hit by get the first stage of malware attack, you can still defeat the crooks if you stop the final payload arriving.
- **Stay away from hookey software.** Assume that the sort of person who's willing to steal software such as Adobe Illustrator and give away tools to crack it "for free" is also willing to accept money from crooks to implant malware in their fraudulent downloads.

LEARN MORE ABOUT STEGANOGRAPHY

If you enjoyed this article, why not watch one of our Naked Security Live videos in which we discuss the weird and wonderful world of steganography?

Watch Video At:

https://youtu.be/q2hD4v8_8-s

You can watch directly on YouTube if the video won't play here.

The articles referenced in the video are: