Shadows in the Rain

medium.com/insomniacs/shadows-in-the-rain-a16efaf21aae

asuna amawaka March 16, 2020

asuna amawaka

Mar 16, 2020

.

6 min read

When I read Trend Micro's report on Operation DRBControl[1] in February, one detail stood out and piqued my curiosity — there were 3 mutexes connecting a *Trochilus RAT* sample in the incident and a *BBSRAT* sample that uses a C2 domain linked to the **Winnti Group**. This came as a surprise to me, because I thought *BBSRAT* was a unique malware family, a "new tool" back in 2015 that was attributed by Palo Alto Networks to the attacker group **Roaming Tiger**. There seem to be no news on *BBSRAT* all these years, and now when it is mentioned again, it is linked to **Winnti Group**? Interesting.

Is that really a *BBSRAT*? Only 1 way to find out — analyse it!

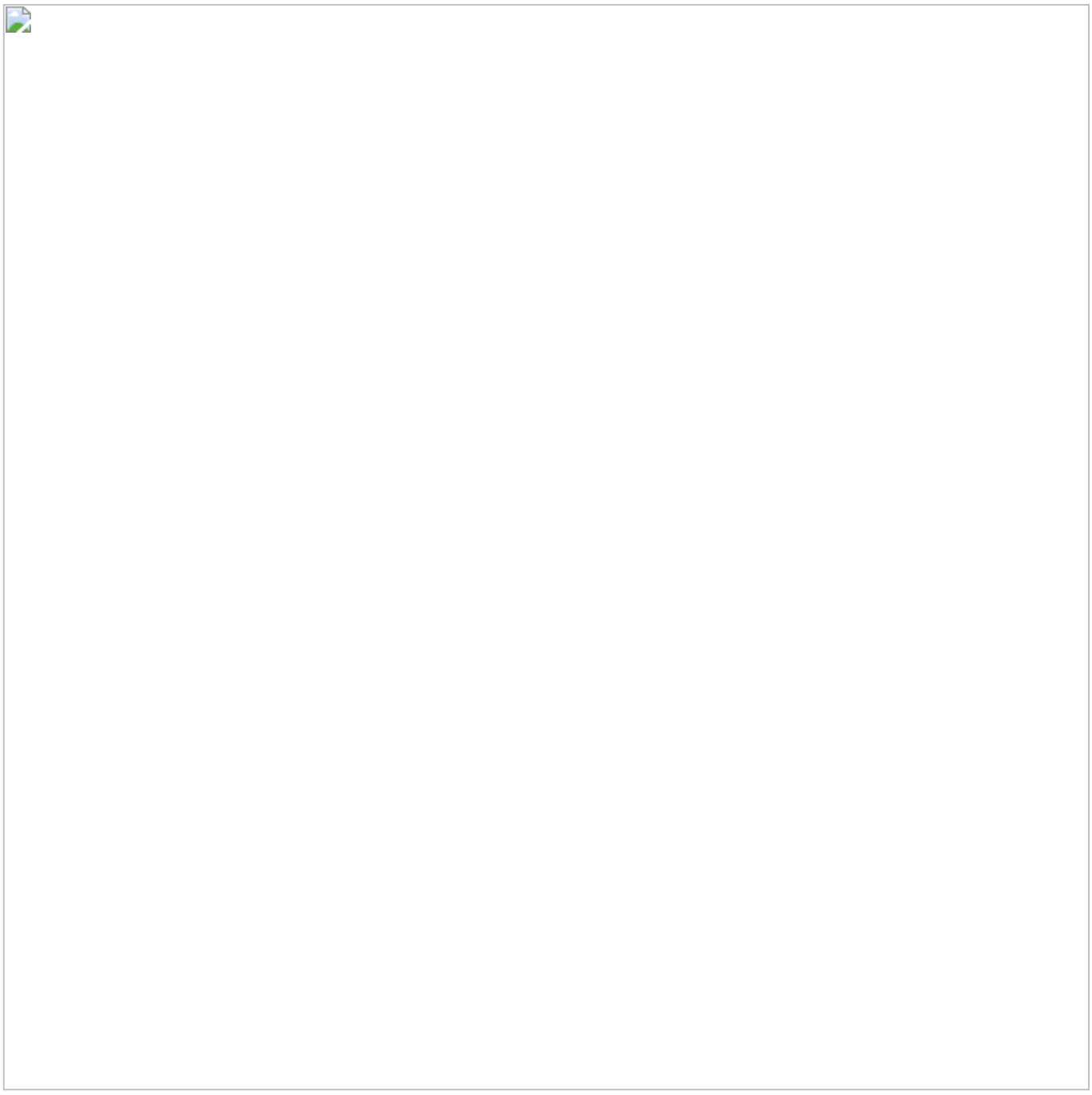
Finding the samples to work on

Mutexes:
cc5d64b344700e403e2sse
cc5d6b4700e403e2sse
cc5d6b4700032eSS

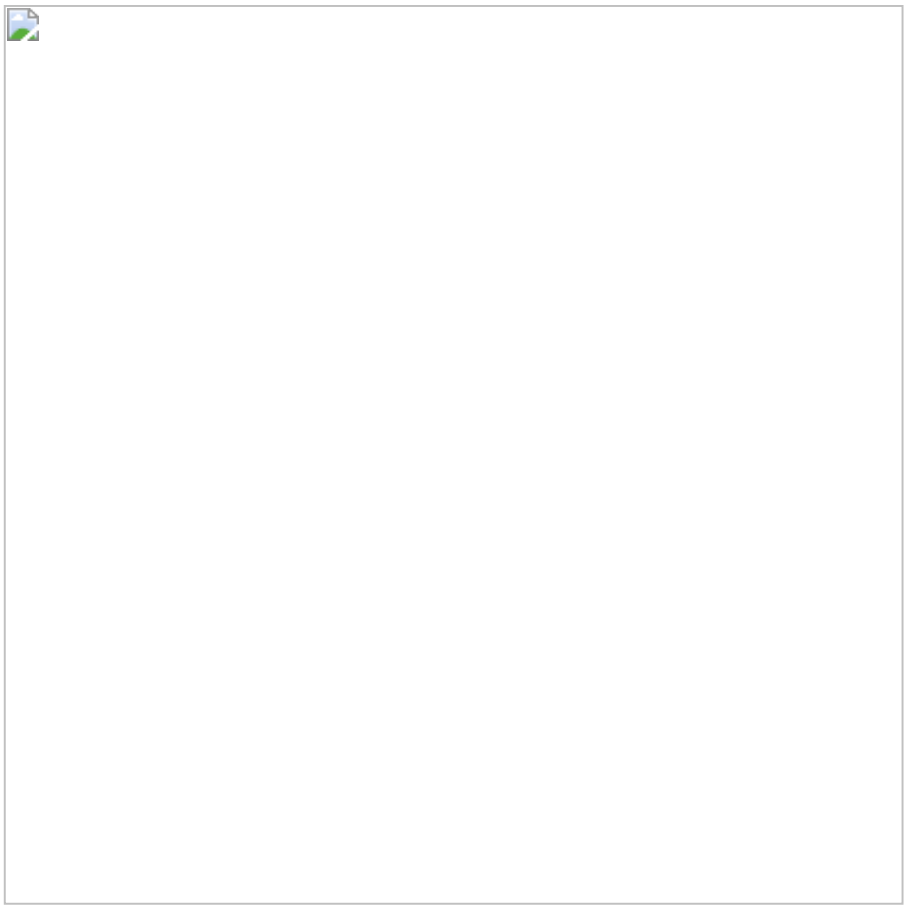
C2:
bot[.]googlerenewals[.]net

Looking up the C2 domain on Virustotal quickly surfaced 3 samples that exhibited callbacks to this C2, and these samples are just the ones we are looking for: they contain the said mutexes! These samples make a copy of itself as *diskshadow.exe* on disk (a name that is close to "*diskwinshadow.exe*" that is the *BBSRAT* mentioned in Trend Micro's report).

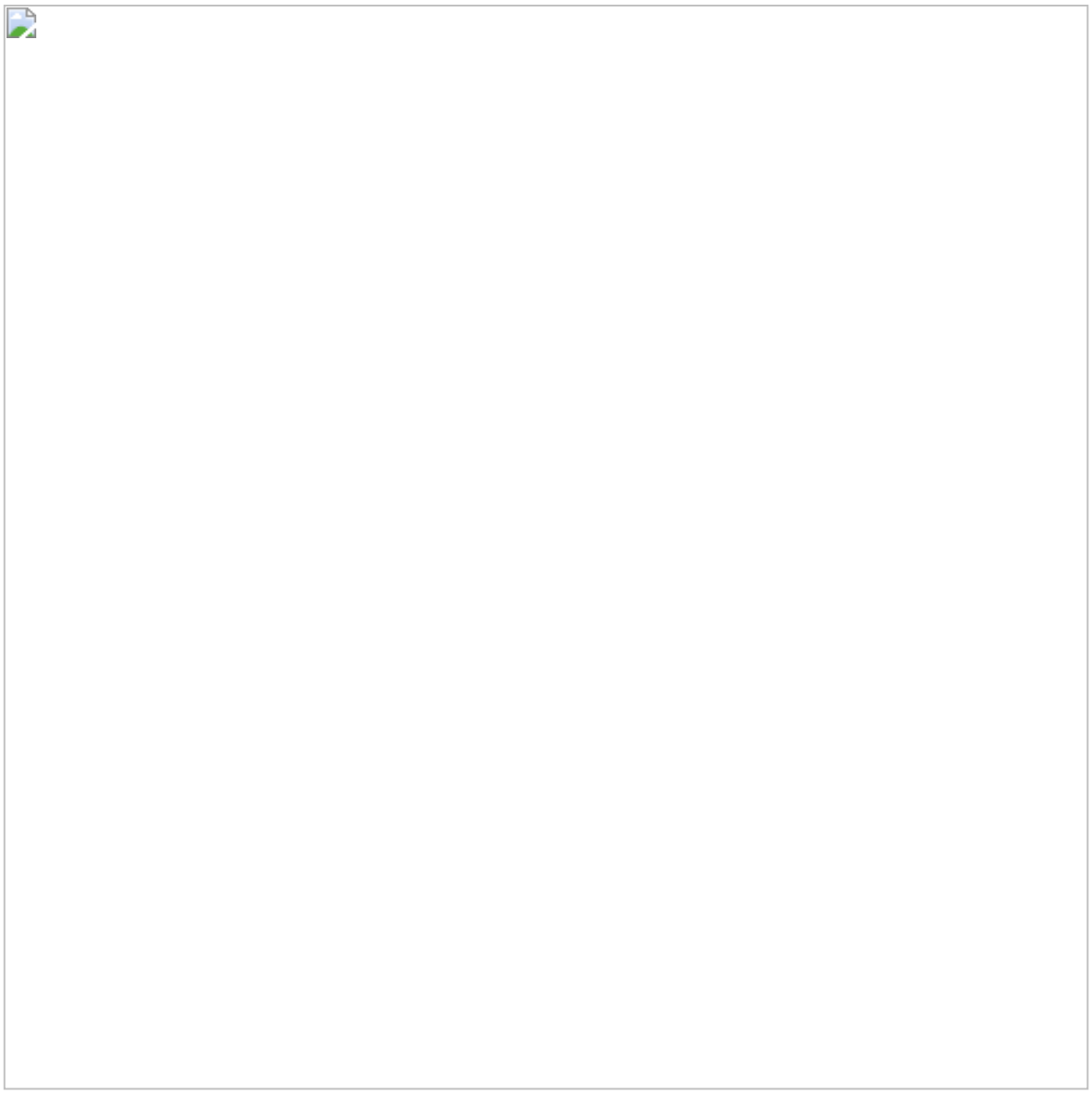
These are self-extracting files that contain other executables within:



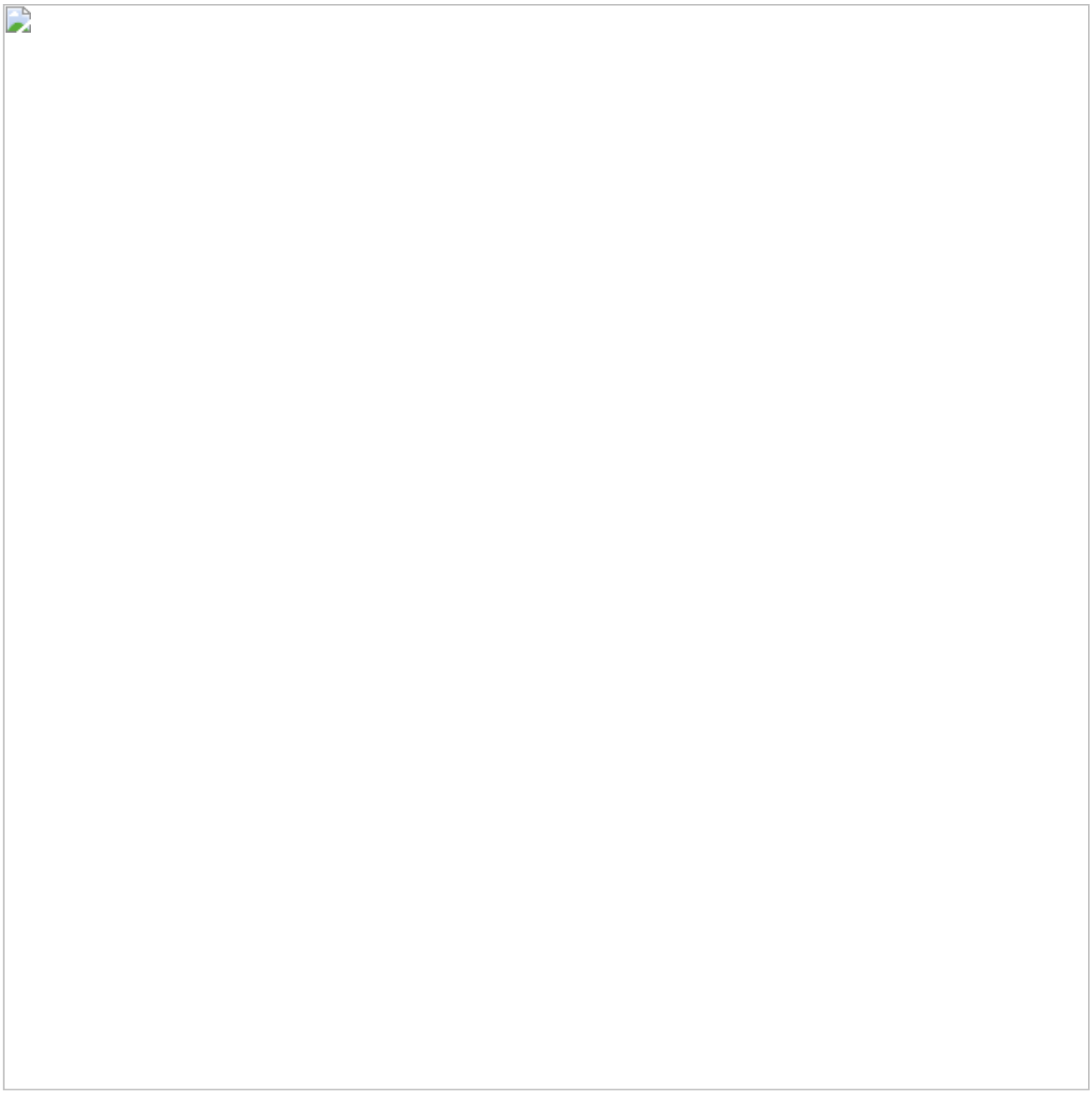
Let’s jump straight into finding out what these “rain.sdb” are, since they are the meat of the malware.



First, they are encoded with a simple inversion, then XOR 0x5. Reversing this encoding would get us an -almost- perfect PE file, just alter the first two bytes to the correct Magic header. This simple trick of obfuscating the magic header could have been intended to fool signature matching defenses.



After decoding, we get three unique rain.sdb files. Notice how the two 64-bit files have the same XOR key in their RICH header despite them having different hashes. Assuming that the RICH header has not been tampered with, this means that they have the source code and compilation environment. This is not surprising, considering the close compilation timestamps they have.

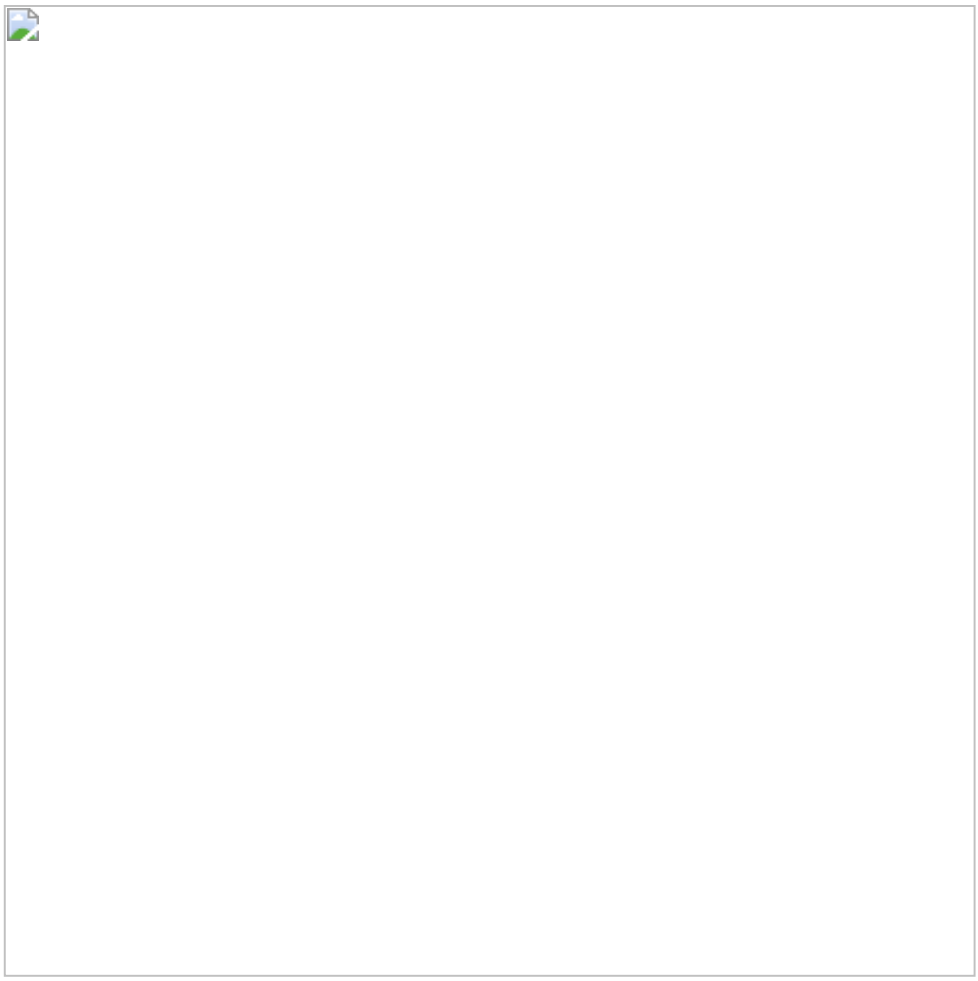


For the rest of this post, I'll focus on findings using the file with MD5 368B555321F56699D2431A3908D52487.

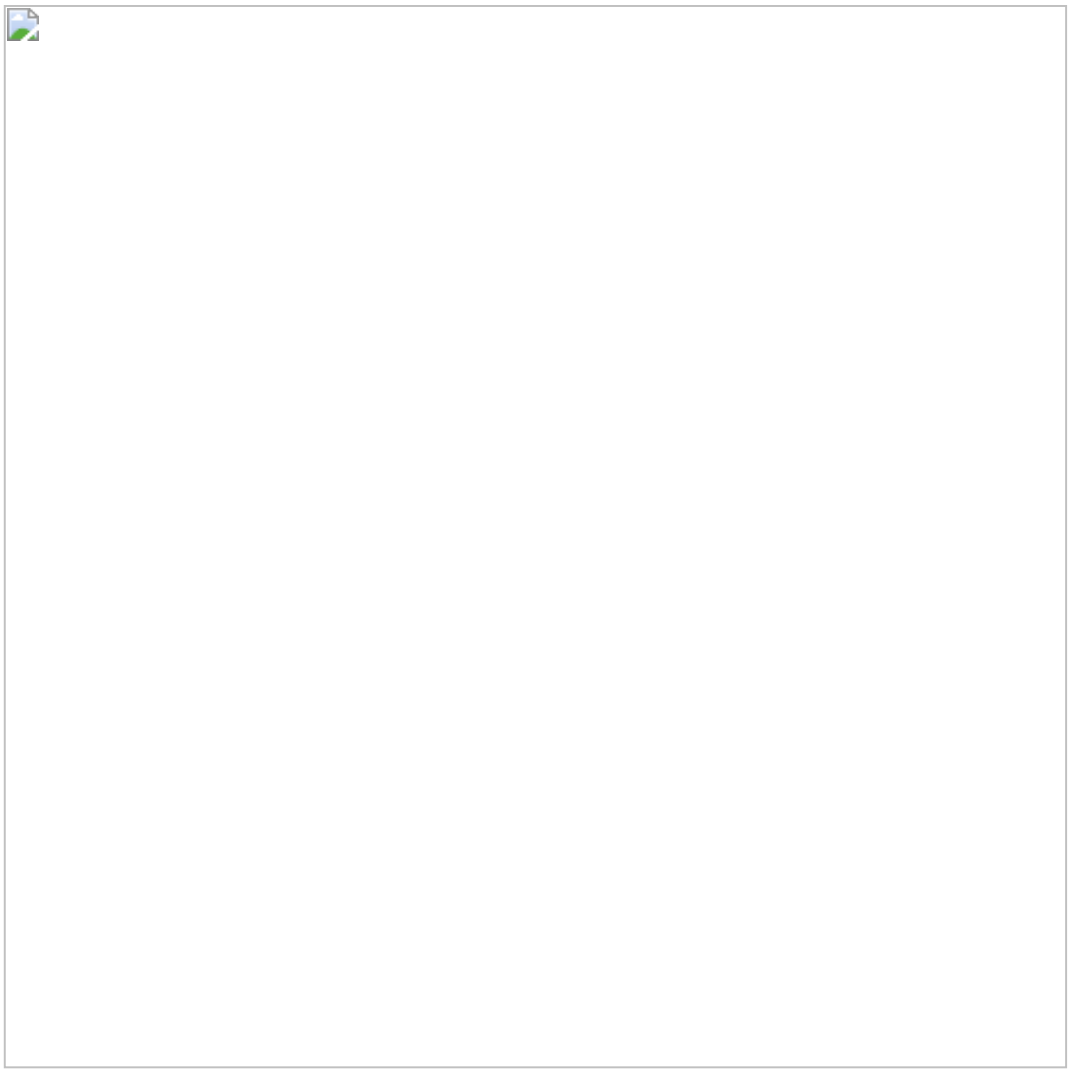
To start off, let's take a look at some of the interesting stuff this sample does.

Hide, hide, hide!

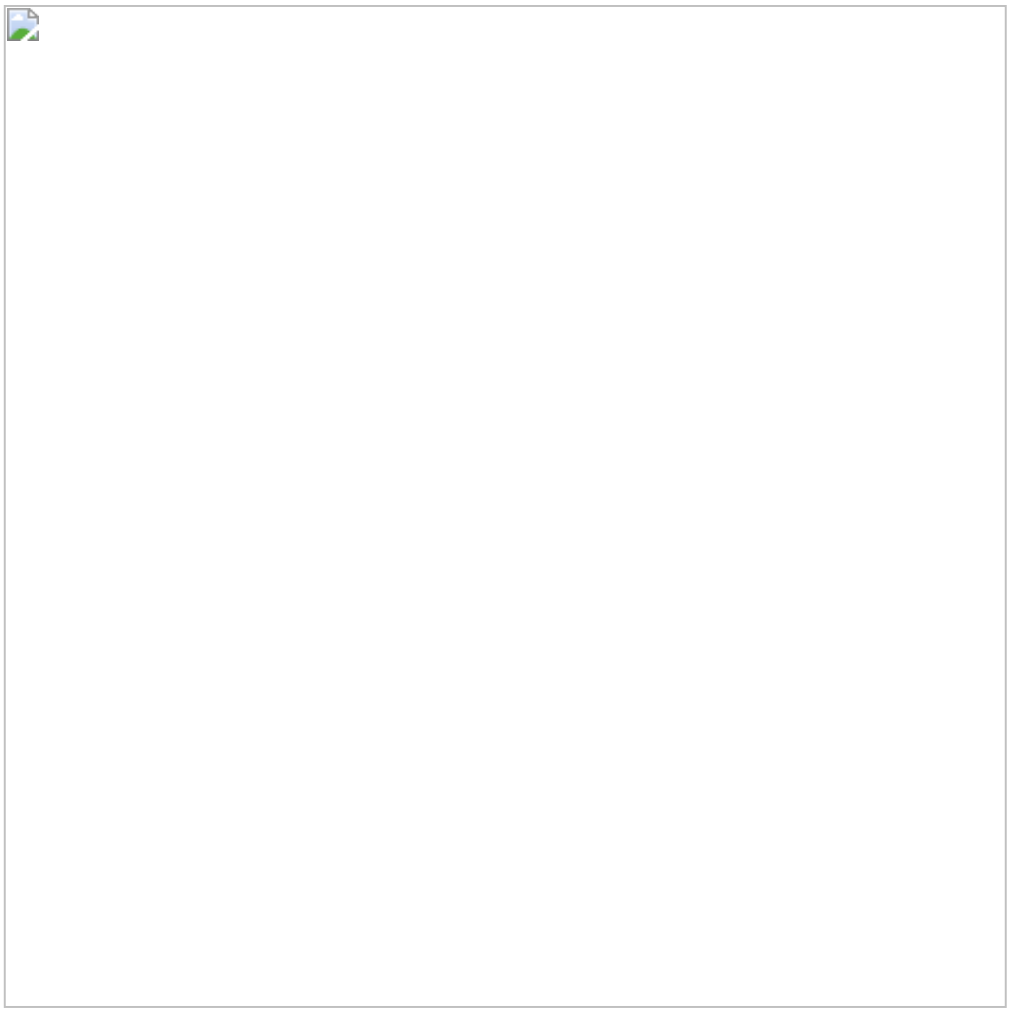
Since the malware comes in a typical trio — legitimate executable, rogue DLL loaded via load-order hijacking and malicious payload, I expect to see some kind of injection to happen. True enough, callback activities are conducted under the cover of *msiexec.exe*. There are also other choices of processes for injection, perhaps used in other variants of this sample. Notice this is where the mutex is created.



Contents from either the file rain.sdb or regkey “HKCU\M\M” are also injected into a created cmd.exe.



Persistency is achieved through services, a different mutex is created to “mark” that the service has already been created.

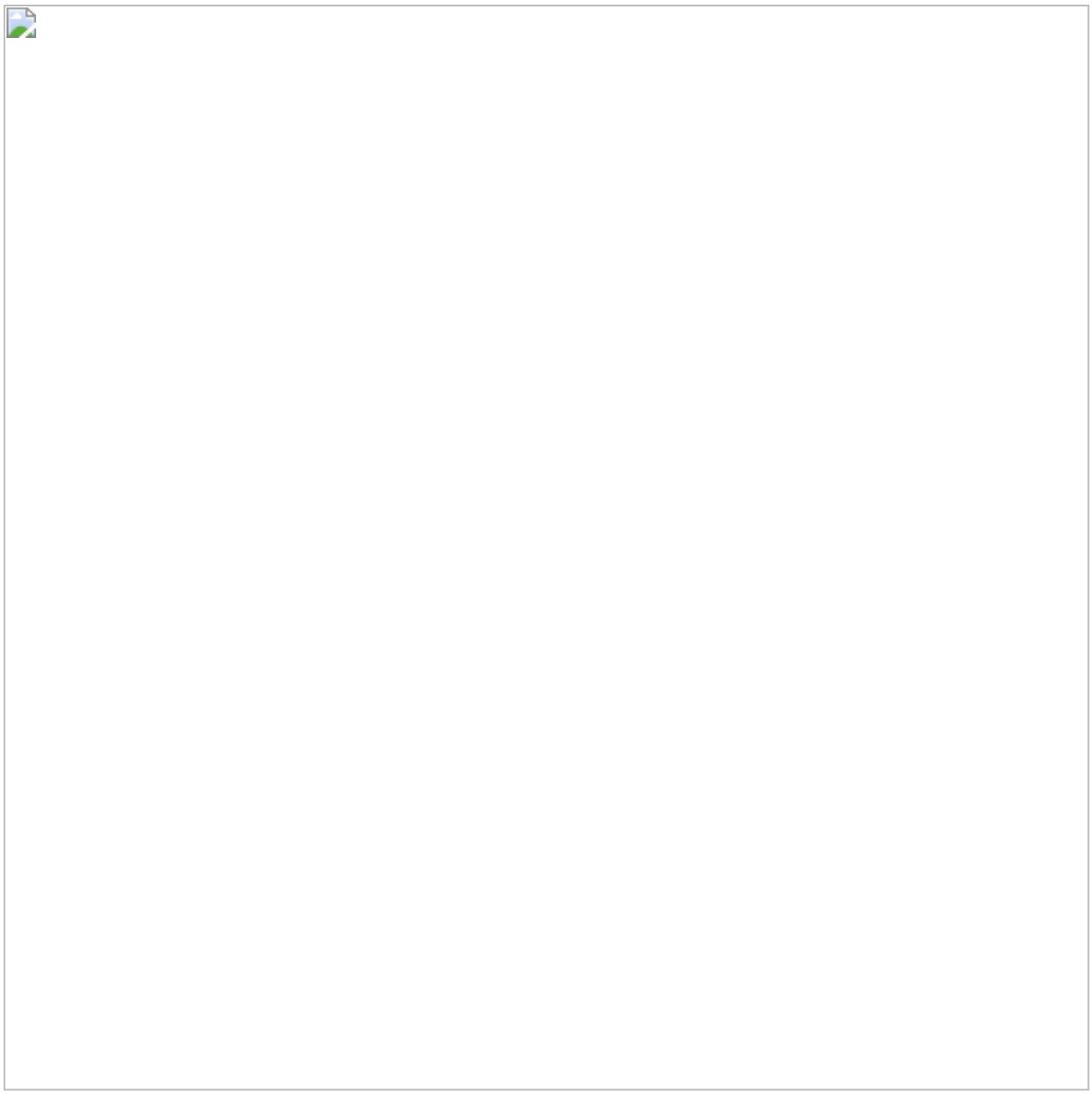


The malware also comes with a feature that replaces “InternalGetTcpTable2” in IPHLPAPI.DLL, in an attempt to hide the C2 connection when a netstat is done.

Leave that door open!

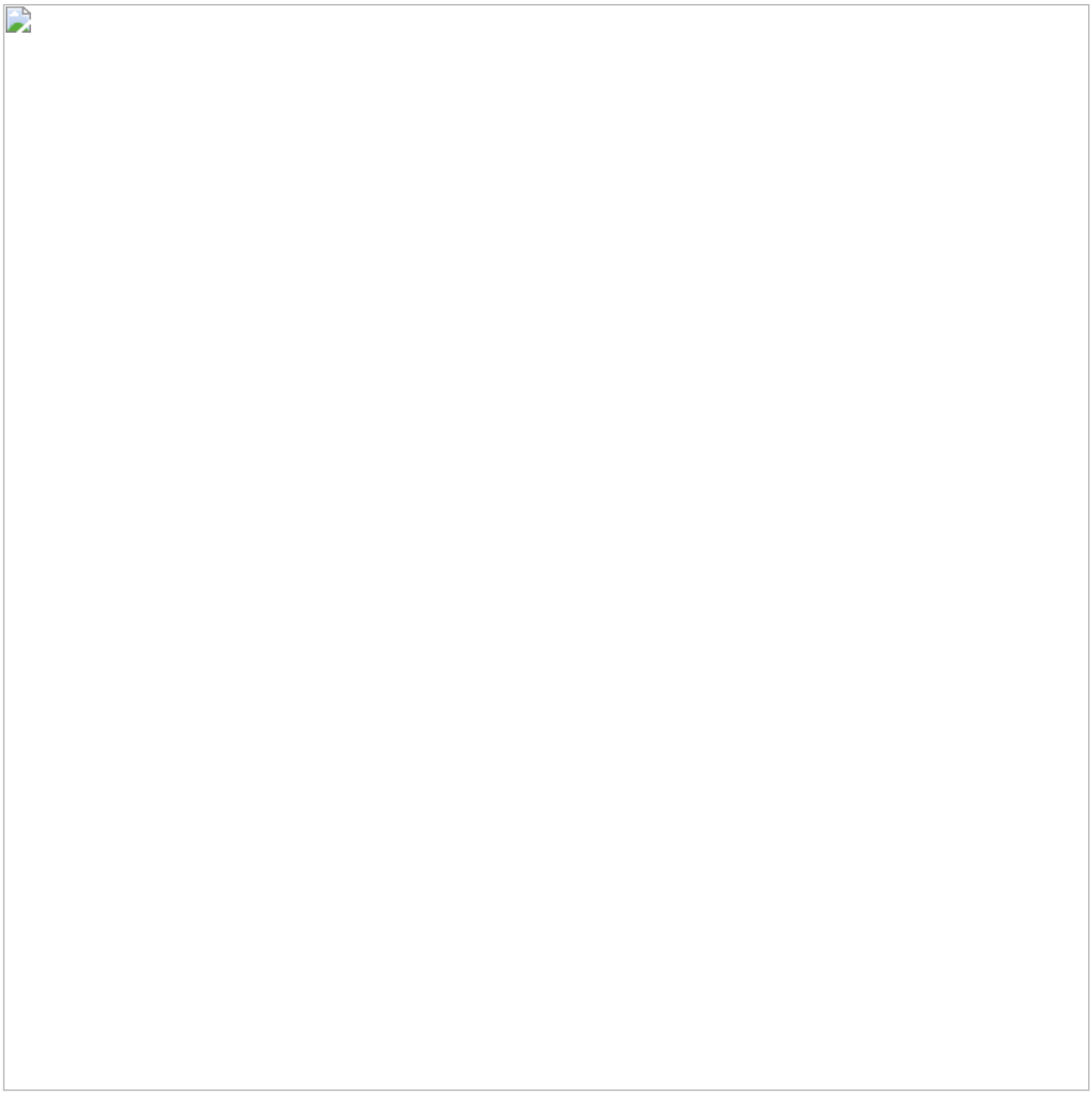
This sample abused Windows’ Bitsadmin utility to execute any powershell script of the attacker’s choice — all he needs to do is to write the powershell commands into the regkey HKCU:/M/S, and the BITS job will execute the command as part of the “notification process” after the job is completed (In this case, the job is the copying of mshta.exe). This job will be executed periodically, and it can stay in the system for 90 days[3] even after the malware has been cleaned up.

This is not a groundbreaking trick, though not commonly seen. According to MITRE ATT&CK’s database, this persistency technique (T1197[4]) has been observed in malware such as *UBOATRAT*.

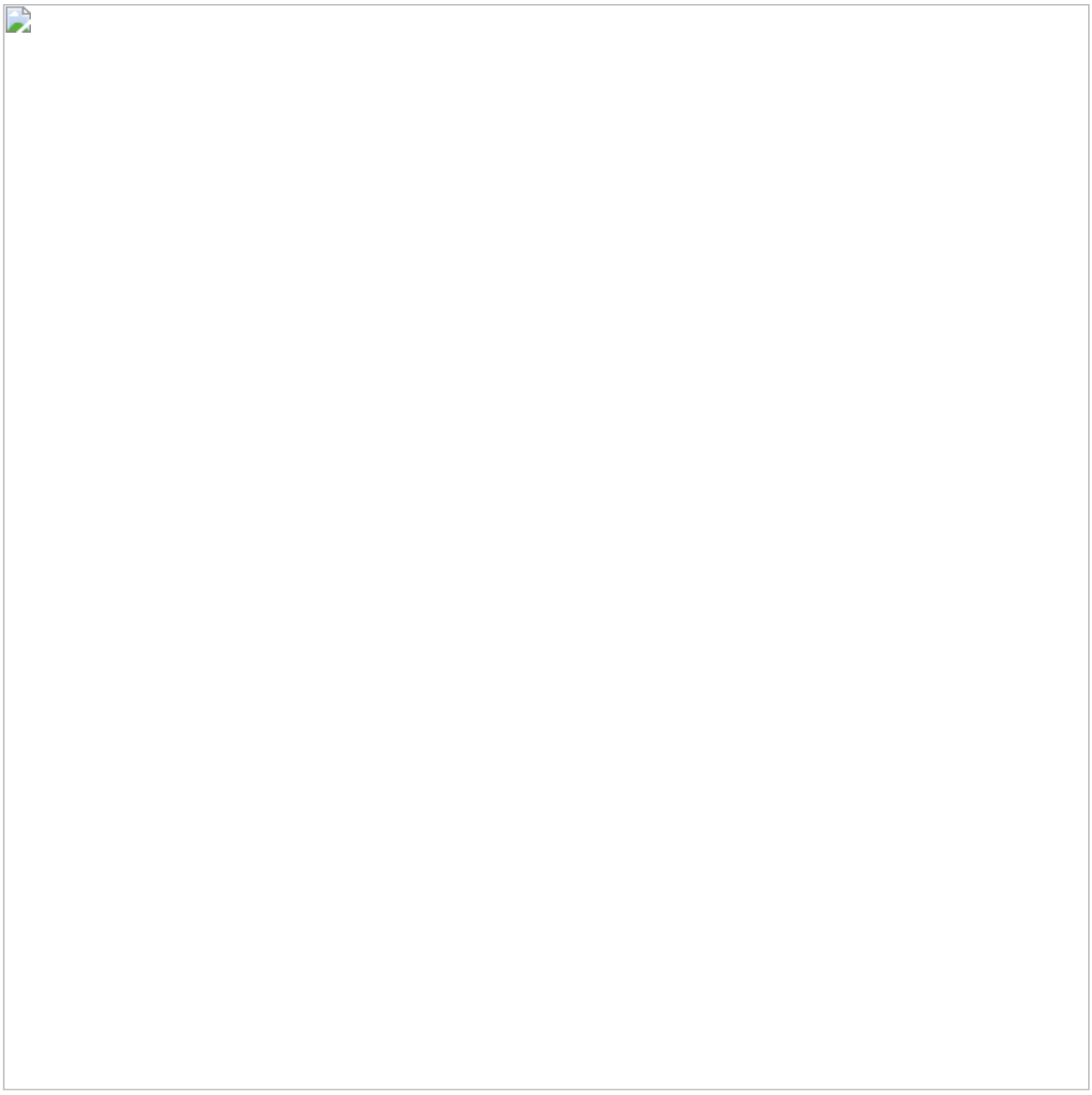


BB phones home

The sample accepts the following commands:



The sample sends data to the C2 in the following structure:

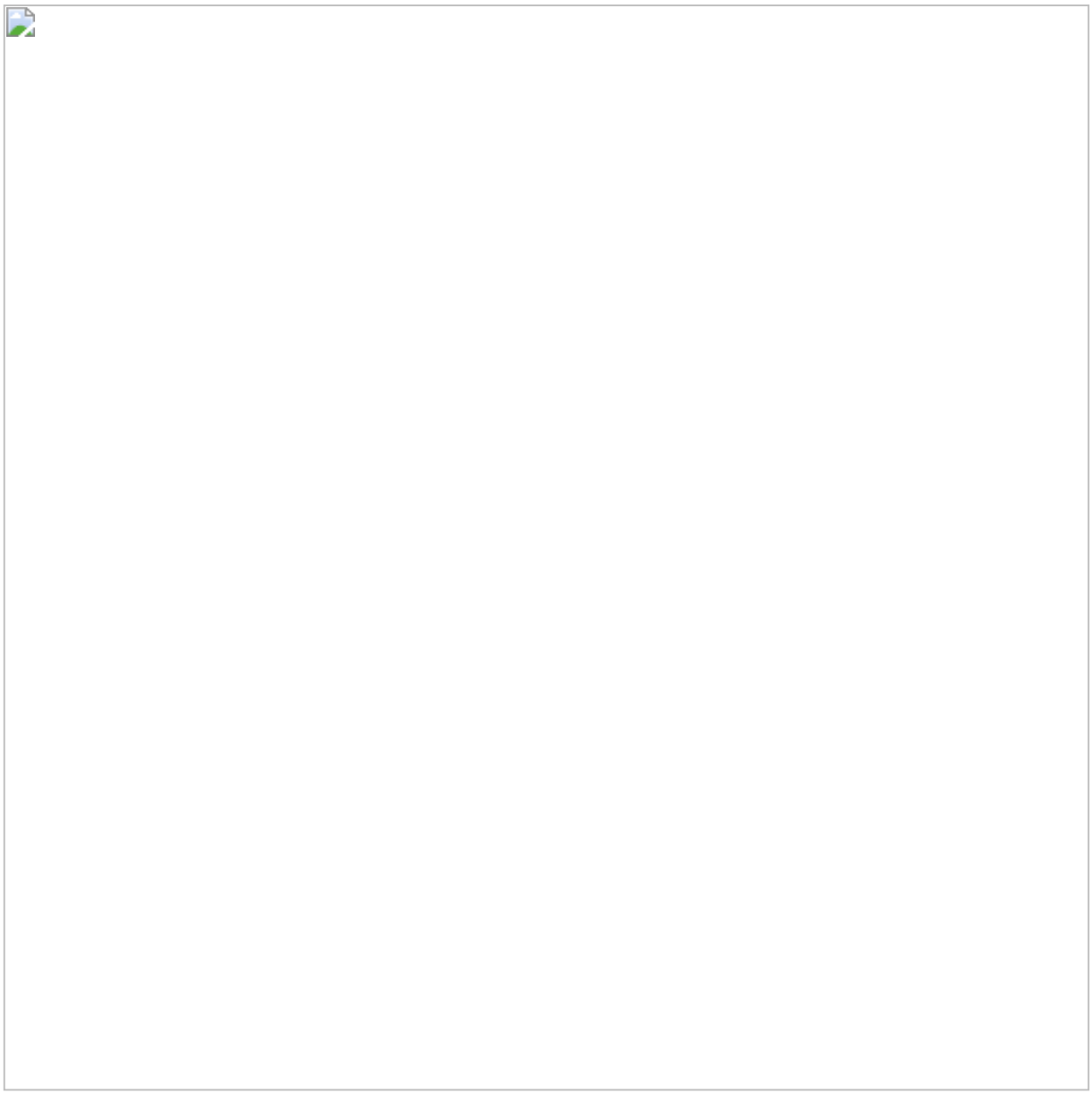


The algorithm used for compression is standard ZLIB v1.1.4.

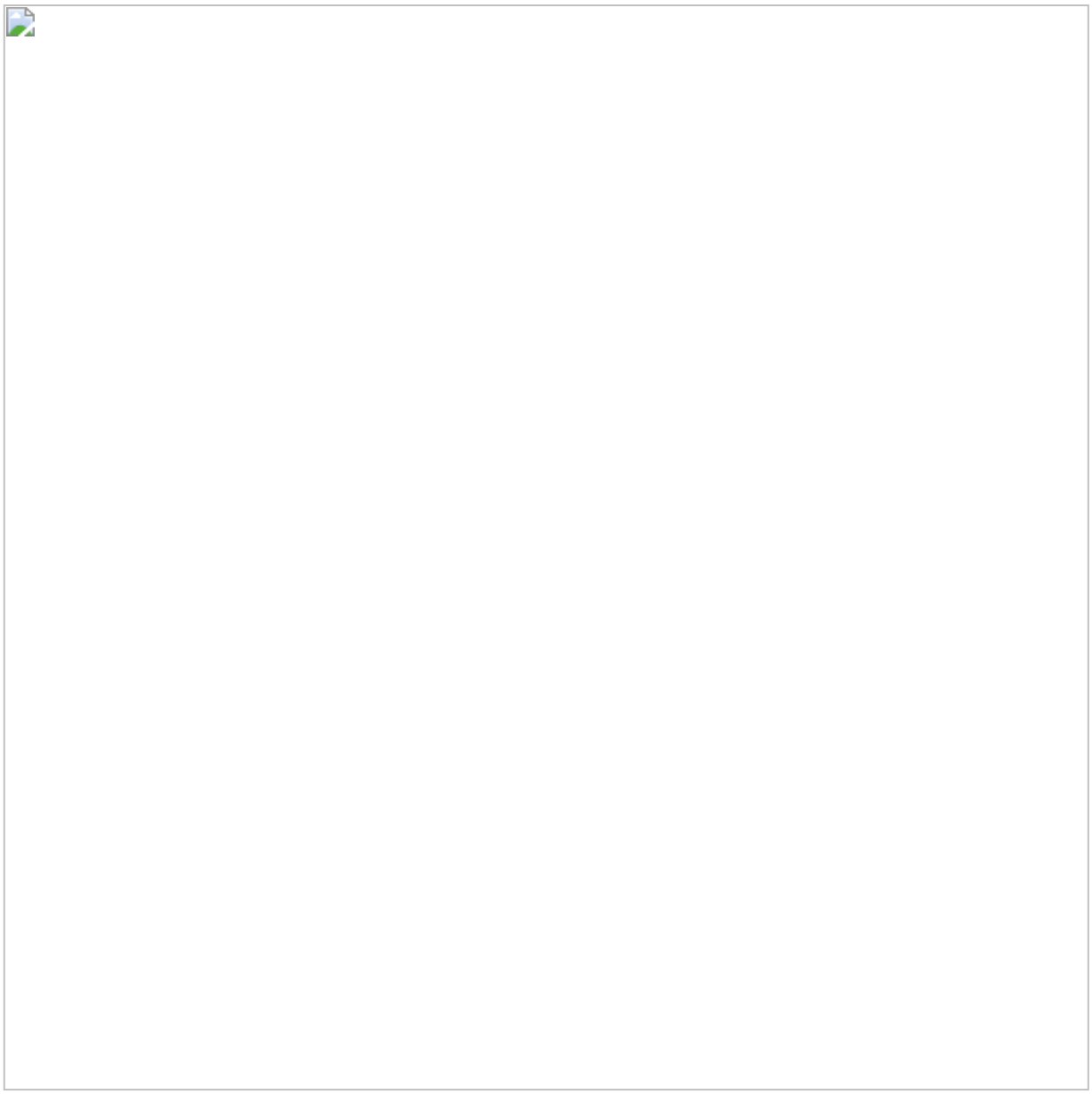
Yes! That's a !

Looking at the C2 commands supported, as well as the structure of the data communicated to/fro the C2, they bear strong similarities with the set of *BBSRAT* analyzed by Palo Alto Networks in 2015.

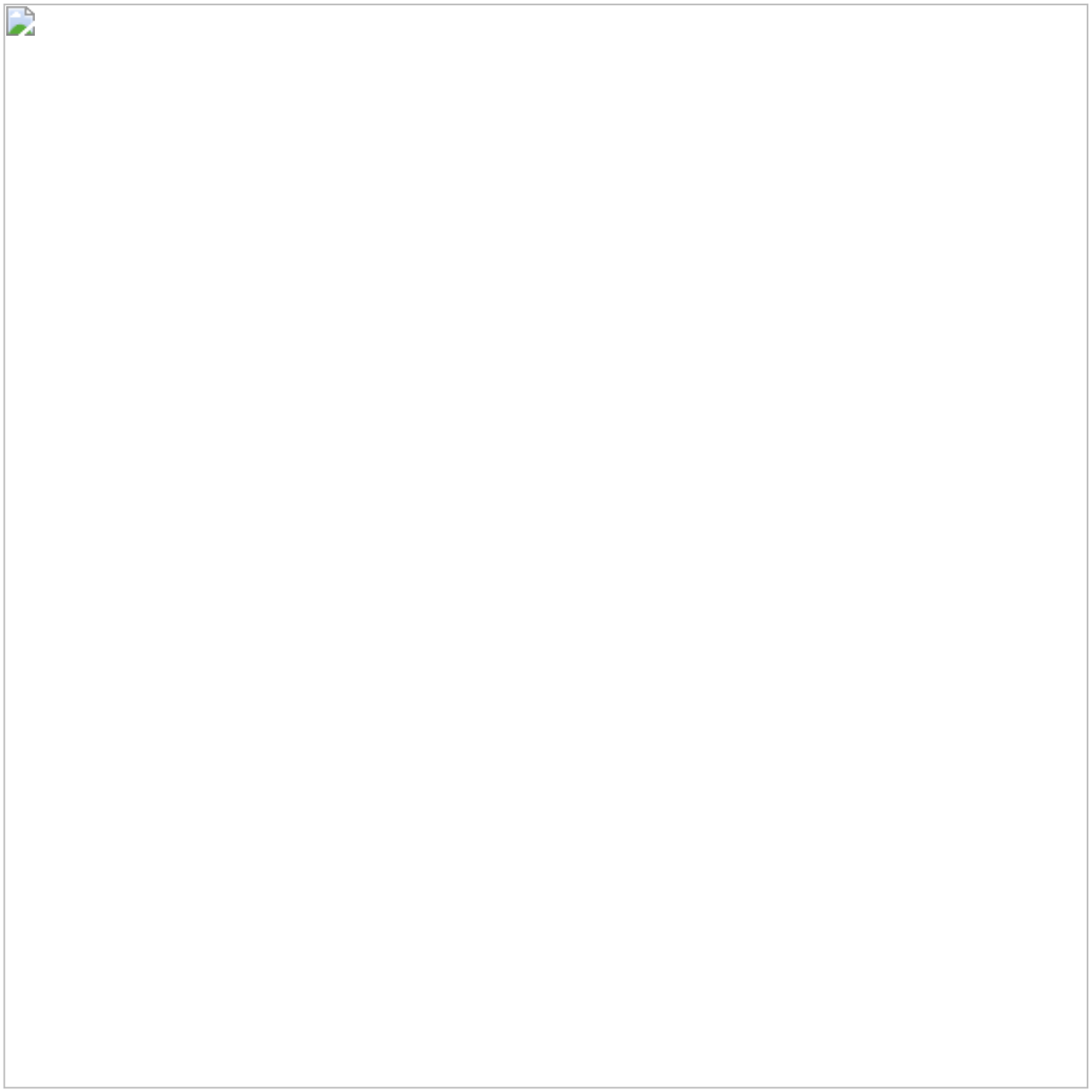
Furthermore, there are direct code overlaps/resemblance with one of the *BBSRAT* sample (MD5 8CD233D3F226CB1BF6BF15ACA52E0E36). Some of them are as follows:



Left: rain.sdb; Right: BBSRAT (Code logic that performs regular beaconing)



Left: rain.sdb; Right: BBSRAT (Code that receives and decompress data from C2)



Left: rain.sdb; Right: BBSRAT (Switch code that acts upon different C2 commands)

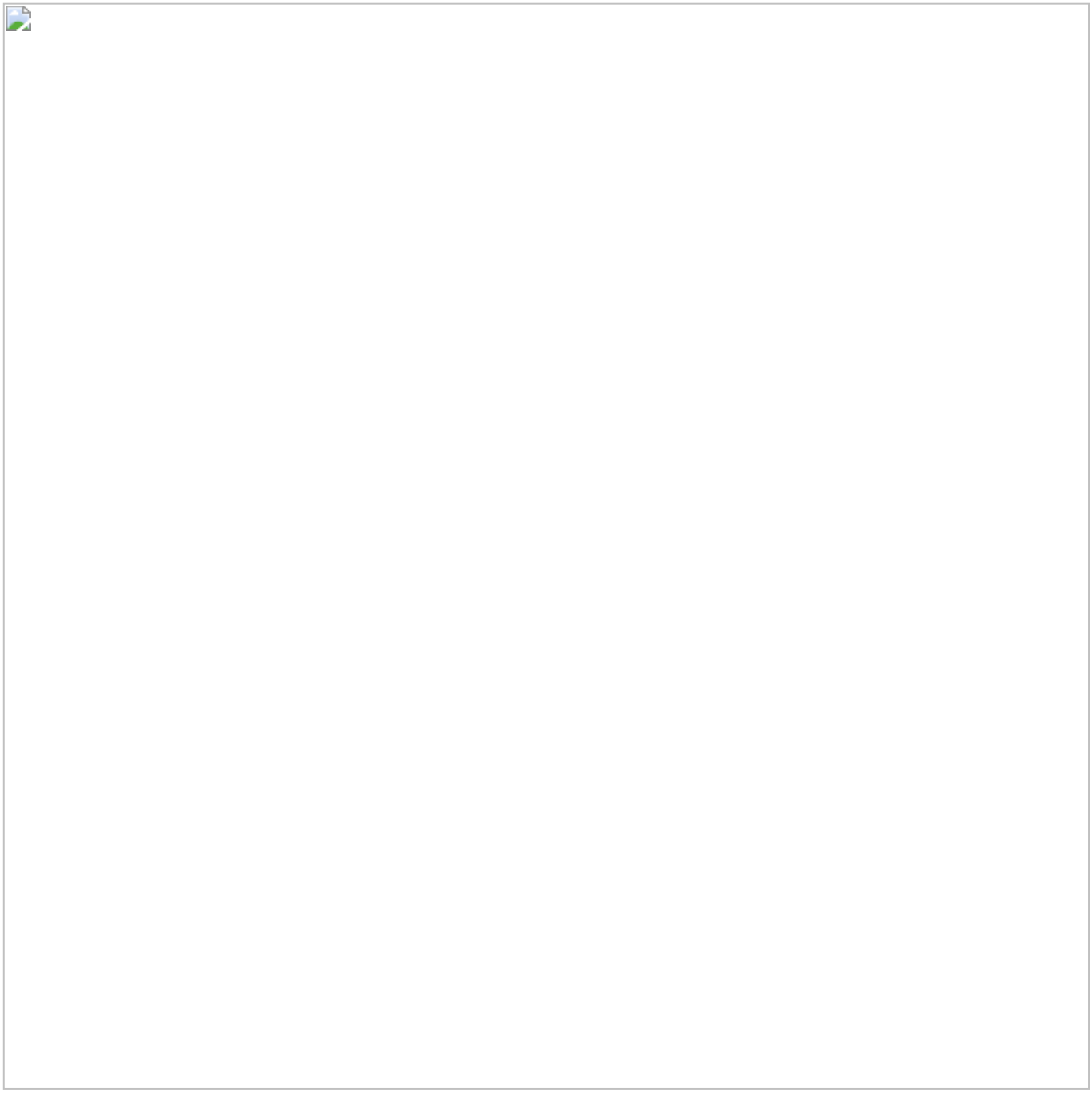
One obvious difference lies in the communications with the C2: the 2015 *BBSRATs*' beacons are HTTP requests (POST with data) that gave it its name (the beacons go to URL with the pattern /bbs/#/forum.php?sid=#); the rain.sdb sample analyzed does not do the HTTP requests, but instead send the compressed data directly to the C2 (on port 53). It may be likely that the change in port and the omission of communication "wrapper" is intentional to fool network signatures that look out for the suspicious URL. It is unknown however, if the backend *BBSRAT* supported port 53 all along, or it had been upgraded after 3 years.

Gh0stly shadows

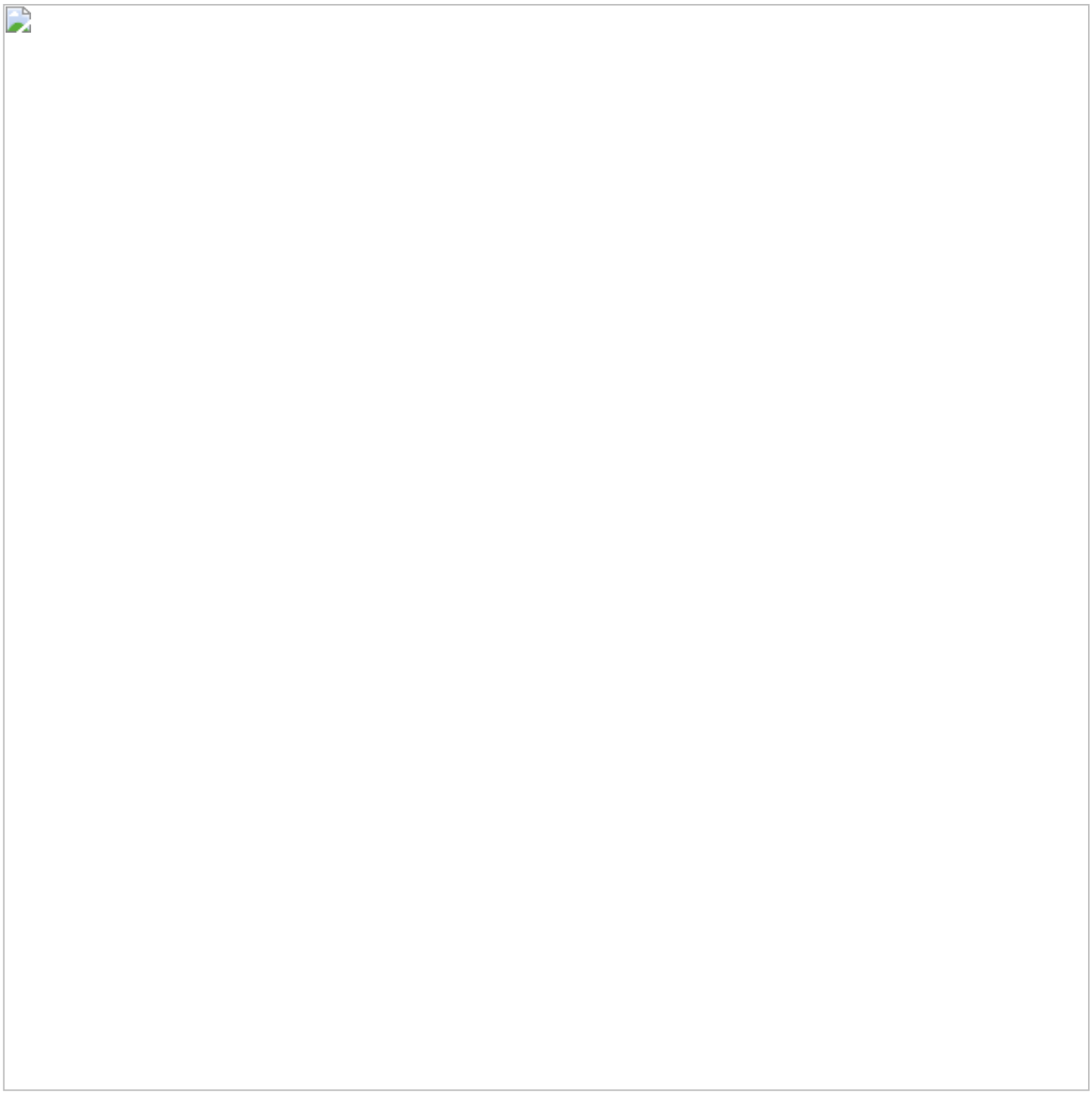
While doing the analysis of the samples, I've noticed some code overlap with another well-known RAT: the *Gh0stRAT*. *Gh0stRAT* is also listed as one of the tools used by the **Winnti Group**, though it is also known to be used by many other actors since its source code is readily available online. The overlaps are observed from the following file:

F0AB7E27B8DE336B14C8756E6CD41CEA rain.sdb

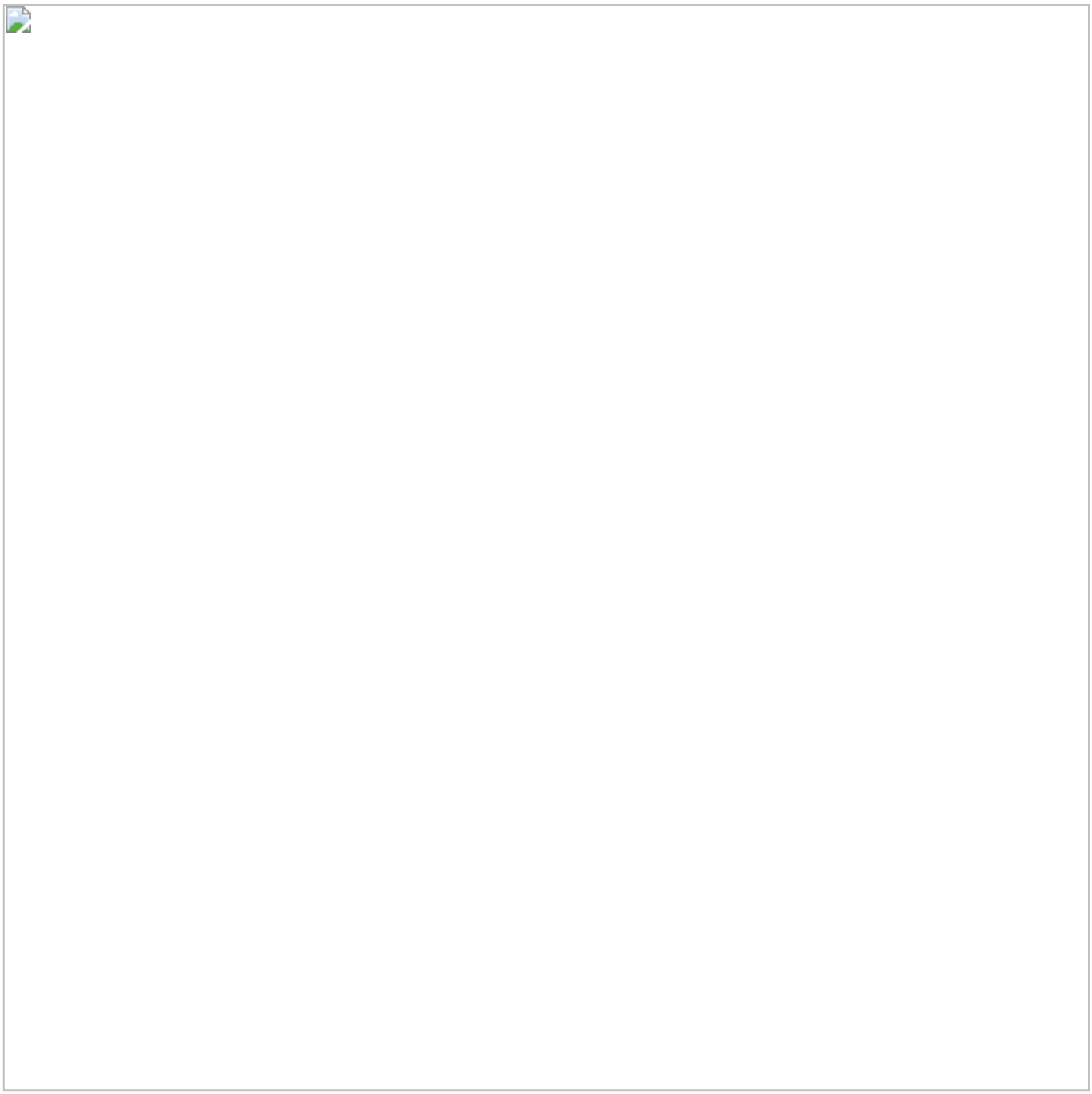
There are two modules within the sample that contains code highly similar to *Gh0StRAT*, one is screencapture (mapped to functions within “ScreenSpy” and “ScreenManager” in *Gh0stRAT*) and the other is shell (mapped to functions within “ShellManager”).



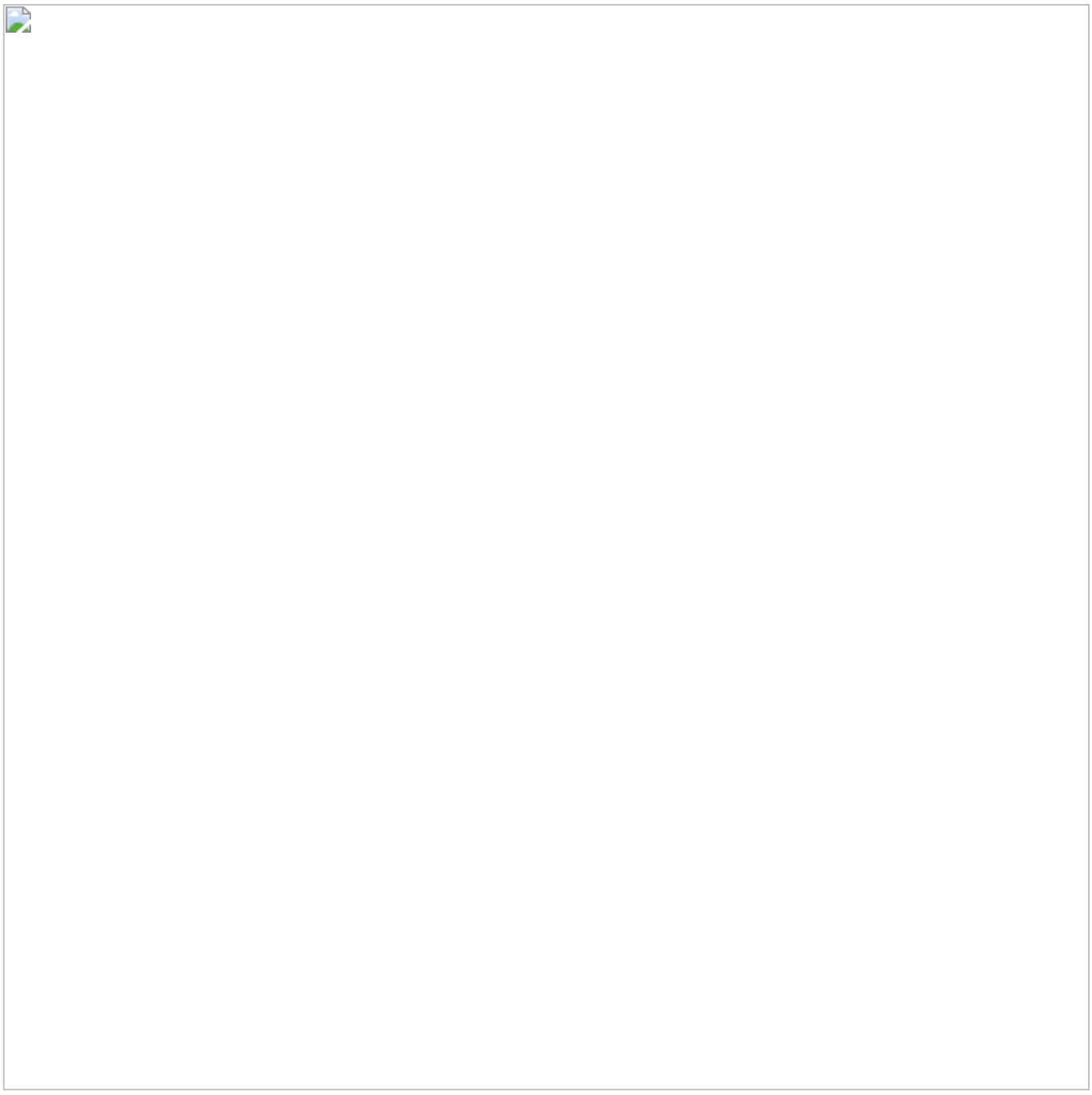
Two modules’ within rain.sdb that uses Gh0stRAT code



Left: rain.sdb; Right Gh0stRAT 3.6 Source Code Screenspy.cpp

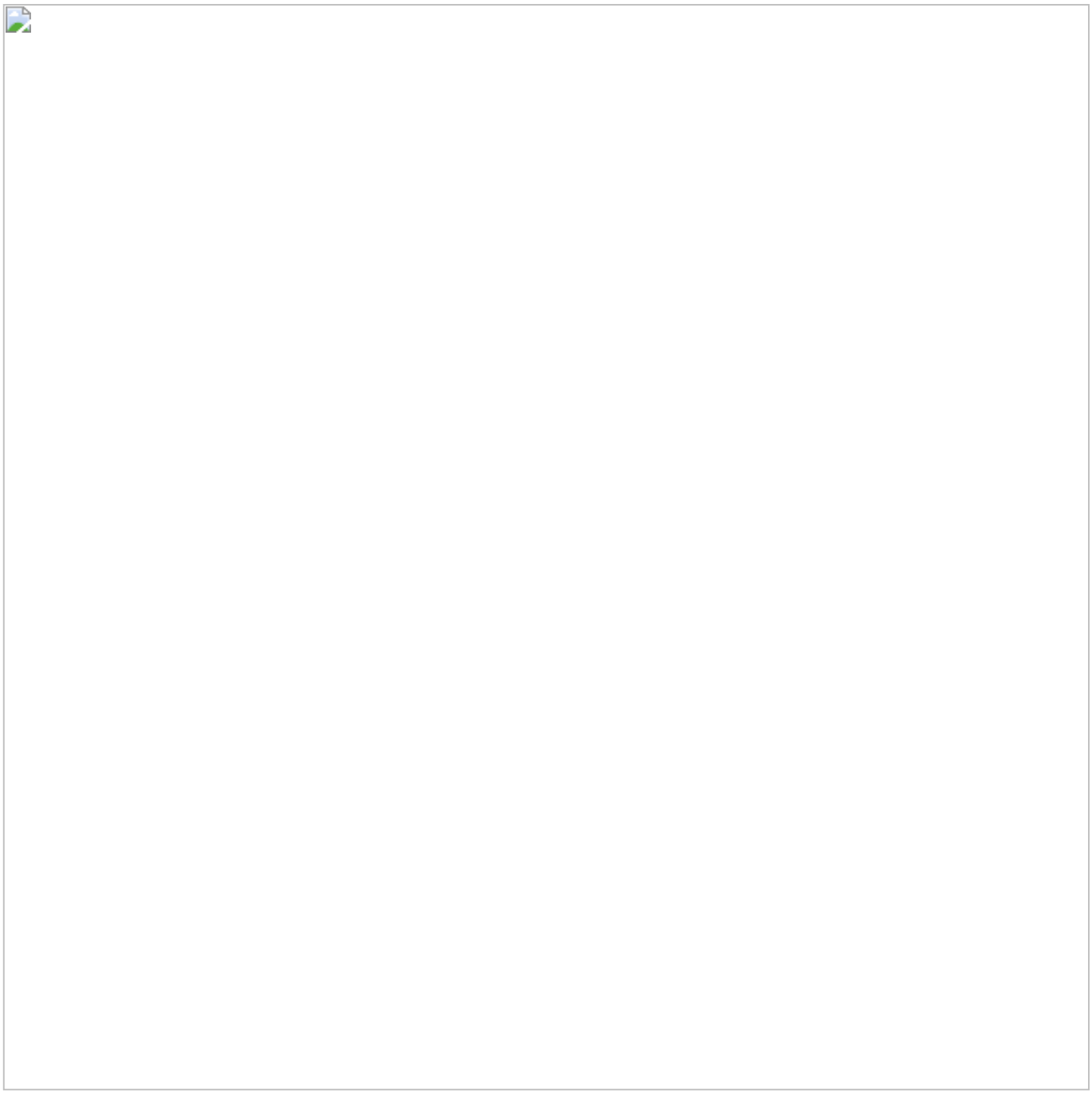


Left: rain.sdb; Right Gh0stRAT 3.6 Source Code Screenspy.cpp



Left: rain.sdb; Right Gh0stRAT 3.6 Source Code ShellManager.cpp

There is also a constructor that seem to come from *Gh0stRAT*'s source code:



Left: rain.sdb; Right Gh0stRAT 3.6 Source Code CursorInfo.h

Last Words

Judging based on the C2 callback and commands, the rain.sdb payloads are definitely a variant of *BBSRAT*. Perhaps the name *BBSRAT* is now not as descriptive as it was in 2015, since the callbacks are no longer HTTP requests to URLs resembling bbs forums.

I was not able to find samples from the **Winnti Group** that contain the mutexes mentioned by Trend Micro, if anyone has any of such samples please feel free to contact me;) I'll be happy to be able to do a matching to see if the binaries share any code!

References:

[1] “Operation DRBControl: Uncovering a Cyberespionage Campaign Targeting Gambling Companies in Southeast Asia”, Trend Micro, 18 Feb 2020

[2] “BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger”, Palo Alto Networks, 22 Dec 2015

[3] “Best Practices When Using BITS”, docs.microsoft.com/en-us/windows/win32/bits/best-practices-when-using-bits

[4] “T1197 BITS Jobs”, attack.mitre.org/techniques/T1197

~~

Asuna

The latest Tweets from Asuna (@AsunaAmawaka). [Malware Analyst]. Binary World

twitter.com

Drop me a DM if you would like to share findings or samples ;)