MM Core In-Memory Backdoor Returns as "BigBoss" and "SillyGoose"

blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

Introduction

by Nicholas Griffin and Roland Dela Paz

In October 2016 Forcepoint Security Labs™ discovered new versions of the MM Core backdoor being used in targeted attacks. Also known as “BaneChant”, MM Core is a file-less APT which is executed in memory by a downloader component. It was first reported in 2013 under the version number “2.0-LNK” where it used the tag “BaneChant” in its command-and-control (C2) network request. A second version “2.1-LNK” with the network tag “StrangeLove” was discovered shortly after.

In this blog we will detail our discovery of the next two versions of MM Core, namely “BigBoss” (2.2-LNK) and “SillyGoose” (2.3-LNK). Attacks using "BigBoss" appear likely to have occurred since mid-2015, whereas "SillyGoose" appears to have been distributed since September 2016. Both versions still appear to be active.

Targeted Regions and Industries

In 2013 MM Core was reported to target Middle Eastern and Central Asian countries. Our own telemetry suggests that both *Africa* and the *United States* have also been recent targets. The following list shows the targeted industries we have observed:

- News & Media
- Government - Defence
- Oil & Gas Manufacturing
- Telecommunications

MM Core Capabilities

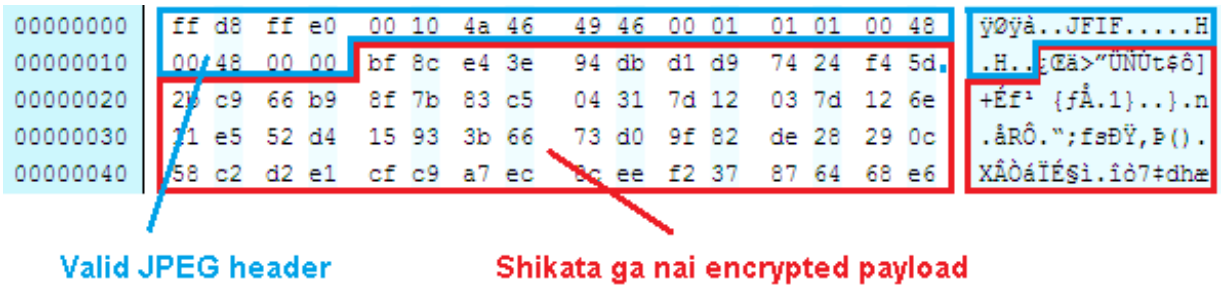
An overview of MM Core backdoor’s functionalities is as follows:

- Send infected system’s computer name, windows version, system time, running processes, TCP/IP configuration, and top level directory listings for drives C to H
- Download and execute file
- Download and execute file in memory
- Update itself
- Uninstall itself

Infection Method

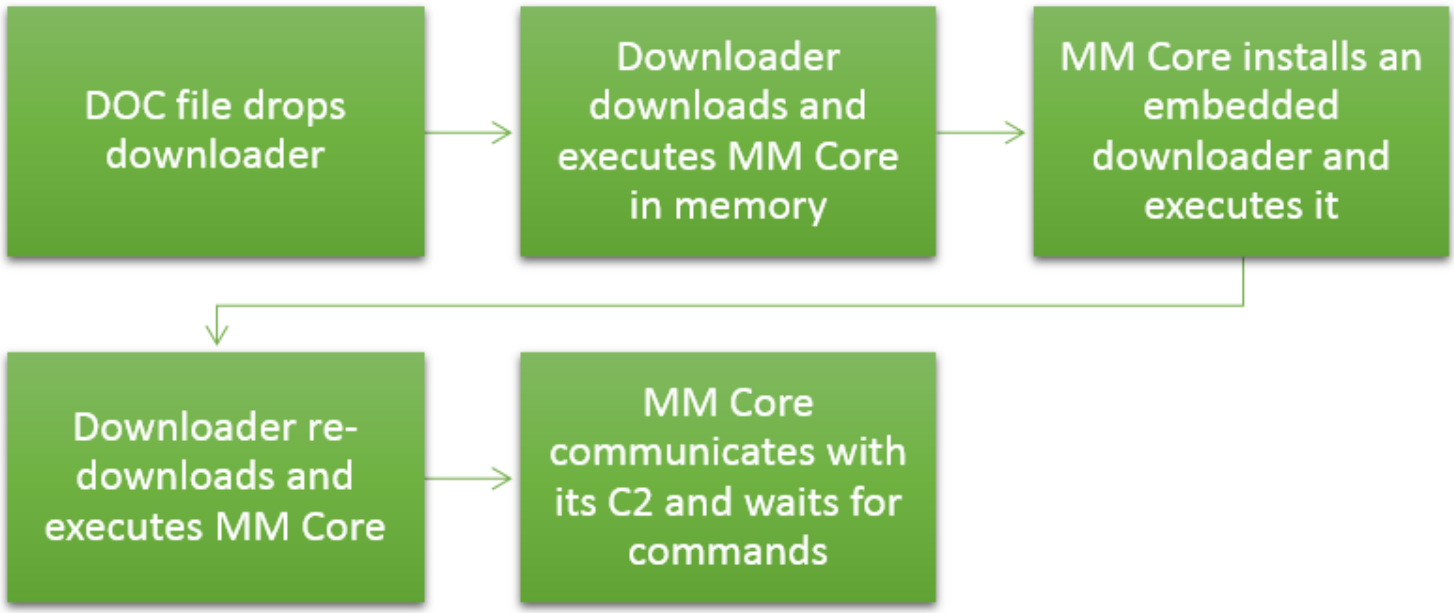
Previously the MM Core downloader component was downloaded and executed through shellcode by a DOC file exploiting CVE 2012-0158. However, the new DOC exploit we found exploits a more recent CVE-2015-1641 Microsoft Word vulnerability which it uses to extract embedded malware. The extracted malware is then executed by leveraging a *DLL side-loading* vulnerability.

The DOC file we analysed (SHA1 *d336b8424a65f5c0b83328aa89089c2e4ddbcf72*) was named “US pak track ii naval dialogues.doc”. This document exploits CVE-2015-1641 and executes shellcode which drops a legitimate Microsoft executable along with a trojanised DLL named “ChoiceGuard.dll”. The shellcode then executes the Microsoft executable, causing the malicious DLL to automatically be loaded into the file when it is run - hence the term "side-loading". The DLL downloads and executes the file-less MM Core backdoor in memory, which uses steganography to hide itself inside a JPEG file. The JPEG contains code to decrypt itself using the Shikata ga nai algorithm.



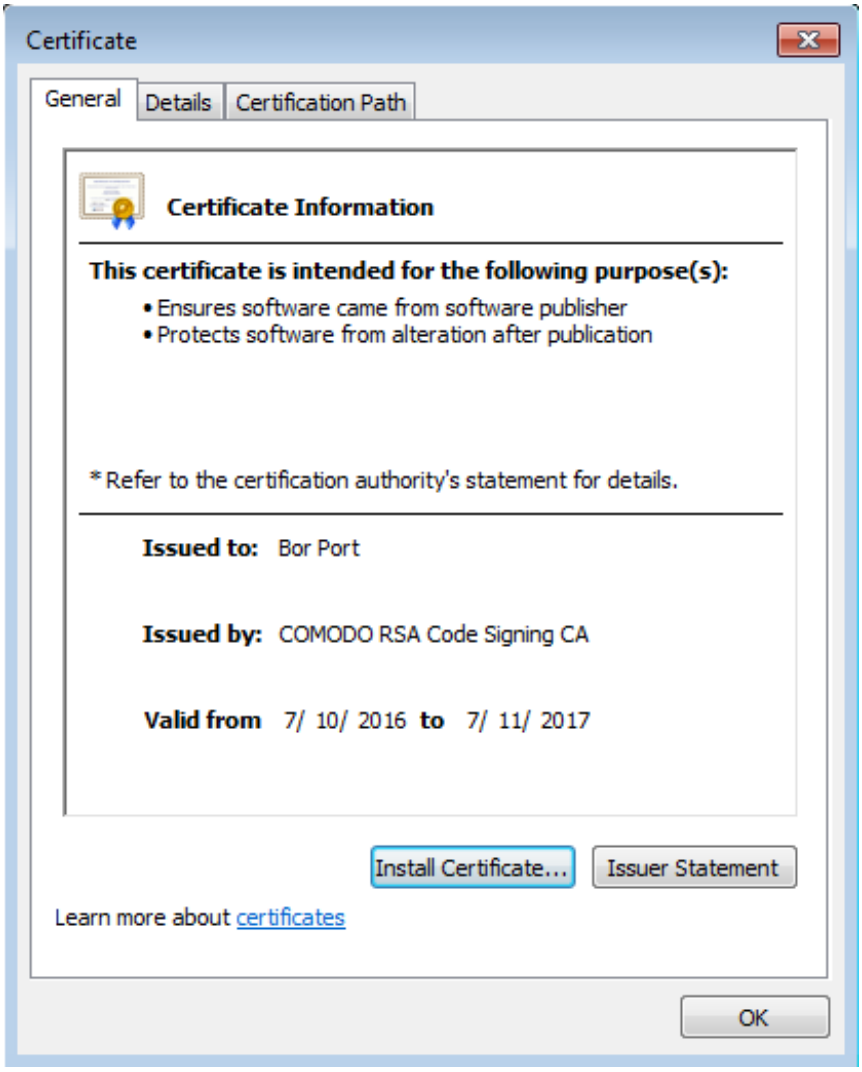
Once decrypted and executed in memory, the MM Core backdoor will extract and install an embedded downloader when it is first run and add it to Windows start-up for persistence. This downloader, which is similar to the first trojanised DLL, is then executed and will download the MM Core JPEG once again, executing it in memory like before. This time MM Core will conduct its backdoor routine which will send off system information and await further commands.

An overview of this infection process is as follows:



Valid Certificates

Some of the downloader components we found (i.e. "ChoiceGuard.dll") are signed with a valid authenticode certificate from Russian organisation "Bor Port":



We suspect that this may be a stolen certificate as it is very unlikely that a malware author would sign malware with their own organisation's certificate.

Updated Malware Artefacts

Newer versions of MM Core use updated version tags, mutexes, and filenames as compared with their 2013 counterparts. These are listed in the table below:

Version (Tag)	Mutex	Start-up File	Downloader Location
2.2-LNK (BigBoss)	4b336e4c79fad73936cde4a6bbc6c15c	%User Startup%\OracleJUP.lnk	C:\ProgramData\Sun18\bb18.dat
2.3-LNK (SillyGoose)	15c4b336e4c79fa6cd739bc36cde4a6b	%User Startup%\JustUpdtr.lnk	C:\ProgramData\Sun18\s23.dat

Evasion Tactics

The MM Core actors have made significant efforts to prevent security researchers from tracking their infrastructure. The first two versions of MM Core back in 2013 used spoofed registrant information in order to register the C2 domains, whereas the new campaigns use C2s registered using a registrant privacy protection service. This makes it more difficult to track the actors' infrastructure using WHOIS data.

The actors have also registered their domains on BigRock, a popular web hosting company, in order to blend in with the noise of legitimate sites that are hosted on the same infrastructure.

Forcepoint Protection Statement

Forcepoint™ customers are protected against this threat via TRITON® ACE at the following stages of attack:

- Stage 5 (Dropper File) - The malware components are prevented from being downloaded and/or executed.
- Stage 6 (Call Home) - Network traffic used by the downloaders and MM Core is identified and blocked.

Conclusion

MM Core is an active threat targeting multiple countries and high profile industries. It is interesting to note that even though MM Core's version has incremented twice, the core backdoor code has remained almost the same apart from the new file and mutex names. Largely this is perhaps due to the file-less nature of its payload, which may also explain why the majority of the updates were in the delivery mechanism. At the same time this demonstrates that the attackers behind MM Core very well know what they are doing, updating the malware just enough to keep their operation under the radar after all these years.

On the other hand, while the volume of related MM Core samples remain low, we noticed that the MM Core downloader shares code, techniques and network infrastructure with a trojan called "Gratem", as well as sharing the same authenticode certificate for recent samples. Gratem is a more active downloader malware family which has been distributed since at least 2014. Ultimately this suggests that MM Core may be a part of a larger operation that is yet to be fully uncovered.

Indicators of Compromise

Documents

```
d336b8424a65f5c0b83328aa89089c2e4ddbcf72 (US pak track ii naval dialogues.doc)
```

Dropper/Downloader Samples (SHA1)

```
f94bada2e3ef2461f9f9b291aac8ffbf81bf46ab
ef59b4ffc8a92a5a49308ba98cb38949f74774f1
1cf86d87140f13bf88ede74654e01853bae2413c
415ad0a84fe7ae5b88a68b8c97d2d27de5b3aed2
e8bfa4ed85aac19ab2e77e2b6dfe77252288d89b
f94bada2e3ef2461f9f9b291aac8ffbf81bf46ab
83e7b2d6ea775c8eb1f6cfefb32df754609a8129
b931d3988eb37491506504990cae3081208e1a66
7031f4be6ced5241ae0dd4315d66a261f654dbd6
ab53485990ac503fb9c440ab469771fac661f3cc
b8e6f570e02d105df2d78698de12ae80d66c54a2
188776d098f61fa2c3b482b2ace202caee18b411
e0ed40ec0196543814b00fd0aac7218f23de5ec5
5498bb49083289dfc2557a7c205aed7f8b97b2a8
ce18064f675348dd327569bd50528286929bc37a
3a8b7ce642a5b4d1147de227249ecb6a89cbd2d3
```

21c1904477ceb8d4d26ac9306e844b4ba0af1b43
f89a81c51e67c0bd3fc738bf927cd7cc95b05ea6

MM Core Unpacked DLL Samples (SHA1)

13b25ba2b139b9f45e21697ae00cf1b452eeeff5
c58aac5567df7676c2b08e1235cd70daec3023e8
4372bb675827922280e8de87a78bf61a6a3e7e4d
08bfdefef8a1fb1ea6f292b1ed7d709fbbc2c602

Related Gratem Samples (SHA1)

673f315388d9c3e47adc280da1ff8b85a0893525
f7372222ec3e56d384e7ca2650eb39c0f420bc88

Dropper/Downloader Payload Locations

hxxp://davidjone[.]net/huan/normaldot.exe

MM Core Payload Locations

hxxp://mockingbird.no-ip[.]org/plugins/xim/top.jpg
hxxp://presspublishing24[.]net/plugins/xim/top.jpg

hxxp://ichoose.zapto[.]org/plugins/cc/me.jpg
hxxp://presspublishing24[.]net/plugins/cc/me.jpg

hxxp://waterlily.ddns[.]net/plugins/slm/pogo.jpg
hxxp://presspublishing24[.]net/plugins/slm/pogo.jpg

hxxp://nayanew1.no-ip[.]org/plugins/xim/top.jpg
hxxp://davidjone[.]net/plugins/xim/top.jpg

hxxp://hawahawa123.no-ip[.]org/plugins/xim/logo.jpg
hxxp://davidjone[.]net/plugins/xim/logo.jpg

MM Core C2s

hxxp://presspublishing24[.]net/plugins/cc/mik.php
hxxp://presspublishing24[.]net/plugins/slm/log.php
hxxp://presspublishing24[.]net/plugins/xim/trail.php

Gratem Second Stage Payload Locations

hxxp://adnetwork33.redirectme[.]net/wp-content/themes/booswrap/layers.png
hxxp://network-resources[.]net/wp-content/themes/booswrap/layers.png

hxxp://adworks.webhop[.]me/wp-content/themes/bmw/s6.png

hxxp://adrev22[.]ddns.net/network/superads/logo.dat
hxxp://davidjone[.]net/network/superads/logo.dat