Katana: a new variant of the Mirai botnet

prod-blog.avira.com/katana-a-new-variant-of-the-mirai-botnet

October 20, 2020

Avira's IoT research team has recently identified a new variant of the Mirai botnet. It has been named **Katana**, after the Japanese sword.

Although the Katana botnet is still in development, it already has modules such as layer 7 DDoS, different encryption keys for each source, fast self-replication, and secure C&C. There are indications that katana may be associated with an HTTP banking botnet in the future.

We've previously looked at how Mirai, an IoT botnet, has evolved since its source code became public. A recent analysis of IoT attacks and malware trends shows that Mirai's evolution continues. For example, variants of Mirai can be bought, sold, or sourced via YouTube channels, in this case, VegaSec. These, and other changes, enable unskilled attackers to create malicious botnets, resulting in an increase in attacks.

Analysis

The Katana botnet attempts to exploit old vulnerabilities via Remote Code Execution/Command Injection vulnerabilities such as LinkSys and GPON home routers. For the last two weeks, a surge of malware binaries has been captured by our honeypot, and it was this that encouraged us to have a closer look.

Although Katana uses old exploits (we assume it is in the testing/development stage), it still attracted our attention because:

- It is actively infecting hundreds of devices daily,
- There are interesting features associated with this botnet

Over a period of time, the botnet is being downloaded with different IPs. The figures below show how it is downloaded:

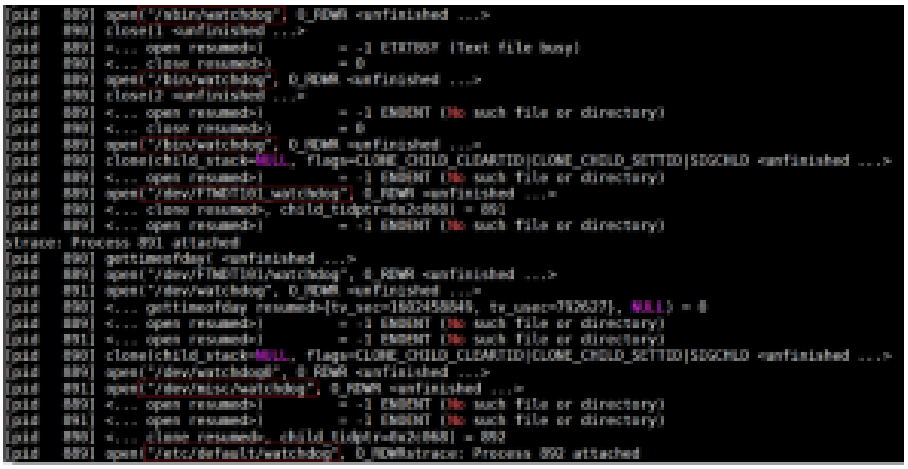
05-10-2020

08-10-2020

12-10-2020

During our analysis, we found that the botnet runs as a single instance by binding different ports, i.e., **53168**, **57913**, **59690**, **62471,** and **63749**. One such example is shown below:

The botnet tries to manipulate the watchdog and prevents the device from restarting. The figure below shows as follow:



In short, Katana retains several Mirai features. These include running a single instance, random process name, manipulating the watchdog to prevent the device from restarting, and DDoS commands. The botnet also configures the **iptables** to drop access to port **37215** of an affected device.

Similar to Mirai, the botnet also supports DDoS commands:

attack_app_http
attack_get_opt_int
attack_get_opt_ip
attack_get_opt_str
attack_gre_eth
attack_gre_ip
attack_init
attack_kill_all
attack_method_http
attack_method_std
attack_method_tcpack
attack_method_tcpstomp
attack_method_udpgeneric
attack_method_udpplain
attack_method_udpvse
attack_ongoing
attack_parse
attack_start
attack_tcp_ack
attack_tcp_stomp

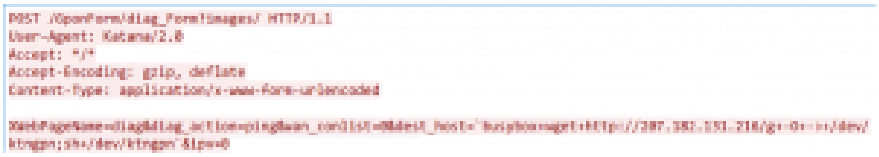
attack_tcp_syn
attack_udp_dns
attack_udp_generic
attack_udp_ovhhex
attack_udp_plain
attack_udp_stdhex
attack_udp_vse

attack_app_http suggests that the botnet is in fact an http botnet. Furthermore, the functions (highlighted bold above) apparently are new commands that this new botnet leverages for its attack.

Network Analysis

Like Mirai, this new botnet targets home routers like GPON and LinkSys via Remote Code Execution/Command Injection vulnerabilities.

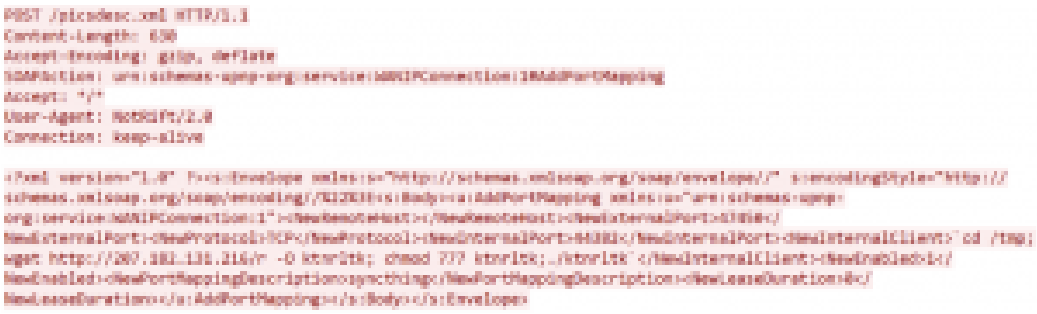
During our analysis, we discovered that it is possible to bypass authentication by simply appending "*?*images" to any URL of the device that requires authentication. In this way, an intruder can manage the device. Traffic below shows how this happens:



During our analysis, we observed that there is a binary CGI executable (*tmUnblock.cgi*) found in some LinkSys routers. This has multiple security holes that permit various attacks on the router. The malware tries to exploit the router via a vulnerable CGI script, as shown below:

The authentication is base64 encoded that is decoded as login: password.

The botnet also tries to exploit different devices that use the **RealTek SDK with miniigd deamon,** which is vulnerable to OS command Injection in the UPnP SOAP Interface. Traffic is shown below:



The Katana botnet also tries to communicate to its following C2 servers:

- 100cnc[.]r4000[.]net
- 1280x1024cnc[.]r4000.net

At this time, the Katana botnet is actively infecting hundreds of devices each day. The following are the top 3 as per our stats until now.

- DSL-7740C DLink
- DOCSIS 3.1 Wireless Gateway
- Dell PowerConnect 6224 Switch

Conclusion

It is important to safeguard IoT endpoints installed in consumer environments. The industry needs to start adopting best practices to improve device security to ensure that their IoT devices are reliable products and are regularly patched.

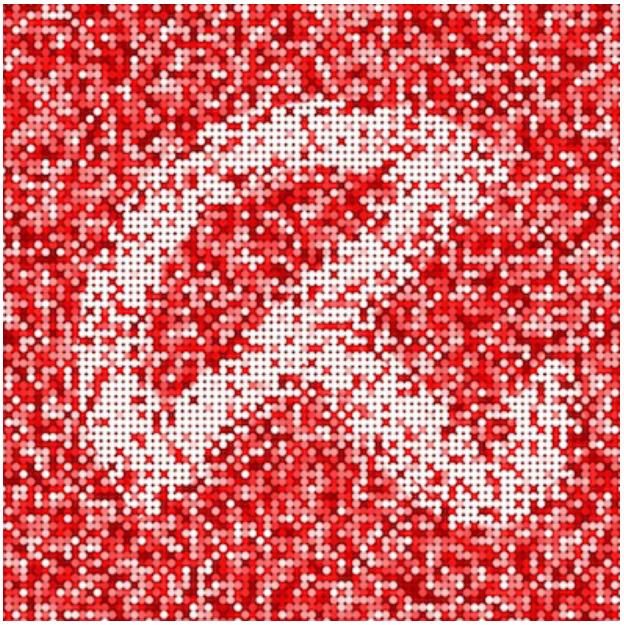
The Avira IoT Research team monitors such new malware families or variants and provide detections for them. Integrating Avira SafeThings and anti-malware technologies can help protect customers from such attacks.

IoCs

Sha256	Target Architecture	Debugging Info
1a8f57c659393b6153d1db58863e2ed99e4505ac89c3cdc5064fc0468a6af740	Intel 80386	stripped
20e5d75056aad8120a3d5bd70910387c02f3bfad5ff7a2f414a223c632927be3	Intel 80386	stripped
4625702c98b9db0fafa1f82647288ccb3afd1e640d3b74199a475e60298ccaba	Renesas SH	stripped
4ecdc38a758773baa1813d8960bb5bf9d4b574526eb6ce09ff04041ad913632c	ARM	with debug_info
607d0a502c0659f31640440fbde3c7ad0c73e208b8e961b0ec038514d0d0b555	ARM	with debug_info
738e80232501dcae0e5ff8dc50a30cc1350f555294b637167dfe1f88cb58b7c1	Motorola m68k	statically linked
8aa7c90ddbaa213f12d4e3bfe2c37cf2593e09008493024a609e5a55cd5abdef	PowerPC or cisco 4500	stripped
9751b5d280c6f7b4ee084ecd7ad51e3dc36cfecbfa837acc388d608d39885b12	x86-64	stripped
be59eaf0ab86c8dd6cad03e772550edf4342fdb63762a8cb44dee3f421bd206c	ARM	with debug_info
d8dd74cf72ff9ef46e2453f4da442a235493e95eb65ff0ff87c60b9dc93ad0d5	ARM	with debug_info
e18c367fe9fb480067173e557606ea7165a9347977311bebcb1d8e05a141f0ed	Intel 80386	stripped
fb6b1d45a0393d609c8d0de355717585ee32eac7495ecb65ddcf0eefcbae05d1	ARM	with debug_info
05666fef3489f9860b795493128da03eaea4d86f4bd6eef614e5ec575169ba20	x86-64	stripped

17712da0934af383baa501ee6f23bea4489707b70d155c807f96e7acc0cbd003	PowerPC or cisco 4500	stripped
203fed7435fb3f8428e57c798b17f30c4eba7b649c0ebf842cbba39499817739	Renesas SH	stripped
2e809192edf97c96eef0005d5fddbfe14ac1d1a4e9c868c29990849432190310	ARM	with debug_info
34ed813148775b3aa0d817fc383d77117972d3055fe813387f7371a50c2dc135	Intel 80386	stripped
37336a15c1757b0f5ddc4ec9cb581e0d333968c5885169871d5b7d80b736cafd	ARM	with debug_info
41e608eaa115b8a9bb326d208592b2657a5978b96ad83c44c66dd0062d589351	ARM	with debug_info
47eddc780e2378a48d5874b9b9e367284f78929dad1dc1a06daf6b99cc1c0466	Renesas SH	stripped
7691f6540c8fb964c5c6aeeee7bd7c8120654d27a474d74be03620164e70a7b7	MIPS	stripped
7af99a666c01aee840f86f89bf9e978553c2f104ba53b63099b3eb060068130c	x86-64	stripped
7f7630859e53161ee167b7ed7c23bc0367307638900dd5a1f9d495683047aa97	Intel 80386	stripped
86ef3b56079c51266e90e1c139675a4e62005612275b97f61cee168a2e47b189	Intel 80386	stripped
9c0c968f5a5277598bc7cfbfab419805c96a587d5a560492f02423f0567b9bae	Intel 80386	stripped
b06dc2342230b7ad67d9f18589bca482263c0a0ef4876cc141e3afcc09a47dc8	Motorola m68k	statically linked
cf168849329fdc05bebe2fc256de7c2afaf9a31c54696e47f2b42c42276acd2d	Intel 80386	stripped
e7bbc103496c541b25754d1e3d69dd61f5462c7a49243b65c3c2c12f8a9785f1	PowerPC or cisco 4500	stripped
ef2f9458b49cf85cf9e807f6dca0c19c78923f71308b6dd61fff971c89cb0f34	Intel 80386	stripped
f109945be0837375bf78a2cee25e20d1167c2add57d0f1aeb982375f672b4352	MIPS	stripped
ff4206109cdaa560eedfeec302616bfc5818ea16adb4e600b3c5007d3fe12501	Motorola m68k	statically linked
1adc1afc26772698e2d0894b25aa16dc3ce9dd70418acb65dda5d12d7e9da31c	Motorola m68k	statically linked
289a20c1d4685c3080ef2c9154dc6340572e4475454e919364e756d1609fee17	MIPS	stripped
37f27fbbac1836d0289bc90bb56c32492b77a4af885e26f065211003ab0c60bd	ARM	with debug_info
6240c85359cc9b97b6e8db08bf5ddab61a19c6ba04970bd3feb6b5792a6ee6c1	MIPS	stripped
7440ee28417403cd69d3e1489866330bcc96079c157bb737004ee0d54c81d254	x86-64	stripped
96a4771ed0bf8802057e654e02d524acea5eb042c41287db5eb8acd4092b47c5	PowerPC or cisco 4500	stripped
9b5be5ce331e1300b36b6929901d8bfccd2fdaa44382b9ef3695779d5fa21b06	Intel 80386	stripped
b9c7a0d43e4d49393669392fdeab45da0991b690d5f03d73f27ce9e17463fb87	Intel 80386	stripped
d18330c627f034226bfa2fcd5a38748496c3ae9b9877aadd763ead65a7c1bbd3	Intel 80386	stripped
da308d1b3d8123ca2f3ebfe1115158a2e2c1a184aa608ff72c192fc333bb3d9c	Renesas SH	stripped
e2a40a2b24850d78e694868f3cafb541374662501c37cac02888eebf98c128ed	ARM	with debug_info

This post is also available in: GermanFrenchItalian



Avira Protection Labs

Protection Lab is the heart of Avira's threat detection and protection unit. The researchers at work in the Labs are some of the most qualified and skilled anti-malware researchers in the security industry. They conduct highly advance research to provide the best detection and protection to nearly a billion people world-wide.