SECURITY BULLETIN:
DD4BC OPERATION PROFILE

1.1 / OVERVIEW / DD4BC, a malicious group responsible for several Bitcoin extortion campaigns last year, is expanding its extortion and distributed denial of service (DDoS) campaigns to target a wider array of business sectors. In recent days, two Akamai customers have fallen into its crosshairs. Akamai’s Prolexic Security Engineering and Research Team (PLXsert) has conducted new research into DD4BC in recent weeks.

DD4BC appears to use Google IP address ranges, and in some cases AppEngine instances, in its attacks. It appears to use common UDP reflection DDoS attack techniques, as well as SYN floods that spoof Google crawler IP addresses, to mask the malicious traffic.

In one threat, DD4BC claimed it had the firepower to launch 400+ Gbps DDoS attacks, though there is no concrete proof it could carry out an assault of that size.

Late last year, the group repeatedly tried to blackmail Bitcoin exchanges and gaming sites – threatening victims with DDoS attacks in order to extort bitcoins. Campaigns typically consisted of an email informing the victim that a low-level DDoS attack was underway against the victim’s website. Emails explained that the DDoS activity could be observed in server logs at low levels in order to not interrupt the victim’s operations. Following this explanation, DD4BC demanded a ransom paid in bitcoins in return for protecting the site from a larger DDoS attack capable of taking down the website.

The targets seemed to have been chosen for their reluctance to involve law enforcement – entities associated with illegal gaming activity or unregulated digital cryptocurrencies, commonly referred to as bitcoins. Given the illegal and/or unregulated nature of their activities, the sites typically do not want to invite the scrutiny of law enforcement.

But given the new threats against Akamai customers, who operate in legal and legitimate business operations, DD4BC appears to be more willing to go after bigger fish – even if it brings the attention of law enforcement.

In an earlier version of this bulletin, we discussed how chaotic actors were exploiting Google services as part of their operations. Some have misconstrued it as Google backing a botnet. To be clear, Google has no part in this activity, and certainly does not condone such activity.

Based on UDP reflection traffic originating from Google IP address ranges, in the latest wave of DD4BC activity, attackers appear to be targeting reflectable services deployed on Google’s AppEngine platform. The attackers may be spinning up Google trial services, deploying reflectable services, and then leveraging the services in their reflection DDoS attacks. This theory is based the observation of exploitable services disappearing after attacks have run their course.
PLXsert has identified about four campaigns against seven Akamai customers where legitimate Google crawler IP addresses were spoofed in SYN floods that helped mask the malicious traffic but could also have long-term impacts on businesses’ search engine rankings if long-term IP blocking were applied. Booter and stresser tactics also appeared to be used as weapons in the latest attacks.

The group is aware that would-be victims may change their IP addresses to defend themselves and has threatened to retaliate. One victim received the following message (Figure 1):

“Changing IPs will not help.”

“Change IP once again and price goes to 20 BTC instantly.”

Figure 1: DD4BC warned a victim not to change IP addresses

1.2 / SAMPLE EXTORTION CAMPAIGN / In one set of exploits, DD4BC had a clear objective of obtaining Bitcoins from online gaming institutions. As the attackers increased their range of victims, they also increased the price of their ransoms. In emails directed at one particular online gaming institution, the initial ransom was 100 BTC, a market value of about $22,000, much larger than what was requested previously (1-10 BTC).

In an email threat against the two sites, shown in Figure 2, DD4BC wrote, “sites are going under attack unless you pay 10 Bitcoin. Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don’t even bother.”

From: DD4BC Team <dd4bct@gmail.com><mailto:dd4bct@gmail.com>>
Date: Thursday, April 16, 2015 at 6:54 AM
Subject: Re: DDOS ATTACK!

And it’s just TCP flood. In case of massive UDP flood, it’s even possible that your ISP will shut down your link to protect other customers.

Stopping for now. You have a few hours left.

On Wed, Apr 15, 2015 at 4:47 PM, DD4BC Team <dd4bct@gmail.com> wrote:

Hello,

To introduce ourselves first:


http://bitcoinbountyhunter.com/bitalo.html

Or just google “DD4BC” and you will find more info.

So, it’s your turn!

All <redacted> sites are going under attack unless you pay 100 Bitcoin.

Pay to 1NhLM43duL2J2tBx2qQwBojEm5fNSoMEp

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don’t even bother.

Right now we are running small demonstrative attack just on your <redacted>

Don’t worry it will stop in 1 hour.
It’s just to prove that we are serious.

We are aware that you probably don’t have 100 BTC at the moment, so we are giving you 24 hours to get it and pay us.

It’s easy to get BTC from Webmoney. Just exchange WMZ to WMX and make withdrawal request to our BTC address at https://wmx.wmtransfer.com/en-US/Home/Withdraw#

Or check this for best exchanger: http://howtobuybitcoins.info/

Current price of 1 BTC is about 220 USD.

IMPORTANT: You don’t even have to reply. Just pay 100 BTC to 1NhLM43duL2J2tBx2qQwBojEm5fNSoMEp – we will know it’s you and you will never hear from us again.

We say it because for big companies it’s usually the problem as they don’t want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service.

But if you ignore us, and don’t pay within 24 hours, long term attack will start, price to stop will go to 200 BTC and will keep increasing for every hour of attack.

ONE MORE TIME: It’s a one-time payment. Pay and you will not hear from us ever again!

Thank you.

Figure 2: A DD4BC email demanding a one-bitcoin ransom from an Akamai customer
An online gaming institution warned its customers of the attacks, according to online media as shown in Figure 3.

Figure 3: A published report on DDoS attacks against an online casino group

1.3 / MIXING THREATS WITH OFFERS OF PROTECTION / PLXsert received several samples of email text used by DD4BC in its latest extortion campaigns. In some of the examples, the emails warn potential victims that their sites are vulnerable to a DDoS attack. The sender then offers to set up better protection in exchange of Bitcoin payments. See Figures 4 and 5.
Figure 4: A sample email from DD4BC offering protection in exchange for one bitcoin

```
Hello

Your site is extremely vulnerable to ddos attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed!
My price is 1 Bitcoin only.

Right now I will star small (very small) attack which will not crash your server, but you should notice it in logs. Just check it.

I want to offer you info on how I did it and what you have to do to prevent it. If interested pay me 1 BTC to 17aLGgw8AwJdq1BtmMMG1QtQJgNQQkiyEsp

Thank you.
```

... attacks are sophisticated and too strong that I can bypass any protection other then PROLEXIC (and I will cost you 5-10 K per month). Google and check how many sites behind CloudFlare and similar shitty protections I crashed.

... 

Figure 5: Snippet from an email transcript where the malicious actor group asserts the ability to take down even sites with DDoS protection

Figure 6 shows a bitcoin transaction to a known DD4BC bitcoin address.
In some cases, DD4BC offers to cease its attack to give the victim time to read its emails and meet the demands (Figure 7).

```
From: dd4bc@outlook.com
To: *
Subject: RE: mpx.co - DDOS ATTACK!
Date: Sat, 15 Nov 2014 17:36:07 +0100

Attack temporarily stopped to give you time to read email and act.

You still have chance to end this for 1 BTC.

If not, attack restarts in 1 hour and price goes to 2 BTC.

***

To: *
Subject: mpx.co - DDOS ATTACK!
Date: Sat, 15 Nov 2014 13:45:59 +0100

Hello,

To introduce myself first:

:)

Now, to business:

My attacks are sophisticated and too strong that I can bypass any protection other then [sic] PROLEXIC ( and i will cost you 5-10 K per month). Google and check how many sites behind CloudFlare and similar shitty protections I crashed.
```
Pay me 1 BTC and your site is "protected" for lifetime. Pay to BTC address: 132EdUarcghK2bahkxgaKQ2XqanchPbWSB

Right now I’m running small attack for 1 hour as proof.

After that I expect your payment.

Please note that if I'm not paid within 2 hours, price will increase to 1 BTC to stop and will keep increasing 0.1 BTC for every hour of attack.

Thank you.

Figure 7: A DD4BC extortion email chain, promising ongoing escalation if the ransom is not paid in time

1.4 / THREAT COMPONENTS /

- **Motivation:** DDoS attacks for ransom.

- **Objective:** Obtain bitcoins as payment. Some of the bitcoin hash addresses are advertised for ransom payment on public forums as a mean of transmitting payments.

- **Members:** Membership is unknown at this point. However, some of the statements are made using first person expressions.

- **Resources:** DD4BC is likely using anonymizing network services and anonymous digital crypto currency to evade trace. Matching sources of DDoS activity suggest use of DDoS-for-hire botnets.

- **Knowledge source:** DD4BC is likely using publicly available tools to launch attacks. The initial assessment of source IPs suggests use of rented botnets from the DDoS-for-hire underground.

- **Victimology:** The earlier targets were typically unregulated bitcoin exchanges and gaming sites, which are unlikely to reach out to law enforcement for help. More recent attacks now include reputable business operations.

- **Typology:** Based on available open source intelligence (OSINT), the attacks are only using publicly available DDoS toolkits, plus resources from rented botnets in the underground.
1.5 / ATTACK ORIGINS / Some victims publicized the source IP addresses of the DDoS attacks. Figure 8 shows some advertised IP address sources involved in the DDoS attack against Bitalo, as shared on the website bitcointalk.org.

PLXsert matched the advertised sources with known DDoS attack sources. Some of the sources have attacked customers who are under Akamai’s DDoS protection. Figure 9 shows the industries previously targeted by IP addresses that were listed in Figure 8.
1.6 / OPERATIONS: SKILLS AND METHODS / Figure 10 shows a bitcoin address, a date of registration in the forum and the last activity time, which dates to November 10, 2014. No information was found on the bitcoin address, however it is very common for malicious actors to create multiple bitcoin addresses and perform multiple transfers. This transaction suggesting DD4BC has received payment for ransom and actively tried to obfuscate the destination of the funds as some of the Blockchain transaction information suggests.
It is very common for malicious actors to create multiple bitcoin addresses and perform multiple transfers in order to obfuscate origin and destination of the BTC funds. PLXsert found one of these addresses advertised as a ransom payment address, as shown in Figure 11.

![DD4BC victim posts information about the attack and ransom demand on October 24, 2014, including the ransom address](image)

Figure 11: A DD4BC victim posts information about the attack and ransom demand on October 24, 2014, including the ransom address

PLXsert found additional activity related to this bitcoin address on November 2 and 3, as shown in Figure 12 and Figure 13. The BTC transactions dated November 2, 2014 show payment and transferring activity to other accounts. It is very likely these malicious actors have already received ransom payments and have actively tried to obfuscate the destinations of these funds, as it shows on the multiple transaction history during Nov. 3, 2014.
1.7 / OBSERVED CAMPAIGNS / PLXsrt identified some of the source IP addresses as having participated in previous DDoS attacks, including SYN floods, DNS reflection attacks, NTP floods, CHARGEN attacks, SSDP floods and new DDoS attack campaigns uncovered in recent days against Akamai customers.

Figure 14 highlights payload samples from a DDoS campaign that occurred on April 16, 2015. It was confirmed that DD4BC group was the malicious actor responsible for this DDoS attack.
Some details of the attack include the following:

- Attack vectors: NTP flood, CHARGEN attack, SSDP flood
- Source ports: 123, 1900, 19
- Destination ports: Randomized (based on targeted host)

--- NTP Flood ---

16:32:53.174807 IP x.x.x.x.123 > x.x.x.x.777: NTPv2, Reserved, length 440
16:32:53.174816 IP x.x.x.x.123 > x.x.x.x.777: NTPv2, Reserved, length 440
16:32:53.174836 IP x.x.x.x.123 > x.x.x.x.777: NTPv2, Reserved, length 440
16:32:53.174837 IP x.x.x.x.123 > x.x.x.x.777: NTPv2, Reserved, length 440

2015-04-16 16:36:52.564778 IP (tos 0x0, ttl 244, id 28541, offset 0, flags [DF], proto UDP (17), length 468) x.x.x.x.123 > x.x.x.x.777: NTPv2, length 440
Reserved, Leap indicator: clock unsynchronized (192), Stratum 38 (reserved), poll 3s, precision 42
Root Delay: 6.001098, Root dispersion: 0.000000, Reference-ID: 0.0.25.199
Receive Timestamp: 1.001221120 (2036/02/07 06:28:17)
Transmit Timestamp: 0.000000000
Originator - Receive Timestamp: +55494754.248648256
Originator - Transmit Timestamp: +554947548.24742135

--- SSDP Flood ---

16:33:09.326321 IP x.x.x.x.1900 > x.x.x.x.80: UDP, length 323
16:33:09.326322 IP x.x.x.x.1900 > x.x.x.x.80: UDP, length 311
16:33:09.326323 IP x.x.x.x.1900 > x.x.x.x.80: UDP, length 307
16:33:09.326329 IP x.x.x.x.1900 > x.x.x.x.80: UDP, length 305

2015-04-16 16:44:10.186132 IP x.x.x.x.1900 > x.x.x.x.53: 18516 updateData
[w2z=0x5450] [11825a] [12081q] [8242n] [12336au]|domain|
....E..B..@.5.C#...._..L.l.P...
HTTP/1.1 200 OK
ST:urn:schemas-ong:server:WANDSLConnectionManagement:1
USN:uuid:22222222-0000-c0a8-0101-b0b2dc1bf030::urn:schemas-ong:server:WANDSLConnectionManagement:1
Location:http://192.168.1.1:5555/DeviceDescription.xml
Cache-Control:max-age=900
Server:Allegro-Software-RomUpnp/4.07 UPnP/1.0 IGD/1.00
Ext:

2015-04-16 16:44:40.186753 IP x.x.x.x.1900 > x.x.x.x.80: UDP, length 294
....E.B..0.5.C#...._..L.l.P...
HTTP/1.1 200 OK
Cache-Control: max-age=120
EXT:
Location: http://192.168.0.1:65535/rootDesc.xml
Server: UPnP/1.0 MiniUPnPd/1.3
ST: urn:schemas-wifialliance-org:service:WFAWLANConfig:1
USN: uuid:b9474e7e-1dd1-11b2-8f7e-c6b7ce97418a::urn:schemas-wifialliance-org:service:WFAWLANConfig:1
16:33:27.892030 IP x.x.x.x.19 > x.x.x.x.8080: UDP, length 2379
16:33:27.894008 IP x.x.x.x.19 > x.x.x.x.8080: UDP, length 506
16:33:27.894557 IP x.x.x.x.19 > x.x.x.x.8080: UDP, length 6956
16:33:27.900713 IP x.x.x.x.19 > x.x.x.x.8080: UDP, length 1642
6:33:32.443615 IP x.x.x.x.19 > x.x.x.x.8080: UDP, length 3064
...E...8x .y.........L......... !"#$%&'()*+, -./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]
!"#$%&'()*+-./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]
!"#$%&'()*+-./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]
!"#$%&'()*+-./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]
!"#$%&'()*+-./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]
!"#$%&'()*+-./0123456789:;?@ABCDEFGHIJKLMNOPQRSTUVWXYZ\]^_`abcdefghigklmnopqrstuvwxyz[]

Figure 14: Payload samples of the DDoS attack traffic

1.7A/ ATTACK DISTRIBUTION BY SCRUBBING CENTER / Figure 15 shows the attack traffic by Akamai DDoS mitigation scrubbing center. Most malicious traffic was mitigated in London, Hong Kong and San Jose, CA.

<table>
<thead>
<tr>
<th>Scrubbing Center</th>
<th>Bandwidth</th>
<th>PPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong</td>
<td>501 Mbps</td>
<td>114 Kpps</td>
</tr>
<tr>
<td>Washington, DC</td>
<td>1.48 Gbps</td>
<td>412 Kpps</td>
</tr>
<tr>
<td>San Jose</td>
<td>470 Mbps</td>
<td>140 Kpps</td>
</tr>
<tr>
<td>Frankfurt</td>
<td>1.2 Gbps</td>
<td>327 Kpps</td>
</tr>
<tr>
<td>London</td>
<td>825 Mbps</td>
<td>219 Kpps</td>
</tr>
<tr>
<td>Tokyo</td>
<td>1.6 Gbps</td>
<td>323 Kpps</td>
</tr>
</tbody>
</table>

Figure 15: Attack traffic distribution by Akamai scrubbing center
1.7b / TARGETED INDUSTRIES / A sample set of industry verticals that have been
targeted by the collected bots over the course of six months include the following three
subsets of high-tech and software companies:

- Hosting, domain name services (DNS), email services
- High tech consulting and services
- Software-as-a-Service

1.7c / ATTACKING IP ADDRESSES / PLXsert gathered the open source intelligence
(OSINT) and identified the attacking IP address attributes shown in Figure 16.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13238</td>
<td>5.255.253.51</td>
<td>5.255.253.0/24</td>
<td>RU</td>
<td>ripencc</td>
<td>2012-09-14</td>
</tr>
<tr>
<td>15169</td>
<td>104.154.38.52</td>
<td>104.154.0.0/15</td>
<td>US</td>
<td>arin</td>
<td>2014-07-09</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>130.211.185.192</td>
<td>130.211.0.0/16</td>
<td>US</td>
<td>arin</td>
<td>2014-05-12</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>146.148.40.57</td>
<td>146.148.0.0/17</td>
<td>US</td>
<td>arin</td>
<td>2014-03-26</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.69.136</td>
<td>66.249.69.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.69.88</td>
<td>66.249.69.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.75.104</td>
<td>66.249.75.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.75.184</td>
<td>66.249.75.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.75.216</td>
<td>66.249.75.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.75.88</td>
<td>66.249.75.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.111</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.119</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.127</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.135</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.4</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15169</td>
<td>66.249.79.95</td>
<td>66.249.79.0/24</td>
<td>US</td>
<td>arin</td>
<td>2004-03-05</td>
</tr>
<tr>
<td>GOOGLE - Google Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36351</td>
<td>184.172.15.235</td>
<td>184.172.0.0/18</td>
<td>US</td>
<td>arin</td>
<td>2010-10-06</td>
</tr>
<tr>
<td>SOFTLAYER - SoftLayer Technologies Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36351</td>
<td>50.97.173.18</td>
<td>50.97.128.0/18</td>
<td>US</td>
<td>arin</td>
<td>2011-04-18</td>
</tr>
<tr>
<td>SOFTLAYER - SoftLayer Technologies Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15286</td>
<td>172.245.55.112</td>
<td>172.245.48.0/21</td>
<td>US</td>
<td>arin</td>
<td>2013-04-22</td>
</tr>
<tr>
<td>SERVER-MANIA - B2 Net Solutions Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62567</td>
<td>104.131.204.15</td>
<td>104.131.192.0/19</td>
<td>US</td>
<td>arin</td>
<td>2014-06-02</td>
</tr>
<tr>
<td>DIGITALOCEAN-ASN-NY2 - Digital Ocean, Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62567</td>
<td>104.131.213.10</td>
<td>104.131.192.0/19</td>
<td>US</td>
<td>arin</td>
<td>2014-06-02</td>
</tr>
<tr>
<td>DIGITALOCEAN-ASN-NY2 - Digital Ocean, Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62567</td>
<td>107.170.150.138</td>
<td>107.170.128.0/19</td>
<td>US</td>
<td>arin</td>
<td>2013-12-30</td>
</tr>
<tr>
<td>DIGITALOCEAN-ASN-NY2 - Digital Ocean, Inc.,US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.8 / CONCLUSION / The nature of the operation and the successes obtained by DD4BC lead PLXsrt to expect the group to continue increasing the range of targets to other verticals, particularly those susceptible of financial loss due to downtime. This modus operandi is similar to what is known as an express kidnapping where criminals simply demand a small ransom that victims or companies can easily pay. The criminals make quick money and the victims are allowed to go on without major damage.

The data suggests the individual or individuals involved in this operation have likely already received payments from the threats made to some victims.

Historically, the verticals may have been selected based on their likely reluctance to involve law enforcement, leaving them the choice of either paying the ransom or seeking DDoS protection services. Some victims have offered bounties to convince others to reveal perpetrators’ identities, but this may be unsuccessful as attempts to bring justice to the malicious actors involved.

However, DD4BC is expanding to targets in more reputable business sectors – including the Akamai customers whose attacks are described in this bulletin, so there is hope that more victims will be forthcoming with law enforcement.

PLXsrt predicts this type of activity will increase as copycats enter the game.
About Akamai® / As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company’s advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.