CASE STUDY: SUMMARY OF OPERATION DD4BC
DDoS extortionist actor group

1.1 / Overview / DD4BC, a malicious group responsible for several Bitcoin extortion campaigns, has expanded its distributed denial of service (DDoS) attack campaigns against Akamai customers in recent months. DD4BC attacks mitigated by Akamai have been measured at up to 50 Gigabits per second (Gbps). That’s greater than the high of 15–20 Gbps observed in early May, but significantly lower than the group’s claims of generating 400–500 Gbps attacks.

A history of the group’s exploits and firepower can be found in Akamai’s Security Bulletin: DD4BC Operation Profile, published in April. In addition, a blog post update with frequently asked questions was published by Akamai in July. The latest attacks involve new tactics and methodology, as described in this case study.

DD4BC now threatens to expose a targeted organization via social media, in addition to the damage caused by the DDoS attack itself. The goal is to publicly embarrass the target, thus harming the company’s reputation and garnering more attention and credibility for its ability to create service disruptions.

The group’s new methodology includes ready use of multi-vector DDoS attack campaigns and revisiting former targets. DD4BC is also incorporating Layer 7 DDoS attacks in its multi-vector attacks, specifically concentrating on the WordPress pingback vulnerability to send reflected GET requests to the target. Akamai researchers have seen this attack method incorporated into DDoS booter suite frameworks, as well.

2.0 / Attack Timeline: September 2014 – July 2015 / The timeline depicted in Figure 1 shows attack bandwidth and million packets per second (Mpps) measurements for Akamai-mitigated DD4BC attack campaigns. In addition, we have included attack dates confirmed through various trusted partners to be DD4BC-related, however, attack measurements are not included in the graph.
The first dd4bc attack observed by Akamai was on September 30, 2014. The number of DDoS attacks was fairly consistent during the group’s early extortion attempts. In May through August 2015, however, attacks by dd4bc increased dramatically. In late July, there was a small drop off in attack totals. The timeline includes events confirmed through July 24; more attacks could have occurred after that date. It remains to be seen if the late-July drop off is an indication of dd4bc losing steam or simply taking a timeout to revise its tactics. A summary of attack statistics is shown in Figure 2.

Akamai mitigated 75 of the 141 attacks. Of significant note, none of the Akamai customers who were proactively configured suffered any adverse effect from the attack traffic. Those 75 attacks averaged 13.34 Gbps and 3.13 Mpps over the course of a 10-month span. At the peak of activity in June 2015 Akamai mitigated eight attacks of more than 23 Gbps. Most of these attacks included multiple DDoS attack vectors, with longer durations. dd4bc was particularly active on June 30, 2015 with six attacks, followed by five more on July 1. Evidence of an uptick in attacks is shown in Figure 3.
3.0 / TARGET INDUSTRIES / Through July 24, DD4BC had targeted 124 unique businesses, and researchers observed that the group expanded its targets into additional business. Figure 4 shows the targeted verticals for confirmed DD4BC attacks.

The financial services sector was targeted in 58% of the attacks. Banks and credit unions accounted for 35% of the attacks on financial services companies, 13% involved currency exchanges, and the rest were payment processing companies. Initial extortion attempts were made against currency exchanges and online gaming sites in 2014. In late April 2015 the group made a bold shift as it began to target banking. The bulk of the attacks against banks and credit unions occurred in June. This is when DD4BC became more of a real threat, because their attacks were now affecting enterprise organizations with greater visibility. Media and entertainment companies were on the receiving end of 12% of DD4BC’s attacks, compared to 9% for online gaming and 6% for retail and consumer goods. Figure 4 provides more details.

Figure 3: DD4BC DDoS attack activity increase dramatically in April, but began tapering off in July
4.0 / SAMPLE EXTORTION TRANSACTIONS / Figure 5 shows five ransom emails received by one victim organization. These demonstrate how DD4BC communicates during an extortion attempt. Not all targeted organizations received all five ransom emails. The emails varied based on the organization’s level of DDoS protection.

***************

First email

Date: Thu, 30 Apr 2015 21:57:19 +0200
Message-ID: <CAOz729CgBVn_RmJf9cqtRh8GTzmBuqDfyoyv3Ni-qB3FMzrLBw@mail.gmail.com>
Subject: DDoS ATTACK!
From: DD4BC Team <dd4bct@gmail.com>
To: [REDACTED]

Hello,

To introduce ourselves first:


http://bitcoinbountyhunter.com/bitalo.html


> Recently we were DDoS-ing [REDACTED]:
> https://[REDACTED]/[REDACTED]/status/583363894665715712

Yes, our attacks are powerful.

So, it=E2=80=99s your turn!
Your site is going under attack unless you pay 25 Bitcoin.

Pay to 198QaeuJ6oMeuau2p5gyDx75odweMWzNXH

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. At least, don’t expect cheap services like CloudFlare or Incapsula to help...but you can try. :)

Right now we are running small demonstrative attack. Don’t worry, it will not be that hard (it shouldn’t crash your site) and it will stop in 1 hour. It’s just to prove that we are serious. Check UDP traffic. :)

We are aware that you probably don’t have 25 BTC at the moment, so we are giving you 24 hours. Find the best exchanger for you on https://localbitcoins.com or http://howtobuybitcoins.info

You can pay directly through exchanger to our BTC address, you don’t even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don=E2=80=939t even have to reply. Just pay 25 BTC to 198QaeuJ6oMeuau2p5gyDx75odweMWzNXH =E2=80=9393 we will know it=E2=80=9399s 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. Or contact us via Bitmessage: BM-NC1jRewNdhxX3jHrufjxDsRWXGdNisY5

But if you ignore us, and don’t pay us within a given time, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

IMPORTANT: It=E2=80=9399s a one-time payment. Pay and you will not hear from =

us ever again!

We do bad things, but we keep our word.

Thank you.

**************************
Second email

In-Reply-To: <CAoz729Cg8Vn_RmJf9cqtRh8GTzmbugDfyoyv3Ni-qB3FMzrLBw@mail.gmail.com>
References: <CAoz729Cg8Vn_RmJf9cqtRh8GTzmbugDfyoyv3Ni-qB3FMzrLBw@mail.gmail.com>
Date: Fri, 1 May 2015 18:40:36 +0200
Message-ID: <CAoz729CsbX3fscx72SBh-f22+TDeEwSENZQ_tBifbZ0rMppCEQ@mail.gmail.com>
Subject: Re: DDOS ATTACK!
From: DD4BC Team <dd4bct@gmail.com>
To: [REDACTED]
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Hello?

A few hours left at this price.

Third email

References: <CAoz729Cg8Vn_RmJf9cqtRh8GTzmbugDfyoyv3Ni-qB3FMzrLBw@mail.gmail.com>
Date: Fri, 1 May 2015 18:46:03 +0200
Message-ID: <CAoz729CsbQO3axd=rpfICOS5iMgdLKLrdctZdwxHvXzQTrMOtrMg@mail.gmail.com>
Subject: Re: DDOS ATTACK!
From: DD4BC Team <dd4bct@gmail.com>
To: [REDACTED]
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

btw. Running small (1 hour) demonstration right now.

Fourth email

References: <CAoz729Cg8Vn_RmJf9cqtRh8GTzmbugDfyoyv3Ni-qB3FMzrLBw@mail.gmail.com>
Date: Fri, 1 May 2015 22:42:31 +0200
Message-ID: <CAoz729B6f9JuxXNJXxebrpnNKK0y=wVe=8wo1pG6KY+yj3=w@mail.gmail.com>
Subject: Re: DDOS ATTACK!
From: DD4BC Team <dd4bct@gmail.com>
To: [REDACTED]
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Maybe it would be more efficient to hit [REDACTED]?

What do you think?

*******************************
As the overall number of attacks increased, the emails sent varied from the standard email template observed earlier, as shown in Figure 6. The emails began to imply that the group would go public about the attacks in order to harm the targeted organization’s reputation.

The sender information also began to vary, which could be an indicator that there were multiple actors associated with the attack events, each using the DD4BC identity.
***************

First email (no variants)

From: DD4BC Team [mailto:extortion@tuta.io]
Date: Friday, July 03, 2015
To: [REDACTED]
Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:
http://bitcoinquandrum.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-ex-
coin-theft-owner-accuses-ccedk-of-withholding-info
Or just google “DD4BC” and you will find more info.

So, it’s your turn! All servers of [REDACTED] group (internationally) are going
under DDoS attack unless you pay 40 Bitcoin. Pay to 16HH1Se5zhXgqg4EBAKZxydMump5Mi-
YgrQ Please note that it will not be easy to mitigate our attack, because our cur-
rent UDP flood power is 400-500 Gbps. Right now we are running small demonstrative
attack on one of your IPs: [REDACTED]. Don’t worry, it will not be hard (we will
try not to crash it at the moment) and will stop in 1 hour. It’s just to prove that
we are serious.

We are aware that you probably don’t have 40 BTC at the moment, so we are giving
you 24 hours to get it and pay us. Find the best exchanger for you on howtobuybit-
coins.info or localbitcoins.com You can pay directly through exchanger to our BTC
address, you don’t even need to have BTC wallet. Current price of 1 BTC is about
250 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don’t even have to reply. Just pay 40 BTC to 16HH1Se5zhXgqg4EBAKZx-
dyMump5MiYgrQ – 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, use Bitmessage: BM NCljRewNdHxX3jHrufjxDSRWXGdNiaY5 But
if you ignore us, and don’t pay within 24 hours, long term attack will start, price
to stop will go to 100 BTC and will keep increasing for every hour of attack. Many
of our “clients” believe that if they pay us once, we will be back. That’s not how
we work – we never attack the same target after we are paid. If you are thinking
about reporting this to authorities, feel free to try. But it won’t help. We are
not amateurs.

REMEMBER THIS: It’s a one-time payment. Pay and you will not hear from us ever
again!
We do bad things, but we keep our word.
Thank you

***************
***************
Second email (Variant 1)

From: DD4BC Team <whosyourdaddy@tutanota.com>
Date: Monday 6 July 2015 16:13
To: [REDACTED]
Subject: Time is running up!

If not paid, massive attack will start, as explained in first email. So far we were running small, demonstrative attacks.

***************
Second email (Variant 2)

From: DD4BC Team <dd4bc@gmail.com>
Date: Friday, May 29, 2015
To: [REDACTED]
Subject: Re: DDOS ATTACK!

Hello,
Please read this email carefully as soon as you see it.

We were running just small attack on your site so far.
And you are ignoring us. Probably because you don’t want to pay extortionists. And you believe that after some time we will give up.

But we never give up.

And if not paid a lot of damage will be made.

Since our intention is not to make damage for nothing, but to make money, once again we will give you 2 more days — until the end of Thursday.

And sooner you pay, sooner we will move to your competition. :)

But please understand that if you keep ignoring us, we will have to restart the attack on your site and if we do it, price will go up! Let’s hope not, but if we keep getting ignorance from you, we will be forced to.

Thank you.

***************
Third email (Variant 1)

From: DD4BC Team <tdd4bc@Safe-mail.net>
Date: Tuesday, May 26, 2015
To: [REDACTED]
Subject: Re: DDOS ATTACK!

We see many complaints on Twitter, so we will stop the attack right now.

***************
***************
Third email (Variant 2)

From: DD4BC Team <dd4bc3@Safe-mail.net>
Date: Wednesday, May 27, 2015
To: [REDACTED]
Subject: DDOS ATTACK - IMPORTANT!

Looks like you decided to ignore us, because you believed that you can mitigate the attack. And you failed.

While your service is down many merchants are suffering, so we will give you another chance.

Another 24 hours.

But consider it to be your last chance as tomorrow, if not paid, long term attack will start.

For now, we will increase the price just a little bit - to 45 BTC.

Pay 45 BTC within 24 hours to 1C2421mUf4e38e7FFbTqKq6xR3B8Cy8YAP and you will never again hear from us.

Ignore us again, long term attack will start, price to stop will go to 100 BTC.

And if you need to contact us for any reason, use Bitmessage: BM-NCljRewNdIxX-3jHrufjDsRWXGdNisY5

***************
Final email (Variant 1)

From: DD4BC Team <dd4bcw@keemail.me>
Date: Fri, Jul 24, 2015
To: [REDACTED]
Subject: Last warning

You are ignoring us.

You probably believe that after some time we will give up. But we never give up.

Maybe you believe that if you pay us once, we will be back? But we never attack the same target twice.

Please note that there are 2 options:
- You pay us, you never hear from us again.
- You don’t pay, your services go offline for a long time. Until you pay more.

Is it worth it?

We will give you another 24 hours.
In 24 hours, if not paid, attack will start. Understand that this is your last chance.

P.S. Another thing: If payment not received, we will start the attack and go publicly on social networks about it, which is going to harm your reputation more then attack itself.

******************************

Final email (Variant 2)

From: “DD4BC Team” <dd4bcwarning@tutanota.com>
Date: Tue, Jun 30, 2015
To: [REDACTED]
Subject: FINAL WARNING!

Don’t expect us to give up. We never give up.

And if not paid, not only that massive attack will start, but we will go publicly, inform users that we are ddosing you, that you can’t protect your site and it’s time to change casino. :)

******************************

Figure 6: The text in the emails from the actor group to target organizations began to vary in May 2015

**5.0 / SAMPLE ATTACK CAMPAIGNS** / Campaign attack attributes for two of the largest DD4BC DDoS campaigns mitigated on behalf of Akamai customers are shown below.

**Attack campaign against Organization A**

Peak bandwidth: 56.2 Gbps
Peak packets per second: 6.9 Mpps
Customer: Organization A
Event time start: May 16, 2015 21:55:00 UTC
Event time end: May 17, 2015 03:42:44 UTC
Attack types: udp flood
Destination ports: Randomized

This first campaign stands as the highest bandwidth DDoS attack confirmed as DD4BC thus far. The 56 Gbps generated solely by a udp flood is fairly large. Still, this DDoS attack falls short of the 400 – 500 Gbps claimed in the emails. Sample payloads are shown in Figure 7. The udp flood was set to a static 600-byte payload length in this attack and a 440-byte payload length in the attack shown in Figure 8.

```
21:57:00.902103 IP xxx.xxx.xxx.xxx.3078> y.y.y.y.1869: UDP, length 600
[static payload size]
21:57:00.902169 IP xxx.xxx.xxx.xxx.44858 > y.y.y.y.17094: UDP, length 600
21:57:00.902222 IP xxx.xxx.xxx.xxx.3072 > y.y.y.y.5528: UDP, length 600
21:57:00.902249 IP xxx.xxx.xxx.xxx.3240> y.y.y.y.43611: UDP, length 600
21:57:00.902249 IP xxx.xxx.xxx.xxx.40225> y.y.y.y.37808: UDP, length 600
```

Figure 7: Payload samples for a UDP flood attack vector launched against Organization A
Attack campaign against Organization B

Peak bandwidth: 42.2 Gbps
Peak packets per second: 13.5 Mpps
Customer: Organization T
Event time start: May 27, 2015 19:58:00 UTC
Event time end: May 29, 2015 16:32:46 UTC
Attack types: UDP flood, udp fragment, NTP flood, SNMP flood, SSDP flood
Destination Ports: 80

The observed attacks are in line with the typical scripted attacks found on the DDoS-for-hire market.

The main DDoS attack types observed from DD4BC are NTP floods (22%), SSDP floods (15%), UDP floods (15%) and SYN floods (13%) — a well-versed portfolio of attacks at Layers 3 and 4 and Layer 7. In addition, six different reflection attack methods accounted for 53% of the attacks. These attack types are shown in Figure 9.
6.0 / REFLECTION ACTIVITY BY COUNTRY / When Akamai first investigated dd4bc, the attacks were directed typically at companies in North America and Asia. dd4bc eventually moved on to European companies, and then focused on companies in Korea, China, Australia, and New Zealand for a period of time. Most recently, the US and Canada have been the primary focus; however we have observed attacks continue to affect various organization globally.

The chart in Figure 10 shows the majority of the most recent dd4bc-related reflection attack traffic (40%) was traced to the US. Other sources include China (22%), Japan (11%), and Korea (9%).

7.0 / RECOMMENDED DEFENSIVE MEASURES / To protect your company from dd4bc attacks, we recommend the following defensive measures:

- Anomaly-based and signature-based DDoS detection methods should be deployed to detect attacks before the site becomes unavailable to users.
- Resources should be distributed to avoid single points of failure due to an attack and to increase resiliency to attacks.
- Layer 7 DDoS mitigation appliances should be deployed on the network in strategic locations to mitigate the DDoS threat to critical application servers.

For the best solution, Akamai recommends web properties run on port 80 and/or 443 on Kona Site Defender with Site Shield properly configured and have Prolexic Proxy or Prolexic Routed services ready to protect other ports and protocols. In addition, traffic that uses Dns port 53 can be protected with Akamai’s Fast dns.
The attacks resemble other volume-based attacks using UDP, SSDP, NTP, DNS, SNMP, ICMP, CHARGEN and SYN floods. In some instances, application-layer GET floods have used the WordPress XML-RPC pingback attack. Attacks are targeted typically at a specific IP address owned by an organization. The targeted IP address is not always the most visible .com site. It can be anything that the group can identify and can use to cause some level of impact to the target.

8.0 / Akamai’s Operational Stance / Akamai customers have not been adversely affected by dd4bc traffic when our cloud security solutions were in place proactively. We have seen the attackers redirect their efforts to alternate organizations once they see an attack is no longer effective, and cease the email notifications.

The exposure of Akamai Security Operations Center (soc) to these campaigns has allowed us to establish a pre-mitigation posture for dealing with dd4bc.

The soc is knowledgeable about the attack signatures, attack traffic patterns, and dd4bc’s attack style. The soc’s expertise with Layers 3 and 4 and Layer 7 DDoS attack types has proved valuable in mounting a strong defense against dd4bc.

9.0 / Conclusion / The nature of the dd4bc’s operation and the successes it has obtained has lead Akamai’s Prolexic Security Engineering and Research Team (PLXsert) to expect the group to continue to increase its range of targets to other verticals,
particularly those susceptible to financial loss from downtime. This modus operandi is similar to an express kidnapping, where criminals demand a small ransom that victims or companies can pay easily.

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 the dd4bc operation have received ransom payments from the DDoS threats made to some victims.

Historically, targets of ransom demands are selected based on their anticipated reluctance to involve law enforcement, leaving them to either pay the ransom or pay for DDoS protection. Some victims offer bounties to encourage others to reveal perpetrators’ identities, but this may be unsuccessful in bringing justice to the malicious actors.

dd4bc is expanding its targets to enterprise-level organizations — including the Akamai customers who were the targets of the described attacks, making it more likely that more victims will be forthcoming to law enforcement.

PLXsert believes copycats will enter the game, increasing these types of attacks. In fact, copycats may already be sending their own ransom letters, piggybacking on the reputation of dd4bc.

If you are currently an Akamai customer utilizing any of our security services and receive a ransom request, please contact the Akamai soc about the active threat. If any routing changes are required by your organization, submit a ticket to the soc identifying the targeted IP address listed in the demand email and move traffic onto the Akamai DDoS mitigation proxy platforms proactively if you are an on-demand customer.

If you are not an Akamai customer, you can contact your local Akamai office.

Please take this group seriously should your organization receive a ransom email. The dd4bc attacks are not a hoax. The threat and resulting DDoS traffic are real. Akamai is able to mitigate the types of attacks generated by this group readily.
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.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.

©2015 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 09/15.