DDoS Attack Mitigation Report

Media/Telecom

KrebsonSecurity

Prolexic Defends Krebs on Security Blog Against Dirt Jumper/Pandora DDoS Attacks

Krebs on Security (www.krebsonsecurity.com), authored by Brian Krebs, an independent investigative reporter, is a popular blog on emerging cyber crime trends, DoS and DDoS toolkits, and the perpetrators themselves. On average, the blog receives 10,000 views or more per day. Not surprisingly, the site has been the target of DDoS attacks and other cyber threats. However, during the last week of July 2012, the denial of service DDoS attackers took a new, more pernicious approach using Pandora, a variation of the Dirt Jumper DDoS toolkit.

On the morning of July 27, Krebs was in Las Vegas for the Black Hat convention and was minutes away from a live interview with one of the conference leaders when availability of krebsonsecurity.com became spotty and eventually went down. Krebs contacted his hosting provider, who delivered the bad news that junk traffic was being pushed to the site by a DNS amplification DDoS denial of service attack.

> Company under DDoS attack

Krebsonsecurity.com, a popular blog that unveils the latest types of cyber threats and their perpetrators

> Type of DDoS attack

DNS amplification attack and Layer 7 flood using Dirt Jumper/Pandora

> Prolexic attack mitigation strategy

PLXproxy mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading SLA

"My hosting provider said, 'Brian, the DNS attack is really starting to affect our other customers.' Thankfully, even as I was conducting the interview, they were able to help me transition the site's DNS to Prolexic's and help mitigate that portion of the attack," Krebs said.

Ultimately, a series of four escalating denial of service attacks were launched against the site. Krebs speculates that the DDoS attacks came in response to a story he had posted several hours before. The site was down for approximately five hours, during which time visitors could not access the site or read content via RSS feeds.

"I make a career out of making people upset with the stories I post, because I tend to expose the things that the bad guys are doing – and who they are. They don't really like that," Krebs says. "The story I had posted, right before the attack started, was about a service for mass registering of domain names for malware and spam. They didn't send me a note or threat, so it's hard to say where the attack really originated."

Krebs has a good relationship with the head of his hosting provider, so Krebs asked for a recommendation. "I respect this person and know that he has experience with DDoS mitigation providers, and I wanted to make his life easier, too," Krebs says. "I knew that Prolexic has a good reputation and thought it would be a good fit. When I asked my hosting provider which vendor he would feel most comfortable with, he said Prolexic. That was enough for me."

Prolexic's DDoS mitigation strategy

Prolexic DDoS mitigation experts quickly identified that the malicious traffic was part of a DNS amplification attack combined with changing attack vectors

PROLEXIC
DDoS Attacks End Here.

launched via the Pandora toolkit. Using more than 20 mitigation tools, many proprietary, Prolexic's engineers were able to write new countermeasures and mitigate each changing signature on the fly. Consequently, availability of Krebs' blog site was restored in minutes and remained protected as all traffic from krebsonsecurity.com was routed through Prolexic's scrubbing centers.

Prolexic's analysis indicated a series of increasingly strong DDoS denial of service attacks over four days as characterized by the following peaks in activity:

- July 24 – GET Flood that peaked at 5.00 Mbps (bits per second), 2.50 Kpps (packets per second), and 35Kcon (connections per second)
- July 25 – GET Flood and POST Flood 105Kbps (peak bits per second), 6Kpps (packets per second), and 25Kcon (connections per second)
- July 28 – UDP Flood and UDP Fragment, 552.00 Mbps (peak bits per second), 121.00 Kpps (peak packets per second)
- July 29 – GET Flood, POST Flood, 275.00 Kbps (peak bits per second), 0.10 Kpps (peak packets per second), 0.15 Kcon (peak connections per second)

Prolexic's DDoS mitigation engineers also determined that all of the various traffic signatures for the GET and POST floods seemed to be created by the same individual using Pandora, a Dirt Jumper DDoS toolkit, which is sold in the cyber underground. Prolexic found that more than 1,500 Pandora-infected bots were used in the denial of service DDoS attack on the site.

"The traffic signatures strongly suggested the involvement of two Dirt Jumper progeny: Di-BoTNet and Pandora," Krebs wrote on his blog. "Pandora is the latest in the Dirt Jumper family, and features four different attack methods. According to Prolexic, one of the methods used against KrebsOnSecurity.com was Attack Type 4, a.k.a Max Flood; this method carries a fairly unique signature of issuing POST requests against a server that are more than 1 million bytes in length."

Staying protected with Prolexic

With Prolexic protection, the Krebs on Security site will remain protected against all DDoS denial of service threats, including DDoS attacks launched via the Dirt Jumper toolkit. Dirt Jumper is a high-risk DDoS toolkit that can be used to launch application layer attacks on web sites. This prepackaged toolkit is now widely available on various underground websites and retails for as little as US$150. Dirt Jumper can be spread via spam, exploit kits, fake downloads and can be pushed out to machines already infected with other forms of malware. Prolexic has developed a security-scanning tool that can be used to detect Dirt Jumper command and control servers. The threat advisory and scanner can be downloaded free of charge from www.prolexic.com/threatadvisories.

"The DDoS problem is not going away and it's only going to get worse," Krebs says. "As illustrated by the denial of service attacks on my site using the Pandora toolkit, it's never been easier to build your own DDoS bot army."

Prolexic informed Krebs that the DDoS attackers compromised open recursive (unmanaged) DNS servers to create extremely large floods of traffic in the DNS amplification attack. These types of unmanaged servers are favorite targets for a denial of service attack because they are configured to accept queries sent from anywhere on the Internet, including forged or "spoofed" queries that are characteristic of DNS amplification attacks.

"In the case of DNS DDoS attacks, I think that ISPs should avoid the use of open recursive servers that get abused over and over again to launch these attacks," Krebs says. "The problem will never go away completely, but we need to change the status quo on protecting servers against DDoS attacks."