

Internal Sales Update

Radware Attack Mitigation System (AMS) Success Fighting Anonymous Group Attacks Revealed!

FBI Chases Anonymous Activists based on AMS Security Event Management (SEM) Logged Data

Even though the FBI started serving search warrants and arresting people suspected in participating in the Anonymous' "Operation Payback" way back in January, it is only after last week's arrests it began to be clear that the FBI is not randomly knocking on doors of people who used the PayPal site at the time of the attack.

The suspicion was confirmed by an FBI [affidavit](#) made public on Tuesday July 27, 2011. It reveals that once PayPal had detected the initial DDoS attack against its blog, they made sure to log the IP addresses bombarding the main site with requests with a **Radware AMS**.

After ten days, the company had collected enough information to compile a list of some 1,000 IP addresses that were involved in the DDoS attack, and they handed the list to the FBI.

That was in December last year, and since then, agents have mounted an investigation that resulted in the January and the recent arrests.

According to [Wired](#), PayPal's **Radware AMS had no trouble distinguishing legitimate requests from those initiated by the Low Orbit Ion Cannon (LOIC) tool used by Anonymous supporters** since those packets contained a specific set of strings such as "wikileaks", "wikileakshttp", "goof", "goofhttp", "block-https-ascii" and "goodnight".



The FBI Affidavit acknowledges AMS Success

The FBI affidavit, released on July 15, 2011, reveals Attack Mitigation System (AMS) success at PayPal. **A complete copy of the Affidavit is available at: <http://www.scribd.com/doc/60998288/Anonymous-Affidavit>**

Key quotes from the FBI Application and Affidavit for search warrant:

Notable quote from the FBI Application and Affidavit	Interpretation & Business value
<p><i>“This application is part of an investigation into DDoS attacks against PayPal, Inc., a company located in San Jose, California.”</i></p>	<p>PayPal was one of the designated targets of Operation Payback, December 2010.</p>
<p><i>“On December 15, 2010, Jon Orbeton, PayPal, provided SA Adam Reynolds a USB thumb drive containing logs and reports detailing information regarding approximately 1,000 IP addresses that sent malicious network packets to PayPal during the DDOS attacks. The 1,000 IP addresses were derived from logs created by a Paypal-owned Radware device”</i></p>	<p>The built-in Security Event Management (SEM), part of Radware AMS, provides advanced reporting, monitoring and alerting engine. It also collects forensics evidence that can be later used as fingerprints to track back the attack origins.</p> <p>Business value: Best-in-class unified monitoring and reporting solution (SEM) providing business centric view of security incidents and drill down up to detailed forensics.</p>
<p><i>“according to eBay’s Forsythe, the Radware device rarely recognizes legitimate network traffic as malicious traffic. This means it would be highly unlikely that the Radware device would confuse someone who is trying to use PayPal service legitimately, with someone who is attacking PayPal.”</i></p>	<p>Radware AMS provides accurate detection and mitigation of network attacks – using static signature and real-time signatures driven by the Network Behavioral Analysis (NBA) module. Forsythe, a leading integrator in the USA, acknowledges that AMS offers most accurate attack mitigation solutions in the market.</p> <p>Business value: Maintain Business Continuity of Operations (COOP) even when the network is under attack.</p>
<p><i>And, in this particular instance due to the specific known signatures used by the LOIC tool, there is a greater degree of certainty that the malicious traffic was accurately identified”</i></p>	<p>Radware Emergency Response Team (ERT) had a valuable contribution in detecting in advance the LOIC attack tool and providing accurate signatures that block the attacks generated by the tool, while reporting on each source IP address into the SEM logs.</p> <p>Business value: Radware ERT supports its customers 24x7 by neutralizing DDoS attacks and restore network status.</p>

What’s next?

Anonymous and LulzSec have reacted to this news by posting a joint [communiqué](#) in which they urged people to close their PayPal accounts in protest.

This acknowledges that **Anonymous have failed to launch DDoS attacks** on PayPal, and now they try other ways to cause harm to PayPal. Cybercrime is no longer an option for them.

From the media

Paypal gives FBI shopping list of 1,000 hackers

By Nick Farrell

27 July 2011

TechEye

While you might be wondering where the Untouchables are getting the names and addresses of Anonymous hackers it is arresting, it turns out that it is from a shopping list given to them by PayPal. According to WIred the online financial outfit is no friend of Anonymous and collected 1000 IP addresses of those carrying out Anonymous' DDoS attacks against PayPal last December. FBI agents began monitoring Anonymous press releases while PayPal collected traffic logs on a Radware intrusion prevention system installed on its network. <http://www.techeye.net/security/paypal-gives-fbi-shopping-list-of-1000-hackers#ixzz1TJWKE00>

Arrested Anonymous activists just a small part of a long list

Zeljka Zorz, HNS News Editor

27 July 2011

Help Net Security

Even though the FBI started serving search warrants and arresting people suspected in participating in the Anonymous' "Operation Payback" way back in January, it is only after last week's arrests that it began to be clear that the FBI is not randomly knocking on doors of people who used the PayPal site at the time of the attack. The suspicion was confirmed by an FBI affidavit made public on Tuesday. It reveals that once PayPal had detected the initial DDoS attack against its blog, they made sure to log the IP addresses bombarding the main site with requests with a Radware intrusion prevention system. According to Wired, PayPal's Radware IPS had no trouble distinguishing legitimate requests from those initiated by the Low Orbit Ion Cannon (LOIC) tool used by Anonymous supporters since those packets contained a specific set of strings such as "wikileaks", "wikileakshttp", "goof", "goofhttp", "block-https-ascii" and "goodnight". <http://www.net-security.org/secworld.php?id=11353>

In 'Anonymous' Raids, Feds Work from List of Top 1,000 Protesters

By Kevin Poulsen

26 July 2011

Wired

It turns out there's a method behind the FBI's raids of suspected Anonymous members around the country. The bureau is working from a list, provided by PayPal, of the 1,000 internet IP addresses responsible for the most protest traffic during Anonymous' DDoS attacks against PayPal last December. According to the affidavit, by FBI agent Chris Thompson, PayPal security officials were in close contact with the bureau beginning on December 6, two days after PayPal froze WikiLeaks' donation account and the first day it began receiving serious denial-of-service traffic. FBI agents began monitoring Anonymous press releases and Twitter postings about Operation Payback, while PayPal collected traffic logs on a Radware intrusion prevention system installed on its network. http://www.wired.com/threatlevel/2011/07/op_payback/

**Also seen on: ARS Technica; Belch Speak; Hacking Expose; Democratic Underground*