the Availability Digest

www.availabilitydigest.com
@availabilitydig

Hacktivism

February 2016

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. Hacktivists are not cybercriminals. They do not hack into computer systems to steal money or data. Rather, they hack into computer systems - typically websites - to make a statement.

A recent report by Imperva, "Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack,"[1] describes in detail an attempted assault by the hacktivist group 'Anonymous,' an assault that lasted 25 days. Though the attack was unsuccessful, the strategy that Anonymous used to perpetrate the attack was closely analyzed by Imperva. The analysis leads to some important strategies to protect a company's computing assets from such attacks.

A key finding is to monitor social media for indications of such attacks. Since it is the purpose of the hacktivist to make a statement, there often are many mentions of the impending attack on Twitter, Facebook, YouTube, and other social-media forums that can give a company time to prepare for the attack.

Anonymous

Anonymous[2] is a loosely associated international network of hacktivists. A website associated with the group describes it as "an Internet gathering" with "a very loose and decentralized command structure that operates on ideas rather than directives." The group became known for a series of distributed denial-of-service (DDoS) attacks on government, religious, and corporate websites.

Anonymous originated in 2003 and represented the views of many online and offline community users. Anonymous members can be distinguished in public by the wearing of the stylized Anonymous mask, a depiction of Guy Fawkes, the best-known member of the Gunpowder Plot attempt to blow up the London House of Lords in 1605.

In its early form, the Anonymous concept was adopted by a decentralized online community acting anonymously in a coordinated manner, usually toward a loosely self-agreed goal. Beginning in 2008, the Anonymous collective increasingly became associated with collaborative hacktivism on a number of issues internationally. Individuals claiming to align themselves with Anonymous undertook protests in retaliation against anti-digital piracy campaigns by motion picture and recording industry trade associations. Later targets of Anonymous hacktivism included government agencies, ISIS, child pornography sites, copyright protection agencies, and corporations such as PayPal, MasterCard, Visa, and Sony.

[1] Hacker Intelligence Summary Report, *The Anatomy of an Anonymous Attack*. http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf
[2] See Anonymous (groups), *Wikipedia.*

Imperva

Imperva is a provider of data and application security solutions that protect business-critical information in the cloud and on-premises. Founded in 2002, it currently generates over $160 million in revenue. It has over 3,700 customers and 300 partners in more than 90 countries worldwide.

Imperva's services protect cloud applications, websites, files, SharePoint systems, critical databases, and Big Data repositories from cyberattacks, theft, and fraud. Its technology uses sophisticated client classification and user tracking that can detect unauthorized users and malicious Web bots. It also employs a research team—the Application Defense Center—comprised of experts in data and application security to root out new attack methods and to stop them before the attacks reach their customers.

Imperva's Hacker Intelligence Initiative (HII) Reports

Issued approximately six times a year, the Imperva Hacker Intelligence Initiative (HII) reports go inside the cyber-underground to provide in-depth, forward-looking analyses at trending hacking techniques and interesting attack campaigns. These research papers aim to understand not solely what has happened in the past but to deep-dive into what is ahead and what's needed to proactively stay ahead of hackers' next moves.

A review of Imperva's HII report, "The Anatomy of an Anonymous Attack," provides the background for this article.

The Anatomy of an Anonymous Attack

In 2011, the hactivist group Anonymous attempted to launch an attack against the web site of an unidentified company. The preparation and final attack was carried out over a twenty-five day period. The web site had a web-application firewall deployed that recorded and repelled the attacks. By analyzing the traffic logs, the Imperva Application Defense Center was able to identify the attack method. The Imperva team also analyzed Anonymous' social media communications in the days leading up to the attack to understand the preparations that Anonymous took. Imperva believes that this is the first end-to-end record of a full Anonymous attack.

Reactive versus Proactive Attacks

In its study of Anonymous attacks, Imperva determined that attacks fell into two categories:

Reactive – Some incidents inspired Anonymous to attack a target. For instance, when MasterCard, Visa, and others stopped allowing payments to Wikileaks, Anonymous launched Operation Payback, intended to bring down their web sites with excessive traffic via DDoS (distributed denial-of-service) attacks.

Proactive – In a proactive attack, Anonymous announced an intention to attack a target.

The Anonymous attack that is the subject of this Imperva report was a proactive attack. In this case, Anonymous hoped to disrupt an event that would take place on a specified date. A website that enabled e-commerce and information dissemination about the event became the Anonymous target.

The Progression of the Attack

The attack took place over twenty-five days in three phases – recruiting, reconnaissance, and attack.

Recruiting (Days 1 -18)

Recruiting took place over the first eighteen days. A small group of Anonymous instigators leveraged social media to promote their message and campaign and to recruit members. They created a website justifying an attack on their target. They used Twitter and Facebook to promote traffic to their website. Additionally, YouTube videos were produced to help rationalize the attacks.

Anonymous requested interested participants to contact them and sign up for the attack. After they had persuaded thousands of volunteers to join, Anonymous' skilled hackers began their reconnaissance.

Reconnaissance (Days 19 - 23)

The reconnaissance phase took place over the next five days. Around ten to fifteen skilled hackers probed the website's applications in an effort to identify weaknesses that could lead to a data breach. They used commonly-available vulnerability assessment tools such as Acunetix, which checks for XSS (cross-site scripting), SQL injection, and other web vulnerabilities. The hackers hid their true identities and places of operation.

They also attempted to use attack software specifically designed to steal data. One such tool was Havij, which is believed to have been developed by Iran. Havij conducts a high volume of SQL injection attacks, performing data extraction and harvesting.

However, the attackers were unable to identify any weakness that could lead to a data breach.

Attack (Days 24 – 25)

Having failed to find a way to expose data, the hackers turned to their base of volunteers obtained during Anonymous' recruitment phase. Several thousand people either downloaded attack software or went to one of Anonymous' custom-built websites that perform DDoS attacks.

The Anonymous custom DDoS website is called the low-orbit ion canon (LOIC). It is just a few hundred lines of Javascript code and can run on mobile devices. When the website is opened via a browser in a PC or in a mobile device, it generates multiple requests to the victim's website. Each request has a variable parameter (the date/time in milliseconds) to avoid the response being in the website's cache memory, thus consuming much more of the website's computing resources. Using this tool, a PC can generate about 200 requests per second. The attacks generated about 500,000 requests per second.

However, when the DDoS attack failed after two days of bombarding the target website with traffic, the attack ended.

Detection and Mitigation

Understanding the Anonymous attack methodology leads to strategies to detect and mitigate such attacks.

Monitor Social Media

Hacktivism is "loud" by definition. The hacktivists want everyone to know that they are going to attack a site. Besides, this advertisement of their intentions is a way to recruit volunteers to join in the attack. Hacktivists use all of the social media the Web offers – Twitter, Facebook, YouTube, blogspot, pastebin, etc.

Consequently, a company should scan proactively the Web for hints of coming attacks. The data obtained can be used to thwart the attack as it may disclose the attack date and the attack means.

A convenient way to monitor the Web for signs of an attack is to use Google Alerts. A Google Alert will send the company an email notification any time Google finds a posting that concerns the company.

Protect Applications

A strong application security program consisting of Web application firewalls, vulnerability assessments, and code reviews can help mitigate the risk of a breach.

Analyze the Alert Messages Generated By Your Security Facilities

In this study, the DDoS attack was preceded by days of reconnaissance. This reconnaissance undoubtedly generated a mass of alert messages from the website's security facilities. By ensuring these alerts are scrutinized, a company can strengthen its security policy and be better prepared for an attack. Daily analysis of alert information will help a company to better prepare for tomorrow's attack.

IP Reputation is Very Valuable

75% of the attack traffic in this study came from only five IP addresses, all of which used anonymity services such as TOR. The reputation of anonymous IP addresses is rated as poor. If the company under attack had checked the IP reputation of the attackers, most of the reconnaissance traffic could have been blocked.

DDoS is the Hacker's Last Resort

Attackers prefer small-scale, effective campaigns that do not require a massive recruitment of volunteers. Therefore, companies should make it their priority to close application vulnerabilities. They then should plan their defenses against a DDoS attack.

Summary

Proactive attacks such as the one analyzed in this Imperva study are well-advertised in advance. By following social media for messages about your company, you may be able to detect such an attack in advance, including its date and the method of attack.

Given this information, it then is very important to monitor your security alert messages so that reconnaissance attempts by an attacker can be blocked. Finally, you should have a DDoS mitigation strategy in place (such as using a DDoS mitigation service) in case DDoS is the final attack methodology used by the perpetrator.