ADVISEN
Insurance Intelligence

HACKTIVISM:
THE GROWTH AND IMPLICATIONS OF THIS 21ST CENTURY METHOD OF PROTEST

December 2012

Sponsored by:

ZURICH®

HACKTIVISM:
THE GROWTH AND IMPLICATIONS OF THIS 21ST CENTURY METHOD OF PROTEST

Executive Summary

"Hacktivism," a movement with origins dating to the early days of the Internet, has only recently become a subject of interest for many outside tech and system security circles. Over the past couple of years, this 21st century method of protest that combines computer hacking with political activism has become more common and more complex. Groups such as the hacker collective Anonymous, with increasing frequency, target companies and government agencies which they deem politically incorrect, sometimes causing significant damage to reputations and profitability. While hacktivists typically go after large, high-profile organizations, no organization should assume it is immune from hacktivists' wrath.

Introduction

As waves of demonstrations swept across the Middle East in response to an American-made, anti-Muslim YouTube film called "The Innocence of Muslims," the Izz ad-Din al Qassam Cyber Fighters had something else in mind to express their outrage.[1] They launched a series of politically motivated denial of service (DoS) web attacks against U.S. financial institutions. Even though the banks had no direct connection to the film, the attacks overwhelmed their websites and caused activity to slow and in some cases shut down entirely. Many of the largest U.S. financial institutions were targeted, including Bank of America, U.S. Bancorp, SunTrust, Capital One, Regions Financial, PNC and Wells Fargo.

In an email claiming responsibility for the attacks the al Qassam group stated:

"In the system where the religion and sacred things are not honorable, and only material, money and finance have value, this seems a suitable and effective way to act and can influence governors and decision makers."[2]

Although the banks had nothing to do with the film, in the eyes of the attackers they represented much of what was wrong with western culture.

Hacktivism is the technology world's approach to political activism. Unlike conventional hacking, cyber-attacks against businesses or goverment agencies are not for financial gain, but rather are intended to cause embarrassment and reputational damage.

Hacktivism is the technology world's approach to political activism. Unlike conventional hacking, cyber-attacks against businesses or government agencies are not for financial gain, but rather are intended to cause embarrassment and reputational damage. Utilizing the skills of computer experts to protest for or against a specific cause, hacktivism in its milder forms can blur the line between illegal hacking and the right to protest, which is an essential element of freedom of speech. In its more extreme manifestations, hacktivists are differentiated only by motive from cyber thieves who plunder digital information for personal gain. Often, hacktivists are more destructive and disruptive than cyber thieves, who typically prefer to slip in and out of systems unnoticed.

Hacktivist attacks are continuously evolving and difficult to prevent. In the al Qassam example, U.S. Defense Secretary Leon Panetta described the attack as "unprecedented" in terms of scale and speed.[3] As the tools have evolved so have hacktivist tactics. Tactics designed to embarrass or disrupt a company through website defacements, virtual sit-ins and denial-of service (DoS) attacks, previously the hacktivist methods of choice, are being replaced by attacks designed to inflict damage and cause embarrassment by stealing sensitive information.[4]

Although Hacktivism has been a component of the activist arsenal since the early days of the Internet, the movement has recently been reinvigorated thanks largely to a loosely affilated international group of individuals referred to as "Anonymous."

Organizations may not imagine themselves to be an attractive target for a hacktivist attack, but increasingly, it is a situation that many will confront. Large, high-profile organizations are preferred targets, but organizations of any size that offend the political or social sensibilities of any of a wide range of hacktivist organizations can find themselves targeted. In the digital realm attacks can originate from anywhere in the world, for any perceived violation of a political principle.

Defending against an attack can be challenging if not impossible. Many of the world's most powerful companies and governments -- those with seemingly limitless financial resources and state of the art defenses -- have found themselves victims of attacks. For this reason it is vital for organizations to understand their exposures, take proactive steps to mitigate their risks and be prepared to respond quickly and effectively if need be. Becoming a victim of a hacktivist attack can have devastating consequences, but investing the time and resources in preparation can significantly improve the outcome.

The Evolution of Hacktivism

"Hacktivist," a term coined in the mid 90's by a member named Omega of the hacker collective Cult of the Dead Cow (cDc) is a movement that has evolved over time. Early hacktivists', campaigning against censorship and human rights abuses, primarily used tactics designed only to embarrass or exploit an organization or government agency. Their aim was not necessarily to cause irreparable damage which is sometimes the case today.

Many early hacktivists also went to great lengths to maintain credibility by remaining consistent in their message and objectives. For example, in 1998 a U.S. hacker group called Legions of the Underground declared cyberwar on Iraq and China. The organization was prepared to execute cyber-attacks in an attempt to disrupt Internet access in protest of human rights abuses. Shortly after the declaration, a world coalition of hackers condemned the move and issued the following statement.[5]

> *We –the undersigned – strongly oppose any attempt to use the power of hacking to threaten to destroy the information infrastructure of a country for any reason. One cannot legitimately hope to improve a nation's free access to information by working to disable its data networks.*[6]

Although Hacktivism has been a component of the activist arsenal since the early days of the Internet, the movement has recently been reinvigorated thanks largely to a loosely affiliated international group of individuals referred to as "Anonymous." With some of Anonymous' activities, the line that was crossed by Legions of Underground back in the 90's is again coming into question. Anonymous originated in 2003 representing the concept of many online and offline community users of an anarchic, digitized global brain. Around this time the blackhat hacker and hacktivist communities began converging, enhancing the capabilities and sophistication of hacktivist attacks.

The resurgent hacktivist movement we see today did not occur until years later, largely as a result of WikiLeaks and its highly publicized and extremely controversial posting of classified documents from the U.S. government. In response to WikiLeaks actions, major businesses such as Amazon, PayPal, MasterCard, Visa and Bank of America among others attempted to distance themselves from the organization. In retaliation for perceived censorship, as part of "Operation Payback," Anonymous began to bombard the websites of the WikiLeaks opponents with distributed denial of service (DDoS) attacks. Operation Payback has since been referred to as the first war over digital information.[7]

Today, seemingly no business or government agency is immune from an attack, attacks that frequently use sophisticated tactics previously common only among blackhat hackers to access sensitive information.

The hacktivist movement, predominately under the banner of Anonymous and its offshoot organizations, has since grown significantly, using web site defacements, DoS attacks, and data theft to champion their vision of Internet freedom and human rights. Anonymous' targets have included Sony, Fox, PBS, HBGary Federal, Verizon, the U.S Secret Service, the FBI, The Vatican, the Dutch National High Tech Crime Unit, and The Australian Federal Police among many others.[8] In fact, as this report was being written, Anonymous declared 'cyberwar' on Isreal and claimed responsibility for taking down Israeli government websites and leaking passwords for what it calls Israel's "barbaric, brutal and despicable treatment" of Palestinians.[9]

While effective in drawing attention to itself, the group, which has no formal leadership, governance structure or even criteria for membership, lacks a consistent message. It is often contradictory in its actions and divergent from what some regard as hacktivism's true purpose. For example, this past election Anonymous was both encouraging people to vote through their "Occupy the Vote" campaign and declaring war on the U.S. government over proposed cyber legislation.[10]

Today, seemingly no business or government agency is immune from an attack, attacks that frequently use sophisticated tactics previously common only among blackhat hackers to access sensitive information. Hacktivism went from simply being a nuisance for a few organizations caught in the cross-hairs of a political or social cause to a significant threat to potentially every business and government agency. In fact, according to a 2012 Cyber Security Survey of IT security professionals by Bit9, 64 percent of respondents believed their organization will be targeted by Anonymous or other hacktivist group within the next six months.[11]

Forms of Hacktivism

"Adaptable" and "creative" are two of the more positive adjectives used to describe the hacktivist community. Both are necessary in order to stay a step ahead of defenses and maintain relevance in the public eyes. As new opportunities and technologies emerge, hacktivists must continuously adapt their methods and strategy. The following are some of the more common hacktivist tactics currently being applied.

Denial-of-Service (DoS) Attack: DoS attacks are designed to prevent legitimate users from accessing information or services from a particular website. The most common DoS attack occurs when an attacker "floods" the server hosting the target website with requests for information. Servers can only process a defined number of requests at any given time and if overloaded will be unable to process a request and cause the server to slow or crash.

Distributed Denial-of-Service (DDoS) Attack: DDoS expand on DoS attacks. In a DDoS attack, hackers activate a network of computers under its control (known as a botnet) to send huge amounts of data to a website. The attack is referred to as "distributed" because the attacker is using multiple computers to launch a DoS attack.[12]

Website Defacements: By gaining unauthorized access to a web server, a hacker can either replace or manipulate a webpage with new information in an attempt to convey a particular message.

Site Redirects: Also by gaining unauthorized access to a web server, hackers can adjust the address settings and cause the website users to go to a website of their choosing.

Virtual Sit-In: A mass form of hacktivism. Virtual Sit-Ins are essentially a DoS attack that involves individual protestors manually reloading web pages.[13]

Hactivists now frequently look to damage and embarrass their targets by stealing sensitive and highly valuable corporate and personal information. Stolen trade secrets, confidential documents, and personal identifiable information (PII) cause significantly more damage and create substantially more publicity for their intended cause.

Information Theft: An increasingly preferred method of hacktivism, this is a method that involves a greater degree of malicious intent. Information theft involves illegally obtaining access to a computer or network and stealing private information.

Warning Tactic: Unlike hackers who use their computer prowess for financial gain, hacktivists' seek publicity for a specific cause. A frequently used tactic designed to draw attention to them and their cause is to warn their targets of an impending attack. In fact, in nearly 75 percent of hacktivist attacks in 2011, the targets were forewarned. This is a tactic not often, if ever, used by financially motivated hackers.[14]

Diversion Tactics: Rarely seen in the past, diversion tactics are becoming increasingly common within hacktivist circles. DoS attacks are used as a distraction mechanism while attackers simultaneously target another part of a company's network. DoS attacks also are used to draw attention away from a more comprehensive plot. For example, while still too early to tell for sure, some experts suggest that the al Qassam attacks are the beginning of a more comprehensive scheme of malware intrusions and insider attacks against banks of all sizes.[15]

Information Privacy Exposure from Hacktivists

In the years following the digital war over Wikileaks, the online world has increasingly become a battleground of conflicting ideals and principles. Consequently, the word hacktivism and hacktivist have become commonplace in the vernacular of many outside those just in tech and information security circles. The magnitude of these online protests, retaliation campaigns and pranks has garnered the attention of individuals at the highest levels of business and government. In fact, according to a Zurich sponsored Advisen study on the current state of and trends in information security and cyber liability risk management, board members and executive management increasingly recognize the risks of a wide range of exposures commonly exploited by hacktivists such as stolen data and violation of privacy laws.[16]

The core tactics of hacktivists have shifted from relatively benign attacks designed to make a statement and/or disrupt a website (e.g. DDoS attacks and website defacements) to those with more sinister intentions and consequences. Hacktivists now frequently look to damage and embarrass their targets by stealing sensitive and highly valuable corporate and personal information. Stolen trade secrets, confidential documents, and personal identifiable information (PII) cause significantly more damage and create substantially more publicity for their intended cause.

In fact, according to a Verizon report, "many, troubled by the shadowy nature of [Anonymous'] origins and proclivity to embarrass victims, found this trend more frightening than other threats, whether real or imagined."[17] According to the same Verizon report, while hacktivists' represented between only 2 to 3 percent of all attackers in 2011, they were responsible for 58 percent of total breached records.

Unlike a DoS attacks or website defacements the consequences of a data breach are far greater and can have lasting implications. Not only can a breach put an organization in violation of any number of data security and privacy regulations and standards, it can have significant financial consequences, including the costs to identify and repair the breach, to comply with state breach notification laws, and potentially to provide credit monitoring services and other loss mitigation services. Most importantly however, is the impact it can have on one of an organization's most important assets, its reputation.

NOTES:

[1] The Izz ad-Din al Qassam attacks may be much more than religiously/socially motivated. The group has been linked to Hamas, and some experts believe it is being financed by Iran, which may be using the video as a cover for retaliation against sactions or for testing stage-sponsored cyber terrorism tactics. See http://openchannel.nbcnews.com/_news/2012/09/20/13990206-officials-see-iran-not-outrage-over-film-behind-cyber-attacks-on-us-banks?lite.

[2] Brian Browdie, American Banker, "Al Quassam Hacktivists Say Cyberattacks on Banks to Continue", (November 2012), http://www.americanbanker.com/issues/177_212/al-qassam-hacktivists-say-cyberattacks-on-banks-to-continue-1054052-1.html?zkPrintable=true

[3] Brian Browdie, American Banker, "Al Quassam Hacktivists Say Cyberattacks on Banks to Continue", (November 2012), http://www.americanbanker.com/issues/177_212/al-qassam-hacktivists-say-cyberattacks-on-banks-to-continue-1054052-1.html?zkPrintable=true

[4] Kelly Jackson Higgins, dark Reading, "'Anonymous' Legacy: Hacktivists Stole More Data Than Organized Crim in 2011 Breaches Worldwide", (March 22, 2012), http://www.darkreading.com/database-security/167901020/security/news/232700065/anonymous-legacy-hacktivists-stole-more-data-than-organized-crime-in-2011-breaches-worldwide.html

[5] Elinor Mills, CNET News, "Old-time hacktivists: Anonyomous, you've crossed the line", (March 2012), http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/

[6] http://www.cultdeadcow.com/news/statement19990107.html

[7] Noah C.N. Hampson, "Hacktivism: A New breed of Protest in a Networked World," 35 B.C. Int'l & Comp. L. Rev. 511 (2012), http://lawdigitalcommons.bc.edu/iclr/vol35/iss2/6

[8] Kelly Jackson Higgins, dark Reading, "'Anonymous' Legacy: Hacktivists Stole More Data Than Organized Crim in 2011 Breaches Worldwide", (March 22, 2012), http://www.darkreading.com/database-security/167901020/security/news/232700065/anonymous-legacy-hacktivists-stole-more-data-than-organized-crime-in-2011-breaches-worldwide.html

[9] John D. Sutter, CNN, "Anonymous declares 'cyberwar' on Isreal", (November 20, 2012), http://www.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html?hpt=hp_bn5

[10] Elinor Mills, CNET News, "Old-time hacktivists: Anonyomous, you've crossed the line", (March 2012), http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/

[10] http://www.cultdeadcow.com/news/statement19990107.html

[11] Steve Ragan, Security Week, "InfoSec Professionals Concerned About Anonymous", (April 2012), http://www.securityweek.com/bit9-survey-infosec-professionals-concerned-about-anonymous

[12] US-CERT: United States Computer Emergency Readiness Team, "Understanding Denial-of-Service Attacks", http://www.us-cert.gov/cas/tips/ST04-015.html

Reputational Damage Exposures from Hacktivists

According to the Zurich-sponsored Advisen study, reputational damage resulting from a data breach was the second highest cyber liability risk management concern, just slightly behind privacy violations due to a breach of customer records. The concern is for good reason as it can take years to develop a good reputation in the marketplace and only moments for it to be tarnished as a result of a breach. Studies by the Ponemon Institute and Javeline Strategy & Research have shown that many consumers have diminished confidence in an organization's ability to protect and manage personal data due to a breach and will be less likely to do business or continue doing business with them in the future. Groups such as Anonymous understand this, which is why they believe their targeted attacks are impactful for the cause and painful for the target.

While there is yet to be a widely accepted method of quantifying the reputational impact of a hacktivist attack, there is consensus that the type of attack and type of company play a role in the severity. For example, financial services, healthcare and retail are three industries frequently targeted by cybercriminals. The reason being, these industries are entrusted with and responsible for a wealth of personal identifiable information including heath records, credit card numbers and social security numbers among others. A breach of any of this information can severely impact customers' and future customers' trust, and have significantly greater reputational consequences.

Organizations can combat some of the reputational consequences of a hacktivist attack, including the breach of PII, by having a plan in place to reduce its impact.

Risk Mitigation

While IT departments are responsible for spearheading data security and privacy initiatives in most organizations, more are beginning to believe that it is an enterprise-wide responsibility to mitigate risks. According to the Advisen/Zurich study, nearly two-thirds of all organizations surveyed have a multi-departmental information security risk management team or committee.

Hacktivism has been referred to as a business problem, not a technology problem[18] and developing an enterprise-wide information security risk management team or committee is an essential first step for a business to manage that problem. By creating a security risk management team, organizations are not only bringing awareness to the issues of cyber security but also forming relationships between important players/departments (i.e. legal and PR) who will play primary roles in breach response.

The security risk management team or committee must first have a comprehensive understanding of the organization's exposures (i.e. the data collected and stored, as well as who has access to it and the means by which it is accessed) in order develop a plan to both secure the system and respond to an attack. A tool to help businesses think about and frame discussions about privacy and data security is the Organization for Economic Co-operation and Development (OECD) Privacy Principles.

Internationally, the OECD Privacy Principles are the most commonly used privacy framework. They are reflected in existing and emerging privacy and data protection laws, and serve as the base for the creation for leading practice privacy programs and additional programs.[19] (See Next Page)

[13] Noah C.N. Hampson, "Hacktivism: A New breed of Protest in a Networked World," 35 B.C. Int'l & Comp. L. Rev. 511 (2012), http://lawdigitalcommons.bc.edu/iclr/vol35/iss2/6

[14] Andy Greenberg, "Verizon Study Confirms 2011 Was The Year of Anonnymous, With 100 Million User' Data Breached by Hacktivists", (March 2012), http://www.forbes.com/sites/andygreenberg/2012/03/22/verizon-study-confirms-2011-was-the-year-of-anonymous-with-100-million-credentials-breached-by-hacktivists/

[15] John Adams, Bank Technology News, "Hacktivists' Next Steps", (November 2011), http://www.americanbanker.com/btn/25_11/tech-and-risk-minds-work-on-locating-next-bank-attack-1053873-1.html

[16] Advisen, "Information Security & Cyber Liability Risk Management", (October 2012), http://corner.advisen.com/pdf_files/Zurich_2012Cyber_SurveyReport.pdf

[17] Verizon, "2012 Data Breach Investigations Report", http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[18] Jeffrey Roman, Bankinfo Security, "Hacktivism: Communication Plays Key Role", (June 2012), http://www.bankinfosecurity.com/hacktivism-how-to-respond-a-4895/op-1

[19] OECD, "OECD Privacy Principles", http://oecdprivacy.org/

[20] OECD, "OECD Privacy Principles", http://oecdprivacy.org/

The following are the privacy principles in the OECD guidelines governing the protection of privacy and transborder flow of personal data:[20]

1. ***Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means an, where appropriate, with the knowledge or consent of the data subject.*
2. ***Data Quality Principle**: Personal Data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*
3. ***Purpose Specification Principle**: The purpose for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*
4. ***Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except:*
   a. with the consent of the data subject: or
   b. by the authority of law.
5. ***Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.*
6. ***Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*
7. ***Individual Participation Principle**: An individual should have the right:*
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller had data relating to him;
   b. to have communicated to him, data relating to him;
   c. to be given reason if a request is denied, and to be able to challenge such denial;
   d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended;
8. ***Accountability Principle**: A data controller should be accountable for comply with measures which give effect to the principles stated above.*

The OCED Privacy Principles provide a framework for complying with privacy laws, but they cannot prevent determined hacktivists from spreading mayhem. Even the most sophisticated companies have been victimized. Hacktivist attacks require a quick, concise and coordinated response and therefore the organization should approach it with a communications strategy in mind. How a business responds to an attack in the eyes of public perception is the most important aspect of reducing the reputational consequences. As part of the information security risk management plan, organizations also should consider specialized insurance designed to cover response costs, including the costs of PR specialists as part of their insurance portfolio.

Conclusion

The fact that Anonymous is now practically a household name is evidence of how effective hacktivism can be. Hacktivists may rarely be successful at getting companies or government agencies to change their behavior, but they can be very effective at drawing attention to their causes. Hacktivists undoubtedly will be a feature of the online world for the foreseeable future, and no company or organization can assume they will not fall victim to a hacktivist attack. As part of their cyber risk management programs, organizations should assume they will someday be victimized, and plan accordingly.