Global Information Assurance Certification Paper

Eva Dadok

HACKTIVISM – A FREE FORM OF EXPRESSION OR A DIGITAL VANDALISM?

It is rather unlikely that you are not aware of havoc malicious hackers can create once they break into a computer system. Words such as cracker, virus, cyber-attack, and system vulnerability made it quickly into our vocabularies, maybe because something negative happens now in the cyber-world almost everyday. Those words became part of our reality. How about HACKTIVISM though? Chances are that the answer to your query will be " No entry found for 'hacktivism' in the dictionary." However, does it mean it is not out there? This new trend seems to be growing stronger, it is global, and at this point, there are no laws restricting or regulating it.

What is hacktivism?

It is a new movement of expressing someone's disappointment with something (usually it has to do with political ideas) by breaking into opponents websites or e-mail system. Activists, who use this form of expressing themselves, also call it a method of allowing them to propagate the idea of Electronic Civil Disobedience (ECD) among citizens.

Who are hacktivists?

According to one definition hacktivists are people who fight for different political reasons and stand up against some issue via creating disruptive actions using Internet. Their purpose is to mobilize public opinion against institutions, most often government, but anyone can became a target. Their reasons for troublemaking are claimed to be good for all humans. For instance: fight for human rights, fight against death penalty, to heal the sick, to raise the dead, to eliminate anarchy and servitude etc. Some sound reasonable, some others me be trivial. Hacktivists like to set themselves apart from pure crackers, who strike computer systems only to reveal system vulnerabilities or to steal information. Their main idea is to "just create disturbance" and to proof that they exist.

When it started?
The first notes about successful hacktivism go back to year 1998 when a group, called the Electronic Disturbance Theater, organized a net based action directed against the Mexican government. The group created a tool called FloodNet. This software helped in flooding the Mexican government websites. This supposed to be a "symbolic gesture" showing the brotherhood in supporting Mexico's Zapatistas. Then another event took place in the spring of 1998. A British hacker, using a nickname of "JF", placed anti-nuclear text and images on about 300 web sites after gaining successful access to them. Last year, during the Seattle protests against the World Trade Organization (WTO), a British group calling themselves "Electrohippies," was able to briefly shut down the WTO's Web site. Many other attacks came after that, including the most recent one such as an incident that happened on Election Day, Nov 7, 2000, when a democrat hacked the Republican National Committee web page and posted there an endorsement text for Vice President Al Gore. However, USA is not the only active spot for hacktivism. There is also dramatic increase in the number of attacks done by hackers associated with either Palestinian or Israeli sites, where they have been attacking each others web sites for weeks now due to the latest conflicts in this region.

How it is done?
Individuals or in most instances entire groups who have some supporting reason, will plan attacks on e-mail servers or openly accessible web pages. E-mail servers will be overloaded with fake e-mail communication and web sites will be hacked into and "decorated" with images or derogatory messages, which supposed to send some kind of political message. Another common strategy is "dos'ing" the enemy possibly via already mentioned tool, FlootNet. This tool allows executing "denial of service" (dos) attack, causing the target server to go down entirely. At a specific time online activists may trigger the message "It is time to commence flooding!" (It might be advertised earlier on their website or send via e-mail etc.) At that point all hacktivists will visit the group's web site and click on an icon that launches FloodNet program. This software can then point hacktivists' web browsers to the "web site of their affection" –>the target. The next step is to requests the same target page over and over again at a rate of about 10 times (or more) per minute. When a target computer receives an unusually large volume of requests it may become overwhelmed and it will crash. On other occasions, access to a target website will

be redirected to hacktivists website.
Although generally, these attacks don't alter operating systems or networks, they still impair services and deny the public access to websites containing information and violate other users' right to interconnect.
Even though IT industry creates better and more effective ways to protect networks, but the underground does always seem to stay ahead with "ready to go" attack scripts and protocols which can be freely downloaded from the Internet and launched against target sites. Unfortunately, attack tools are nowadays not only more sophisticated, but they have also become easier to use.

Can hacktivists be dangerous to your company?
You bet… If your network becomes a target, and your busiest server goes down, you are probably not likely to laugh about it. Your web site may get unwanted facelift with "never seen before" images or tasteless passage. Those elements are called electronic graffiti or digital vandalism, as people altering websites do it without permission.
The early attacks were performed mainly on government sites: the FBI, the US Defense Department, the Pentagon, as well as other countries governments including Mexican, Chinese and Indonesian. Those actions were related mainly to expressing anger about environmental degradation, poor working conditions etc.
A new group known as the "Yellow Pages" is forming in the US, Canada, and in Europe and wants to use Internet to fight for human rights in China. The group no longer wants to waste time on targeting government websites. They plans to target many US companies doing business with China such AT&T, Motorola, Yahoo, Sun Microsystems, Dell, Lucent, and Excite. The group says that the best form to be really noticed is to create severe damage and monetary losses by attacking those companies' networks. It is also necessary to realize the strength those groups actually have, because normally, 50 people protesting on the streets will not do much harm, where 50 people on line and equipped with good tools may have a good chance to cripple any network relatively easily.

Conclusion
It would be rather unwise to believe that this movement will just go away, knowing that the exploding use of the Internet allows reaching more people, more rapidly and less expensively than any other forms of communication.
Security professionals believe that there is no prevention of cyber-

attacks and the only solution is active defense and dealing with an event as it happens. Most companies are taking the threats very seriously and are installing sophisticated security mechanisms. Many also started to deploy plans directed toward 24x7 monitoring of their networks. Others fight the flood attacks by re-configuring their upstream routers. All security experts seem to agree that the number of attacks will only increase as more and more people are learning how to use computers. Unfortunately many still think that there is no need for ethics and etiquette in the cyber-space, and that there is nothing wrong in using computers and Internet to express their political disagreement, aggression and hate simply by vandalizing adversaries web pages or crashing the servers. The only problem with this approach is that it may eventually lead to very heavy Internet regulations, which will probably not bring a win-to-win situation for anyone.
But then again-who knows for sure?

References:

Hulme, George and Bob Wallace. "Beware of Cyber-attacks." Information Week, (November 13, 2000) : 22-24.

Martin, Hugh J. "Hacktivism: the new protest movement" April, 2000.URL: http://www.spark-online.com/april00/trends/martin.html

Vatis, Michael A. "NIPC Cyber Threat Assessment [FBI Seal]" October 6, 1999. URL: http://www.securitymanagement.com/library/fbi_nipc.txt

Slambrouck, Paul Van. "Newest Tool for Social Protest: The Internet." June 18, 1999. URL: http://www.globalpolicy.org/globaliz/special/internet.htm

McKay, Niall. "The Golden Age of Hacktivism" Sep. 22, 1998.URL: http://www.wired.com/news/politics/0,1283,15129,00.html

Graham-Rowe,Duncan. "To the virtual barricades" Sep 18, 1999.URL http://www.newscientist.com/ns/19990918/newsstory10.html

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS