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: April 26th, 2018

Upcoming Training

SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Mentor Session - AW SEC401	Detroit, MI	May 01, 2018 - May 17, 2018	Mentor
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS Bethesda SEC401 @ USO - Academy	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event