Know Your Enemy:
The Social Dynamics of Hacking

The Honeynet Project
http://www.honeynet.org

Thomas J. Holt– The Spartan Devils Chapter of the Honeynet Project
Max Kilger – The Spartan Devils Chapter of the Honeynet Project

Last Modified: *28 May 2012*

INTRODUCTION

The Know Your Enemy paper series is a collection of professional papers designed to provide in-depth insight into current security threats, as well as technical discussions of the application and analysis of new research tools and technologies. The focus on technological challenges and solutions is critical to improve security, though it is also vital to recognize the human element behind any technical attack. Attackers have various motives, skills, and relationships, though these may often be ignored when focusing on security solutions to defeat their efforts. The human element must, however, be given greater consideration in order to improve our knowledge of all facets of attackers. In fact, individuals can engage in attacks from around the world and target any resource from critical infrastructure to financial institutions using varied techniques. Though a substantive body of research examines both the continuing evolution of attack techniques in the attacker community and technical solutions to mitigate these tactics, there is a relative lack of research on the social dynamics and human aspects behind these actions. Such information is vital, however, to improve our understanding of the nature of attackers around the world. In this paper, we will explore the various facets of the global hacker community, including the distribution of skill, social relationships between actors, and common motives of attackers. We will also explore the prospective future of attacks and attacker behavior in order to improve our general understanding of the hacker community.

The Composition of Skill in the Hacker Community

The development of the Internet and modem technology transformed the nature of hacking from local computer enthusiasts working together to share information into a worldwide network of skilled and unskilled actors with diverse interests and capabilities. While there are myriad definitions for hacker (Bachmann, 2010; Jordan & Taylor, 1998; Schell & Dodge, 2002; Taylor, 1999), the most comprehensive and accurate terms identify hackers as individuals with an interest in technology who use their knowledge to access computers and devices with or without authorization from the owner (Schell & Dodge, 2002). This definition recognizes that hacking involves an application of knowledge and may done legitimately with permission from a system manager, or maliciously without approval. It is unknown how many individuals are actually involved in hacking due to the secretive nature of this subculture. For example, Jordan and Taylor (1998) estimated that there are at least 100,000 hackers worldwide, though this figure has undoubtedly increased substantially over the last 15 years. Despite difficulties in quantifying the hacker population, there is substantive evidence that the hacker community is a strong meritocracy where individuals are judged on their skill and ability to manipulate technologies in ways never before seen or intended. Those who can devise unique tools and identify new vulnerabilities garner respect from their peers and develop a reputation for skill and ability within the subculture.

The distribution of skill within the hacker community is pyramidal in nature (see Figure 1). At the top resides a very small number of skilled actors who have substantive abilities to identify new vulnerabilities, create exploits, and implement new programs that can be used for various attacks. These individuals are what Holt and Kilger (2008) refer to as “makecraft” hackers because of their capacity to make whole-cloth tools that otherwise did not exist. Other researchers may call these individuals elite hackers, or black/white/grey hat hackers (Furnell, 2002; Jordan and Taylor, 1998) depending on their ethical outlook. Attackers that possess these high level skills pose the greatest threat because they have both the creativity and knowledge base to identify unknown exploits and unusual attack vectors that may have been otherwise ignored.

Below these high skill actors resides a larger population of semi-skilled actors who can recognize and use various tools and exploits, though they often do not have the technical proficiency or interest to generate these tools on their own. As a result, they may utilize tools and tactics from the makecrafters in order to engage in various attacks. These individuals may also be called "techcrafters" as they can implement and adapt existing tools to suit their needs, but generally do not create these tools on their own (Holt & Kilger, 2008). This population of hackers have become extremely important in the hacker community over the last decade with the emergence of malware and stolen data markets (Chu, Holt, & Ahn, 2010; Franklin, Paxon, Perrig, & Savage, 2007). The middle tier of skilled hackers can often buy tools from extremely proficient actors, and apply these resources in the course of attacks. In turn, the information or data they acquire can be resold to others for a profit.

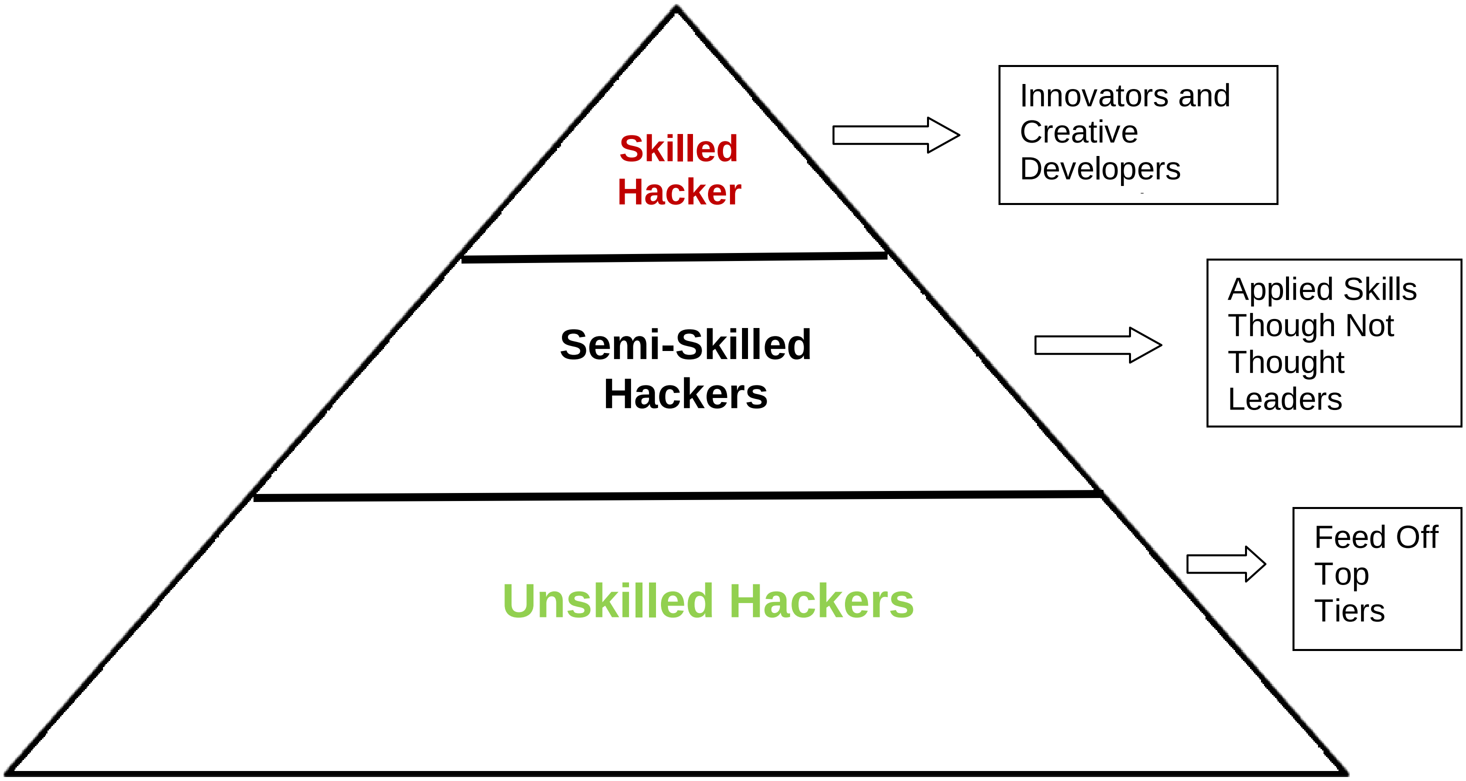

Skilled Hacker
Innovators and Creative Developers
Semi-Skilled Hackers
Applied Skills Though Not Thought Leaders
Unskilled Hackers
Feed Off Top Tiers

Figure 1: The Distribution of Skill in the Hacker Community

Finally, the bottom of the pyramid is populated by low or unskilled hackers who may otherwise be referred to as script kiddies or noobs (Furnell, 2002; Jordan & Taylor, 1998). These actors have little understanding of the mechanics of an attack or compromise, and depend entirely upon the ingenuity of other hackers in order to engage in attacks. They recognize and value engaging in different compromises, but do not have a functional appreciation for the ways that an exploit actually impacts system processes. As a consequence, their attacks are often of little consequence and pose at best a nuisance to computer security personnel and administrators.

At the same time, script kiddies can serve as an attack point for more skilled hackers. For instance, many script kiddies will download copies of existing malware in the hopes of using it for their own agendas. These kits may, however, be joined with rootkit malware to infect that script kiddie's computer by a more skilled actor (see Chu et al., 2010). In turn, these infected computers can be used as an effective launch site, or monitored in order to mask the activities of skilled hackers. In addition, these infected computers may act as an early warning system for more skilled hackers. When authorities investigate the script kiddie, this alerts the more skilled hacker that they may need to move on from this source and alter their malware coding in the process to reduce the likelihood of detection.

It is also important to note that the emergence of the on-line black market have enabled low skill attackers to pay for hacking services managed by moderate and highly-skilled actors. For instance, a mid-tier hacker operating a large botnet can lease out their infrastructure to others for DDoS attacks, spam distribution, or proxy servers to low or unskilled actors. This means the script kiddie can now more effectively engage in attacks while at the same time create a lucrative business model for the more proficient actors in the community (see Chu et al., 2010; Holt & Lampke, 2010). This evolution in information sharing and resource generation has had a profound impact on the hacker community, and on the nature of computer security and investigation as a whole.

The Global Distribution of Skill

The distribution of skill appears to be somewhat consistent in industrialized nations including China, Russia, the United States, and other early adopters of the Internet. It is not clear, however, if these populations are truly equal across place. For instance, there are certain attacks that can be regularly associated with actors from a given nation, such as the use of web defacements by hackers in Turkey, Pakistan, and India (Holt, 2009b). Similarly, there is substantive evidence that a number of actors in Brazil, China, Russia, and Romania are involved in the creation and distribution of malware and sophisticated zero day exploits targeting financial institutions and government agencies. As a consequence, there is a need for substantive research to assess the size and skill of hacker populations across place. A small number of studies have tried to accomplish such a task with extremely limited success such as Chiesa, Ducci, and Ciapi (2008) recently attempted to survey a wide population of hackers across the globe. They received 216 completed surveys from over 20 countries, though the participants were not evenly distributed across geographies and had to voluntarily participate. As a result, this large sample is not likely representative of the larger hacker community, especially active criminal hackers. Thus, there is a need for expansive study in this area to identify the distribution of ability within and across different geographies.

It is also not clear how hacker populations in nations that have just come on-line in the last decade, such as northern and central Africa and parts of Latin America, may engage in different forms of attacks. Since the Internet enables geographically dispersed groups to share information and attack tools, it is plausible that it will take less time for emerging hacker communities to expand their overall efficacy. Kilger (2007) has suggested that there is a potential emerging serious threat as a consequence of some of these developing countries coming online. Countries where there are a large proportion of individuals living in poor economic conditions with little hope of mobility and significant amounts of time on their hands and a digital window into a global economy with electronic access to vast amounts of capital would seem to be a fertile breeding ground for cybercriminal activity. This is evident in the emergence of 419 scammers operating out of Nigeria and other parts of Africa where economic opportunities are scarce and success can be made through persistent operations against victim populations (Adineran, 2007; Holt & Graves, 2007; King & Thomas, 2010; Warner, 2011).

In fact, Holt (2008) tracked the creation of various pieces of free malware moved across multiple nations with attribution to various creators in a relatively short period of time. One stand-alone DDoS attack tool called Try2DDOS which was created by a French hacker appeared as a download in diverse hacker sites across the globe, including Argentina, China, Ecuador, Guatemala, and Russia (see Figure 2). This demonstrates that hacker groups look at websites across disparate geographic places in order to find new tools, and will share resources with others when it appears to be effective. In turn, this exchange of exploits may enhance the skill-sets of hacker communities over time as they study the exploit examples they have acquired and may facilitate and accelerate the evolution of more highly skilled hacking groups at a faster pace than seen in previous decades.

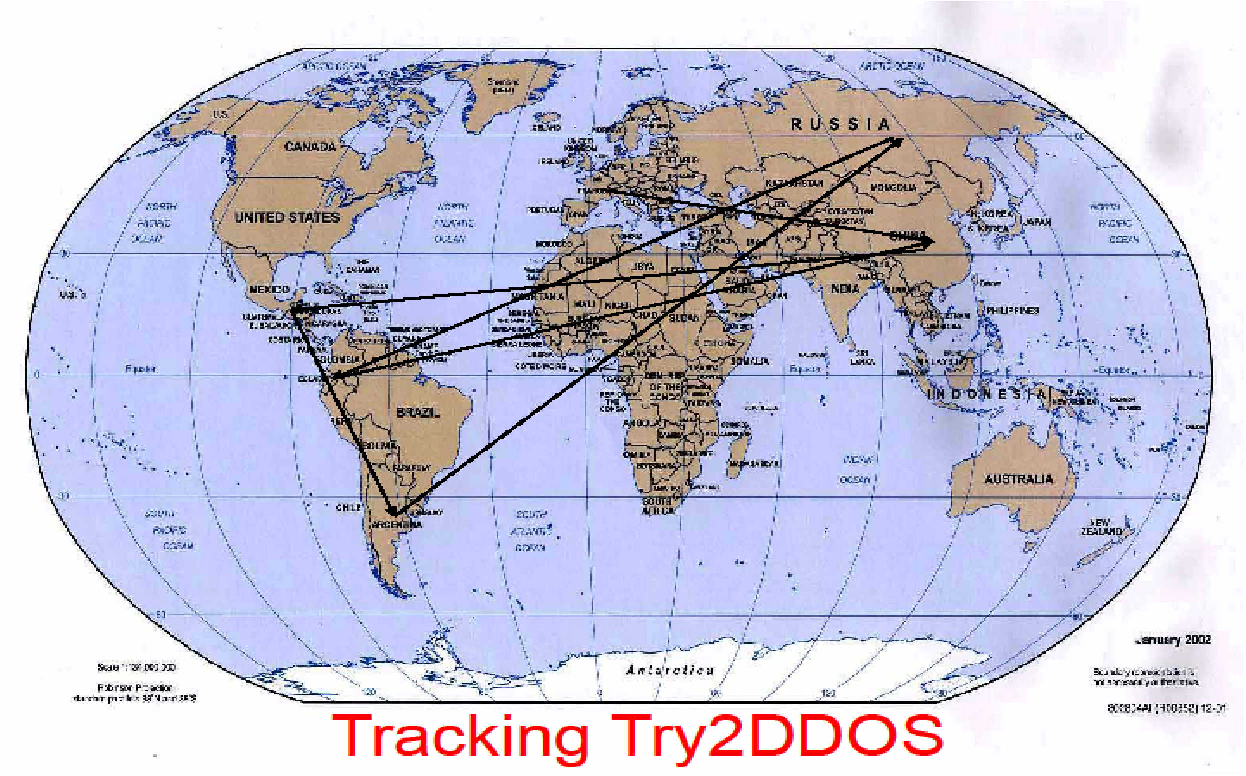


Figure 2: Examining the Distribution of Malware Around the World

Social Relationships in the Hacker Subculture

Hackers are not born, but rather emerge slowly from the confluence of native technical aptitude, access to technology, and prolonged virtual and face-to-face socialization with others who share similar norms and values. Often researchers focus upon virtual socialization experiences that help instill the norms and values of this subculture, but some of the most important relationships develop in face-to-face settings (Holt, 2007). The different environments in which these social processes occur play an important role in the early formative years of persons who eventually identify themselves as hackers. In this section, some of the social processes and forces involved in shaping both hacking and the hacker community are discussed.

The importance of technology for hackers often emerges early in youth. Many who become involved in the hacker community report developing an interest in technology at an early age. Hackers report gaining access to computers in their early teens or even younger for hackers in the late 1990s to the present (Bachmann, 2010; Holt, 2007). Simply utilizing computers in public cafes and schools can also help pique a hackers' interest in technology (Holt, 2009b). In fact, in nations where home Internet access is expensive, like Turkey and Iran, hackers often report using computers in cafes and other public locales in order to connect with others. Identifying peers who share their affinity for technology on or off-line is also extremely valuable because it helps to maintain their interests.

On-line Relationships

Hackers maintain loose peer associations with individuals in on-line environments that may be useful in the development of their skill and ability (Holt, 2009, 2010; Holt & Kilger, 2008; Meyer, 1989; Schell & Dodge, 2002; Taylor, 1999). There are myriad communities operating via computer-mediated communications across the globe for hackers at every skill level to identify others who share their interests, including Internet Relay Chat (IRC), forums, blogs, social networking sites, and other on-line environments (Holt, 2007, 2009a, b, 2010). Hackers have operated in Bulletin Board Systems (BBS) since the late 70s and early 1980s to provide information, tools, and techniques on hacking (Meyer, 1989; Scott, 2005). The content was posted in plain text, and occasionally featured images and art made from ASCII text, in keeping with the limitations of technology at the time. These sites allowed asynchronous communications between users, in that they could post a message and respond to others. In addition, individuals hosted downloadable content including text files and tutorials, though some also hosted pirated software and material called warez (Meyers, 1989). The BBS became an important resource for new hackers since experienced technology users and budding hackers could share detailed information about systems they explored and discuss their exploits (Landreth, 1984).

The BBS allowed hackers to form groups with private networks and password protected boards to keep out the uninitiated and maintain privacy (Landreth, 1984; Meyer, 1989). Closed BBS were initially local in nature based on telephone area codes, but changed with time as more individuals obtained computers and sought out others on-line. Local hacker groups grew to prominence as a result of BBS based on their exploits and intrusions into sensitive computer systems, such as the Masters of Disaster and the Legion of Doom (Slatalla & Quittner, 1995). As a result, it is common for modern hackers to belong to multiple forums and websites in order to gain access to pivotal resources on-line (see Figure 3; Holt et al., 2009).

As on-line communications services evolve, so too do the communication practices of hacker groups. In fact, the global distribution of the hacker population has resulted in regional variations in CMCs based on local preferences. For instance, Russian hacker groups appear to utilize IRC, forums, and some social networking sites like Vkontakte or LiveJournal in order to connect with others (Holt et al., 2009), though they utilize ICQ for instant messaging and private exchanges (Chu et al., 2010). Turkish hackers, however, prefer MSN messenger, forums, and email and find IRC to be of limited value (Holt, 2009b). Finally, some Chinese hackers appear to use Baidu and QQ more frequently in order to communicate (Holt, Soles, & Leslie, 2008). Thus, security researchers and law enforcement must consider the local communications preferences of a given nation in order to properly investigate malicious actor groups.

In addition, communication services can aid in the identification of links between hackers within and across various groups. In fact, some hackers maintain membership in multiple hacking groups and identifying friendship networks can provide important clues to the social dynamics of both intra-group as well intergroup interactions. Figure 3 below illustrates social ties among a number of active Russian hacking groups. The thickness of the connecting line represents the strength of social ties and communications among the different groups (Holt et al, 2009).

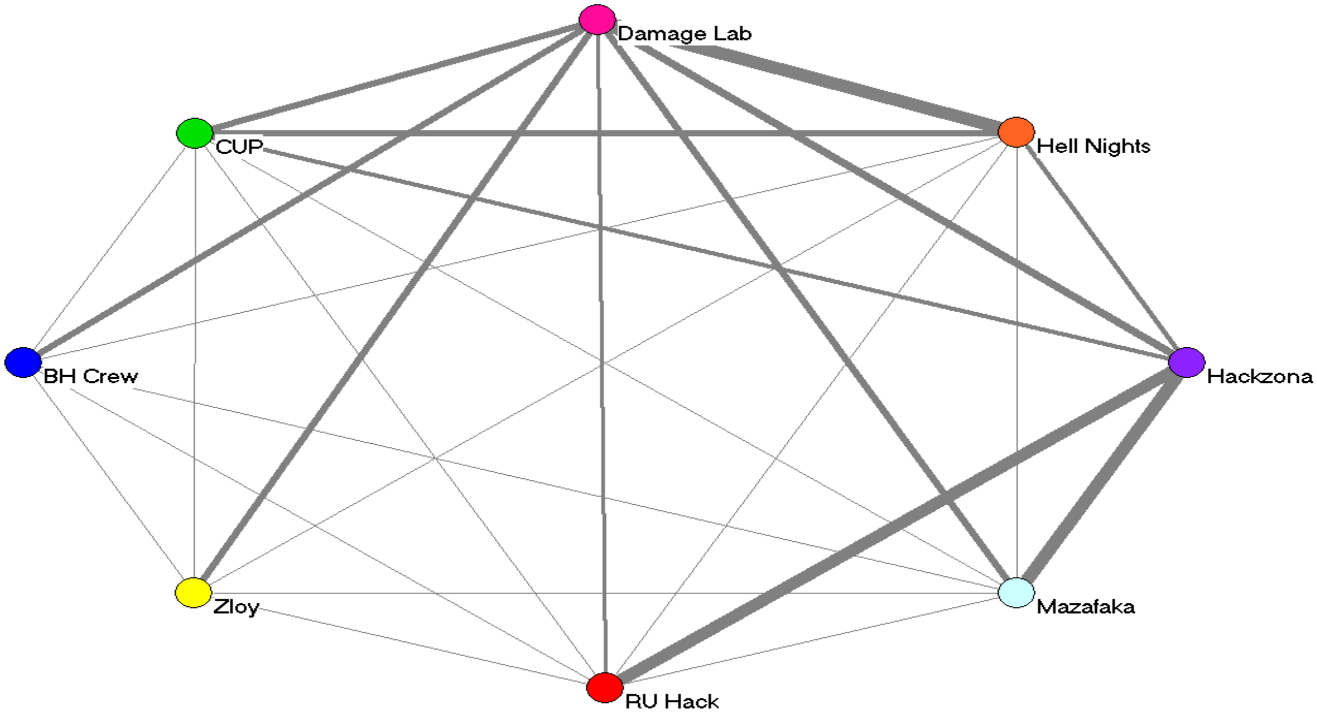
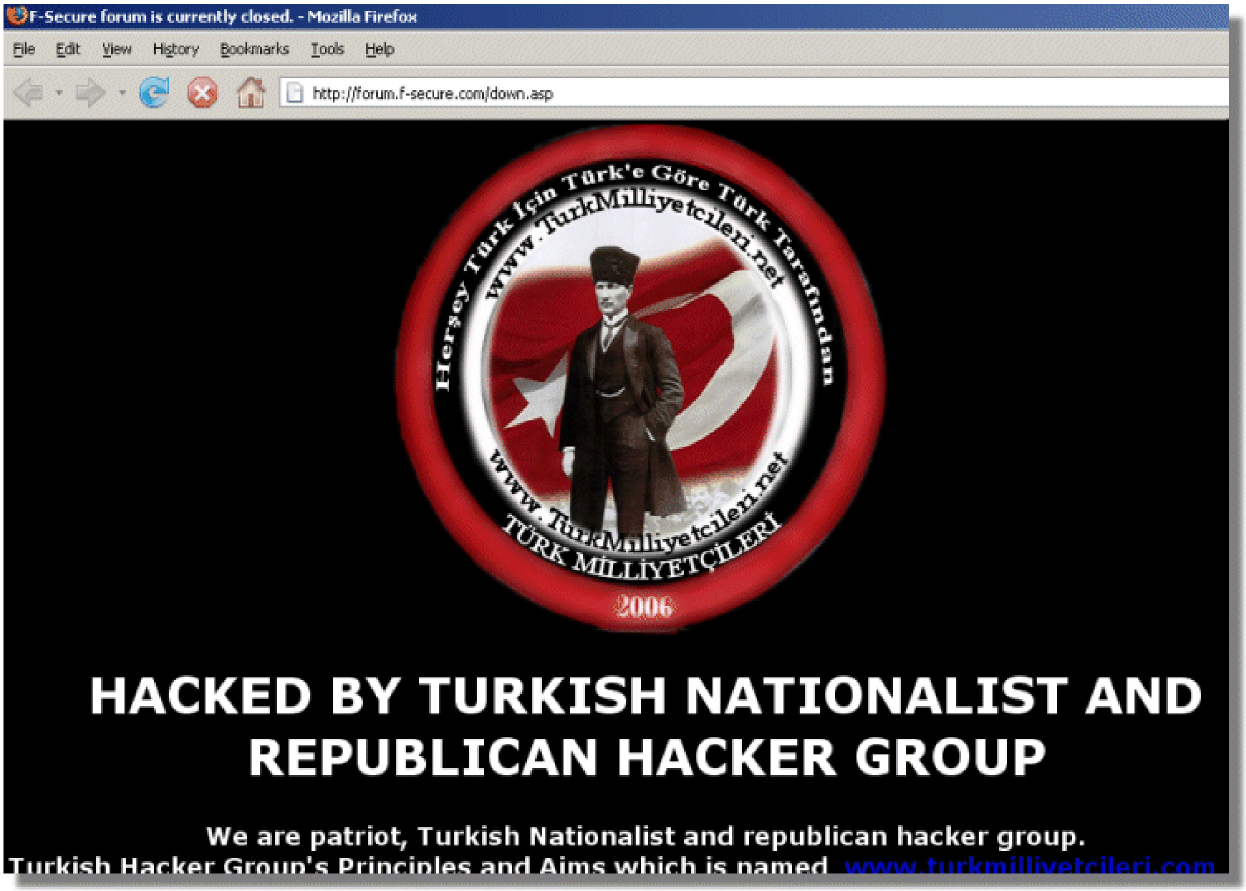


Figure 3: Visualized Relationships between Participants in Russian Hacker Forums (from Holt et al. 2009)

It is also important to note that there are variations in the way that hacker groups share information with others. Skilled hackers may create and post tutorials or how-to manuals on various topics ranging from the use of certain exploits to techniques involving credit card fraud and data manipulation (Chu et al., 2010; Holt 2009b).

The emergence of video sharing sites like YouTube has also enabled individuals to create detailed guides on attack techniques. In fact, the Turkish hacker Iscorpitz regularly posted videos detailing how he performed mass web defacements against various targets (Holt, 2009b). Additionally, Turkish hacker groups regularly create videos featuring images of the websites they deface along with shout outs to the members of their group and others who they feel deserve respect (see Figure 4; Holt, 2009b).


F-Secure forum is currently closed. - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://forum.f-secure.com/down.asp
Herşey Türk İçin Türk'e Göre Türk Tarafından
www.TurkMilliyetcileri.net
www.TurkMilliyetcileri.net
TÜRK MİLLİYETÇİLERİ
2006

HACKED BY TURKISH NATIONALIST AND REPUBLICAN HACKER GROUP

We are patriot, Turkish Nationalist and republican hacker group.
Turkish Hacker Group's Principles and Aims which is named www.turkmilliyetcileri.com

Figure 4. An Example of a Turkish Defacement

Off-line Relationships

In addition to on-line relationships, hackers often report close peer associations with individuals in the real world who are interested in hacking (Holt, 2009a, b; Meyer, 1989; Schell & Dodge, 2002). These networks may form through schools or casual associations in community groups. One of the more unique ways that social connections may form are through hackerspaces, which emerged over the last decade as a way for individuals with knowledge of technology to come together in order to share what they know with others in the real world (Hackerspaces, 2011). A hackerspace incorporates aspects of the modern maker movement of creating innovative and unique devices, along with elements of the hacker community from the 1960s and 70s emphasizing the free exchange of information and the use of technology to bring about change, art, and beauty (Hackerspaces, 2011). There are now over 500 hacker spaces operating around the world, often in warehouses or large buildings rented by non-profit groups in order to give individuals a chance to experiment with various new technologies in an open and encouraging environment (see Figure 5; Hackerspaces, 2011). These hackerspaces also serve as mentor centers where more experienced and skilled individuals occasionally visit and provide informal as well as more structured mentoring sessions and opportunities for less skilled individuals. These interactions stimulate interest in technology and expand individual social networks for hackerspace members as well as providing a more heterogeneous environment in terms of skill levels to a larger number of people who share their interests.

Peer relationships can also form through participation in more traditional hacker groups such as those found in the local affiliates of national and international hacker groups, like the 2600 and DefCon, or DC groups (Holt, 2009a). For example, local 2600 groups began to form around the publication of the underground hacker/phreaker magazine of the same name in the early 1980s (2600, 2011). These chapters operate in order to connect interested individuals together to share their knowledge of computers and technology with others. Chapter meetings are often held in shopping malls where gatherings of individuals were not unusual, and afforded early hackers the opportunity to observe the approach of law enforcement or other security officials in order to avoid apprehension.

(https://www.noisebridge.net/images/a/ad/Noisebridge_at_night.jpg)

Figure 5: The Noisebridge Hacker Space in Action

There are also a number of regional and national conferences in the United States and Europe focusing on hacking and computer security (Holt, 2009b). They range from regional cons organized by local groups, such as PhreakNIC in Nashville, Tennessee and CarolinaCon in Raleigh, North Carolina, to high profile organized meetings arranged by for-profit industries like DefCon. In fact, DefCon has been held since 1993, and is now one of the preeminent computer security and hacking conferences in the globe (DefCon, 2011). This conference draws in speakers and attendees from law enforcement, the intelligence community, computer security professionals, attorneys, and hackers of all skill levels for discussions on a range of topics from hardware hacking, phreaking, cryptography, privacy laws, and the latest exploits and vulnerabilities in everything from ATMs to cell phone operating systems (Holt, 2007). In fact, there is evidence that individuals in the hacker community attend mainstream security conferences. For instance, the Black Hat conference series that occurs each year just a few days prior to DefCon in Las Vegas draws in members from the security and hacker community alike. It is not uncommon for members of the community to have a speaking engagement at Black Hat which can pay an honorarium which in turn helps defray their expenses Las Vegas in general and DefCon more specifically. Being an active participant at these more mainstream conferences and contributing to the knowledge of the information security community at those venues is not an unusual pattern for a non-trivial segment of the hacking community.

In addition, hacker conferences serve a very important function in reducing conflict within the community. Typically, communications between hackers occur through computer email, IRC, chatrooms and other communication channels which do not provide the verbal and non-verbal cues needed to help communicate one's position in a status hierarchy. The lack of verbal and nonverbal cues have been hypothesized to encourage status conflict within the hacking community, often taking the form of "flaming" and other disparaging types of activities (Holt, 2007; Kilger, 2004). Communications between individuals at conferences can, however, provide verbal and nonverbal cues related to negotiating one's position in the local and more global status hierarchy within the hacking community (Holt, 2009a). In turn, hackers can sort out status differences and significantly reduce conflicts that can arise in on-line communications. In addition, participants can and do connect with one another outside of panels and sessions by sitting down at tables and in hallways to drink and talk. It is common to see people sharing files and discussing ideas with one another. Thus, cons play an important role in sharing information about technology and connecting hackers in the real world which might not otherwise happen in on-line environments. At the same time, conventions can serve as social unity building mechanisms among individuals and thus promote more social cohesion across the hacking community at large.

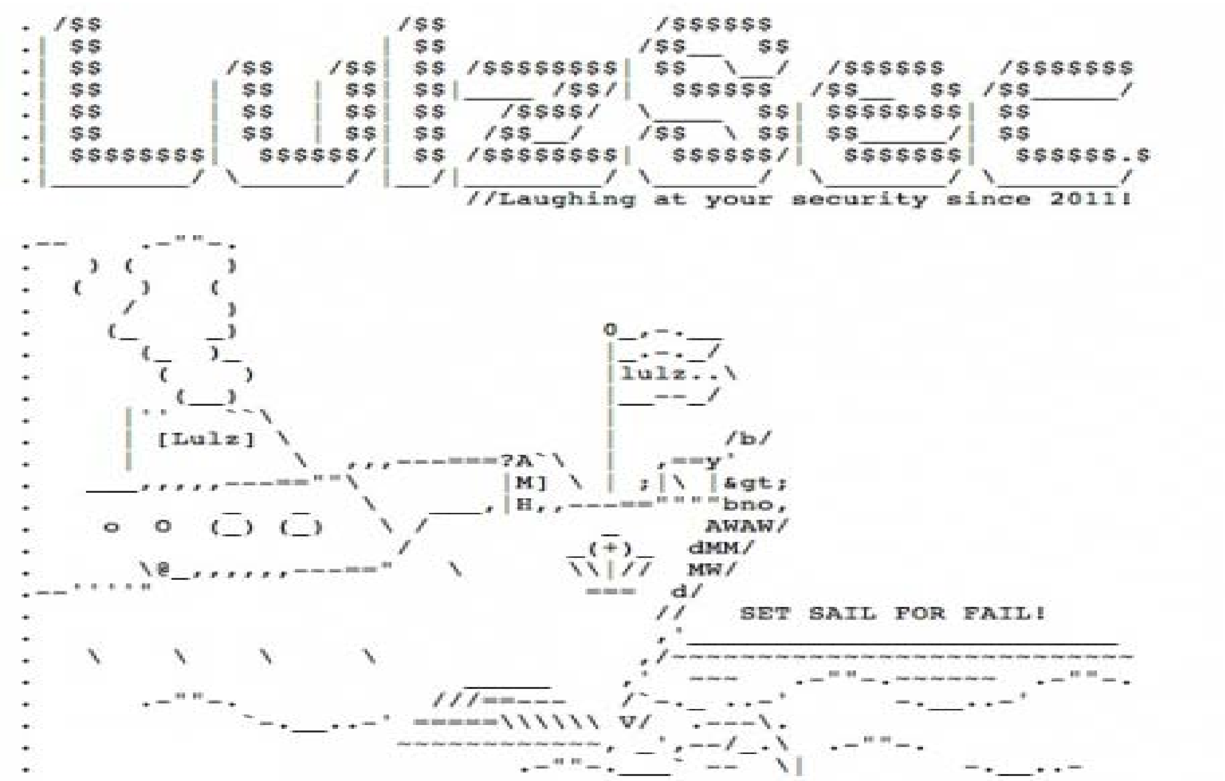
Motivations for Hacking

In keeping with the range of skill evident in the hacker community, there are multiple motives for hacking that reflect various elements of the hacker subculture. One of the most cited discussions suggests that there are six key motives in the hacker community: entertainment, ego, status, entrance to a social group, money, and cause (Kilger, Stutzman, & Arkin, 2004). Motivations may vary across time and place such that what is a driving force in one country may be nominal in another. In addition, an individual may be motivated by multiple factors at any given point in time, making it difficult to identify a single motive that may affect participation in a cyberattack (Kilger, 2010). For example, both white hat and black hat hackers share these motivations, though the only difference between these groups is the nature of the outcome of their attack. Specifically, a person may be motivated by money or political agendas regardless of whether the result of the hack is malicious, illegal, or the outcome is normative and approved of by society in general.

Entertainment

Entertainment is a motivation that has remained constant in the hacker community since the emergence of computer technology (Kilger et al., 2004; Kilger, 2010). The intense desire to understand technology means that hackers will play around with technology for fun in order to learn how these resources work, and identify the limits of any piece of hardware or software. When the concept of hacking emerged in the 1950s, individuals at MIT engaged in hacks while goofing off, and for fun in the manipulation of technology (Levy, 2001). In the 70s and 80s, individuals frequently used hacking techniques to explore telephone systems and computers to understand the largely unknown landscape of connected computers. Cap'n Crunch's successful attempts to phone phreak with a toy whistle were both for fun, and as an experiment in exploration (Furnell, 2002). This desire to play with technology for entertainment purposes is also evident at hacker conferences like DefCon (Holt, 2007). Attendees can engage in a variety of contests to develop new technologies or hack existing tools to rapidly cool beer or hack cars in order to better optimize the tuning and operating system of the vehicle (Holt, 2007). Even some malicious hacks can serve as entertainment because the actors can laugh at their achievements (Holt et al., 2008).

Recently, the entertainment derived from some hacks relates to the concept of "lulz." One apt definition explains lulz as a variation of 'LOL' or 'laugh out loud,' where individuals find joy in disrupting another's emotional equilibrium (Schwartz, 2008). In fact, a new hacking group calling itself LulzSec began a series of attacks on a number of different types of targets in 2011 including Sony, Fox News, gaming websites for Minecraft, as well as government sites such as the public website for the Central Intelligence Agency and the official U.S. Senate website. LulzSec has on numerous occasions stated that their actions were motivated simply by the lulz involved in the attack and has even turned down financial rewards for its hacking efforts. The artwork that the group chose to publish on the Internet often incorporated elements of this particular variation of entertainment/humor (see Figure 6). While their actions appear to be primarily motivated by entertainment, there are also elements that involve chiding their targets for their lack of security and taunting agencies involved in the investigation of LulzSec. In fact, the short-lived path of LulzSec might be rooted in the nature of their motives for attacks. If the objective of their attacks are to humiliate and disrupt the emotional equilibrium of targets, repeatedly engaging in attacks may quickly remove the novelty and lulz. In addition, the familiar practice of taunting its victims may also hasten the demise of LulzSec in that disclosure of information can assist law enforcement authorities in deducing clues about the identities of the members of the group.



(http://greyhat-security.com/lulzsec-releases-sony-developer-network-source-clears-irc-exposure)

Figure 6: An Example of LulzSec Imagery

Entertainment can also be linked to the motivation of ego based on the psychological and emotional boost a person may feel after the successful completion of a hack (Kilger et al., 2004; Kilger, 2010). Since the hacker subculture is a meritocracy, the sense of satisfaction and social rewards an individual may gain from their peers may serve as a key motive for hacking (Holt, 2007; Jordan & Taylor, 1998; Kilger, 2010; Taylor, 1999). For instance, individuals report feeling good when they are able to make a program function properly or identify a new vulnerability in software or hardware (Holt, 2007; Voiskounsky & Smyslova, 2003). The more difficult or elegant the attack or exploit, the more positive effects the attack has upon the person doing the hacking. Additionally, individuals receive positive feedback from others when they post useful or new information in forums and on-line communities (Chu et al., 2010; Holt, 2007). The social support individuals receive from such comments may increase an individuals' sense of personal value, and in turn makes ego a critical motive for some hackers over time.

Ego

Another critical motive related to ego is status garnered from hacking (Kilger et al., 2004). Individuals can generate substantive respect and recognition from others based on their ability to hack hardware and software in novel ways (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999). Individuals may gain status through the theft or acquisition of sensitive information, like Kevin Mitnick who became a legend in the hacker community because of his technical skill and ability to run from the law. This desire for status must often compete with the norm of secrecy as an individual must often reveal how their attack was completed or share stolen information through the underground to vet their claims. The disclosure of information reduces the hidden nature of the attack method used or can generate unwanted attention from law enforcement agencies (Holt, 2007; Taylor, 1999). Thus, the repetition of status-based malicious activity may be hard to maintain over time without substantially increasing the risk of arrest or sanction (Holt, 2007; Taylor, 1999).

Entrance to a Social Group

Hacking skills can also be useful in order to gain entrance to various groups, whether for malicious or non-malicious activities (Kilger et al., 2004; Kilger, 2010). This issue is longstanding, going back to the early

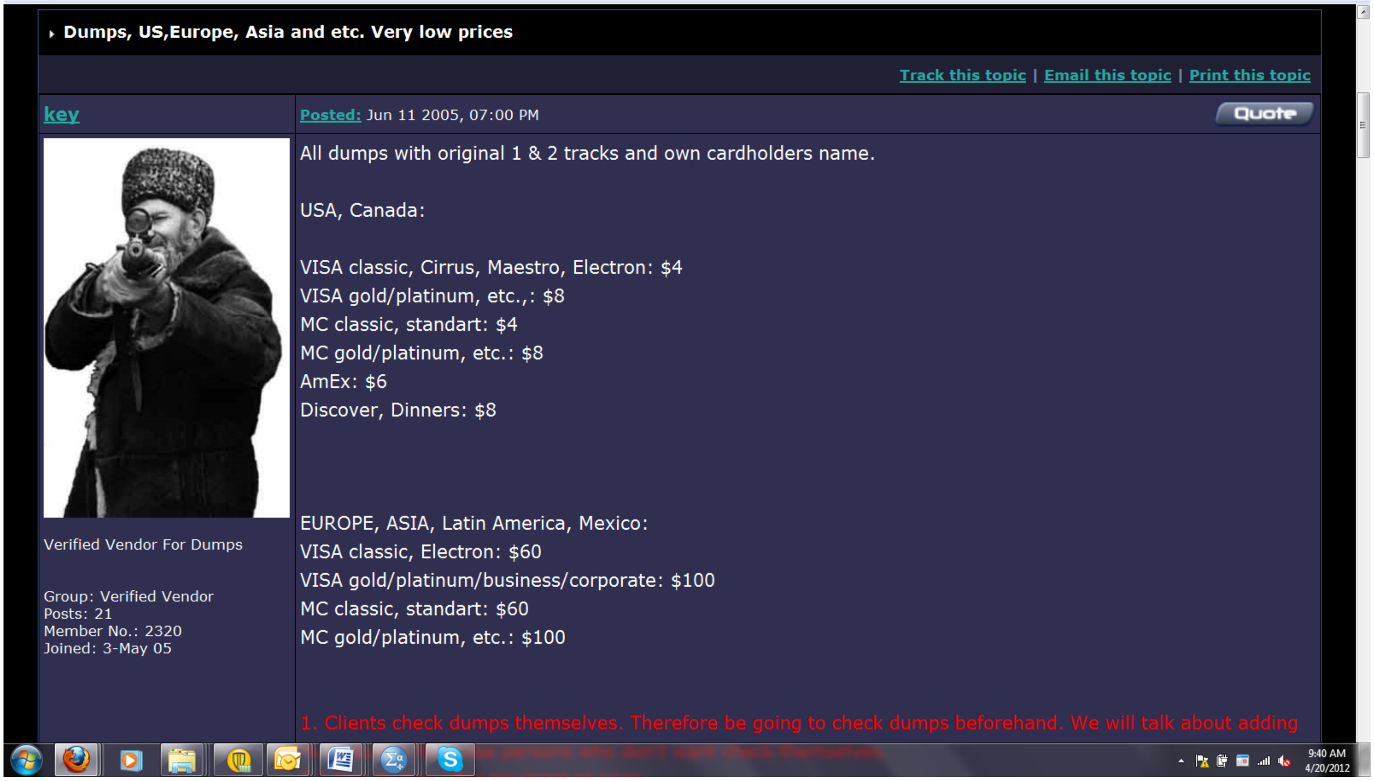
BBSs of the 80s, and is deeply intertwined with the importance of technology and knowledge (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999). In the 80s and 90s, individuals who developed and applied their skills in unique ways generated attention from highly skilled actors in the hacker community (Holt, 2007; Meyer, 1989). Those who could demonstrate their skill would receive invitations into closed BBS and forums where highly skilled actors could better assess their talents (Kilger, 2010; Meyer, 1989). In turn, they may receive access to tools and information that were otherwise unavailable, like pirated software and games.

The increasing specialization of technology, including software, hardware, and cellular telephony since the late 90s has made it difficult for hackers to truly understand all facets of emerging modern digital technologies. Hackers are now increasingly specialized in programming languages, platforms, and devices, creating pools of skill where individuals have certain proficiencies that others do not possess (Kilger, 2010; Kilger et al., 2004; Meyer, 1989). As such, a hacker with a certain demonstrable programming skill or knowledge set may be integrated into a group in order to expand their overall capacity. For instance, Holt, Soles, and Leslie (2008) identified Russian and Chinese hacker groups whose members had different programming skills, but worked together to create exploits and tools with distinct applications against various targets. In turn, skill and ability are an increasingly important way that individuals are indoctrinated into hacker groups.

Money

The motives of money and cause are more modern in nature and have grown from shifts in the use of technology and its penetration across society. For example, money as a motivation was much less common among hackers through the 1980s due to the limited volume of digital information and materials available, the lack of networked computers and servers, the stigma then attached to hacking for money, and the attractiveness of competing motivations (Kilger, 2010). The increased dependence on technological resources in the public and private sectors since the development of the World Wide Web has dramatically increased the amount of sensitive financial and personal information now available on-line (Franklin et al., 2007; Holt & Lampke, 2010; Newman & Clarke, 2003). As a result, modern hackers frequently target retailers and financial institutions through the use of phishing attacks (Huang & Brockman, 2010; James, 2005) and large scale data compromises (Holt & Lampke, 2010).

Data acquired through different forms of attack are increasingly sold through open markets to generate a profit for hackers (Chu et al., 2010; Franklin et al., 2007; Holt & Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011). Individuals regularly sell credit card numbers, bank account information, login information, and other related financial service products (see Figure 7; Holt & Lampke, 2010). Similarly, active malware and botnet infrastructure can be leased or purchased directly from the operators for a lost total cost (Chu et al., 2010; Motoyama et al., 2011). These markets enable skilled actors to profit from their capabilities while at the same time increasing the overall efficacy of the hacker community as a whole. Thus, money has become a particularly important motivation for malicious and criminal hackers over the last two decades.



Dumps, US,Europe, Asia and etc. Very low prices

key

Posted: Jun 11 2005, 07:00 PM

Verified Vendor For Dumps

Group: Verified Vendor
Posts: 21
Member No.: 2320
Joined: 3-May 05

All dumps with original 1 & 2 tracks and own cardholders name.

USA, Canada:

VISA classic, Cirrus, Maestro, Electron:	$4
VISA gold/platinum, etc.,:	$8
MC classic, standart:	$4
MC gold/platinum, etc.:	$8
AmEx:	$6
Discover, Dinners:	$8

EUROPE, ASIA, Latin America, Mexico:

VISA classic, Electron:	$60
VISA gold/platinum/business/corporate:	$100
MC classic, standart:	$60
MC gold/platinum, etc.:	$100

1. Clients check dumps themselves. Therefore be going to check dumps beforehand. We will talk about adding

Figure 7: An Example of an Advertisement in a Carding Forum

Cause

In addition, there has also been a substantial increase in the number of cause-driven hacks over the last two decades due to the expansion of the Internet and its use in expressing political, nationalistic, and religious beliefs (Denning, 2010; Holt, 2009b; Kilger, 2010; Jordan & Taylor, 2004). Causes vary based on the location of a group in the world and their cultural, ideological, political, and religious orientations. Malicious hackers can often apply their knowledge and skills to engage in attacks on behalf of a particular belief system in order to exert influence over policies or actions made by another group (Denning, 2010; Kilger, 2010). For example, the group Anonymous engaged in a number of attacks against MasterCard, Visa, and PayPal after they cut financial service processing for the website WikiLeaks (Halliday, 2011). The group began a campaign of DDoS attacks to express their dissatisfaction with these companies' practices after the release of sensitive diplomatic cables from the United States. These attacks involved individuals who do not necessarily have hacking skills, but were able to attack through the use of easy-to-use tools (Halliday, 2011). As a result, cause-based attacks are changing through the emergence of simple tools and audiences interested in expressing their opinions through on-line environments (Denning, 2010; Kilger, 2010).

The Emerging Future and Nature of CyberAttacks

Gaining a better understanding of the motivational, social, political and economic forces at work in the hacking community provides substantive context to understand how social forces shape the nature of new emerging digital threats. A more comprehensive perspective will enable researchers and policymakers to better predict the characteristics of cyberthreats that will emerge in the next few years and help them marshal resources and plan for these threats before they appear on the event horizon.

One of the most serious cyber threat vectors comes from non-state actors with no actual affiliation to a particular nation. Lynn (2011) argues that nation states are not the most likely to initiate a catastrophic attack, but rather a terrorist group or even just a group of programmers. A number of researchers have outlined the emerging threat posed by individuals and groups to perform potentially serious cyberattacks (Denning, 2010; Kilger, 2010; Holt & Kilger, 2012). This is a consequence of the changing technological landscape that allows non-nation state actors to effectively target the various resources of a nation state (Kilger, 2010, Holt & Kilger, 2012; Holt, Kilger, Chiang, & Yang, 2012). Specifically, attackers need minimal financial and man-hour resources in order to produce attacks with a high probability of success while generating a low likelihood of being apprehended. The result is a fundamental shift in the traditional power relationship between the individual and the nation-state. Single actors or small groups of actors not associated with the formal apparatus of a nation-state can now plan and execute effective cyberattacks that can have non-trivial effects on the critical infrastructure, economy and national security of a targeted nation-state.

As a consequence, these actors have been identified as "civilian cyber-warriors" referencing their roles as non-military or state actors targeting government resources (Holt & Kilger, 2012; Holt et al., 2012; Kilger, 2010). The intended targets of cyberattacks by cyberwarriors do not necessarily have to be a foreign nation-state. In a recent study it was found that not only were some individuals willing to propose a cyberattack on a foreign country in retribution for an act that harmed their fellow citizens, some of these study participants proposed cyberattacks on their own homeland in retaliation for harmful acts that their homeland committed against their own country (Holt & Kilger,2012). In addition, a number of tools are emerging for use in cyber-attacks by individuals with varied technical skill. Specifically, social networking sites and other media platforms have been used to identify and elicit participation in DDoS attacks against various targets, as in the recent attacks against Iranian presidential candidates (Ollmann, 2010). The increasing ease with which individual citizens can be co-opted into politically motivated attacks demands greater research into both the identification of individuals willing to engage in politically driven hacking (Denning, 2010; Holt & Kilger, 2012; Kilger, 2010) and the technical means to defeat these attacks (Ollmann, 2010).

Further research is also needed on the ways that the hacker community will serve a supporting role in the facilitation of social movements. One important example of the application of hacking skills toward a specific cause are the recent events surrounding the Arab Spring which began in 2011. The Egyptian government sought to shut down communications between activists during the uprising of January and February 2011 due to protesters using social media, including Twitter and Facebook, as platforms to demonstrate opposition to the government and coordinate protest actions. Thus, individuals resorted to alternative services such as Google's speak 2tweet and software hacks provided by various members of the hacking community to circumvent government restrictions (Dunn, 2011). It is clear that as social media becomes a vital resource for social movements that the hacking community will serve a pivotal role in the circumvention of government censorship and promotion of digital communications in the success or failure of small-scale as well as large national scale social movements.

In addition to disaffected individuals or small groups of hackers, there is increasing evidence that nation-state conflicts will utilize cyberspace as a combat vector. Much has been made of the threat of "cyberwar," (Clark, 2010; Brenner, 2008), but many experts in the field including the White House's cyber security coordinator Howard Schmidt declare that there is no such thing (Schmidt, 2010). Instead many researchers point to the term cyberconflict to describe the efforts of nation-states to gather intelligence from and plan the disruption of key industrial and military computer networks. Probably the most famous cyberconflict incident is that of Stuxnet, a computer worm that is designed to attack only Programmable Logic Controllers (PLCs) that run Siemens step 7 software using a specific configuration that matched those centrifuges used by Iran at its Natanz uranium enrichment facilities (Clayton, 2010; Kerr, Rollins, & Theohary, 2010). Further, the Stuxnet worm deployed a strategy that resulted in significant suboptimal enrichment of uranium as well as inflicting physical damage to the centrifuges in a stealthy manner that made it difficult to discern that there was a systematic attack on the machinery. There is no doubt that Stuxnet was of the most sophisticated cyberattacks on an industrial system that has ever been uncovered (see Shakarian, 2011 for a more complete description of the worm and its consequences)

One of the hottest topics of debate about Stuxnet was in terms of its attribution. Many in the popular media have speculated as to the origins of the program and its deployment. While there have been suspicions that it was mostly an Israeli effort with assistance from the United States based on clues and supposition with the program code (Clayton, 2010; Kerr et al., 2010), no compelling evidence has surfaced that this is the case. It has long been asserted that the attribution of an attack is a difficult issue in the field of information security and often many attacks ultimately are not attributable to an identifiable individual or group of individuals (Brenner, 2008). An even more slippery situation is where attribution is claimed by a group that has no self-proclaimed leadership, hierarchy or formal structure or membership as is exemplified by the hacktivist group Anonymous (Denning, 2010).

A closer look at the consequences of attribution suggest that it could possibly play less of an important role in cyberconflict than originally thought, at least in this early age of cyber warfare. The classic use of attribution in nation-state conflict is to identify the parties responsible for a specific act or acts that cause harm to that country or its allies with the purpose of responding to that hostile act with a retaliatory act against the aggressor or one or more of the aggressors' allies. That is a dangerous and slippery slope that could lead to considerable conflict and damage both to critical infrastructures of nation-states as well as significant economic loss and non-trivial loss of life. It is hoped by the time that this juncture is reached that policymakers will have developed effective strategies that will diffuse serious cyberconflict situations so that they do not end up being resolved with kinetic solutions. At least one researcher has suggested that there are some lessons to be learned in the cyberconflict arena from the early years of deployment of nuclear weapons where policymakers successfully threaded a complex and serious set of issues that eventually resulted in policies for developing, stationing, using and limiting strategic weapons that prevented exchanges of nuclear weapons that might have eliminated a significant portion of the world's population (Nye, 2011).

The last topic concerns the increased participation in cybercrime by individuals who possess insufficient technical skills to otherwise complete the acts that they engage in. Historically, the archetype of script kiddies were those who would collect malicious scripts or tools written by more skilled individuals and deploy them against targets without understanding the theory or principles behind the strategy (Furnell, 2002; Jordan & Taylor, 1998). Being a low skilled script kiddie does not necessarily eliminate the threat that person poses for infrastructure managers and system administrators. For instance, Michael Calce, aka Mafiaboy, was a Canadian high school student with modest computing skills who deployed malicious software he had obtained on the Internet in a number of large DDoS campaigns against a number of high profile companies including Yahoo, Dell, CNN and others. While estimates of the damage caused vary, most of the estimates are in excess of $1 billion dollars worth of damage caused when users could not access websites for the aforementioned companies (Palmer, 2011).

Another scenario involves low skilled actors deploying sophisticated attack and exploit tools that they did not author against valuable but systemically unstable industrial or critical infrastructure systems (Brodscky & Radvanovsky, 2010). Sometimes the mere fact that an unsophisticated individual has gained access to and is "wandering around" in an industrial control system that is highly susceptible to changes in configurations or ill-timed commands can pose serious problems if they unwittingly disturb some element of the system. The third concern is that some small proportion of these low skilled actors will continue down the path towards becoming a skilled cybercriminal. If being a script kiddie is an evolutionary step which some may move beyond (Holt, 2010), then there is the distinct possibility that low skilled cybercriminals may evolve into more highly skilled, expert cybercriminals who are capable of writing their own sophisticated malware. In fact, the risk of detection or arrest for involvement in cybercrimes is substantively lower than that of traditional crimes due to difficulties in attribution, jurisdictional complications, and evidentiary issues (Brenner, 2008). Additionally, the intense social nature of the hacking community and the power of computer mediated communication provide a fertile environment for individuals who do not know each other to mentor others in terms of programming skills, knowledge of networking protocols, information security techniques and vulnerability discovery/exploit development skills and strategies. All of these factors contribute towards the potential continued growth of a segment of the population who are increasingly disposed to malicious online behaviour.

SUMMARY & CONCLUSIONS

While the information security field has placed significant emphasis on the technical issues of vulnerability identification and protection of systems, there is less attention paid to the social elements that often shape and drive efforts to compromise servers, networks and critical infrastructure systems. The objective of this discussion has been to encourage information security professionals to consider the key role that social processes and forces play in the motivations of online malicious actors as well as outline how social forces may shape emerging cyberthreats in the near term. Further research into how social forces form and shape the cyberthreat matrix is clearly needed, as well as theoretical and empirical research into the social aspects of cyberthreats to provide the field with a perspective that deviates from its traditional defensive, reactive reply to information security threats. It is hoped that this discussion will spur further thought, discussion and progress in this critical area.

ACKNOWLEDGEMENTS

We would like to thank Christian Seifert (CEO, The Honeynet Project) for his substantive support and feedback, as well as Franck Guenichot (French Chapter), Francois-Rene Hamelin (French Chapter), Adel Karimi (Iranian Chapter), Felix Leder (Giraffe Chapter), Cameron Malin (Southern California Chapter), Kara Nance (Alaska Chapter), Sebastian Poeplau, Jamie Riden (UK Chapter), Lukas Rist (German Chapter), Arrigo Triulzi (Global Chapter), Sjur Eivind Usken (Norwegian Chapter), and Jianwei Zhuge (Chinese Chapter) who provided commentary and revisions on previous drafts of the manuscript.

REFERENCES

2600. (2011). *2600: The Hacker Quarterly*. Retrieved from http://www.2600.com/

Adineran, A. I. (2007). The Internet and emergence of Yahooboys sub-culture in Nigeria. *The International Journal of Cyber Criminology, 2,* 368-381.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *The International Journal of Cyber Criminology*, *4*, 643-656.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brodscky, J., & Radvanovsky, R. (2010). Control Systems Security. In T. J. Holt & B.Schell (Eds.),*Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 187-203). Hershey, PA: IGI-Global.

Chiesa, R., Dutti,S., & Ciappi, S. (2008). Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. New York: Auerbach.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On Line*. Washington, DC, National Institute of Justice. Retrieved from www.ncjrs.gov./pdffiles1/nij/grants/230112.pdf.

Clark, R. A. (2010). *Cyber War: The next threat to national security and what to do about it.* New York: Harper Collins.

Clayton, M. (2010). Stuxnet malware is "weapon" out to destroy… Iran's Bushehr Nuclear Plant. *Christian Science Monitor*, 21 September, 2010. Retrieved from http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

DefCon. (2011). *What is DEF CON?* Retrieved from http://defcon.org/html/links/dc-about.html

Denning, D. E. (2010). Cyber-conflict as an Emergent Social Problem. In T. J. Holt & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. (pp. 170-186). Hershey, PA: IGI-Global.

Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*, Washington D.C.: Department of Defense. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Dunn, A. Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising. The Fletcher Forum of World Affairs, vol 35, #2, pp. 15-24

Ellyson, S. And Dovidio, J. Power, dominance and nonverbal behaviour: Basic concepts and issues. In S. Ellyson and J. Dovidio (eds.) Power, Dominance and Nonverbal Behavior, pp. 1-27. NewYork: Springer-Verlag.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An Inquiry into the nature and cause of the wealth of internet miscreants. Paper presented at CCS07, October 29-November 2, in Alexandria, VA.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London: Addison- Wesley.

Hackerspaces. (2011). *About hackerspaces*. Retrieved from http://hackerspaces.org/wiki/Hackerspaces

Halliday, J. (2011). Police arrest five over Anonymous WikiLeaks attacks. *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2011/jan/27/anonymous-hacking

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior 28*,171-198.

Holt, T. J. (2009a). Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 336-355). Upper Saddle River, NJ: Pearson Prentice Hall.

Holt, T. J. (2009b). The Attack Dynamics of Political and Religiously Motivated Hackers. In T. Saadawi & L. Jordan (Eds) *Cyber Infrastructure Protection*. (pp. 161-182). New York: Strategic Studies Institute.

Holt, T. J. (2010). Examining the Role of Technology in the Formation of Deviant Subcultures. *Social Science Computer Review*, *28*, 466-481.

Holt, T. J., & Graves, D. (2007). A qualitative analysis of advance fee fraud email schemes. *The International Journal of Cyber Criminology, 1,* 137-154.

Holt, T. J., & Kilger, M. (2008). Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers. WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 67-78.

Holt, T. J., & Kilger, M. Forthcoming. Examining Willingness to Attack Critical Infrastructure On and Off-line. *Crime and Delinquency*.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C.S. (2012). Comparing civilian willingness to attack critical infrastructure on and off-line. Proceedings of the 12th European Conference on e-Government.

Holt, T. J., Kilger, M., Strumsky, D., & Smirnova, O. (2009). *Identifying, Exploring, and Predicting Threats in the Russian Hacker Community*. Presented at the Defcon 17 Convention, Las Vegas, Nevada.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies*, *23*, 33-50.

Holt, T.J., Soles, J., & Leslie, L. (2008). Characterizing malware writers and computer attackers in their own words. Paper presented at the 3rd International Conference on Information Warfare and Security, April 24-25, in Omaha, Nebraska.

Huang, W., & Brockman, A. (2010). Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails. In Holt, T. J. (Ed.), *Crime On-line: Causes, Correlates, and Context* (pp. 87-112). Raleigh, NC: Carolina Academic Press.

Information Warfare Monitor. (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network.* Retrieved from http://www.f-secure.com/weblog/archives/ghostnet.pdf

James, L. (2005). *Phishing Exposed*. Rockland: Syngress.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*, 757-780.

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyber Wars*. London: Routledge.

Kerr,, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Washington D.C.; Congressional Research Service.

Kilger, M. (2007). An Example of a Successful International Information Security Research Alliance. Third Annual European Network and Information Security Conference, Vilnius, Lithuania, November, 2007.

Kilger, M. (2010). Social dynamics and the future of technology-driven crime. In T. J. Holt & B. Schell (Eds.), Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications (pp. 205-227). Hershey, PA: IGI-Global.

Kilger, 2010b. Motivations for Malicious Online Behavior and Consequent Emerging Cross National Cyber Threats, 2010 Workshop on Cyber Security and Global Affairs, Zurich, July, 2010.

Kilger, M., Stutzman, J., & Arkin, O. (2004). Profiling. In The Honeynet Project (2nd Ed.), *Know your enemy*. Addison Wesley Professional.

Landreth, B. (1984). *Out of the Inner Circle*. Washington: Microsoft Press.

Levy, S. (2001). *Hackers: Heroes of the Computer Revolution*. Penguin (Non-Classics).

Lynn, W. J. (2011). Remarks at the 28th Annual International Workshop on Global Security. June 16, 2011.

Markoff, J. (2009). Vast spy system loots computers in 103 countries. *The New York Times*. Retrieved from http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1

Meyer, G. R. (1989. *The social organization of the computer underground*. Master's thesis, Northern Illinois University.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An Analysis of Underground Forums. *IMC'11*, 71-79.

Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Cullompton, NJ: Willan Press.

Nye,J. Jr. (2011). Nuclear lessons for cyber security. *Strategic Studies Quarterly*, *5*, 18-38.

Ollmann, G. (2010). *The Opt-In Botnet Generation: Social Networks, Hacktivism, and Centrally-Controlled Protesting*. Damballa. Retrieved from http://www.damballa.com/research/optinbotnet/index.php

Palmer, E. (2011). London Conference on CyberSpace: The Biggest Cyber Attacks of All Time. Retrieved from http://www.ibtimes.co.uk/articles/241238/20111101/biggest-cyber-attacks-time-hacking-china-google.htm,

Schell, B. H., & Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How*. Westport, CT: Quorum Books.

Schmidt, H. 2010. Retrieved from http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ March 12, 2012.

Schwartz, M. (2008). The Trolls Among Us. *The New York Times Magazine*. Retrieved from http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?_r=1&pagewanted=all

Scott, J. (2005). *BBS: The Documentary*.

Shakarian, P. 2011. Stuxnet: Cyber revolution in military affairs. Small Wars Journal, April 15, 2011, retrieved from http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf March 12, 2012.

Slatalla, M., & Quittner, J. (1995). *Masters of deception: The gang that ruled cyberspace*. New York: Harper Collins Publishers.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime*. London: Routledge.

Thomas, T. (2010). Google confronts China's three warfares. Parameters,. 101-113.

Voiskounsky, A., & Smyslova, O. (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & Behavior*, *6*, 171-180.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology*, *5*, 736-749.

Wu, X. (2007). *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*. Lexington, KY: Lexington Books.

ABOUT THE AUTHORS

Thomas J. Holt is an Associate Professor in the School of Criminal Justice at Michigan State University and has been a member of the Spartan Devils Chapter of the Honeynet Project since 2008.

Max Kilger is currently the Chief Membership Officer for the Honeynet Project, a past member of the board of directors, and has served as a profiler with the Project for the past eleven years. He has also been a member of the Spartan Devils Chapter of the Honeynet Project since 2008.