Researchers expose the human side of cybercrime

April 4 2013

In a perfect world, a door could remain unlocked without evoking the curiosity of strangers and criminals. This not being the case, humans have developed sophisticated security systems and intrusion deterrents. These efforts are continually countered, however, by those who wish to enter the door and have a peek, or a piece, of what lies on the other side. The same phenomenon applies to cyberspace. The ability of hackers to bypass security measures and gain entry to networks worldwide drives the development of technology in a neverending cycle.

But cybersecurity efforts often fail to address the underlying questions: Who is trying to get in, and why? How do they respond to different configurations of the attacked system? How will understanding these phenomena help us better protect ourselves and our valuable online

information?

Dr. Michel Cukier, ssociate professor of reliability engineering at the A. James Clark School of Engineering, associate director for education in the Maryland Cybersecurity Center and director of the Advanced Cybersecurity Experience for Students (ACES), and Dr. David Maimon, assistant professor of criminology and criminal justice, have partnered to study the behavior of hackers and victims alike. They conduct research on how end-users' online routines determine their vulnerability to cybercrime incidents, and to answer some of the fundamental questions surrounding criminal behavior.

"It's a human problem," says Cukier. "Theoretically, we shouldn't need a password. Yet people are constantly trying to gain access. There is a massive human component to this phenomenon that we need to understand."

To study this dynamic, Maimon and Cukier have established a truly cross-disciplinary research collaboration, combining principles of criminological, sociological and engineering methods in a way that has never before been attempted. Leveraging their own expertise, as well as that of graduate students from each discipline, they are seeking to bring a deeper and more socially-focused understanding to the Internet and its dangers. It all starts with "Why?"

The Internet & cybercrime

In its infancy, the Internet was a global communications network and a repository for information. However, as users began to store valuable data, develop e-commerce platforms, and share personal information, it drew increasing attention from creative hackers and cybercriminals.

"There is a market [for private information]. There's money behind

that," explains Cukier. "It creates incentives, similar to any criminal enterprise. Where there are valuable assets, people will chase after them."

Beyond the direct theft of information, hackers also commonly seek to infiltrate individual computers to use them as tools in their attacks. By gaining control of an individual computer or network, hackers can install malicious software, manipulate the computer's settings, and even disguise their attack's origin by turning the compromised computer into a "bot" which carries out their assault. In doing so, often multiple times, it becomes extraordinarily difficult for technicians and authorities to discover the true perpetrator of the attack. For this reason, the science of understanding the behavior of hackers, and their victims, is increasingly important and valuable.

Research foci

Maimon and Cukier's NSF-funded, collaborative research—which is supported by the efforts of Gary LaFree from the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and Anthony Lemieux from Georgia State University and has previously been supported by the SANS Institute—has three foci; understanding hacker response to situational stimuli in the attacked computer system, learning about users' online routines that expose them to threats in cyberspace, and developing practical tools to help guide IT managers improving their cyber security systems. Their research has focused exclusively on the University of Maryland's network, which offers a large, diverse and complex community of computer users from around the globe, and of all age groups.

"It's us," says Maimon. "Computer networks are a type of social network. And similarly to the influences of any social network on its members, our computer network's social composition shapes our

experience with cybercrime. Our computer network demographic and social characteristics influences the timing, origin and types of attacks we get...and we get many."

Maimon estimates that the University of Maryland receives over 6,000 attacks per day, and nearly 700,000 attacks each year – each of which is noted by the university's highly monitored network security infrastructure.

Working closely with the University of Maryland's Office of Information Technology, Cukier and Maimon have several ongoing projects that collect data on network attacks and hackers' behaviors, providing the basis for some truly fascinating research findings.

Honey pots

Crime and opportunity often go hand in hand. In general, cybercriminals do not systematically attack every computer within a network. Instead, they randomly probe computers within a given network, looking for vulnerabilities and weaknesses. In some cases, once a target has been identified, hackers will attempt to "break in," despite being challenged by some level of security protection. The random nature of these attacks gives Maimon and Cukier a strategic advantage in the form of camouflage. They deploy "honey pots," or computers that appear to be part of a network, but are actually isolated, highly monitored systems designed to study hackers and precisely document their tactics. By using several hundred "honey pots," altering their individual characteristics and observing how hackers respond, Maimon and Cukier learn a great deal about the attacks and the attackers.

"We provide opportunity to the hackers, but not real incentive. Once inside, hackers will not find any valuable information to steal. The systems are highly monitored and controlled, so there is no real danger in

allowing the intrusions," explains Cukier.

IPS

In criminology, the "Routine Activities Theory" (RAT) posits that for a successful crime to take place, motivated criminals and susceptible victims must come together in the absence of capable protectors at the same time and place.

"The absence of physical dimension in cyberspace makes the task of testing RAT's claims challenging," says Maimon.

However, applying UMD's Intrusion Prevention System (IPS) reports, Maimon, Cukier and their students tested the idea that the UMD computer users' online routine determines the timing and origin of attacks against the system. The IPS is a device, installed in a given network of computers, which monitors traffic in order to detect and prevent malicious attacks and intrusions to the network. In many cases, computer users' activities (such as opening suspicious emails, downloading illegal software, or clicking on malicious adware) directly prompt the 'attacks.' Once detected, the IPS sends an alert to network administrators, prevents the attack from developing, and records a number of data points about the attack – including the origin, severity, and type of attack used. By collecting the university's IPS data between 2007 and 2009, then appending information about the university's number of computer users, their countries of origin and the technological infrastructure in those countries, Maimon and Cukier were able to discover intriguing facts about computer users' behaviors and how they influenced attacks on the University of Maryland's computer network.

According to their research findings, more than 50 percent of computer attacks against the network occur between 9 a.m. and 5 p.m. – the

university's business hours. "Our analysis demonstrates that computer-focused crimes are more frequent during times of day that computer users are using their networked computers to engage in their daily working and studying routines," Maimon explains. Put differently, this means that hackers, no matter where on Earth they are attacking from, have aligned their tactics with our local schedule of high network usage and activity.

Perhaps more intriguing was the correlation discovered between foreign network users, such as international students, and attacks against the network. According to their findings, an increase in the rate of foreign network users at UMD increases the number of attacks originating in these users' countries of origin as much as 40 per cent. "Users expose the network to attacks," Maimon explains. "Simply by browsing sites on the Web, Internet users make their computers' IP addresses and ports visible to possible attackers. Subsequently, network users' behavior reflects on the entire organization's security."

Maimon offers a deeper, more socio-criminological conclusion of their research findings.

"Our study demonstrates that network users are clearly linked to observed network attacks, and that successful future security solutions need to account for the human element of cyber crime."

As part of the NSF funded project, Maimon and his student Theodore Wilson (Criminology and Criminal Justice) designed a cyber security awareness campaign (Think Before You Click) that is aimed at educating residents in UMD dormitories regarding the hazards of risky online behaviors.. This awareness campaign, which is supported both by Resident Life and the Division of IT, is part of the research team's effort to promote campus-wide 'cyber hygiene,' a general collection of best practices to help network users avoid risky online behaviors and

suspicious websites. By training the students, faculty and staff on how best to reduce hackers' effectiveness, these scholars seek to offer solutions to one of our nation's greatest threats.

Provided by University of Maryland