Cybercrime—

Can we protect ourselves from the hazards of an online world?

TEAM CYMRU

An Epidemic

Painted in the broadest of strokes, cybercrime essentially is the leveraging of information systems and technology to commit larceny, extortion, identity theft, fraud, and, in some cases, corporate espionage. Who are the miscreants who commit these crimes, and what are their motivations? One might imagine they are not the same individuals committing crimes in the physical world. Bank robbers and scam artists garner a certain public notoriety after only a few occurrences of their crimes, yet cybercriminals largely remain invisible and unheralded. Based on sketchy news accounts and a few public arrests, such as Mafiaboy, accused of paralyzing Amazon, CNN, and other Web sites, the public may infer these miscreants are merely a subculture of teenagers. In this article we provide insight into the root causes of cybercrime, its participants and their motivations, and we identify some of the issues inherent in dealing with this crime wave.

Cybercrime is pervasive, nondiscriminatory, and dramatically on the increase. Countless dollars are being siphoned from innocent individuals and large corporate entities alike. With minimal risk, people are turning to cybercrime in ever-escalating numbers because of its low-

skill entry requirements and promise of extremely high rates of financial return.

Simply log into one of the 30 or 40 underground-economy IRC (Internet Relay Chat) channels (such as #ccpower) and you will see the magnitude of illegally obtained financial accounts, some involving millions of U.S. dollars. Yet, economic institutions continue to encourage customers to embrace electronic commerce and banking to reduce their brick-and-mortar expenditures. Some of these institutions are failing to make commensurate expenditures for computer security; they provide their users with static logins and passwords for authentication, making keystroke-logging and packet-sniffing malware highly effective against these victims. This penchant for convenience and ease of use typically sacrifices security, thus providing cybercriminals with a bountiful harvest.

THE LAW ENFORCEMENT PERSPECTIVE

What about bringing these cybercriminals to justice? Both nationally and internationally, law enforcement is ill equipped to stem the rapidly rising tide of cyber-

Cybercrime—An Epidemic

crime. Insufficient training, limited resources (personnel, equipment, budget), barriers to cooperation, outdated or nonexistent legal remedies, a paucity of cross-border cooperation, high-latency cross-border cooperation processes, and individual organizations' cultural paradigms create a fertile ground for success in cybercrime. In the U.S., computer crime statutes such as the Wiretap Act or the Computer Fraud and Abuse Act are woefully outdated and inadequate to handle the pace of technological advancement in today's world. The Computer Fraud and Abuse Act was written in 1986, before information systems became such an integral part of American life. Consequently, prosecutors must find plausible ways to apply the law and hope the judiciary and the juries understand the severity of the crime and can, within the limitations dictated by the law, mete out appropriate punishments.

Many victims do not seem to draw the correlation between their losses and cybercrime; worse, they often view it as a crime that is impossible to investigate and prosecute. For cybercrime to be acknowledged as an important issue, the victims must report such incidents to a receptive law enforcement community with a well-informed judiciary. Attempts such as the president's National Strategy to Secure Cyberspace¹ represent a significant first step in the right direction. To have the desired impact, however, the detailed provisions delineated as action/recommendations must be implemented. The beginnings of international cooperation and collaboration, articulated by the Council of Europe Convention on Cybercrime treaty,² have yet to be ratified by all participating nations. The effort to establish a comprehensive cyber defense and the identification of critical national cyber assets remain incomplete.

Alliances between the public sector and private enterprise are at an initial stage of development with limited success so far. Public-private partnerships (with government participation or sponsorship in some instances), such as the National Security Telecommunications Advisory Council (NSTAC), the National Security Information Exchange (NSIE), and the Cyber Security Industry Alliance (CSIA), have had some measure of success in executing overarching policies and practices for securing cyberspace in a critical sector. Other nations, such as the UK, have instituted the NSIE model for their own public-private cooperative relationships. Initial attempts at paral-

leling this collaborative structure in the international law enforcement community are under way but as of yet lack sufficient resources and skills to have substantial impact on the cybercrime juggernaut.

Of perhaps greater success are similar efforts sponsored by the private sector. Software vendors are anxious to ensure that their customers view the Internet as a safe haven for recreation and business. Thus, they have created global forums of private industry, law enforcement, and policy makers. Microsoft has provided one example, the Botnet Task Force, as detailed by Scott Charney, vice president of Microsoft's Trustworthy Computing initiative.³

Pockets of individual expertise do exist in the U.S. government and international law enforcement community, however, and they masterfully employ an informal network of trust relationships, both within their respective domains and with private-sector counterparts, for their collaborative endeavors. Rather than foster and encourage this informal arrangement between the public sector and private enterprise, there will inevitably be pressure to formalize and institutionalize this construct, thus severely limiting the flexibility and responsiveness that now exist.

As an example of the current arrangement, the agil-

Hacking used to be
performed merely for the status
it provided its practitioners...

ity of the informal network provides the ability to track miscreant activity across multiple Internet-connected networks. Recently, an organization was under a 1-Mpps (million packets per second) DDoS (distributed denial of service) attack. This was a UDP port 53 attack from nonspoofed source IPs. Using only the list of IP addresses attacking the organization's name servers, the informal network was able to track back to the command and control point in less than seven minutes. This provided the ability to direct the attacking command and control traffic into unusable network space and thus end the attack. Although results with this expediency are not always achievable, it does illustrate the ability to both actively

affect and passively detect and track the activity of the criminals through an informal, trusted network.

NO FEAR

These three aspects—flexibility, collaboration, and responsiveness—are paramount in combating cybercrime. The miscreants are predisposed to being mobile and elusive, given their freedom of movement within cyberspace. In such an environment they can operate with impunity and arrogance. Countless conversations in open and public forums demonstrate their absolute lack of fear of law enforcement. Evidence indicates miscreants are paid to compromise networks, or write tools to compromise networks, or just sell that which they have compromised.

Hacking used to be performed merely for the status it provided its practitioners, but now hacking for hire is on the rise. Why develop the skills when automated tools and the underground economy make these same skills so readily available? Miscreants are not averse to paying for what they require. For example:

<A> can anyone screw up a PHP website, I am willing to pay who will do that

Here another miscreant highlights the trials of those who bring in a steady stream of ill-gotten revenue:

<A> my gf just ask me
<A> how u get somuch money
<A> are u a dealer
<A> >_
 lol
<A> lol i told my gf
<A> iam a hacker and steal money from americans
<A> and she started to laugh :D

Cybercriminals do share insight, though they don't label it as such. When a miscreant is arrested, it is common to spot that same individual back online within hours sharing his or her tale of woe and the specific law enforcement agency involved, often identifying the agents who were responsible.

In the following conversation, several miscreants discuss the FBI agents involved in the Foonet case, as well as some other law enforcement organizations. The names of the agents have been obfuscated for this article.

<A> how do u know r*****
 r***** was responsible for shutting foonet down
<C> fbi waste time

<C> in these places
<C> they really come ?
<A> leo.gov is law enforcement online
<A> tis what most of feds use
 this guy that got his hdd's raided [hdd is hard disk drive]
 got them back after 3 years
 the day after [CRIMINAL] was arrested
<C> if u do something illegal
<C> then make ur hd
<C> easy access
<C> so u can kill it
<C> in half a second
<C> before feds can even walk in house
<D> mine just sits there, not screwed in
<D> rip it straight out
 also
 m*****@fbi.gov
 ***** division manager

Do they worry about being apprehended? Here two miscreants confer about that possibility. Encryption and obfuscation complicate matters, but in their twisted logic, their type of crime is not that serious anyway.

<A> Well i am 90% confident that encryption will make me impossible to trace, that's for sure, unless the fbi decide to spend millions to end the project then bust me
<A> You know how many of these so called 'criminals' get caught? 1% apparently
 dont think fbi wud pay much attention to it
<A> yeah, what makes you think that?
 well modeling site wudnt be that important to them
 plus the way u wud make money isnt going to draw there attention
<A> i see what you mean, it's not really a very intrusive hostile form of money making is it

It is important to note that at present this open criminal conduct is conducted without regard to security, privacy, or encryption. The underground economy, wherein the gains of online crime are traded, is open to all comers. These exchange points are widely advertised and have no authentication, security, or privacy provisions.

Because of the lack or inadequacy of criminal statutes for cybercrime both in the U.S. and internationally, the miscreants conduct their criminal activities without hesitation or concern. They brag of their exploits, post visual evidence of themselves and their misdeeds, and celebrate the inability of law enforcement to apprehend them.

Cybercrime—An Epidemic

To be clear, the problem doesn't generally reside with law enforcement. While many law enforcement agencies across the globe are technically adept and eager to investigate online crime, they find a paucity of support from prosecutors, judges, and policy makers. Law enforcement needs greater support from these entities, as well as the systems of global collaboration.

The response to criminal activity in the physical world is rarely replicated in the cyberworld. Granted, the criminal statutes and penalties are clearer and more definitive for such physical criminal events, yet this merely highlights the necessity for more comprehensive cybercrime statutes with more substantial, severe sentences handed down for this form of crime. Perhaps it may even be appropriate to invoke RICO (Racketeer Influenced and Corrupt Organizations) statutes and asset forfeiture. Online crime is, after all, often quite organized and involves a number of criminal specialists, collaboration, and planning. This assumes, though, that cybercrime statutes even exist; in many countries such statutes do not exist, are incomplete, or are poorly written.

While governments and law enforcement agencies lament this stark realization, underground Internet criminals are exceptionally insightful; they can perpetrate their activities with virtually no threat of legal retribution. Even ironclad cases with undeniable evidence and an uncontested chain of custody fail to result in incarceration.

One of the notable outcomes from some cases, though, is the unprecedented demonstration of how multiple international law enforcement agencies can work together, share information and techniques to gather evidence, identify the perpetrators, and arrest them. This level of collaboration is the exception rather than the rule, however. In far too many instances, political or cultural impediments preclude that level of cooperation and interaction. Breaking down these barriers and achieving some equivalence or consistency in statutory restriction are essential to waging a comprehensive campaign against cybercrime worldwide.

TECHNICAL PROWESS NOT REQUIRED

Over the years, the proportion of highly technical miscreants has decreased. Entry skill requirements are now very low, despite the perception to the contrary in some circles. While technical prowess may provide an edge or an

additional revenue opportunity, it is not required. This is not to say that there aren't extremely talented and technical miscreants in the underground, but their numbers have decreased as a percentage of the entire cybercrime universe. This has occurred not because they have lost their prowess, but because of the open and burgeoning nature of the online criminal underground. In general, a miscreant can conduct online crime with a Web browser, IRC client, and merely the ability to use both.

Given this precept, it behooves governments and law enforcement to embark first on activities that raise both the cost and the risk to the miscreants. The methodologies, techniques, and practices to accomplish this are not the subject of this article. Rather, the intent is to highlight the root causes of the cybercrime epidemic: poor security practices, legal shortfalls, insufficient coordination, and lack of recognition of the existence and/or severity of cybercrime on multiple levels.

Certainly, cybersecurity practitioners can help instill good security practices, highlight the importance of recognition and reporting, and assist with the coordination aspect, but thwarting or diminishing the incidence of online crime will come through the nearly ubiquitous creation of carefully considered policy and its proper global application. Q

1. National Strategy to Secure Cyberspace; <http://www.whitehouse.gov/pcipb/>.
2. Council on Europe; <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=8/18/2006&CL=ENG>
3. Charney, S. 2005. Combating cybercrime: a public-private strategy in the digital environment; <http://www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc>.

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

TEAM CYMRU (www.cymru.com) is an altruistic group of researchers focused on making the Internet more secure. Through a wide variety of published documents, projects, and partnerships, Team Cymru aims to raise awareness of the real threats facing those who use the Internet.

© 2006 ACM 1542-7730/06/1100 \$5.00