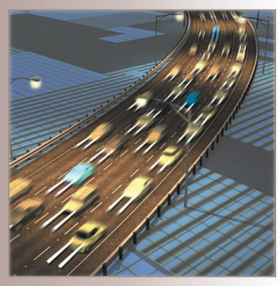

Cybercrime: Dissecting the State of Underground Enterprise

Cybercrime's tentacles reach deeply into the Internet. A complete, underground criminal economy has developed that lets malicious actors steal money through the Web. The authors detail this enterprise, showing how information, expertise, and money flow through it. Understanding the underground economy's structure is critical for fighting it.

Aditya K. Sood
Michigan State University

Rohit Bansal
Independent Security Researcher

Richard J. Enbody
Michigan State University

Cybercrime is crime that requires a computer, a network, and a human interface. To better understand cybercrime, we can look at various taxonomies. For instance, Marc D. Goodman categorized cybercrime into three types.[1] The first includes crimes in which the computer is the end target, the second involves using a computer to conduct cybercrime, and the third merely requires the presence of a computer that's incidental to the crime. Another cyberattack taxonomy, AVOIDIT, characterizes cyberattacks based on certain classifiers, such as attack vectors, operational and informational impact, type of defense, and target.[2] This classification aims to help organizations in their response to attacks.

Most computer-based crime exploits users' ignorance and their inability to deal with flourishing technology and security mechanisms. Consequently, much cybercrime goes unnoticed,[3] and the growing number of online users obscures the problem's magnitude. The US Federal Trade Commission (FTC) conducted an identity-theft survey and estimated that cybercriminals steal close to 9 million identities every year in the US (see www.ftc.gov/bcp/edu/microsites/idtheft/). Identity theft can be monetized in various ways, but most involve securing credit, especially with credit cards. In 2009, McAfee collaborated with academic researchers and security professionals to study the impact of intellectual property (IP) theft.[4] A key finding was that IP has become a new currency for cybercriminals. It has value to both companies and countries because it lets businesses be competitive without the risk and expense of developing their own IP. Companies in the survey estimated that they lost an average of US$4.6 million worth of IP in 2008 (not all of it through cybercrime).

Rosemary Clandos observed that 63 percent of reported cybercrime occurs

 Published by the IEEE Computer Society 1089-7801/13/$31.00 © 2013 IEEE

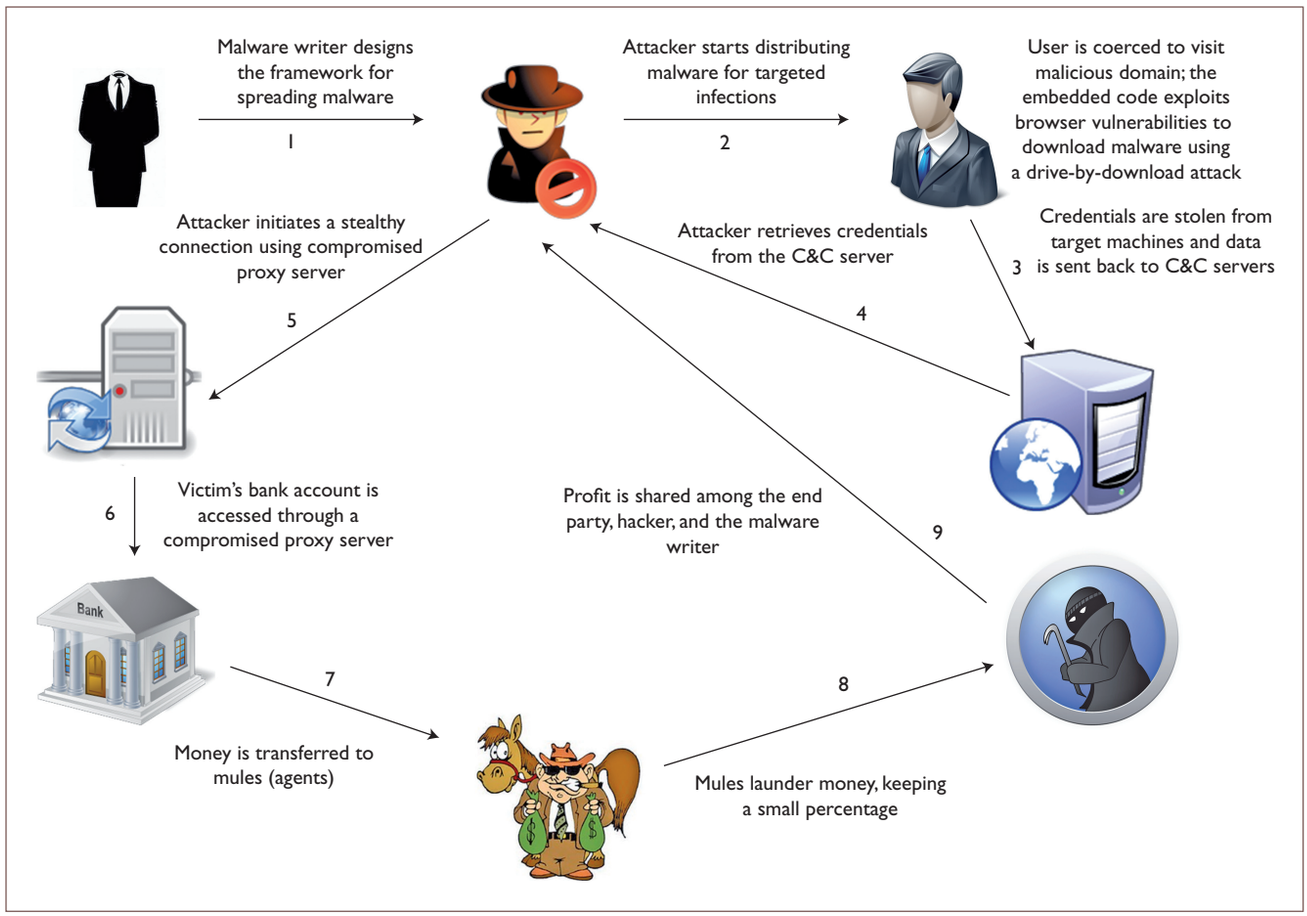

Figure 1. The online fraud life cycle. The life cycle has a multilayer malware-distribution model with segments based on services.

in the US, where reporting is very high when compared to other countries.[5] Underreporting can occur when organizations are unwilling to report cybercrime to government agencies because they fear a loss of reputation and the expense of legal battles, not to mention have concerns that the government will potentially disclose sensitive business information to rival companies through the US's Freedom of Information Act (FOIA).

In 2004, 30 countries signed a treaty for fighting cybercrime in which participants agreed to implement consistent cyberlaws.[6] Additionally, signatory countries promised to extradite cybercriminals to other member countries for prosecution. This treaty shows that governments are taking active steps to fight cybercrime, but to date, these efforts have been insufficient. Cybercrime is a major, growing, and international criminal enterprise with an emerging underground economy to support it. Here, we present details of that economy based on observations made while testing and analyzing a variety of malware. We present the cybercrime economy's complete life cycle to show the nature of this underground business.

Online Fraud Life Cycle

The current online fraud life cycle has a multilayer malware-distribution model with segments based on services (see Figure 1). There are dedicated communication and money-transfer functions, malware authors license their malicious software, and attackers can rent botnets for hours under pay-for-play (PFP) schemes. At one end, skilled personnel develop and sell vulnerabilities (including zero-day exploits), while at the other, common criminals turn online financial data into cash. This cash works its way up through the hierarchy to those skilled practitioners. In this way, cybercrime has become organized and sophisticated.

At the top of the hierarchy, a malware writer designs automated malware frameworks and

sells them to other criminals who use them to spread malware across the Internet. Such frameworks get combined with a common distribution technique, the *drive-by-download* attack,[7,8] in which an adversary lures users to a malicious domain and exploits their browsers to silently download malware to their machines. How the malware exploits the browser depends on the type of vulnerability present in different components, as described in the browser malware taxonomy.[9] Once installed, the malware steals credentials and critical information from users' machines and sends it back to a command-and-control (C&C) server. With credentials in hand, the attacker can transfer money from user accounts while protecting him- or herself by connecting to banks using an intermediate proxy server. The cybercriminal transfers the money to agents (called *mules*) who convert the transfers to cash. Once the transaction successfully completes, the various parties share the profits. The original vulnerability is thus converted to hard cash in a way that's far removed from the malware developer.

Targeted Cyberattacks and APTs

A targeted attack is a cyberattack that's directed toward a specific entity (individual, group, business, or government body). A sophisticated targeted attack requires a combination of tools, social engineering tricks, and tactics for operational coordination. In 2011, several targeted attacks occurred against organizations such as RSA, Comodo, US defense contractors, and Tibetan organizations. Details of the targeted attack against RSA and the XLS exploit are available elsewhere.[10] Many targeted attacks are initiated with a phishing attack on individuals who belong to the targeted organization. Spear phishing attacks deliver exploits embedded in Word, PDF, XLS, or PPT files as attachments. Opening the file triggers the exploit, and thus compromises the targeted victim's machine. Figure 2 illustrates a targeted attack life cycle.

Advanced persistent threats (APTs)[11,12] are a subset of targeted attacks — that is, they're persistent threats delivered using targeted attacks that then evolve continuously over time. APTs can be coverted to attain long-term goals and can persist until they succeed. In contrast, other targeted attacks target relatively large groups of people, attack opportunistically, and are satisfied if only some succeed. Targeted attacks and APTs are both built on vulnerabilities, but APTs' customized attack structure makes them expensive to develop, so they're used most often against high-value targets. For example, Operation Aurora was an APT conducted against 30 companies in the US,[13,14] including Google. Duqu and Stuxnet (see www.crysys.hu/publications/files/BencsathPBF12eurosec.pdf) are examples of APTs that were used for industrial espionage. They used sophisticated (and expensive) zero-day exploits and kernel rootkits to dismantle industrial control systems.

APTs use various exploitation vectors, including Internet-based malware, physical infections, and external interface infections that infect cloud and different hosts present on the same server. Human intelligence is critical to APTs because custom, hands-on control is needed to initiate the attack. In the end, APTs' intelligence gathering bridges cybercrime and cyberwarfare.

Underground Digital Currency

The underground market is built primarily on digital currency, or e-currency. The basic concept is to start with an established national currency (known as a *fiat currency*) such as the USD or Euro and convert it to an intermediate digital currency until the transaction is over, at which point the currency is converted back into a fiat currency. This lets criminals exchange money with anyone in the world. Multiple digital currencies have arisen; they differ from other kinds of online systems such as PayPal because transactions are irrevocable, so repudiation isn't possible. Also, no direct transactions need to occur between the sender and the receiver. To initiate the process, the sender finds and pays a digital currency exchanger to convert a fiat currency into digital currency (some will accept credit cards). Later, an exchanger will convert digital currency back into a fiat currency. In many cases, the firm who created the digital currency will be independent from the exchanger. Essentially, all digital currencies operate outside of Western countries but will handle Western fiat currencies. Digital currencies that operate offshore depend on trust rather than legal infrastructure — a user must trust that the digital currency can be fairly converted into a fiat currency. Finally, terms of use specify that digital currencies aren't to be used

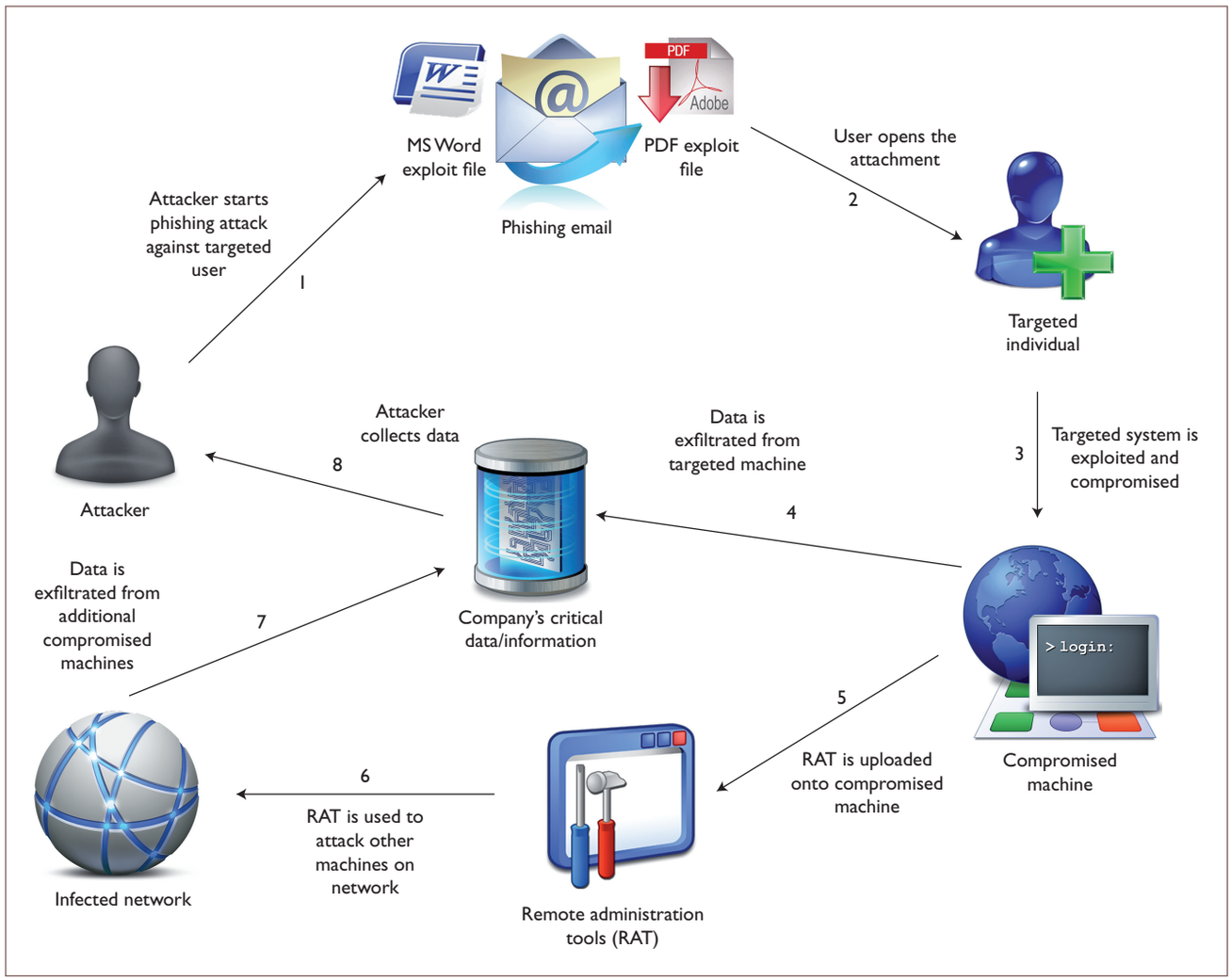

Figure 2. The life cycle of a generic targeted attack. A targeted attack is directed toward a specific individual, group, business, or government body.

for criminal activities or money laundering, but these restrictions are essentially unenforceable.

E-Gold used to dominate the underground economy, but currently Web Money and Liberty Reserve are prevalent. Web Money deals in different digital currencies such as Web Money-USD (WMZ), Web Money-Euro (WME), Web Money-Russia (WMR), and Web Money-Gold. It's popular for transactions completed in Russia. Liberty Reserve, on the other hand, is popular for European transactions. The biggest underground market is in these two continents.

Inside the Underground Economy and Market

We can split the complete cybercrime life cycle into three separate cycles. To illustrate, let's assume that a client (an underground buyer) wants to launch an attack to collect financial credentials. First, he needs tools, so he heads to the underground market.

Cycle 1

The underground economy is built on a vibrant communication network in which participants share information about new products and malware frameworks on a regular basis. Thus, in the first cycle (see Figure 3), the client searches different underground forums and IRC channels to find a seller offering a complete malware framework that can build a botnet.

Figure 3 shows how the client gets in touch with a seller to purchase a malware infection framework such as Zeus or SpyEye. Currently, the going rate is between US$4,000 and $7,000, depending on the product's complexity and efficiency.

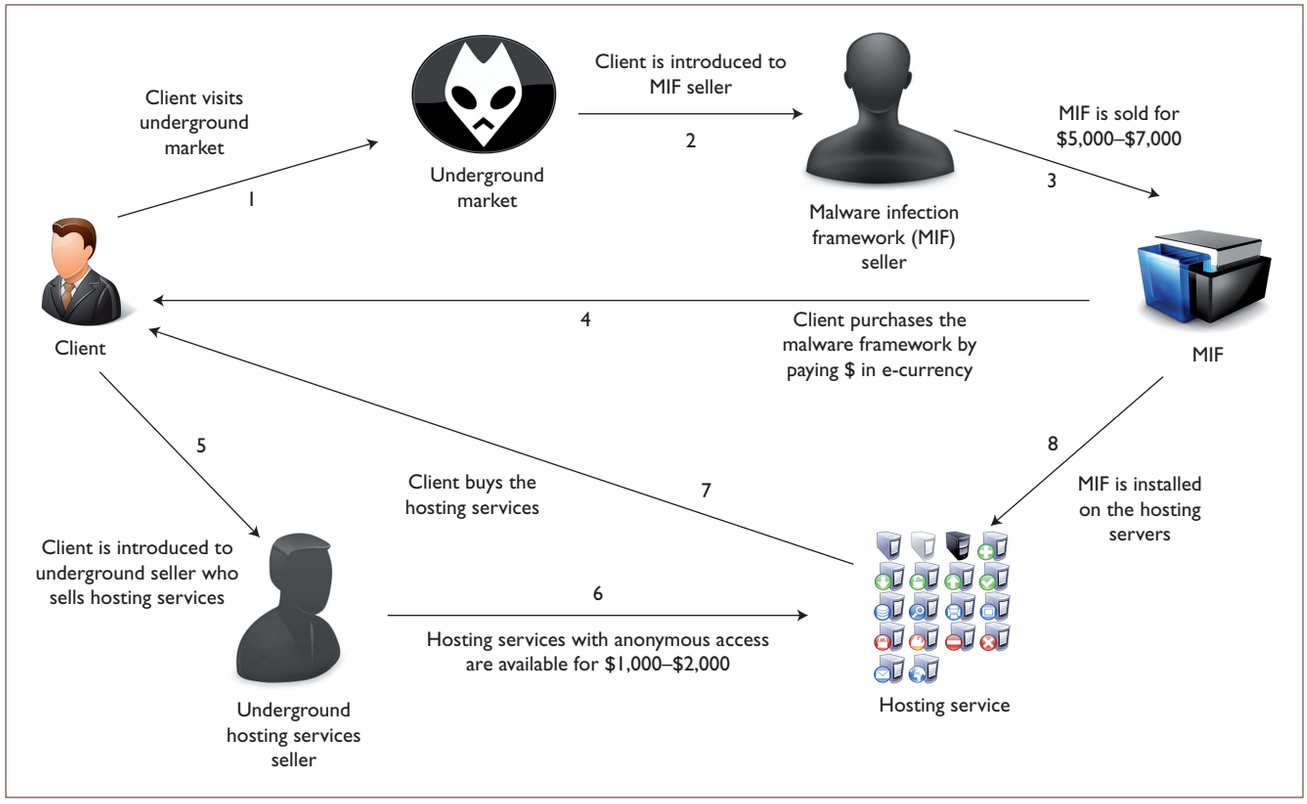

Figure 3. Cycle 1 of the underground economy. In the first cycle, the client searches different underground forums and IRC channels to find a seller offering a complete malware framework that can build a botnet.

If the client and seller successfully conclude the deal, the client receives a license for the malware infection framework for a specific time period. The client pays with e-currency. The malware framework comes with documentation, including step-by-step details for installation and configuration. Consequently, the client doesn't need to understand how the framework works, nor does he require much technical expertise. With the framework in hand, he must next install it on an anonymous hosting service to avoid reverse hacking. Several such services are regularly sold in the underground economy by attackers who have compromised public hosting servers. Malware frameworks are hosted primarily on servers in Russia and China, mainly to avoid cyberlaws. At this point, the client can install the malware framework, including the C&C server and back-end database, on the hosting service. Once the client's tool is installed, the first cycle is complete.

Cycle 2

In the second cycle (see Figure 4), the client begins the infection process. Most malware infections come from drive-by downloads, so our client must find a malicious website from which to launch the infection — that is, he must bargain with an underground marketer of compromised websites.

Once he's purchased access, the client needs a tool to infect visitors — that is, he needs an automated exploit framework known as a *browser exploit pack* (BEP). The client embeds the compiled binary of the malware infection framework purchased in cycle 1 as a payload in the BEP. He'll pay between $1,500 and $3,000 to host a BEP on the compromised website. The client pays for access to a website with a significant number of unique visitors every day — more visitors spread the infection more widely. *Pay per install* (PPI) infection services help the client to broadly infect users by injecting an obfuscated iframe into a high-volume website that points to the malicious domain. A recent study on PPI shows that approximately 12 of the top malware families use PPI services to infect machines.[15]

When a user visits the compromised website, his or her browser encounters the BEP.

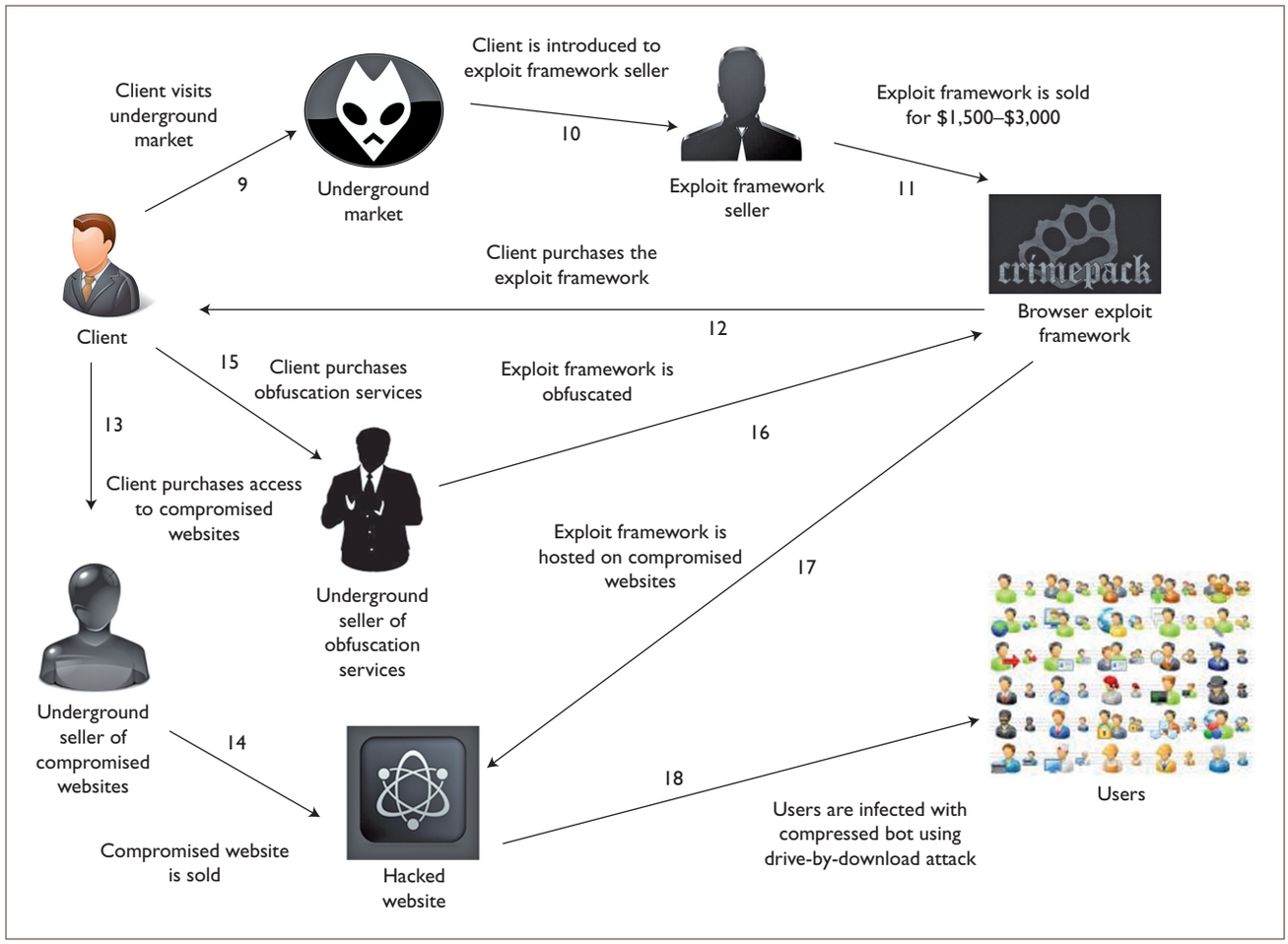

Figure 4. Cycle 2 of the underground economy. In the second cycle, the client begins the infection process.

Usually, the BEP fingerprints the browser by scanning the user-agent string that the browser sends. In addition to this, JavaScript and Document Object Model (DOM) functions can also be used to fingerprint browser versions. This string identifies the kind of browser and version number so the BEP can deliver a specific exploit for that browser version. If the exploit executes successfully, the BEP serves the payload in the form of a dropper/bot through the browser and compromises the users' machines. If done well, users will be unaware that they now have a bot installed on their computer. Once users' machines are infected, they become part of the botnet the client (sometimes called the *bot master*) is now managing. Active protection mechanisms and antivirus technologies create a signature of the bot once it's discovered, letting defenders easily detect it with a valid bot signature. To minimize this risk, the malicious client can purchase tools that obscure the bot.

The underground market provides another set of services that pack and obfuscate the malicious binary so it can sneak past host-based detection technologies. Styx.net provides obfuscation services at a large scale with affordable prices. Once the client purchases such services, the bot is compressed and updated again in the victim machines via the C&C server. Purchasing these services greatly reduces the rate of bot detection, resulting in more usefully infected computers. This completes the second cycle.

Cycle 3

In the third cycle (see Figure 5), the client waits for the bot to install and begin sending critical information from infected machines to the C&C server.

The most useful information extracted from users is financial credentials: bank account numbers and passwords, or credit-card numbers and security codes. The bot sends the stolen information to the back-end C&C database

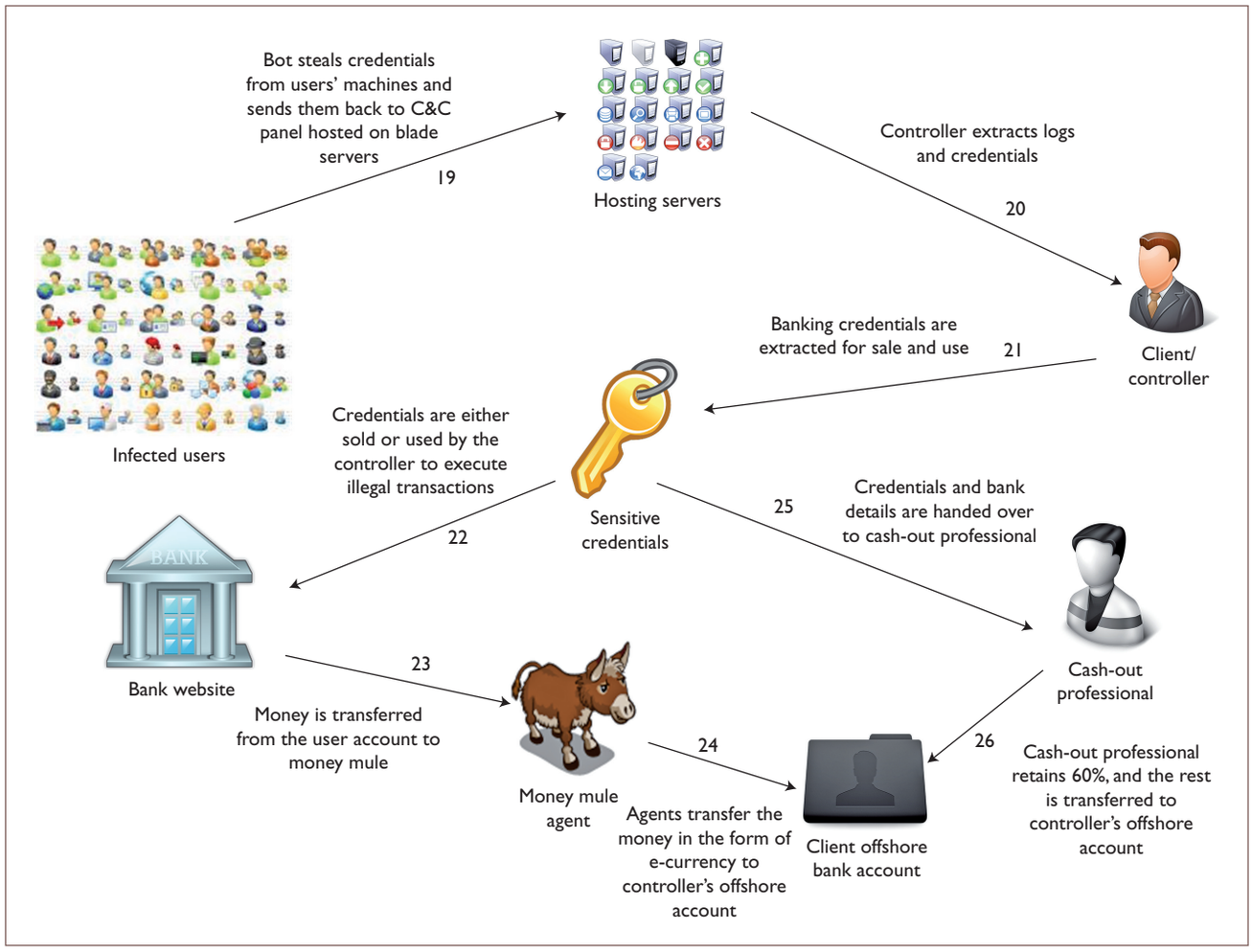

Figure 5. Cycle 3 of the underground economy. In the third cycle, the client waits for the bot to install and begin sending critical information from infected machines to the command-and-control (C&C) server.

for storage. The latest malware provides the client with an elegant GUI to the C&C server and information database. One particularly useful part of the interface is the form-grabbing panel that runs automated queries to extract desired financial data. Over a few weeks, the client can retrieve and store quite a lot of data. The client can use the raw data in two ways.

In the first case, the client can use the bank account information to transfer funds from user accounts to money mule agents who launder it. The agents convert the stolen money to e-currency and transfer some of it back to the client.

In the second case, the client sells the raw data directly to others in the underground market. For a price, the client can avoid direct involvement in money laundering. Figure 6 shows an advertisement from madtrade.org forums explaining how to sell raw data. Any other criminal party can buy these financial credentials for illegal activities. To raise the information's value, the seller can extract a set of accounts that promise to be particularly profitable. Alternatively, the seller can contract with cash-out people — that is, criminals who specialize in forging user identities and executing transactions in person at a bank. This process is risky and therefore expensive. Our client usually gets 40 percent of the transaction amount, with the remainder going to the cash-out people. Yet another alternative is for a seller to rent the form-grabber panel directly to a buyer for a specific time period. All these services depend on trust within the business model.

Real-Time Underground Websites

Many websites are part of this underground economy. Currently, styx-crypt.com provides

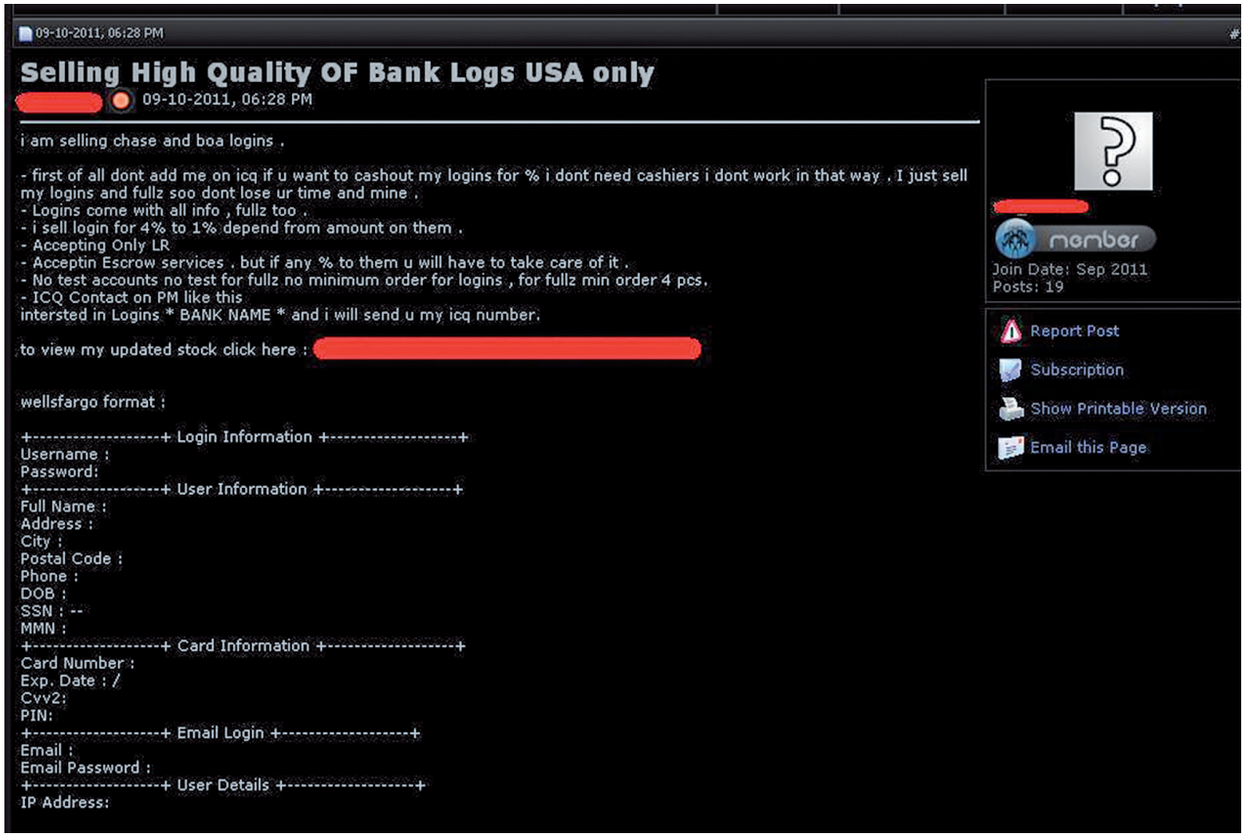

Figure 6. Underground economy advertisement. This advertisement from the madtrade.org forums explains how to sell raw bank account information.

automated online obfuscation and morphing services for hiding malicious code that remains undetectable. This website also provides the styx exploit pack, which is a complete framework that includes obfuscating exploits. For underground trading, online forums such as darkcode.com, madtrade.org, and exploit.in are popular for buying and selling sensitive information, including personal data, access to compromised domains, and email addresses for phishing attacks. For traffic infection, smartprivate .net provides PPI services to broadly infect online traffic. To verify the authenticity of credit and debit cards, madc.su provides an online service for verifying whether the credit cards are active. This sophisticated service informs attackers about the value and validity of potential victims. Additionally, steklo.cc offers an explicit service for designing fake bills and fake ID, including high-value documents such as passports. Credit-card skimming services are provided by validhshop.su, and several other underground websites and forums provide similar services.

Attackers are succeeding in exploiting security vulnerabilities in online financial transaction mechanisms. The underground market has become a complete enterprise that creates a lucrative business for its members. Many key players contribute to the success of underground activities, each with different skills. To build defenses against cybercrime activities, we must understand the nitty-gritty details of this economy's key players and how they interact.

References

1. M.D. Goodman, "Why the Police Don't Care about Computer Crime," *Harvard J. Law & Technology*, vol. 10, no. 3, 1997, pp. 465–494.
2. C. Simmons et al., *AVOIDIT: A Cyber Attack Taxonomy*, tech. report, Univ. of Memphis, Oct. 2009;

http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf.
3. H.K.H. Chan, "A Comparative Study of Reported and Unreported Computer Crimes," doctoral dissertation, Hong Kong Univ. Science and Technology, 2000; http://dl.acm.org/citation.cfm?id=932832.
4. *Unsecured Economies: Protecting Vital Information*, tech. report, McAfee, 2009; www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.
5. R. Clandos, "Eye on Cybercrime," *IEEE Security & Privacy*, vol. 1, no. 4, 2003, pp. 10–11.
6. C.P. Meinel, "Cybercrime Treaty Could Chill Research," *IEEE Security & Privacy*, vol. 2, no. 4, 2004, pp. 28–32.
7. B. Stone-Gross et al., "Peering through the Iframe," *Proc. IEEE INFOCOM*, IEEE, 2011, pp. 411–415.
8. F.-H. Hsu et al., "BrowserGuard: A Behavior-Based Solution to Drive-by-Download Attacks," *IEEE J. Selected Areas in Communications*, vol. 29, no. 7, 2011, pp. 1461–1468.
9. A.K. Sood and R.J. Enbody, "A Browser Malware Taxonomy," *Virus Bull.*, vol. 23, no. 6, 2011, pp. 8–12.
10. R. Branco, "Into the Darkness – Dissecting Targeted Attacks," blog, 30 Nov. 2011; https://community.qualys.com/blogs/securitylabs/2011/11/30/dissecting-targeted-attacks.
11. *Advanced Persistent Threats*, tech. report, McAfee, 2010; www.mcafee.com/us/resources/solution-briefs/sb-advanced-persistent-threats.pdf.
12. M. Daly, "The Advanced Persistent Threat (Information Force Operations)," *Proc. 23rd Usenix Large Installation System Administration Conf.* (LISA 09), Usenix Assoc., 2009; www.usenix.org/event/lisa09/tech/slides/daly.pdf.
13. *Vulnerability Based Protection and the Google Operation "Aurora" Attack*, tech. report, NSS Labs, 2010; www.nsslabs.com/reports/vulnerability-based-protection-and-google-operation-aurora-attack-q1-2010.
14. *The Command Structure of the Aurora Botnet*, tech. report, Damballa, 2010; www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf.
15. J. Caballero et al., "Measuring Pay-per-Install: The Commoditization of Malware Distribution," *Proc. 20th Usenix Conf. Security*, Usenix Assoc., 2011, p. 13; http://static.usenix.org/events/sec11/tech/full_papers/Caballero.pdf.

Aditya K. Sood is a senior security researcher/consultant and PhD candidate at Michigan State University. His research interests include Web security, malware analysis, mobile security, and penetration testing. Sood has an MS in cyber law and information security from the Indian Institute of Information Technology, India. Contact him at soodadit@cse.msu.edu.

Rohit Bansal is an independent security researcher. His research interests include malware analysis, reverse engineering, and Web application security. Bansal has a BE in computer science from Uttar Pradesh Technical University. Contact him at rb@secniche.org.

Richard J. Enbody is an associate professor in the Department of Computer Science and Engineering at Michigan State University. His research interests include computer security, computer architecture, Web-based distance education, and parallel processing. Enbody has a PhD in computer science from the University of Minnesota. Contact him at enbody@cse.msu.edu.