DOI:10.1145/2461256.2461266

Stas Filshtinskiy

Privacy and Security

Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air?

Where reality stops and perception begins.

In the past the media focused on cyber criminals. For the last two years, whenever I see a news report related to unscrupulous developments in cyberspace, there is almost always a mention of weapons, the military, or an intelligence service. Nowadays, even when criminals are blamed for performing a major cyber heist, vendors call it "Operation Blitzkrieg" and the mass media announce, "Russian Hackers Declare War on USA." A *New York Times* article attributed an attack by "Izz ad-Din al-Qassam Cyber Fighters" against U.S. banks to the state of Iran without any evidence other than "a level of sophistication far beyond that of criminals."[2]

Has the world really changed that much in two years? I don't think so. Even the most complex cyber attacks are within the reach of cyber criminal enterprises.

Criminals have always raced ahead of the pack, figuring out how to steal from somewhere before the rest of the population realized there was money to be had. Cyber criminals have sites where they sell and buy things. In the early 2000s, criminals were selling credit card numbers.[6] Then banks went online, and criminals invented phishing. As losses grew, the financial institutions responded by improving their security technologies. But cybercrime had already moved on to the next best fraud.

Even the most complex cyber attacks are within the reach of cyber criminal enterprises.

Criminals are open-minded when it comes to new ways of stealing money. They learn fast. The biggest change in the business of cybercrime occurred when the most advanced groups moved from selling goods (stolen data or computer viruses) to the establishment of the criminal cyber services (stealing data, providing access to infected computers, or writing tools to steal data).

This transition in criminal business models was good for risk-averse cybercriminals.[3,4] It gave them stable cash flow and reduced their risks. It allowed them to interact with their customers (other criminals) without ever getting physically close to them. This approach attracted much less attention from law enforcement and old-style criminals—those carrying guns instead of laptops. Computer crime became an industry comparable in size to weapons trafficking and drug trafficking. Various sources put individual monetary losses from cybercrime as more than $100 billion. Symantec in the 2012 Norton Cyber-

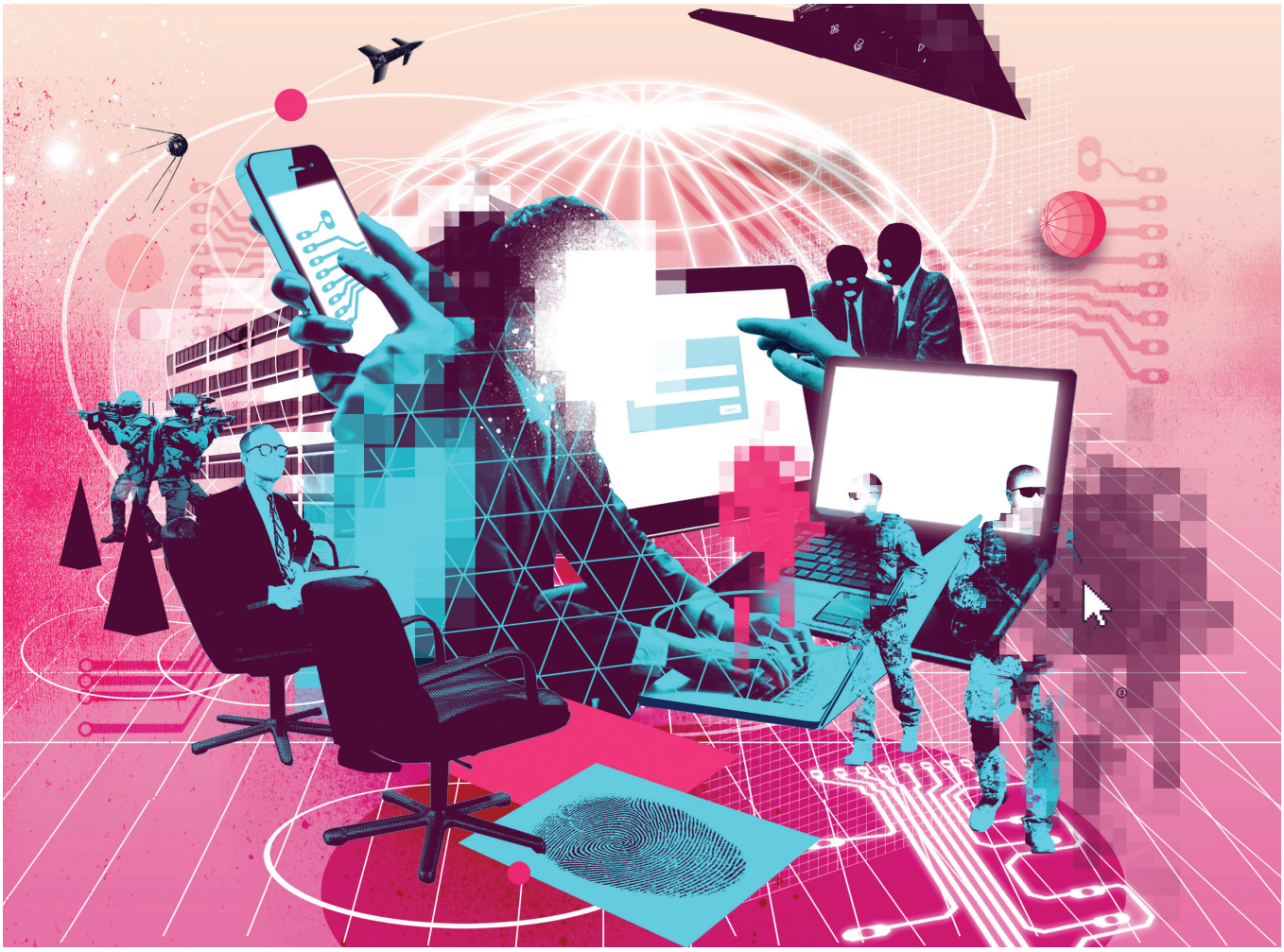

ILLUSTRATION BY MARIO WAGNER

crime report estimated an annual cost of up to $110 billion.[8] Such reports might or might not be accurate, but even 1% of the perceived losses is a lot of money.

How can such money be made? Garden-variety criminals cannot pull off such expensive heists. That money comes from sophisticated, interlinked services that criminals have on offer. Here the some of the services available on cybercriminal trade portals:

- Sending unsolicited messages of all sorts—this now includes not only email messages, but also Twitter and social network messaging.
- Writing malware on-order, which includes online support and regular updates for additional licensing fees.
- Bulletproof—or as it is often termed, "abuse resistant"—hosting, for those criminals who need to have Web presence.
- Botnet access.
- Anonymous access to the Internet.
- Getting your video to the top of YouTube.
- Hacking in general.

These services are on the market for anyone who wants to buy them—governments, activists of all persuasions, terrorists, and criminals. These services facilitate other criminal activities and are available for anyone who can pay. According to an interview with a provider,[1] a denial-of-service attack is priced between $50 and $500 per day,[a] depending on the site and deployed defenses. This provider estimated the price of shutting down the popular blogging site LiveJournal.com at $250 to $400 per day.

Criminals have advertised:

- The price for hacking a private email address is between $30 and $50.
- A forged copy of an identity document of virtually any country in the world costs less than $30.
- Custom-made software to automatically register new accounts on popular Web sites and bypass CAPTCHA protection costs less than $500.
- Custom-built malware costs $1,500 plus monthly support and consultation fees.

Cybercrime services allow businesses (for example, street gangs with soldiers on the ground) to buy a supply line of stolen credit card data or bank credentials belonging to individuals or companies local to their area. Once they pay for the service, these "businesses" can exploit this information at their own risk. The suppliers are not there if the exploiters of the data are caught. They are jurisdictionally and logically far away from the crime and out of law enforcement's way. Successful arrests of providers of cybercriminal services are rare and require a long-term sting operation or entrapment like Operation Card Shop, which was a two-year undercover effort by the FBI that concluded in mid-2012.

Cyber criminals' capabilities are impressive. Now consider some attacks that have been attributed to intelligence services, often with language about cyberweapons. According to media reports, the proverbial

a All prices are in U.S. dollars

crown jewels of the well-known security vendor RSA were stolen and allegedly used to attack multiple targets, including financial organizations and weapons manufacturers. The attack was not very advanced—it started with a known exploit, continued for some time, and ended with exfiltration of the data through a typical channel.

The Stuxnet attack occurred when a uranium enrichment plant in the Islamic Republic of Iran was sabotaged. The attack allegedly used specially crafted malware, delivered to the target by uncontrolled USB devices. The attack exploited previously known and unknown vulnerabilities in industrial control systems to damage centrifuges.

Georgia, a small nation in the Caucasus Mountains, got into the bad books of its bigger neighbor Russia over the future of two pro-Russian separatist regions. It resulted in military conflict. Separatists' online news agencies were allegedly compromised by hackers associated with Georgia while the online capabilities of Georgia were severely degraded by a massive denial-of-service attack. Georgian official and private websites were also defaced.

An attack sponsor need not be a hacker or social engineer to profit from the theft of valuable data.

The main shared feature of each of these stories is that those attacks used nothing more than was available in the criminal markets at the time. Some of the example attacks may have been the work of government agencies,[b] but they are also within reach of determined criminal groups. Similar attacks can be easily designed from building blocks available on the market. Sophisticated malware can be ordered online. Unknown (so-called zero-day) vulnerabilities can be purchased and turned into exploits. Computing power equivalent of multiple, top-of-the-range supercomputers is on offer. Databases of already-hacked passwords are available.

An attack sponsor need not be a hacker or social engineer to profit from the theft of valuable data. A decent project manager capable of understanding what items are in demand can identify particular information as marketable and build and execute a project plan using purchased components and services. Custom exploits can deliver the payload into a protected perimeter, unique malware can search and eventually reach valuable data, and individually crafted software can exfiltrate the loot. The sponsor of the attack can then sell the data wholesale or piece by piece to any party able to pay, whether a criminal organization, intelligence service, or terrorists. The scariest thing of all is that most of these recent attacks could be the work of a criminal.

According to security vendors, policymakers, and media, the world is rife with secret services, intelligence operatives, and military commands engaged in cybercrime. This perception is partially based on truth: intelligence agencies and military do operate in cyberspace. But this perception leads to bad decisions. Business leaders are not sure how best to invest in protection. Political leaders pass laws that reduce freedom of information on the Internet and empower counterintelligence services. Society is exposed because defenses appropriate to the threat are not built.

Most attacks, regardless of who is paying for them, are perpetrated by cyber criminals. We need to oppose them through better international enforcement efforts, even though this has been difficult to achieve. We must also disrupt their business models by taking down their ability to offer and deliver their services. This has been done somewhat successfully by U.K. banks.[5] Most important, we must recognize that most attacks are executed by criminal enterprises, and not by nation-states. These attacks can be defended against if we put in the tools to do so. C

b The Stuxnet attack was attributed to the U.S. government according to David Sanger.[7]

References

1. AiF 2011 in Russian. Interview with the hacker about DDoS attacks; http://www.aif.ru/techno/article/42414.
2. Bank hacking was the work of Iranians, officials say. *The New York Times* (Jan. 8, 2013); http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0&pagewanted=print
3. Chiesa, R.N. Cybercrime and underground economy: Operating and business model; http://www.flarenetwork.org/report/enquiries/article/cybercrime_and_underground_economy_operating_and_business_model.htm.
4. Filshtinskiy, S. Cyber criminal economy. In *Proceedings of the AusCERT 2007 Conference*.
5. Financial Fraud Action U.K. 2011. Fraud, the facts; http://www.financialfraudaction.org.uk/Publications/#/52/.
6. Kabay, M.E. A brief history of computer crime; http://www.mekabay.com/overviews/history.pdf
7. Sanger, D. *Confront and Conceal.* Crown Publishers, 2012, 197–203.
8. Symantec. 2012 Norton cybercrime report. 2012 Norton Cybercrime Report. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

Stas Filshtinskiy (Stas.Filshtinskiy@baesystemsdetica.com) is a principal consultant with BAE Systems Detica in Melbourne, Australia.