MIT Technology Review

Welcome to the Malware-Industrial Complex

The U.S. government is developing new computer weapons and driving a black market in "zero-day" bugs. The result could be a more dangerous Web for everyone.

By Tom Simonite on February 13, 2013

Every summer, computer security experts get together in Las Vegas for Black Hat and DEFCON, conferences that have earned notoriety for presentations demonstrating critical security holes discovered in widely used software. But while the conferences continue to draw big crowds, regular attendees say the bugs unveiled haven't been quite so dramatic in recent years.

One reason is that a freshly discovered weakness in a popular piece of software, known in the trade as a "zero-day" vulnerability because the software makers have had no time to develop a fix, can be cashed in for much more than a reputation boost and some free drinks at the bar. Information about such flaws can command prices in the hundreds of thousands of dollars from defense contractors, security agencies and governments.

This trade in zero-day exploits is poorly documented, but it is perhaps the most visible part of a new industry that in the years to come is likely to swallow growing portions of the U.S. national defense budget, reshape international relations, and perhaps make the Web less safe for everyone.

Zero-day exploits are valuable because they can be used to sneak software onto a computer system without detection by conventional computer security measures, such as antivirus packages or firewalls. Criminals might do that to intercept credit card numbers. An intelligence agency or military force might steal diplomatic communications or even shut down a power plant.

It became clear that this type of assault would define a new era in warfare in 2010, when security researchers discovered a piece of malicious software, or malware, known as Stuxnet. Now widely believed to have been a project of U.S. and Israeli intelligence (U.S. officials have yet to publicly acknowledge a role but have done so anonymously to the *New York Times* and NPR), Stuxnet was carefully designed to infect multiple systems needed to access and control industrial equipment used in Iran's nuclear program. The payload was clearly the work of a group with access to government-scale resources and intelligence, but it was made possible by four zero-day exploits for Windows that allowed it to silently infect target computers. That so many precious zero-days were used at once was just one of Stuxnet's many striking features.

Since then, more Stuxnet-like malware has been uncovered, and it's involved even more complex techniques (see "The Antivirus Era Is Over"). It is likely that even more have been deployed but escaped public notice. Meanwhile, governments and companies in the United States and around the world have begun paying more and more for the exploits needed to make such weapons work, says Christopher Soghoian, a principal technologist at the American Civil Liberties Union.

"On the one hand the government is freaking out about cyber-security, and on the other the U.S. is participating in a global market in vulnerabilities and pushing up the prices," says Soghoian, who says he has spoken with people involved in the trade and that prices range from the thousands to the hundreds of thousands. Even civilian law-enforcement agencies pay for zero-days, Soghoian says, in order to sneak spy software onto suspects' computers or mobile phones.

Exploits for mobile operating systems are particularly valued, says Soghoian, because unlike desktop computers, mobile systems are rarely updated. Apple sends updates to iPhone software a few times a year, meaning that a given flaw could be exploited for a long time. Sometimes the discoverer of a zero-day vulnerability receives a monthly payment as long as a flaw remains undiscovered. "As long as Apple or Microsoft has not fixed it you get paid," says Soghioan.

No law directly regulates the sale of zero-days in the United States or elsewhere, so some traders pursue it quite openly. A Bangkok, Thailand-based security researcher who goes by the name "the Grugq" has spoken to the press about negotiating deals worth hundreds of thousands of dollars with government buyers from the United States and western Europe. In a discussion on Twitter last month, in which he was called an "arms dealer," he tweeted that "exploits are not weapons," and said that "an exploit is a component of a toolchain … the team that produces & maintains the toolchain is the weapon."

The Grugq contacted *MIT Technology Review* to state that he has made no "public statement about exploit sales since the *Forbes* article."

Some small companies are similarly up-front about their involvement in the trade. The French security company VUPEN states on its website that it "provides government-grade exploits specifically designed for the Intelligence community and national security agencies to help them achieve their offensive cyber security and lawful intercept missions." Last year, employees of the company publicly demonstrated a zero-day flaw that compromised Google's Chrome browser, but they turned down Google's offer of a $60,000 reward if they would share how it worked. What happened to the exploit is unknown.

No U.S. government agency has gone on the record as saying that it buys zero-days. But U.S. defense agencies and companies have begun to publicly acknowledge that they intend to launch as well as defend against cyberattacks, a stance that will require new ways to penetrate enemy computers.

General Keith Alexander, director of the National Security Agency and commander of the U.S. Cyber Command, told a symposium in Washington last October that the United States is prepared to do more than just block computer attacks. "Part of our defense has to consider offensive measures," he said, making him one of the most senior officials to admit that the government will make use of malware. Earlier in 2012 the U.S. Air Force invited proposals for developing "Cyberspace Warfare Attack capabilities" that could "destroy, deny, degrade, disrupt, deceive, corrupt, or usurp the adversaries [sic] ability to use the cyberspace domain for his advantage." And in November, Regina Dugan, the head of the Defense Advanced Research Projects Agency, delivered another clear signal about the direction U.S. defense technology is heading. "In the coming years we will focus an increasing portion of our cyber research on the investigation of offensive capabilities to address military-specific needs," she said, announcing that the agency expected to expand cyber-security research from 8 percent of its budget to 12 percent.

Defense analysts say one reason for the shift is that talking about offense introduces an element of deterrence, an established strategy for nuclear and conventional conflicts. Up to now, U.S. politicians and defense chiefs have talked mostly about the country's vulnerability to digital attacks. Last fall, for example, Defense Secretary Leon Panetta warned frankly that U.S. infrastructure was being targeted by overseas attackers and that a "digital Pearl Harbor" could result (see "U.S. Power Grids, Water Plants a Hacking Target").

Major defense contractors are less forthcoming about their role in making software to attack enemies of the U.S. government, but they are evidently rushing to embrace the opportunity. "It's a growing area of the defense business at the same time that the rest of the defense business is shrinking," says Peter Singer, director of the 21st Century Defense Initiative at the Brookings Institution, a Washington think tank. "They've identified two growth areas: drones and cyber."

Large contractors are hiring many people with computer security skills, and some job openings make it clear there are opportunities to play more than just defense. Last year, Northrop Grumman posted ads seeking people to "plan, execute and assess an Offensive Cyberspace Operation (OCO) mission," and many current positions at Northrop ask for "hands-on experience of offensive cyber operations." Raytheon prefaces its ads for security-related jobs with language designed to appeal to stereotypical computer hackers: "Surfboards, pirate flags, and DEFCON black badges decorate our offices, and our Nerf collection dwarfs that of most toy stores. Our research and development projects cover the spectrum of offensive and defensive security technologies."

The new focus of America's military and defense contractors may concern some taxpayers. As more public dollars are spent researching new ways to attack computer systems, some of that money will go to people like The Grugq to discover fresh zero-day vulnerabilities. And an escalating cycle of competition between U.S and overseas government agencies and contractors could make the world more dangerous for computer users everywhere.

"Every country makes weapons: unfortunately, cyberspace is like that too," says Sujeet Shenoi, who leads the U.S.-government-sponsored Cyber Corps Program at the University of Tulsa. His program trains students for government jobs defending against attacks, but he fears that defense contractors, also eager to recruit these students, are pushing the idea of offense too hard. Developing powerful malware introduces the dangerous temptation to use it, says Shenoi, who fears the consequences of active strikes against infrastructure. "I think maybe the civilian courts ought to get together and bar these kinds of attacks," he says.

The ease with which perpetrators of a computer attack can hide their tracks also raises the risk that such weapons will be used, Shenoi points out. Worse, even if an attack using malware is unsuccessful, there's a strong chance that a copy will remain somewhere on the victim's system – by accident or design – or accidentally find its way onto computer systems not targeted at all, as Stuxnet did. Some security firms have already identified criminal malware that uses methods first seen in Stuxnet (see "Stuxnet Tricks Copied by Criminals").

"The parallel is dropping the atomic bomb but also leaflets with the design of it," says Singer. He estimates that around 100 countries already have cyber-war units of some kind, and around 20 have formidable capabilities: "There's a lot of people playing this game."

Updated 2.13.2013 to include a response from The Grugq.

Tom Simonite IT Editor, Software & Hardware

I'm *MIT Technology Review*'s IT editor for hardware and software and enjoy a diverse diet of algorithms, Internet, and human-computer interaction with chips on the side. Working in our San Francisco office, I cover new ideas about what computers can do for us, whether they spring from tech... continue »

About Tom »

Follow

Image by Dan Page

Reprints and Permissions | Send feedback to the editor