THE CODE WAR

THE INTERNET IS A BATTLEFIELD, THE PRIZE IS YOUR INFORMATION, AND BUGS ARE THE WEAPONS

BY LEV GROSSMAN

PHOTOGRAPH BY BRENT HUMPHREYS FOR TIME
AARON PORTNOY STARTED HIS HACKING CAREER WHEN
he was still in high school, at the Massachusetts Academy of Math & Science in Worcester, which not coincidentally was the institution he hacked. He did it as follows: Portnoy had a friend call one of the dorms, posing as tech support. The students were more than happy to give him their passwords. Hiding behind those borrowed accounts and routing his approach through proxies in various foreign countries, Portnoy wormed his way into the school's network through a bug in the system that's technically known as a vulnerability, or even more technically as a zero-day. "I had access to every email, grades, everything," he says. "They had a number of issues with their configurations that allowed me to just kind of spread everywhere."

Showing what in retrospect seems like considerable restraint, Portnoy tweaked the school's website to say something uncomplimentary about another student. Then he got out. Later the school brought in tech experts to trace the intrusion, but they could never quite track it back to him.

So naturally Portnoy did it again the next year and got caught. The academy encouraged him to find an alternative venue for his education. It didn't really matter. He graduated from a local high school instead and went on to Northeastern University. It was all excellent preparation for what he does for a living now: researching and selling software vulnerabilities, which since his high school days have become one of the world's newest and more controversial commodities.

Portnoy, now 28, is the co-founder of a two-year-old company in Austin called Exodus Intelligence. Its mission statement reads, "Our goal is to provide clients with actionable information, capabilities, and context for our exclusive zero-day vulnerabilities." Which means—translated from the quasi-paramilitary parlance that's endemic to the software-security industry—that Exodus Intelligence finds and sells bugs, specifically the kind of bugs that could potentially give a third party access to a computer, the same way Portnoy got access to his high school's network. They're worth a lot of money. Vulnerabilities in popular applications and operating systems have been known to change hands for hundreds of thousands of dollars each.

They're worth a lot because although you wouldn't know to look at it, the Internet is a war zone. Even as it gets outwardly ever glossier and more social and easier to please, below that surface the Net is becoming a hostile, contested territory where private companies, law enforcement, criminals, the military and various international intelligence agencies are engaged in constant low-level cyberwarfare. This conflict only occasionally becomes visible to the naked eye—in May, for example, when the U.S. indicted five members of the Chinese army for stealing data from American companies, including Westinghouse and Alcoa. That wasn't an anomaly; it's the norm, and it's getting more normal all the time. Retired Army general Keith Alexander, who formerly headed both the NSA and U.S. Cyber Command, has called China's ongoing electronic theft of American intellectual property "the greatest transfer of wealth in history." Two weeks ago several security firms confirmed that a group believed to be backed by the Russian government has been systematically hacking the U.S.'s energy infrastructure since at least 2012. According to IBM's security division, the average American company fielded a total of 16,856 attacks in 2013.

Cyberwar isn't the future; it's already here. It's business as usual. In this war, the battlefield is everywhere, bugs are weapons, and people like Portnoy are arms dealers.

THE IDEA THAT A SOFTWARE BUG CAN BE WORTH ACTUAL dollars and cents is an odd one. Bugs are mistakes; people generally pay money to fix them. The fact that there's a market for them is a consequence of the larger oddness of our present technological era, in which our entire world—our businesses, medical records, social lives, governments—is emigrating bit by bit out of physical reality and into the software-lined innards of computers in the form of data. A lot of people are interested in that data, for reasons both good and bad. Some of those people are spies. Some of them are criminals. Bugs are what they use to get at it.

In 2009 there was a good object lesson in what makes vulnerabilities so useful. The U.S. and Israel had jointly developed a complex computer worm that was designed to penetrate and compromise a specific uranium-enrichment facility in the Iranian city of Natanz. The worm, which is now known as Stuxnet, was arguably the first true cyberweapon. It was introduced into the
facility’s computer system by a double agent with a USB drive. The worm checked out the place and sent detailed intelligence back to its masters. Then it really let down its hair and went after the computers that controlled the centrifuges used to enrich the uranium. It eventually destroyed about 20% of them. (All this has been deduced after the fact by security experts and journalists, since both the U.S. and Israeli governments are still mum on the subject.)

What made Stuxnet so effective? In a word: bugs. To get the access it needed, Stuxnet took advantage of at least four distinct vulnerabilities, including one in Microsoft Windows. These vulnerabilities—or rather, the knowledge needed to exploit them—were themselves not unlike the enriched uranium the Iranians were working on, but in software form: expensive, highly refined munitions that formed the core of an extremely sophisticated weapons system. They made Stuxnet all the more destructive when—unsurprisingly to anyone who’s seen Jurassic Park—it got loose from the Natanz facility and infected around 100,000 computers worldwide.

The idea of paying money for bugs goes back a lot further than Stuxnet. In 1995 Netscape announced a “Bugs Bounty” program that paid cash to anybody who could find flaws in its browser. The company wasn’t trying to destroy centrifuges; it just wanted to fix holes in its software. In 2002 a security firm called iDefense started buying up vulnerabilities of all kinds; another company, TippingPoint, launched a similar program in 2005. Both programs were created as alternatives to the increasingly active and chaotic exchange of zero-days on the open market—essentially they acted as safe zero-day disposal facilities, a bit like radioactive-waste repositories. If you found a bug, instead of selling it to the highest bidder, who would do God knows what with it, you could sell it to iDefense or TippingPoint for a reliable price, and they would alert their clients to the problem and work with the software vendor to get the bug patched. iDefense and TippingPoint had something else in common too: they both, in successive years, 2005 and 2006, hired an intern named Aaron Portnoy.

Portnoy in no way resembles Matthew Broderick in WarGames. He’s a confident, affable, articulate guy who makes good eye contact and just happens to be a supercyberintrusions expert. In 2006, Portnoy dropped out of Northeastern to work at TippingPoint full time, then in 2012 he left to go into the vulnerabilities business on his own. Exodus Intelligence joined a small, elite field that includes Vupen, which is based in the south of France; Revulsn in Malta; Netragard in the U.S., and Telus in Canada. (Netragard wins for best corporate motto: “We protect you from people like us.”) Exodus’ headquarters are in an office park in Austin, which it shares with accountants and real estate agents. The place is spartan even by tech-startup standards: there’s exactly one piece of interior decoration, a pirate flag tucked up on a wall.

Its nine inhabitants spend their days banging on software looking for ways in: browsers, email clients, instant messaging clients, Flash, Java, industrial control systems, anything an attacker could use as an entry point. “One thing we try to maintain is a capability in every major backup software out there, because that’s one of the juiciest targets,” Portnoy says. “If you get on an enterprise network, what is an administrator going to want to protect? Their important information. What do they use to protect that? Backup software.”

When a researcher at Exodus finds a vulnerability, he or she types it up in a professional-looking report along with technical documentation that explains what it does, where it lives, what it gets you, how to spot it, what versions of the software it works on, how one could mitigate it and so on. Most important, Exodus provides you with an exploit, which is the procedure you’d have to follow to actually trigger the bug and take advantage of it. “Every single vulnerability that we give our customers comes with a working exploit,” Portnoy says. “If we can’t exploit it, we don’t even bother telling anyone. It’s not worth it.” Voila, one freshly minted zero-day vulnerability.

(A note on that term, zero-day: it refers to a bug’s freshness. Bugs, like fish, don’t age well, and zero-day means that the bug has been public for exactly zero days, hence no one has tried to fix it yet. The term is so ubiquitous that it has gone from adjective to noun: Portnoy sells zero-days.)

Portnoy takes pride in the superior quality and effectiveness of Exodus’ exploits. “We try to make them as nasty and invasive as possible,” he explains. “We tout what we deliver as indicative of or surpassing the current technical capabilities of people who are actually
actively attacking others." When a company hires Exodus, it does so on a subscription basis: you get a certain number of bugs a year for such-and-such amount of money. Subscriptions start at around $200,000.

The vulnerabilities business has a mixed reputation, based on the presumption that the bugs it provides are being used for criminal or unethical purposes. A Washington, D.C., company called Endgame that sold vulnerabilities to the government for years was dubbed "the Blackwater of hacking" by Forbes magazine. Last year, when Endgame announced that it was getting out of the game, it did so triumphantly, as if it were kicking a heroin habit. "The exploit business is a crummy business to be in," its CEO said.

The reality is more complex. Exodus’s clients come in two basic types, offensive and defensive. Playing for the defense are security firms and antivirus vendors who are looking for information they can integrate into their products, or who want to keep their clients up to speed on what threats are out there. On offense are penetration testers, consultants who use Exodus’s zero-days to play the "red team" in simulated attacks on their own or other people’s networks. "If they want to show what a real attack would look like from a determined adversary," Portnoy says, "we give them the tools to do that."

And then there are the ones who aren’t just playing. Portnoy is discreet about his client list, but others have been less so. It’s well known that the NSA and the FBI are fond of implanting surveillance software on target computers to gather intelligence; the FBI is even now lobbying the courts to make it easier to get warrants to do just that. How do you implant software on somebody’s computer without them knowing about it? One way is to exploit a vulnerability. Last year the FBI busted a company called Freedom Hosting, which it called “the largest facilitator of child porn on the planet.” Freedom Hosting operated on the Tor network, which anonymizes Web traffic. To get around the anonymity, the FBI used a vulnerability in Firefox.

As for the NSA, the Washington Post’s analysis of the Edward Snowden leaks revealed an NSA budget that included $25.5 million for “additional covert purchases of software vulnerabilities,” suggesting that they both buy zero-days and roll their own internally. (In September, the investigative journalism site Mother Jones obtained a copy of a contract between the NSA and Vupen, which has just opened a satellite office outside Washington.) That same budget provided a remarkable X-ray of a secret NSA initiative code-named GENIE, funded at $652 million, to implant malware on foreign computer networks on a mass scale. By the end of 2013, GENIE was expected to control around 85,000 machines.

On the day I interviewed him, Portnoy was just back from a meeting at the Pentagon. “We’re dealing a lot more in the government space,” he says. “That’s been a big change. It wasn’t really something that we had taken into account with our business model, but it turns out that the government has a hard time staffing people who can do what we do.”

It’s learning. According, again, to the Snowden documents, the U.S. mounted 231 offensive cyberoperations in 2011 against China, Russia, Iran and North Korea, among others—and that was 2011, ancient history in cybertime. The 2015 defense budget includes $5 billion for cyberspace operations, which is a very general term for an arena about which not much is known. Verizon estimates, in its annual Data Breach Investigations Report, that 12% of data breaches last year were attributable to cyberespionage operations. But the report also acknowledges that solid information about cyberespionage is “really hard to come by.” The action is covert, and even when you can spot it, cyberespionage is difficult to distinguish from the industrial kind, or from plain old cybercrime, because it’s so hard to pinpoint the source and intent of an attack.

Given their offensive potential, you’d think the government would want to control the trade in vulnerabilities the way it does, say, the trade in fighter jets and land mines. But regulators are just now catching up with it. The Wassenaar Arrangement, which is the international agreement that governs arms sales among the U.S. and 40 other participating nations, was modified in December to include “intrusion software”—in its list of restricted dual-use technologies, but so far that change hasn’t been enforced. “It’s not a market that right now the government has really looked at regulating,” a senior Administration official told TIME. “We’ve been much more in the voluntary best-practices-and-standards space. And I think that you’ll see us continue to focus on that.”

Which sometimes places Portnoy and his colleagues in the odd position of having to make their own ethical choices about whom they will and won’t sell to. Portnoy stays out of politics as much as possible—“we try to distance ourselves from what our customers’ use case is,” is how he puts it—but no question, there’s a line. He won’t work with embargoed countries: North Korea, Sudan, Iran, Cuba. “We do some due diligence when we’re talking to potential customers,” he says. “We will run it through the State Department. We’ll run it through some military organizations that we have some contacts at...but there’s no currently legally binding statutes that we have to abide by. That will probably change.”

Vupen takes a similar position, according to its CEO, Chaouki Bekrar, who weighed in via email. “Our unique goal and motivation is to help our government customers fight crime and save lives using our zero-day exploits, and to have successes every week all around the world, thus all allegations and bad press about zero-day technologies is just gossip and bullsh-t.” Nevertheless, people will talk. “For media and press releases, they’re going to say, ‘Yeah, we only sell to these markets,’ but nobody has any idea,” says John Pirc, CTO of the information-security research firm NSS Labs. “Things are under NDA. There’s no telling who they sell to.”

The potential for abuse is real, anyway. Zero-days don’t care whose computer you’re accessing or why. On April 28 researchers at the security firm Kaspersky Lab disclosed the existence of a zero-day vulnerability in Adobe Flash that could be used to install malware on a target machine, if the user of that machine could be induced to visit a certain specific website. For good measure the researchers checked out who was hosting that specific website. In this case it turned out to be the Syrian Ministry of Justice. One could reasonably theorize that the Syrian government was taking advantage of a zero-day to surveil its own dissidents.
The real nightmare scenario is an attack on public infrastructure by a political group un restrained by any national affiliation. Terrorists, for example. “Zero-day vulnerabilities, if you’re able to identify one of them, can do serious harm,” says Mary Gallagher, formerly the special agent in charge of cyber and special operations in the FBI’s New York office, currently at Deloitte and Touche. As an example she mentions SCADA, which stands for Supervisory Control and Data Acquisition, the software used to control industrial systems. That’s what Stuxnet went after. “Everything that we think of—manufacturing floors, the electrical grid, or the water supply, or elevators—that are run with data equipment, it’s connected to the Internet. The real concern is, that’s the part that least protected.”

Even if tin-pot dictators and cybercriminals can’t shop at Exodus, there’s a lively black market for vulnerabilities, although information about it is scarce. Some people consider it a serious problem; some don’t. “It would mystify me why people would do this for criminal means when you can make so much money doing it legally,” says Dave Aitel, CEO of the security firm Immunity and a former researcher for the NSA. “I’m not saying you’re going to buy a Ferrari, but you’re definitely 100% going to have a top-of-the-line Honda Civic.” But a report by the Rand Corp. published in March characterized the black market for vulnerabilities as “a playground of financially driven, highly organized and sophisticated groups.” Katie Moussouris, formerly senior security strategist lead at Microsoft and now chief policy officer for HackerOne, a startup in the vulnerability space, says black market prices can be even higher than those in the legitimate marketplace. “I’ve seen pricing models where a six-figure payout will go out as a lump sum, and then a monthly recurring fee will be paid to the researcher to encourage them to keep quiet and not use it and not double-sell it.”

Portnoy is snifflly about the quality: most of what’s on the black market doesn’t have that zero-day freshness. Criminals typically target older vulnerabilities, for which fixes have already been released, and just troll the Net till they find somebody who hasn’t updated their software yet, zero-day, shmero-day. “It’s more like, ‘It’s going to work 10% of the time, but that’s good enough for us because that gets us our payday,’” Portnoy says. But there’s good hunting out there: according to Symantec’s Internet Security Threat Report 2014, 1 in 8 websites it scanned had a serious unpatched vulnerability. “One of the things that we talk about is, How do you undermine the economics of that market?” says a senior Obama Administration official. “How do you actually get people to patch their systems much faster, how do you get it to be done automatically...so now you can’t use that same crappy piece of malware and that attack vector over and over again?”

Then there’s still another market, on the other side from the black one, which is run by the people who wrote the buggy software in the first place. Big software companies are increasingly finding it cost-effective to buy up their own bugs and fix them before anybody else can exploit them—it’s kind of like doing your beta testing after you ship the product. In 2010 Google helped set the trend by offering rewards for vulnerabilities in Chrome; this year its total payouts have reached the $3.3 million mark. Now bug-bounty programs are standard practice—even Etsy has one. Microsoft will pay up to $100,000 for a serious security flaw in Windows. Last year Facebook paid out $4.5 million for a total of 687 bugs. Facebook’s program comes with its own special flourish: you get a branded White Hat Bug Bounty Visa debit card.

But there’s still a noticeable gap between the prices companies will pay for vulnerabilities and the amounts those bugs will fetch on the open market. There’s an annual hacking event called Pwn2Own in which contestants compete to find flaws in popular software—Portnoy directed the first Pwn2Own in 2007. In 2012 the Vupen team beat the security on Chrome, which would have qualified them for a $60,000 prize—except they turned the money down, even when Google offered to double it. They kept the vulnerability for their clients. It’s reaching the point where software companies can’t afford their own bugs.

**There’s a lively debate going on in Washington** over whether vulnerabilities should be kept secret at all. After the Heartbleed bug became public in April, *Businessweek* ran a story claiming that the NSA not only already knew about it but had even been using it to spy on people for years. The White House and the NSA deny this—the NSA even tweeted about it, so you know they’re serious—but the idea that U.S. intelligence
agencies are sitting on a private arsenal of software vulnerabilities that they blithely use to penetrate other people's computers, rather than reporting them and getting them fixed, makes a lot of people uncomfortable.

But there's a counterargument, which is that you have to strike a balance between public-spiritedly debugging the world's software on the one hand, and defending the country on the other. "I don't think the NSA has any obligation, if you're talking about legal obligations, to disclose vulnerabilities," says Jack Goldsmith, a professor at Harvard Law School. "The NSA has always been in the business of finding vulnerabilities in communications technology. That's what they do." On a more practical level, even if the NSA does give up its vulnerabilities, the Chinese and Russians won't, which leaves us on the wrong end of a vulnerability gap. "You have a tendency to say, 'Let's fix all the problems, but all that does is completely defang the NSA and leave all the power in the hands of our opponents,'" Aitel argues. He thinks the NSA should hoard its zero-days at all costs. "It's the only hope. It is the Obi-Wan of our intelligence efforts."

Current policy, per a December report by the President's Review Group on Intelligence and Communications Technologies, is that the government will disclose zero-days except when they're needed for "an urgent and significant national security priority." A senior Administration official adds that they disclose the vulnerabilities when they find "a very large percentage of the time," more than three-quarters. "There's this image that we have this _Raiders of the Lost Ark_-style warehouse full of these things someplace," he says. "That's just not how it works. The truth is that most of the time the interest that we have is actually on the defensive side—it's actually getting the vulnerability to the vendor and identifying it for them, actually getting it fixed."

The dream, of course, is a world where there are no more vulnerabilities, where software can be perfected, security will be total, and we can move on and find something else to worry about. But the trend is going the other way. The more we ask computers to do for us, the more urgently we need them to be secure—but the more computers have to do, the more complex their software has to be, and therefore the more bugs they have, and round and round—it's a vicious cycle. The operating system on your laptop consists of tens of millions of lines of code. Threw

16,856
Number of attacks on the average American company fielded in 2013, according to IBM's security division.

a bunch of applications on top of that, most of which have been rushed to market three-quarters finished, then connect your laptop to millions of other devices, tablets and phones included, each with its own configuration of hardware and software, and the situation rapidly becomes unmanageable. "There are a finite number of bugs in a given piece of software," Portnoy says. "However, that given piece of software is updated and added to and changed, and underlying operating systems change, and they have to support a legacy this, that, and the other thing. Windows XP—when was that released? In 2000? 2007? You have to support systems that are 15 years old. And there's new software being released every day, and new classes of vulnerabilities being discovered. As long as that's the case, we'll have a job."

PATCHING VULNERABILITIES IS A BIT LIKE BAILING THE OCEAN: YOU'RE NEVER DONE. CODING PRACTICES AND STANDARDS ARE GETTING BETTER, BUT NOT FAST ENOUGH. THE NATIONAL VULNERABILITY DATABASE—MAYBE YOU DIDN'T KNOW WE HAD ONE, BUT WE DO—CURRENTLY LISTS 65,239 VULNERABILITIES; RESEARCHERS FOUND AN AVERAGE OF 13 A DAY LAST YEAR. IN MARCH IT CAME OUT THAT THE FEDERAL GOVERNMENT NOTIFIED 3,000 U.S. COMPANIES THAT THEY'D BEEN HACKED LAST YEAR. THE WALLS AROUND OUR DATA DON'T JUST HAVE CHINKS IN THEM; THEY'RE MORE CHINK THAN WALL. THE LONGER YOU TALK TO PEOPLE IN THE COMPUTER-SECURITY BUSINESS, THE MORE YOU REALIZE THAT THERE IS NO SUCH THING: IT DOESN'T EXIST.

WE'VE BEEN SO SUCCESSFUL IN BUILDING A CONNECTED PARADISE WHERE INFORMATION FLOWS FREELY, AND SO EAGER TO MOVE OUR LIVES INTO IT, THAT WE'VE GOTTEN AHEAD OF OUR ABILITY TO KEEP INFORMATION FROM FLOWING WHEN WE DON'T WANT IT TO. THE RESULT IS A NEW KIND OF WAR—ET ET ANOTHER ONE, IN A MILLENIUM THAT SEEMS TO SPECIALIZE IN THEM. IT'S UNOBTRUSIVE BUT CONSTANT AND PERSUASIVE. IT MAKES LITTLE DISTINCTION BETWEEN MILITARY AND CIVILIAN, PRIVATE AND PUBLIC, POLITICS AND BUSINESS. ITS VICTIMS BLEED PERSONAL DATA AND INTELLIGENT PROPERTY, AND BY THE TIME THEY FIGURE OUT THEY'VE BEEN HIT, IT'S ALREADY MUCH TOO LATE. "There are always going to be zero-days out there," says a senior Administration official. "It's not just about the protection, the walls and moats and the barbed-wire equivalents in cyberspace. You have to work under the assumption that some of the time the bad guys are going to get in."—WITH REPORTING BY SAM FRIZELL/NEW YORK AND MASSIMO CALABRESI/WASHINGTON