STAYSAFEONLINE.org
National Cyber Security Alliance
Homeland Security
USA TODAY Education

Week 2

Meet A-Z: He's behind a cybercrime wave

Multimillion-dollar hacker makes a name for himself

By Byron Acohido
USA TODAY

He goes by the nickname A-Z and is one of Russia's bright young tech stars. He's a crack programmer, successful entrepreneur and creator of sophisticated software tools that help his customers make millions.

Trouble is, A-Z's masterstroke is a computer program called ZeuS that helps cybergangs steal people's identity data and pull off Web scams on a vast scale. Last fall, German criminals used ZeuS to pull off an Ocean's Eleven-like caper, hijacking $6 million from banks in the United States, United Kingdom, Spain and Italy, says SecureWorks, an Atlanta-based company that monitors Internet crime and supplies security systems for 2,100 companies and government agencies.

A few years ago, skilled hackers such as A-Z concentrated most of their efforts on setting loose globe-spanning Internet viruses, mainly for bragging rights. But cybercrime is now a fast-expanding, global industry, security researchers and law enforcement officials say. Because it most often goes undetected and unreported, cybercrime is difficult to measure. A benchmark widely cited by the tech-security community is that its value tops $100 billion a year, outpacing global drug trafficking.

"All you need is a computer, Internet access and programming skills, and now you have a viable career path in front of you," says Nick Newman, a computer crime specialist at the National White Collar Crime Center, a federally funded non-profit that trains local law enforcement. "It's easy money, and because the Internet is anonymous you don't think you'll ever get caught."

A-Z is an archetypical new-generation hacker. No one outside of his close associates knows his true identity, virus hunters say. But security researchers and government authorities have exhaustively triangulated his presence in the cyber-underworld for nearly two years. Based on A-Z's marketing activities in Russian chat rooms and forums, and distinctive coding signatures in ZeuS, investigators peg him to be a male in his early 20s, living in Moscow, working full time as an independent software developer for hire.

"He's well-spoken, business-savvy and discreet," says Don Jackson, a senior researcher at SecureWorks who has investigated A-Z's movements online. Jackson belongs to a fraternity of about 200 other professional virus hunters who shadow hackers and scrutinize Internet traffic to flush out data-stealing programs and curtail Web scams. A-Z is "very careful to maintain a professional image, and he always leaves his clients wanting more."

Crafting a sneaky ZeuS

Hackers such as A-Z craft the code that enables crime groups to continually inundate your e-mail inbox with spam scams and taint millions of popular Web pages with snares to take control of your PC.

"Cybercrime has evolved into big business and created a market for highly specialized individuals," says Steve Santorelli, director of investigations at research firm Team Cymru, who has studied how ZeuS helps cyber-intruders control infected computers. A-Z identified an underserved market niche and hustled to fill it, Jackson says. He recognized latent demand for software that could more efficiently infect home and workplace PCs and turn them into bots — obedient machines that could be controlled remotely without the owners' knowledge or consent. Cybergangs now routinely assemble thousands of infected PCs in networks, called botnets, which they then use to spread spam, infect other computers, steal data and hijack online accounts.

As seen in USA TODAY August 5, 2008

Anatomy of a cyber bank heist

In summer 2007, a German gang skilled at pilfering online bank accounts forged a partnership with a Russian hacker known as A-Z, who security analysts say created ZeuS, a versatile tool for infecting PCs. The collaboration produced a lucrative score.

Step 1: Infection
They blast waves of e-mail spam carrying purported links to greeting cards, news stories and celebrity videos. Clicking on a link installs generic ZeuS on your PC.

Step 2: Data Harvesting
Generic ZeuS collects data typed on your banking pages and other Web forms; it also turns the PC into a "bot," that can be used by others remotely.

Step 3: Datal Culling
Gang members spend summer and fall stealing personal data from PC users with commercial accounts at banks that allow online cash transfers.

Step 4: 2nd Stage Infection
E-mail is sent to bank patrons asking them to "click here" to reset their security codes. Thousands fall for the ruse, installing a custom version of ZeuS.

Step 5: The Inside Set Up
Custom ZeuS issues an alert each time the PC user logs into the account.

Step 6: The Score
Alerts get distributed to the bots created by generic Zeus; each bot stands ready to complete a cash transfer in a few seconds.

Step 7: The Take
In two weeks, ZeuS extracts $6 million from thousands of accounts at banks in the USA, U.K., Italy and Spain.

The Shutdown
Authorities shut down a computer server in Turkey discovered to be holding key instructions for transferring funds.

Source: SecureWorks

A-Z perfected ZeuS — a customizable botnet creation and management program that readily slips through computer firewalls and sidesteps detection by anti-virus filters. He began hawking ZeuS for $3,000 on Internet forums, where hackers and scammers congregate. By early 2007, ZeuS began to catch on, according to reports from Sunbelt Software, Symantec, McAfee, Kaspersky Lab, Finjan and other security firms.

One customer used ZeuS to steal user names and passwords from patrons of a Russian online stock-trading site. Another used ZeuS to take control of at least 150,000 PCs and encrypt personal files stored on the hard drives, leaving behind a ransom note demanding $300 for the keys to decrypt the files.

ZeuS was also deployed to swipe 1.6 million sensitive records from job seekers at Monster.com and several other online job sites. Monster has since taken an "extremely aggressive approach" to preventing fraud, says spokesman Steve Sylven. "We continually refine our site technologies to prevent unauthorized access to Monster services," he says.

ZeuS was so effective that it inspired cheap knockoffs. This cut into A-Z's revenue and tarnished his reputation, Jackson says. "His money began to dry up when U.S. and German groups began selling counterfeit versions."

Much as a young Bill Gates did

when hackers began to pirate early versions of Microsoft Windows, A-Z took steps to prevent the theft of his intellectual property, Jackson says. A version of ZeuS began to circulate with a statement strictly limiting the purchaser's use of his brainchild. Violators, A-Z warned, would have key coding revealed to the anti-virus companies, effectively neutralizing their copies of ZeuS.

In spring 2007, soon after the restricted version of ZeuS showed up, A-Z adopted a lower profile. He stopped advertising ZeuS for sale on criminal forums and began supplying ZeuS only to repeat or referred customers, Jackson says.

Theft on a grand scale

In early summer 2007, A-Z agreed to form a partnership with a German cybergang to pursue an ambitious heist worthy of a Hollywood thriller, Jackson says. The gang was known for executing "man-in-the-middle" attacks. This involved infecting a PC with a virus that sits dormant until the user logs into an online bank account. The virus then comes alive and tries to execute a cash transfer to an account controlled by the crooks — while the victim is logged on and doing other banking, says Ken Dunham, research director at iSight Partners, a Dallas-based risk-management firm.

"The really bad actors are using code that can mess with your transactions on the fly," says Dunham. "They're manipulating what comes into and leaves your browser in real time."

Still, man-in-the-middle attacks are notoriously hit-and-miss. Some banks have moved to thwart them by only allowing cash transfers from commercial accounts, and requiring bank patrons to type in a special code, called a security certificate.

Jackson caught wind of the alliance between A-Z and the German gang and began reporting on it within tech-security circles. Here is what Jackson has extensively documented about the partnership's elaborate caper:

It was executed in two stages. In Stage 1, the gang sent millions of spam e-mail messages purporting to carry a Web link to Father's Day greeting cards, celebrity videos, stories on real and bogus news events and other ruses. Anyone who clicked on such a link received an error message — and the PC got infected. A generic version of ZeuS then began to harvest all data typed by the PC user on any Web forms: shopping pages, online applications, account logon pages and the like. ZeuS also slotted each infected PC into a large botnet standing at the ready and awaiting further commands.

Through the summer and fall, gang members combed through the stolen data that poured in from generic ZeuS infections. They were on the hunt for PC users with online access to commercial bank accounts equipped with the ability to make online cash transfers. By November, the gang had a list of several thousand such accounts and was ready to move to Stage 2, which hinged on a "spear phishing" campaign, Jackson says.

Generic phishing scams that try to trick people into typing their usernames and passwords at spoofed Web pages are typically mass-e-mailed indiscriminately. By contrast, spear phishers target specific individuals. The gang began spear phishing the commercial bank account holders.

The e-mails advised the account holders that their security certificates were "out of sync" and asked them to "click here" to reset them. Since the messages included great detail about the individual and did not ask for any sensitive data, the ruse was "very convincing," Jackson says.

According to Jackson, several thousand online banking patrons fell for the ruse and clicked on the hyperlink. A fresh copy of their security certificate, indeed, popped up. But a fresh infection also got installed: a customized version of ZeuS tweaked by A-Z to alert the gang the next time the PC user logged into the account, Jackson says.

Anticipating that ZeuS would reel in thousands of such alerts, A-Z prepared the botnet created in Stage 1 to lend a helping hand. Jackson says the botnet was set to automatically react to alerts. Each alert triggered a cash transfer of

$5,000 to $10,000 that took only a few seconds to complete, he says. According to SecureWorks, British law enforcement and affected banks compiled an estimate of ZeuS' total take over the course of two weeks: $6 million.

A break in the case came when Jackson discovered a computer server in Turkey where the gang stored instructions for making cash deposits into accounts it controlled. Network operators in the U.K., Germany and Turkey cooperated with U.S. law enforcement to shut down the server and curtail the scam, SecureWorks says.

Though the robbery was widely discussed in tech-security circles, the names of the banks that suffered losses were never disclosed. Members of the German gang and A-Z remain at large and under investigation by U.S. authorities. The FBI and U.S. Secret Service declined comment.

As a rule, tech-security firms help banks under non-disclosure agreements. The names of the 20 affected banks have remained undisclosed.

Hacker's free to 'live large'

Pursuing cybercrooks, especially hackers who mainly write code, is a low priority for Russian police, says John Pironti, a banking security expert at systems integration firm Getronics. As long as A-Z doesn't leave Russia, he is effectively beyond the rule of law. "Unless he causes someone physical or political harm, he can live large," Pironti says.

A-Z, in fact, has admirers in legitimate tech circles. Yuval Ben-Itzhak, a virus hunter at San Jose-based security firm Finjan, marvels at the finesse it took to develop ZeuS. "To write a program that needs to run on millions of PCs all around the world and not break them is truly an art," Ben-Itzhak says. "I'm telling you, I'd be willing to hire a person like this at any price."

In online chats, Jackson says, A-Z has told him that he presumes his clients used ZeuS strictly for legal endeavors, and expressed a desire to be taken seriously as a programmer. In one chat session, A-Z divulged his goal to earn enough to trade in his 1995 Zhiguli sedan for a Mercedes-Benz SLR sports coupe. In another chat, Jackson asked A-Z about ZeuS' history of being used for mass infections and other criminal activity. Jackson says the hacker insisted that his materials are provided for research purposes and said that he could not control his clients' actions.

Such facile answers come as no surprise to security experts and social scientists who track the behavior of hackers and scammers immersed in a virtual world where cheating and stealing — and getting away with it — are badges of honor.

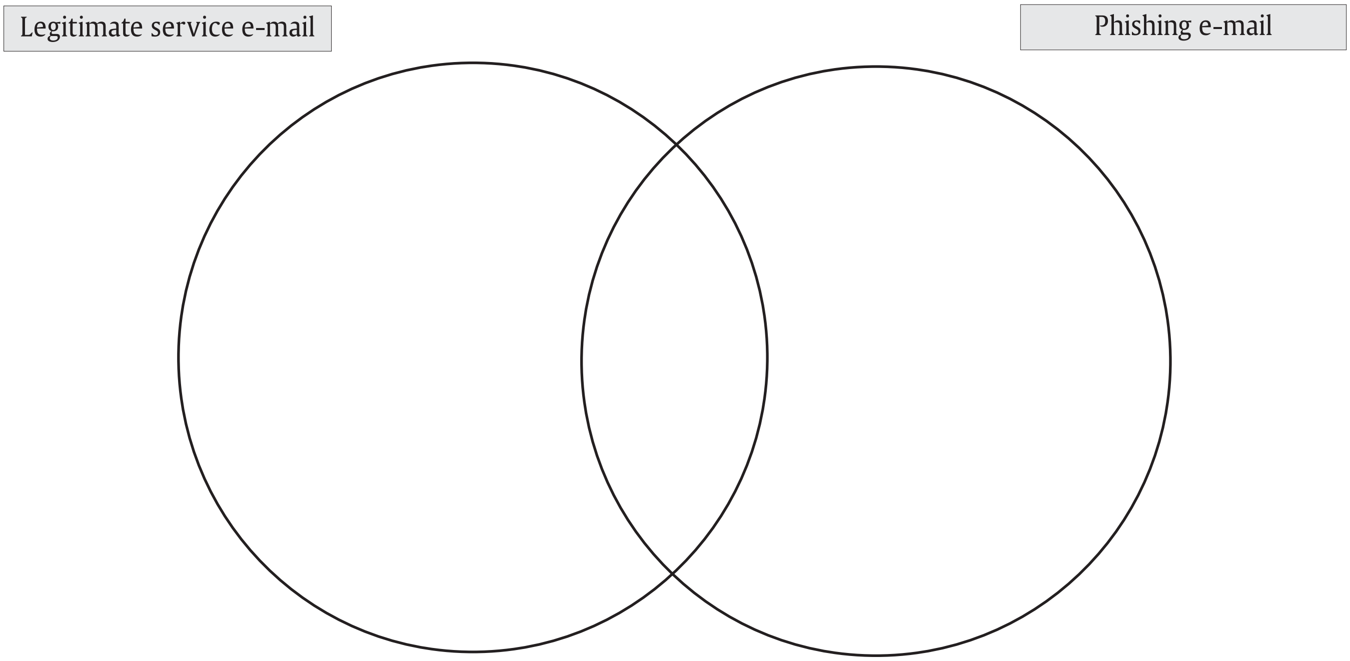
"Unfortunately, many of these new specialists rationalize their actions in the absence of ethical guidance," says Santorelli of Team Cymru. "They represent a serious challenge to those who seek to protect Internet users."

Discussion

1. Why are the effects of cybercrime difficult to measure?
2. Why is cybercrime a particularly attractive way to steal?
3. How does ZeuS work?
4. What is known or surmised about A-Z, the creator of ZeuS?
5. What does Jackson say is A-Z's attitude about how his clients use ZeuS?
6. Why are A-Z and the German gang responsible for the $6 million heist still at large?
7. What is the difference between generic phishing and spear phishing?
8. If you had been one of the account users who had received the spear phisher e-mail with the hyperlink to "reset" their password, would you have been fooled? Why or why not?

Activity

Re-read the characteristics of the spear phisher e-mail. What aspects of it convinced recipients of its legitimacy? Cybercrimes are often perpetrated through generic or spear phishing e-mail scams. So often, it is difficult to tell a legitimate service e-mail from a phony one. With a partner, take a piece of paper and create a Venn Diagram (see example below). Label the left circle "legitimate service e-mail" and the right one "phishing e-mail." Then, populate the circles with traits you believe generally characterize each. Where the circles are joined, list the traits both e-mails would have in common. Then, beneath your diagram, list three ways you can protect yourself from falling prey to a phishing scam. For more information, visit the United States Computer Emergency Readiness Team page on phishing at www.us-cert.gov/cas/tips/ST04-014.html.



TEACHER'S GUIDE

Week 2

Lesson objectives:

In this lesson, students will:

- Read about cybercrime.
- Recall specific traits of cybercrime.
- Assess the characteristics of hackers.
- Determine the difference between a legitimate and phishing e-mail.
- Ascertain ways to safeguard against phishing scams.

Time requirements:

Step 1: Read the article (20 minutes).
Step 2: Answer the discussion questions (15 minutes).
Step 3: Create a Venn Diagram and ascertain ways to protect against phishing scams (15 minutes).
Step 4: Share diagrams and safety measures as a class (10 minutes).

Total: 60 minutes

Recommendations:

- Step 1: Because of the lengthiness of the article, you may want to assign it as homework.

- Step 2: It is best to facilitate a whole class discussion to ensure student understanding of the concepts. You may also wish to direct students' attention to the heist timeline that accompanies the article to help students better understand the multiple steps the cybercriminals took to successfully steal $6 million. Ensure students understand the terms bot (obedient machines that are implanted in a personal computer and can be controlled remotely) and botnet (a network of bots).

- Step 3: Before students get into pairs, you may wish to model the activity by creating a Venn Diagram on the board and have students provide a few descriptive terms for each circle. Circulate to ensure students remain on task and understand their task.

- Step 4: To close the lesson, have students share some of the traits they've listed in their Venn Diagram and add them to the diagram on the board. Finish the discussion by having students offer how they would safeguard themselves against a phishing scam. Perhaps create a class list of the safety measures.

Links:

- National Cyber Security Alliance — StaySafeOnline www.staysafeonline.org
- United States Computer Emergency Readiness Team www.us-cert.gov
- i-SAFE www.i-safe.org
- Wired Safety Organization www.wiredsafety.org
- Federal Trade Commission: OnGaurdOnline onguardonline.gov
- Multi-State Information Sharing and Analysis Center www.msisac.org/awareness