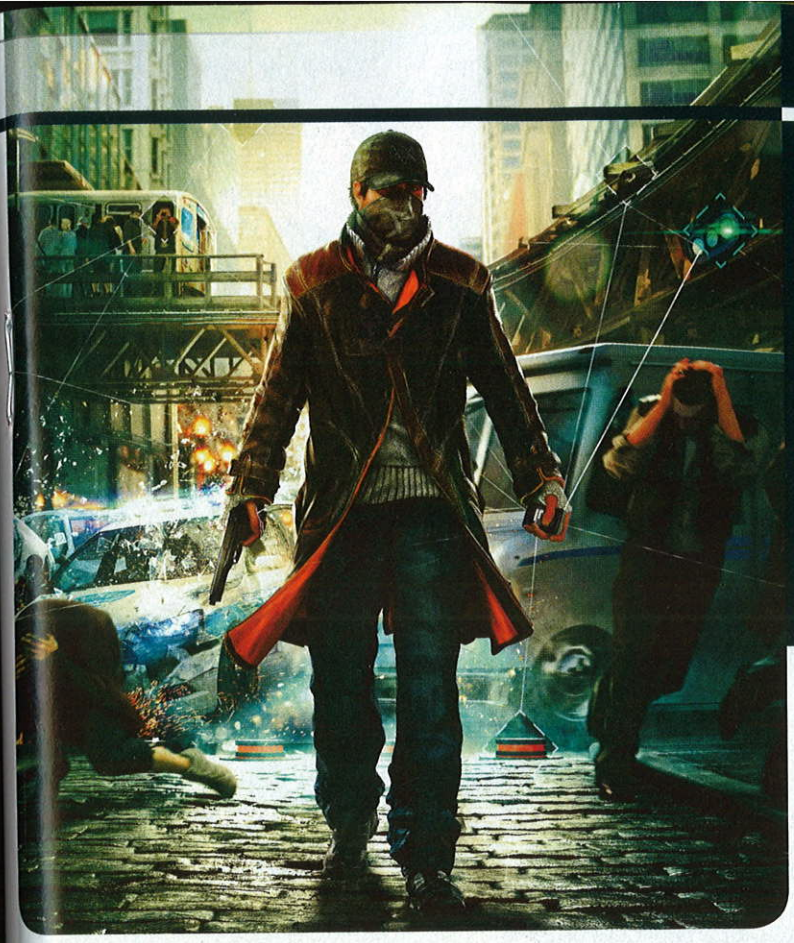

## THE ULTIMATE LIVE HACKER

**There are 25,000 surveillance cameras for every 2.7 million citizens in America—and hardly any city is more networked than Chicago. That's why Ubisoft has made this city the setting for its new video game *Watch Dogs*. The protagonist is hacker Aiden Pearce (at left), who is on the hunt for the man who killed his niece. Gamers can step into his role and use his hacking capabilities to change the color of traffic lights, hack mobile phones, and manipulate the whole city. According to experts, such tricks are actually feasible. "The only unrealistic part is the pace," says IT security expert Vitaly Kamluk. "In real life, hackers sometimes spend months at their computers. They must analyze every line of software code to find the weak spots. Only then can they write a code that will exploit the vulnerabilities." *Watch Dogs* was released worldwide on May 27, 2014.**

says Jonathan Morin, the creative director of the game. "And in terms of technology, they've been successful," Brossard confirms. "The hacks are all totally doable." In addition to Brossard, Ubisoft consulted with Kaspersky Lab. "I was surprised at how current some of the hacks were—like when the main character manages to empty the ATMs. We are investigating a similar crime in Russia," says Kamluk, Kaspersky's principal security researcher.

## HOW CAN YOU MANIPULATE AN AUTOMATED TELLER MACHINE?

In the cash machines of Moscow, cybercriminals have installed what amounts to a back door in the software. What does the back door do? "It allows unauthorized access to a machine. Even though you are not a bank employee, the back door enables you to manipulate the cash machine via the network or right at the location," explains Kamluk. A back door is essentially malware—a new software component that contains a code that can be used to empty an ATM. After the malware is installed, the back door observes which PIN numbers are entered. Once a hacker types the special code into the ATM, the terminal shuts down—communication with its network is cut off and the machine starts spitting out the cash. The firm grasp the perpetrator has on the machine is difficult and expensive to break. "To find malicious code, millions of lines must be sifted through," says Kamluk. But how do you go about finding the infected portion?

"Each time a program is executed on a Windows system, it leaves a trail on the computer's hard drive. We start by scouring logs for new files or newly activated programs," Kamluk says. As soon as a new program is found, the analysis begins: How does it store data? How does it interact with the user? "Normally a program will ask the user before copying things like password files. Malware does not. It duplicates data as discreetly as possible. But that is precisely what can lead us to the malware when we do our analysis," explains Kamluk. Identifying a cyberattack is one thing, but how do you actually find the hackers responsible for perpetrating it?

## WHAT TRACES DO HACKERS LEAVE BEHIND?

Malware expert Kyle Wilhoit has used a "honeypot trap" when he's hunting down malicious hackers. His strategy: He constructed a simulated hydroelectric pump station in his basement, complete with a SCADA system. What was actually a collection of devices he bought on eBay appeared to hackers like the real public water utility of a small town—and it's apparently a very appealing target. Over the course of just a few months, Wilhoit registered 74 attacks, many of which had come from China. Using malware he developed himself, Wilhoit traced the source of the cyberattacks to get a rough idea of the hackers' location and which IP addresses they were using.

The development of such hacker traps is becoming increasingly important for security experts. "The Internet of Things has already become the area of the Web with the most serious security issues and the greatest risk of damage during a cyberattack," says security researcher Marc Rogers. As long as our surveillance cameras, our infrastructure, and even our industrial facilities remain inadequately secured, it is child's play for cybercriminals to plunge our cities into chaos.

PHOTOS: PR.