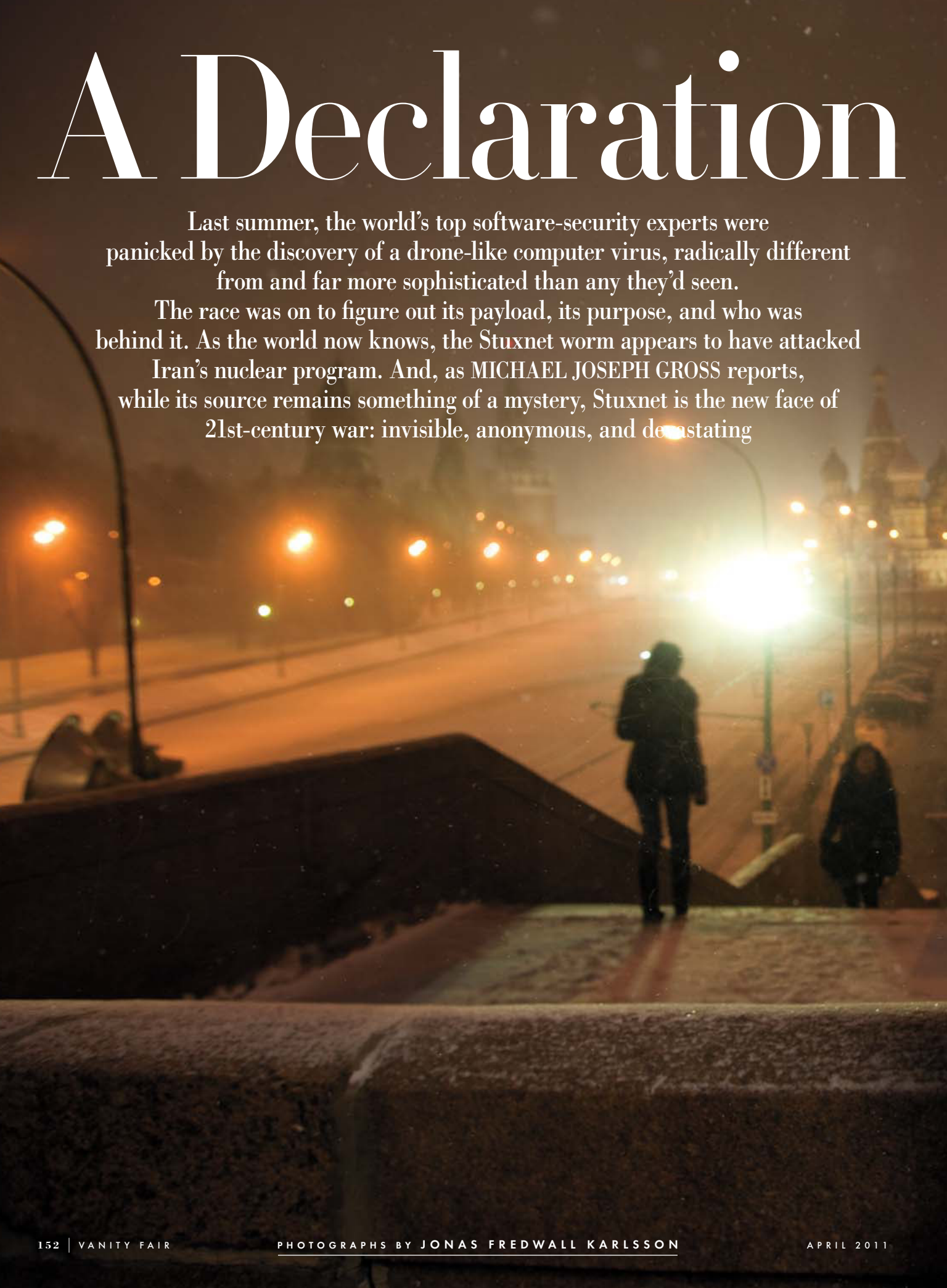
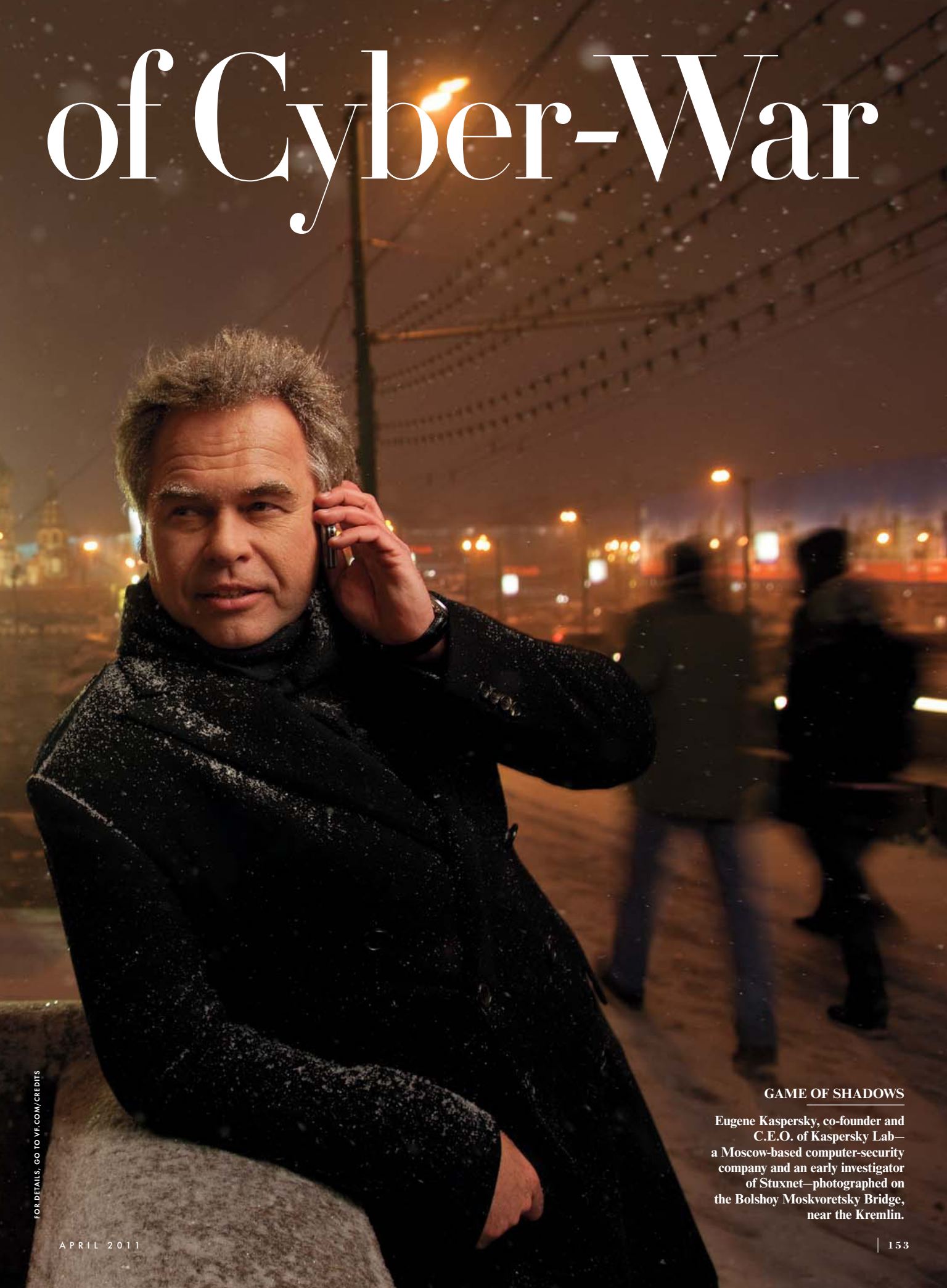
A Declaration

Last summer, the world's top software-security experts were panicked by the discovery of a drone-like computer virus, radically different from and far more sophisticated than any they'd seen. The race was on to figure out its payload, its purpose, and who was behind it. As the world now knows, the Stuxnet worm appears to have attacked Iran's nuclear program. And, as MICHAEL JOSEPH GROSS reports, while its source remains something of a mystery, Stuxnet is the new face of 21st-century war: invisible, anonymous, and devastating



PHOTOGRAPHS BY JONAS FREDWALL KARLSSON

# of Cyber-War



GAME OF SHADOWS

Eugene Kaspersky, co-founder and C.E.O. of Kaspersky Lab—a Moscow-based computer-security company and an early investigator of Stuxnet—photographed on the Bolshoy Moskvoretsky Bridge, near the Kremlin.

FOR DETAILS, GO TO VF.COM/CREDITS

"PERSON OF INTEREST"

Computer-security researcher Frank Rieger, one of the first to study the Stuxnet worm closely, at Berlin's Chaos computer Club. Stuxnet's code is diagrammed in the background.

IF THE FACTORIES SHUT

DOWN, IF THE POWER PLANTS WENT DARK, HOW LONG COULD SOCIAL ORDER BE MAINTAINED? WHO WOULD WRITE A PROGRAM THAT COULD POTENTIALLY DO SUCH THINGS?

All over Europe, smartphones rang in the middle of the night. Rolling over in bed, blinking open their eyes, civilians reached for the little devices and, in the moment of answering, were effectively drafted as soldiers. They shook themselves awake as they listened to hushed descriptions of a looming threat. Over the next few days and nights, in mid-July of last year, the ranks of these sudden draftees grew, as software analysts and experts in industrial-control systems gathered in makeshift war rooms in assorted NATO countries. Government officials at the highest levels monitored their work. They faced a crisis which did not yet have a name, but which seemed, at first, to have the potential to bring industrial society to a halt.

A self-replicating computer virus, called a worm, was making its way through thousands of computers around the world, searching for small gray plastic boxes called programmable-logic controllers—tiny computers about the size of a pack of crayons, which regulate the machinery in factories, power plants, and construction and engineering projects. These controllers, or P.L.C.'s, perform the critical scut work of modern life. They open and shut valves in water pipes, speed and slow the spinning of uranium centrifuges, mete out the dollop of cream in each Oreo cookie, and time the change of traffic lights from red to green.

Although controllers are ubiquitous, knowledge of them is so rare that many top government officials did not even know they existed until that week in July. Several major Western powers initially feared the worm might represent a generalized attack on all controllers. If the factories shut down, if the power plants went dark, how long could social order be maintained? Who would write a program that could potentially do such things? And why?

As long as the lights were still on, though, the geek squads stayed focused on trying to figure out exactly what this worm intended to do. They were joined by a small citizen militia of amateur and professional analysts scattered across several continents, after private mailing lists for experts on malicious software posted copies of the worm's voluminous, intricate code on the Web. In terms of functionality, this was the largest piece of malicious software that most researchers had ever seen, and orders of magnitude more complex in structure. (Malware's previous heavyweight champion, the Conficker worm, was only one-twentieth the size of this new threat.) During the next few months, a handful of determined people finally managed to decrypt almost all of the program, which a Microsoft researcher named "Stuxnet." On first glimpsing what they found there, they were scared as hell.

"Zero Day"

One month before that midnight summons—on June 17—Sergey Ulasen, the head of the Anti-Virus Kernel department of VirusBlokAda, a small information-technology security company in Minsk, Belarus, sat in his office reading an e-mail report: a client's computer in Iran just would not stop rebooting. Ulasen got a copy of the virus that was causing the problem and passed it along to a colleague, Oleg Kupreev, who put it into a "debugger"—a software program that examines the code of other programs, including viruses. The men realized that the virus was infecting Microsoft's Windows operating systems using a vulnerability that had never been detected before. A vulnerability that has not been detected before, and that a program's creator does not know exists, is called a "zero day." In the world of computer security, a Windows zero-day vulnerability signals that the author is a pro, and discovering one is a big event. Such flaws can be exploited for a variety of nefarious purposes, and they can sell on the black market for as much as $100,000.

The virus discovered by Ulasen was especially exotic, because it had a previously unknown way of spreading. Stick a flash drive with the virus into a laptop and it enters the machine surreptitiously,, uploading two files: a rootkit dropper (which lets the virus do whatever it wants on the computer—as one hacker explains, "'Root' means you're God") and an injector for a payload of malicious code that was so heavily encrypted as to be, to Ulasen, inscrutable. The most unsettling thing about the virus was that its components hid themselves as soon as they got into the host. To do this, the virus used a digital signature, an encrypted string of bits that legitimate software programs carry to show that they come in peace. Digital signatures are like passports for software: proof of identity for programs crossing the border between one machine and the next. Viruses sometimes use forged digital signatures to get access to computers, like teenagers using fake IDs to get into bars. Security consultants have for several years expected malware writers to make the leap from forged signatures to genuine, stolen ones. This was the first time it was known to have actually happened, and it was a doozy of a job. With a signature somehow obtained from Realtek, one

of the most trusted names in the business, the new virus Ulasen was looking at might as well have been carrying a cop's badge.

What was this thing after that its creators would go to such extravagant lengths? Ulasen couldn't figure that part out—what the payload was for. What he did understand was the basic injection system—how the virus propagated itself—which alone demanded an alert. Ulasen and Kupreev wrote up their findings, and on July 5, through a colleague in Germany they sent a warning to the Microsoft Security Response Center, in Redmond, Washington. Microsoft first acknowledged the vulnerability the next day. Ulasen also wrote to Realtek, in Taiwan, to let them know about the stolen digital signature. Finally, on July 12, Ulasen posted a report on the malware to a security message board. Within 48 hours, Frank Boldewin, an independent security analyst in Muenster, Germany, had decrypted almost all of the virus's payload and discovered what the target was: P.L.C.'s. Boldewin posted his findings to the same security message board, triggering the all-points bulletin among Western governments.

The next day, July 15, a tech reporter named Brian Krebs broke the news of the virus on his blog. The day after that, Microsoft, having analyzed the malware with the help of outside researchers, issued the first of several defenses against the virus. At this point it had been detected in only a few sites in Europe and the U.S. The largest number of infections by far—more than 15,000, and growing fast—was found in Asia, primarily in India, Indonesia, and, significantly, Iran.

In the process of being publicly revealed, the virus was given a name, using an anagram of letters found in two parts of its code.

"STUXNET" SOUNDED LIKE

SOMETHING OUT OF WILLIAM GIBSON OR FRANK HERBERT—IT SEETHED WITH DYSTOPIAN MENACE. MADISON AVENUE COULD HARDLY HAVE PICKED A BETTER NAME.

"Stuxnet" sounded like something out of William Gibson or Frank Herbert—it seethed with dystopian menace. Madison Avenue could hardly have picked a name more likely to ensure that the threat got attention and to take the image of a virus viral.

Yet someone, apparently, was trying to help Stuxnet dodge the bullet of publicity. On July 14, just as news of its existence was starting to spread, Stuxnet's operators gave it a new self-defense mechanism. Although Stuxnet's digital signature from Realtek had by now been revoked, a new version of Stuxnet appeared with a new digital signature from a different company, JMicron—just in time to help the worm continue to avoid detection, despite the next day's media onslaught. The following week, after computer-security analysts detected this new version, the second signature, too, was revoked. Stuxnet did not attempt to present a third signature. The virus would continue to replicate, though its presence became easier to detect.

On July 15, the day Stuxnet's existence became widely known, the Web sites of two of the world's top mailing lists for newsletters on industrial-control security fell victim to distributed-denial-of-service attacks—the oldest, crudest style of cyber-sabotage there is. One of the first known acts of cyber-warfare was a DDoS attack on Estonia, in 2007, when the whole country's Internet access was massively disrupted. The source of such attacks can never be identified with absolute certainty, but the overwhelming suspicion is that the culprit, in that instance, was Russia. It is not known who instigated the DDoS attacks on the industrial-control-security Web sites. Though one of the sites managed to weather the attack, the other was overloaded with requests for service from a botnet that knocked out its mail server, interrupting a main line of communication for power plants and factories wanting information on the new threat.

The secret of Stuxnet's existence may have been blown, but clearly someone—someone whose timing was either spectacularly lucky or remarkably well informed—was sparing no effort to fight back.

Omens of Doomsday

The volcanoes of Kamchatka were calling to Eugene Kaspersky. In the first week of July, the 45-year-old C.E.O. and co-founder of Kaspersky Lab, the world's fourth-largest computer-security company, had been in his Moscow office, counting the minutes until his Siberian vacation would start, when one of his engineers, who had just received a call about Stuxnet from Microsoft, came rushing in, barely coherent: "Eugene, you don't believe, something very frightening, frightening, frightening bad."

After VirusBlokAda found Stuxnet, and Microsoft announced its existence, Kaspersky Lab began researching the virus. Kaspersky shared its findings with Microsoft, and the two undertook an unusual collaboration to analyze the code. Symantec, ESET, and F-Secure also published extensive analyses of Stuxnet, and Symantec later joined Microsoft's formal collaboration with Kaspersky to study the worm.

Kaspersky is a 1987 graduate of the Soviet Institute of Cryptography, Telecommunications and Computer Science, which had been set up as a joint project of the K.G.B. and the Russian Ministry of Defense. He has beetling gray eyebrows and a flair for the dramatic. He drives a Ferrari, sponsors a Formula 1 racing team, and likes Jackie Chan movies so much that he hired Chan as a company spokesman. It would be an exaggeration to say that Stuxnet thrilled him, but he and many of his colleagues had been waiting for something like this to happen for years. Computer security, like many of the fixing professions, thrives on unacknowledged miserabilism. In omens of doomsday, its practitioners see dollar signs. As one of Kaspersky's top competitors told me, "In this business, fear is my friend."

To help lead his Stuxnet team, Kaspersky chose Roel Schouwenberg, a bright-eyed, ponytailed Dutch anti-virus researcher who, at 26, has known Kaspersky for almost a decade. (When he was in high school, Schouwenberg took it upon himself to troll the Web for viruses and, for fun, e-mail daily reports on them to the C.E.O. he had read about online.) Analysts at Kaspersky and Symantec quickly found that Stuxnet exploited not a single zero-

MAN VERSUS WORM

Industrial-control-systems-security expert Ralph Langner (at the Hamburg Airport) figured out the rudiments of what Stuxnet's payload did—and was the first to identify Iran as a possible target.

day flaw but in fact four of them, which was unprecedented—one of the great technical blockbusters in malware history.

As the zero days piled up, Kaspersky says, he suspected that a government had written Stuxnet, because it would be so difficult and time-consuming for an outsider to find all these flaws without access to the Windows source code. Then Kaspersky lowers his voice, chuckles, and says, "We are coming to the very dangerous zone. The next step, if we are speaking in this way, if we are discussing this in this way, the next step is that there were a call from Washington to Seattle to help with the source code."

To Schouwenberg and many others, Stuxnet appears to be the product of a more sophisticated and expensive development process than any other piece of malware that has become publicly known. A Symantec strategist estimated that as many as 30 different people helped write it. Programmers' coding styles are as distinctive as writers' prose styles. The worm's development reportedly took some 10,000 man-days. Once Stuxnet was released into the wild, other technicians would have maintained the command-and-control servers in Denmark and Malaysia to which Stuxnet phoned home to report its current locations and seek updates.

Most curious, there were two major variants of the worm. The earliest versions of it, which appear to have been released in the summer of 2009, were extremely sophisticated in some ways but fairly primitive in others, compared with the newer version, which seems to have first circulated in March 2010. A third variant, containing minor improvements, appeared in April. In Schouwenberg's view, this may mean that the authors thought Stuxnet wasn't moving fast enough, or had not hit its target, so they created a more aggressive delivery mechanism. The authors, he thinks, weighed the risk of discovery against the risk of a mission failure and chose the former.

There seemed no end to the odd surprises that Stuxnet had to offer. In a July 15 posting, Alexander Gostev, who wrote Kaspersky Lab's blog on the worm, mysteriously quoted from a botanical entry in Wikipedia: "Myrtus (myrtle) is a genus of one or two species of flowering plants in the family Myrtaceae."

"Why the sudden foray into botany?," Gostev asked. His answer: "Because the rootkit driver code contains the following string: b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb." Gostev went on to raise the specter of a "Project 'Myrtus'" and added portentously: "To be continued?" Although Gostev never returned to his musings on Stuxnet's botanical allusion, he had planted a seed that would very quickly sprout.

At the end of July, just before Eugene Kaspersky came home from the volcanoes, Schouwenberg started trying to persuade a writer from *The New York Times* to cover Stuxnet. Without specific information on the source or the target, though, the topic was a nonstarter. Then, on September 16, an industrial-control-systems-security expert in Hamburg made a sensational blog posting about Stuxnet, whose deployment he would soon dub "operation myrtus." And he was pretty sure he knew what the myrtle reference signified. The man had never been quoted in a newspaper before, but he was about to shift the global conversation about Stuxnet in a radically new direction.

Self-Directed Stealth Drone

"Am I crazy, or am I a genius?" The question would not leave Ralph Langner alone. He was having trouble sleeping. Sometimes he thought the C.I.A. was watching him. Langner, a voluble man of 52, is built like a whippet, with short hair neatly parted to the side. His Hamburg-based company is a big name in the small world of industrial--control-systems security, and counts some of Germany's largest automotive and chemical corporations among its clients. Langner had been reverse engineering the payload of Stuxnet throughout August, and he was the first analyst to announce that it contained two components that he called "warheads." Langner had come to believe that Stuxnet was aimed at Iran's nuclear program. Iran has been suspected of trying to build a nuclear bomb for several years, and in 2003 it failed to disclose details regarding uranium-enrichment centrifuges to inspectors from the International Atomic Energy Agency. Western governments have been trying to stop Iran's nuclear program ever since, using diplomatic pressure, trade embargoes, and covert operations.

Stuxnet had initially grabbed the tech world's attention as a hack of the Windows operating system—a virus that exploited an unknown vulnerability. This was like learning that someone had found his way into your house, and figuring out how they got inside. Next, Frank Boldewin had discovered what valuables the intruder was after—programmable-logic controllers. Specifically, the target was P.L.C.'s made by the German engineering conglomerate Siemens. Finally, Langner figured out the rudiments of what Stuxnet's payload did—that is, how the intruder went about his work. When Stuxnet moves into a computer, it attemps to spread to every machine on that computer's network and to find out whether any are running Siemens software. If the answer is no, Stuxnet becomes a useless, inert feature on the network. If the answer is yes, the worm checks to see whether the machine is connected to a P.L.C. or waits until it is. Then it fingerprints the P.L.C. and the physical components connected to the controller, looking for a particular kind of machinery. If Stuxnet finds the piece of machinery it is looking for, it checks to see if that component is operating under certain conditions. If it is, Stuxnet injects its own rogue code into the controller, to change the way the machinery works. And even as it sabotages its target system, it fools the machine's digital safety system into reading as if everything is normal.

Industrial-control systems have been sabotaged before. But never have they been remotely programmed to be physically altered without someone's fingers on a keyboard somewhere, pulling the

IN TERMS OF SHEER SIZE, THIS WAS THE LARGEST PIECE OF MALICIOUS SOFTWARE THAT MOST RESEARCHERS HAD EVER SEEN, AND ORDERS OF MAGNITUDE MORE COMPLEX IN STRUCTURE.

virtual trigger. Stuxnet is like a self-directed stealth drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done. This is revolutionary. Langner's technical analysis of the payload would elicit widespread admiration from his peers. Yet he also found himself inexorably drawn to speculation about the source of the malware, leading him to build a detailed theory about who had created it and where it was aimed.

Near the start of September, Langner Googled "Myrtus" and "Hebrew" and saw a reference to the book of Esther, a biblical story in which Jews foil a Persian plot against them. He then Googled "Iran" and "nuclear," looking for signs of trouble, and discovered that the Bushehr power plant had been experiencing mysterious construction delays. (Although Bushehr is only a power plant, its nuclear reactor could produce plutonium in low-enriched uranium fuel that could be re-purposed for weapons.) Next, Langner sent an e-mail about Stuxnet to his friend Joe Weiss, who organizes the top industrial-control-systems cybersecurity conference in the U.S. (and wrote the standard book on the topic, *Protecting Industrial Control Systems from Electronic Threats*). Langner would later post that e-mail to his blog: "Ask your friends in the government and in the intelligence community what they know about the reasons why Bushehr didn't go operational last month. BTW, did somebody from Israel register to attend the conference? :)" Eventually, Langner decided to just put it out there. He would post his theory that Stuxnet was the first literal cyber-weapon, and that it had been aimed by Israel at Bushehr, and see what happened.

Plenty happened. *The Christian Science Monitor* published a report on Langner's theory on September 21. The next day, a German newspaper published an article by another German computer expert, Frank Rieger, claiming that, in fact, the cyber-weapon had been aimed not at Bushehr but at Iran's Natanz uranium-enrichment facility. The Iran speculation pinged across the Web. Two days later, Riva Richmond posted a version of Langner's theory on the *Times*'s technology blog, Gadgetwise. The *Times*'s David E. Sanger then took the ball and ran with it, suggesting that Stuxnet may have been part of a covert U.S. intelligence operation to sabotage Iran's nuclear program that had started under President George W. Bush and had been accelerated after Barack Obama took office. One Iranian-government official reportedly admitted that the worm had been found in government systems, but another official claimed that the damage was "not serious." Then the Iranian government announced that it had arrested "nuclear spies," possibly in connection with the Stuxnet episode, according to the *Times*. Rumors swirled online that the accused spies had been executed.

"If I did not have the background that I had, I don't think I would have had the guts to say what I said about Stuxnet," Langner says now, finishing his second glass of wine during lunch at a Viennese restaurant in Hamburg. Langner studied psychology and artificial intelligence at the Free University of Berlin. He fell into control systems by accident and found that he loved the fiendishly painstaking work. Every control system is like a bespoke suit made from one-of-a-kind custom fabric—tailored precisely for the conditions of that industrial installation and no other. In a profession whose members have a reputation for being unable to wear matching socks, Langner is a bona fide dandy. "My preference is for Dolce & Gabbana shoes," he says. "Did you notice, yesterday I wore ostrich?" Langner loves the attention that his theories have gotten. He is waiting, he says, for "an American chick," preferably a blonde, and preferably from California, to notice his blog and ask him out.

Last fall Langner and I spent two days CONTINUED ON PAGE 195

STYLED BY CHRISTINE HAHN; HAIR BY SHAWN MOUNT; MAKEUP BY DEANNA MELLUSO; SET DESIGN BY WADE & STRAUSS; FOR DETAILS, GO TO VF.COM/CREDITS