_THE_DIGITAL_DETECTIVE

The war against computer malware is escalating – and Mikko Hypponen is on the front line. Meet the man who tracks down thousands of virus files every hour in his mission to tame a criminal industry worth an estimated $338 billion a year

_WORDS BY GREG WILLIAMS

_ PHOTOGRAPHY: AORTA

_01_caption1: mikko hypponen at f.secure's hq

F-5E C9 CS 55
J-GE C9 HS 73
3 FE FF-74 13 6A 02-57 56 FF 15-A4 10 00 01

_01002190:

One morning in December 2011 Mikko Hypponen, the chief security research officer at F-Secure, an anti-virus software company, scrolls down the screen of his laptop examining the latest of the 200,000 malware files to arrive in his office every day in Helsinki. As he does so, the data shifts downwards, the most recent files at the top. "This sample, PA3control.exe, arrived eight minutes ago," he says. "It's infected with a virus we're aware of, which means we don't have to do anything. We already know what it is."

Hypponen is typing hard in short bursts. He is dressed in black except for a mustard-coloured shirt. His hair is pulled into a blond ponytail and he wears small, round spectacles. "Let's look at this file deeper," Hypponen says, clicking on another data point. "So what do we know? First of all, it's very small. It's two kilobytes, which is suspicious. We look at the file type... It's a Windows executable." An executable is a file in a format that the computer can accomplish itself, intended not to be read by humans. "When did we get it? Where did we get it? What's the file hash? [A hash is an encrypted number generated from a string of text used in security networks.] How many times have we received it? What do we know about its structure? How many of our users have executed this file in the past week, or ever?"

Hypponen pulls up another window. "What I'm looking at is the report for this file," he says. "It takes two or three minutes to generate, but I'm thinking that this file might not do anything interesting because it's too small. What is more likely is that it's corrupted. It looks suspicious because the header, the part of an executable that reveals what's in the file, is missing, so it doesn't look right. It's likely that it will just crash."

Hypponen is right: when the file is executed, it doesn't even run. He looks down the list of data points before him. Some are in red, meaning that they haven't been analysed yet. Further down the screen, the digits turn green: they have been processed.

As at every security company across the world, the Malware Sample Management System (MSMS) at F-Secure demonstrates a steady, and growing, onslaught of toxic binary fizzing through the internet, looking for vulnerabilities. Today, criminals are producing malware on an industrial scale. Security company McAfee identified six million unique malware samples in the second quarter of 2011 alone. And each sample means countless files containing the original virus loose online. Malware – Trojans, worms, spyware, backdoors, fake antivirus software, rootkits and others – is developed and sold to third parties, who will alter the source code for their own illegal purposes.

Hypponen checks another data point: his team claim to have logged 46,655 unique pieces of malware in just the past 24 hours.

_01002120: 49 2M G3 GG-

Eleven months earlier, late in January 2011, Hypponen had found himself wandering down a dusty street in Lahore, the second-largest city in Pakistan. Hypponen, 42, is often on the road talking to government agencies and the companies he helps to protect – including AT&T, Vodafone and Orange – but this was his first trip to Pakistan. On a side street sandwiched between the University of the Punjab and a park, he stepped from the sunshine into a boxy, concrete building with large metal doors and air-conditioning units poking from the walls. He found himself in the offices of Brain, a telecommunications company owned, in part, by two brothers, Amjad and Basit Farooq Alvi.

Hypponen's journey was prompted by events that had occurred nearly a quarter of a century before, when, in late 1986, some users of IBM PCs and compatibles running PC-DOS or IBM-DOS operating systems inserted floppy disks containing software into their machines and received the following message on their screens:

```
Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN PHONE :430791,443248
```

0 0 0

What those PC users could not have known was that they were among the first to experience something that, according to security firm Symantec, now forms a significant part of the $338 billion (£213bn) a year cost to the global economy. Their computers were infected with a virus.

For Hypponen, the trip was a pilgrimage. Having spent most of his life combating malware, he had come to meet the two men credited with creating its patient zero.

The Alvi brothers, Basit and Amjad, don't look like archetypical hackers – they're middle-aged men in suits with combed hair and moustaches who run a successful teleco business; among other things, they have a licence to lay fibre-optic cable. And, unlike malware peddlars – whom the security industry categorises as hacktivists, nation states and (by far the largest) criminal gangs – they weren't trying to harm those they infected.

In 1984 the brothers were discussing the vulnerability of DOS. They created a piece of software which altered the instructions that a computer executes on startup when a disk is inserted, replicating the same message on every disk it infected. It was harmless, and the purpose, the brothers say, was to protect their own software from piracy. Modern malware is largely distributed on the internet but, in the mid 80s, the only way for a virus to travel was to be installed on a disk and inserted in a drive. The brothers left their phone number so that legitimate users could be debugged. They wanted to understand how the virus might spread – and were staggered when the first call they got was from Miami University.

"I'm not sure how it went out all [that] way," Amjad says. "I was worried that I will be in trouble. I contacted my lawyer and froze the first piece of code, so if someone modified it, it should not be blamed on me."

Hypponen handed the brothers a floppy disk. It was a copy of the original virus, one of millions of malware samples that he keeps in his laboratory. He says his trip to Lahore was inspired by a fascination with malware, and he wanted to bring the virus home.

In the nearly 20 years since he started disassembling malware, Hypponen has become a prominent face in the anti-virus industry. He took down the network used by the Sobig.F worm in May 2003, and was the first to warn of the Sasser worm a year later. In 2007, he named the Storm botnet. The F-Secure blog, which was started on January 30, 2004 – when Hypponen posted an entry on the Mydoom worm – is one of the most widely read in the business. In 2010, Hypponen gave briefings on what has become the world's most devastating worm, Conficker. He has consulted for law-enforcement organisations in Europe, Asia and the US, and spoken at NATO's Cooperative Cyber Defence Centre of Excellence. He was among *Foreign Policy*'s 100 Top Global Thinkers of 2011. In 2007 *PC World* named him one of the 50 most important people on the web.

Hypponen points out that only ten years ago the enemy was mostly mischievous teenagers. That changed on May 8, 2003, with Fizzer – the first virus designed solely to make money. Fizzer was a worm. A virus needs human action to infect a computer – clicking an attachment, say – but a worm spreads itself and seeks to avoid detection. It sent itself to all the contacts in the computer's Windows Address Book. This allowed the attacker to steal passwords and other data. When attacked by antivirus programs it tried to terminate them.

Hypponen first noticed Fizzer on an intentionally infected test system that experienced a spike in email traffic. "Instead of stealing information, [the criminals] stole the *resource*," he says. This marked the creation of botnets – groups of infected computers that can be controlled remotely.

Suddenly, PCs across the world were in the hands of crooks. "Conficker has more processing power than any university," says Hypponen. "Criminals own the largest supercomputer on the planet."

01 caption2: Hypponen's collection of early disc-based viruses

01_caption3: Amjad and Basit Alvi discuss their Brain virus with Hypponen

2X-8D D1 2X 56
3U-PE D3 MS 53

iPad extra!
Download the WIRED app to see Hypponen with the Alvi brothers

Hypponen's days are spent foiling these gangs (he refers to them "clowns"). It's 10am in Helsinki and Hypponen is sitting in F-Secure's headquarters in the Jätkäsaari neighbourhood. One floor up from the atrium, through two sets of glass security doors, is the lab where he and his team (there are around 500 people working in R&D) spend their days. It's calm and orderly, perhaps stereotypically Scandinavian, although the team includes Filipinos, Russians, Indians, Americans and Finns. There are F-Secure offices in 20 other cities.

In the middle of the floor there's a conference table in front of three screens. Around it offices house the response unit, which handles malware samples, and the specialist teams dealing with firewalls, spam, parental control, development and admin. In the radio-frequency lab, where mobile devices are analysed, there are dozens of active phones lying on tables next to a Faraday cage which allows the researchers to work with viruses without their leaking to other devices. On another table there's a plastic box containing 3½-inch floppy disks of malware from 1992 and 1993.

Nowadays much of what AV companies do is mechanised: complex algorithms sift through the millions of files of malware pushed online every day and block them. Before 2007, each was examined by hand, analysts combing through the thousands of lines of code that make up a typical file. "Today only 'special cases' are hand-examined," Hypponen says.

He sits at his laptop punching in code, hitting the return key hard. To ensure a secure network, researchers in the lab are not allowed to use a direct connection from their computers to access systems that handle viruses. So Hypponen is looking at the screen of another computer – more accurately, not a physical computer, but a virtual machine – at one of F-Secure's data centres. He scans the MSMS for anything unusual.

When malware samples are processed they are cast into a "sandnet" – a network of virtual computers – to see what would happen should a user open the file. In most cases it's easy to tell what the virus might do and where it is similar to other pieces of malware. It's like a digital Petri dish. "It scans the network to find more computers to infect those as well," Hypponen says. "It tries going online, it tries denial-of-servicing Microsoft.com. It will continue running because it believes that it's online."

When the analysts are looking at a new virus, they reverse engineer the executable. Malicious programmers tend to code in Lua, a simple programming language. "It's an almost human language to program with," says Sean Sullivan, security adviser at F-Secure. "It does everything for them." Analysts work in something far more complex: they decompile the high-level language and work in what are known as low-level programming languages, which are, effectively, the instructions imparted by the computer's central programming unit.

Virus samples come from many sources. "We run our own honeynets and we co-operate with large honeynet operators around the world, so we get sample feeds in real-time constantly," Hypponen says. Other sources are F-Secure's operator partners – "because they see all the traffic in their network" – and VirusTotal, an online platform that scans uploaded malware. They also share samples with the other major players, such as Symantec, McAfee and Sophos.

He's investigating a server hosting a Trojan – malware that attaches itself to a legitimate piece of software but has a covert purpose, such as data theft. He looks up, smiling: "Let's see where this goes, because it's fresh it's highly likely this site is still up and running... Yep, it's up and running... That's where the attackers are right now. And most likely if they run any kind of HIPS [host intrusion prevention system, basically monitoring software] they just saw a ping come in from F-Secure.com and they were like 'Oh, shit!'" He punches in more data. "Buenos Aries," he says seconds later.

Thirteen thousand kilometres away, someone in Argentina will soon have his server shut down.

Malware is now produced on a vast scale. Programmers create toolkits – adapting malicious code – that are marketed to spammers and other online nuisances. A Trojan named Zeus, which targets banks and is being marketed by Russian criminal gangs, is available for sale for around £500. In 2009 it was found to have compromised, among others, Nasa, Bank of America and Cisco.

"Cybercrime is constantly evolving and becoming more mainstream," says DCI Terry Wilson of Scotland Yard's e-Crime Unit. The easier cyber becomes, the more criminals will be drawn to the low-risk, high-yield benefits. One of the reasons online crime is growing rapidly is because it's very cheap to run. Sullivan says a spammer only needs a 0.0001 per cent response rate to be in profit. According to Norton, in the 24 countries it surveyed for its Cybercrime Report 2011, 431 million adults had experienced cybercrime, it claims. Another recent report, from the Cabinet Office, estimated the annual cost of cybercrime in the UK to be £27 billion.

Law enforcement is rarely coordinated and legislation often outdated. In Brazil, electronic fraud losses in the first six months of 2011 totalled $460m – a 36 per cent rise on the same period the previous year. Yet the laws governing cybercrime date from the 1950s. The internet, designed by academics and the military for communication and research, has spread in an unplanned, ad hoc manner, meaning that the network is not only vast and complex, but also that large parts of it are woefully outmoded.

"Most of the protocols, most of the design, most of the parties who have put up servers and services haven't really given much thought to security or privacy," says Professor Eugene Spafford, of the

Hypponen on who's at risk:

'The total amount of Apple computer malware is still very small, a fraction of one per cent, meaning a few hundred Mac OSX Trojans/backdoors compared to tens of millions for Windows malware. We see more mobile-phone malware than Mac malware, so you're more likely to get hit on your Android device. But they do exist and the numbers are growing'

department of computer sciences at Purdue University, Indiana, and the editor of *Computers & Security*. "Far too much has been built without appropriate protections, and the amount of attention paid to fixing things hasn't been large. We know how to fix things but it would be very expensive and we don't want to pay."

And buying a botnet is relatively cheap and simple. To demonstrate, Hypponen logs into message boards used by criminals using Tor, the anonymising protocol. The screen is black with green text, making it look like a DOS file on an Amstrad 8256.

"This guy is selling UK and European dumps [the personal information contained on the magnetic strip of a credit card]," Hypponen says, scrolling down the page and reading the small ads. "Here are 'Bank accounts from Asia, EU... high valid rate', and 'Bank accounts from the UK, Germany, Russia all obtained with SpyEye'." He reaches an advertisement for a botnet: "Here we are: 'Denial of service: standard host or domain taken down one hundred bucks per day. Payment: Western Union, MoneyGram, Bitcoin."

According to Hypponen, the cost of a botnet depends on the territory – North American and European computers are most valuable; at the other end of the spectrum are the Russian and Chinese. He continues reading the list, pausing at an advert for an available hired assassin. "Former French Foreign Legion. No fish too big no job too small". Potential clients are advised that the cost of the service is $20,000, to be paid in Bitcoin, and that they will be billed for travel expenses.

In the past decade, cybercrime has merged into a wider criminal ecosystem. Sullivan draws a parallel with the drugs trade. "It's like the difference between a meth dealer who's a self-starting entrepreneur in his garage versus the cocaine drug lord of Colombia," he says. "The organised criminal ecosystem is using information technology just like the legitimate business community."

And catching the bad guys is difficult, given the anonymity of the web and the number of jurisdictions that online crime crosses. The day before, Hypponen had been contacted by an individual worried about his account at a large Scandinavian bank. The man sent Hypponen a screenshot of a "please wait" holding message that had suddenly appeared after he had logged into his account. Hypponen detected that he had been the victim of a modified version of Zeus. The digital trail of IP addresses and servers shifted from Finland to India, Russia, Lithuania and Holland.

"The real guy to catch would be the guys developing Zeus and taking them offline," Hypponen says. "But it's too late – the source code was released around half a year ago. They were clever. I don't think they ever stole money, they just wrote a tool."

Others are relatively easy to detect because of their youth: thinking that it's possible to maintain a separate online identity from that of their illegal activities and continue to post on forums and social-networking sites. "You only have to make one mistake – and that's over the duration of your online life," Hypponen says. "If you screw up, in many cases you can be found."

In one unusual instance, a gang member got so angry with one of Hypponen's blog posts about his organisation that he sent an email of complaint from a fake email address. With some detective work, Hypponen found a link to a post the criminal had made on a Nintendo forum: at the bottom of the page he had listed his real email address.

"But this guy has gold-plated his Nintendo system," says Hypponen, who collects vintage arcade games. "It's the coolest thing I've ever seen."

_01_caption4: handsets kept virus-free

For security reasons, Hypponen prefers not to talk about his private life. "We are not so far from St Petersburg," he explains. Growing up in Helsinki, he was introduced to computing by his mother, who worked at the state computing centre from 1969 until her retirement. "That's the reason we had a computer very early, around 1982," he says. The device was a Commodore 64. He started programming straight away and sold his first software at 16. "I was selling routines [pieces of code within a program that perform a specific task] to a software company, to do stuff like speed up downloading, or graphics. And I was selling text-based adventure games in Finnish."

He graduated from Helsinki's Institute of Information Technology, and began studies in computer science at the University of Helsinki. At the same time he started working part-time at a company called Data Fellows, which was founded in 1988 by entrepreneurs Risto Siilasmaa and Petri Allas, to construct databases. (The company was renamed F-Secure in 1999 because, according to Hypponen, "it just sounds cool".) Allas left the company when it went public that year, but Siilasmaa remains chairman and is F-Secure's biggest shareholder. As well as being a prolific angel investor in Finnish startups, he has been nominated to take over as chairman of the board of directors at Nokia in May.

Hypponen joined full-time in 1991 as employee number six. "One of the fields we were working on was data-security consulting. People would ask for recommendations for an antivirus product, and we didn't really have a good product to recommend. We realised there was an opening." So he became a virus researcher. He was the only person in the company with an assembly-language background ("you can't be an antivirus researcher without that," he says). His first analysis was conducted on September 13, 1991. There was very little precedent for what he was doing, so he read through manuals, printed out the assembly code of the binary and went through it line by line. After a few hours he mastered how the virus replicated. His next discovery was that the malware would print out the omega character every Friday 13th. He was hooked. "I analysed the first samples and we realised that I shouldn't be doing anything else," he says.

_01_caption5: the ray-proof testing lab

_04_2012

Hypponen on who's in control:

'Conficker is still the biggest supercomputer on the planet – it has more processing power than any university. Criminals own the largest supercomputer on the planet'

Contemporary malware is rarely so benign. Eugene Spafford is convinced that we need clearer international protocols as, with more than two-thirds of the world still to come online, the problem will grow. "There is a parallel to what is happening in Mexico," he says. "For many years the people running drugs bribed the local officials and had a tacit understanding that they would not commit crimes in Mexico. But now they feel so powerful that they still pay bribes but they're committing crimes in the country. They're well financed and they're a threat to the government. The danger is that anyone making enough money is going to expand and include other kinds of activities."

"We have to do this better," Hypponen says. "Nobody's getting caught and even if they are the sentences aren't much. I don't want to promote limiting the freedom of the net. I'm not talking about starting global police forces to hunt torrent feeders or hate speech. But nobody wants these Russian crime gangs around. We should focus international cooperation on catching them."

In the 25 years since Brain plodded around the globe, the AV industry has grown significantly. A 2011 report by research company Gartner estimated that the global market grew 12 per cent in 2010 to $16.5 billion. Symantec, which had 18.9 per cent of the market in 2010, has a market capitalisation of $12.38 billion.

But, according to Professor Stefan Savage, from the computer science department at the University of California, San Diego, the scale of risk is questionable. "In the security community there is a willingness to take one data point and extrapolate," he says. "There's not a countervailing interest to argue that the numbers are less than they are. So we end up with this escalating series of claims about the cost of cybercrime. It started about five years ago when we had someone in the US government saying online crime generates more revenue than drugs. And then the number just gets bigger until Ed Amoroso from AT&T estimated that it was $1 trillion, and the Obama administration repeated it. It's is kind of laughable, because that's more than a third of the GDP of Germany." Savage conducted his study to get an idea of the revenue generated by pharmaceutical spammers. "Based on the numbers we have, which are from the biggest outfits, it would be surprising if the total revenue there was much more than $100 million," he says.

The industry, of course, points to the destruction caused by malware, the armies of botnets that remain under criminal control and the national security threats posed by rogue states which are constantly prodding for weaknesses in each others' critical infrastructure. Driving around Helsinki, Hypponen describes the spirit of co-operation that exists among the analysts in the antivirus industry.

"People rarely leave this industry," he says. "Everyone knows everyone else. We share. We're different. Generally in the IT industry the enemy is your competitor. In security, it's the bad guys." W

Greg Williams is executive editor of WIRED. *He blogs at howwecreatevalue.com*