

Talking Computer Security with Mikko Hypponen of F-Secure

Mikko Hypponen is the Director of Anti-Virus Research at F-Secure Corp. of Helsinki, Finland. Hypponen and his dedicated research team have been dubbed “Mikko Hypponen and his band of Finnish computer virus hunters” by *BusinessWeek*, “Sleuths” by the *New York Times*, and “the Code Warriors” by *Vanity Fair*.

Their reputation has been growing for years. F-Secure’s research team, headed by Hypponen, cracked the SoBig F virus while working in conjunction with the FBI. Since then, Hypponen’s partnership with the FBI and other law-enforcement agencies has continued as they work to track and prevent new threats. The team was the first to locate, analyze and build protection against the LoveLetter virus, the largest virus incident in the world. In April 2000, they also tracked down the guy who broke the Kournikova ring.

For the past 13 years, Hypponen has worked as the No. 2 guy at F-Secure, the international data security company. Well-versed on all security breaches and the criminals behind them, he is the go-to person for Cyber Security special agents, NATO and the Finnish Army, among others.

CyberDefense Magazine (CDM) sat down with Hypponen to discuss several computer security issues.

CDM: With the proliferation of viruses and worms, is there evidence to show that organized Internet crime gangs have formed and are writing viruses for

financial gain?

Hypponen: We have concrete evidence showing that some virus groups are writing viruses just to make money. Machines are being taken over with email worms and then they are used for malicious purposes benefiting the virus group. Often such overtaken machines are resold for the day’s rate.

So yes, it’s organized. And yes, it’s criminal. So it’s organized crime. That doesn’t still mean this would be the work of traditional mafia or real-world crime gangs ... it still mostly seems to be done by teenagers. But the big profits go to the ones benefiting from the spamming, they’re the ones that we really should be after.

CDM: What are the chances of catching them?

Hypponen: This year has been really good for catching virus writers. But all the arrests have been kids and small-time players; none of the professional virus writers have been caught. It’s important to catch these people because it discourages others from following in their footsteps. But in order to really put a dent in the virus writing business, we have to go after the organizations that are making money off their viruses.

CDM: Are they doing this for profit?

Hypponen: It seems like they are. Looking at some of the latest operations, the target is to create a very large network of interconnected computers and either turn them into spam proxies,

free hosting servers or parts of DDoS attack networks. Such machines are also often targets of data theft, including information like credit card numbers, passwords and bank accounts. By far the largest benefit is spamming; most spam today is being sent from infected DSL- or cable-enabled home computers.

There are layers. You don’t just have the virus writer scripting a virus and then using the computers to send spam. You have one group writing the viruses. Once they create a list of infected IP addresses, they might sell those on underground bulletin boards, many of which are run in Russia or China. That probably gets resold a couple of times before a spammer picks it up and starts using it. It really gets hard to trace the route backwards. Virus writers today definitely have found ways to capitalize on their abilities.

CDM: What do you think of Microsoft and others offering bounties to catch virus writers?

Hypponen: I think it’s great that Microsoft is offering bounties. What’s most important is that they put pressure on virus writers so they become afraid of others ratting them out. Obviously Microsoft can afford to put up the bounties, though it hasn’t had to pay anything yet.

CDM: Who is winning this battle?

Hypponen: The virus writers always have the upper hand because they have access to antivirus products. They can

download the latest antivirus, test-drive it against their virus and then modify the virus until it's undetectable. Why would they release a new virus that could be detected by McAfee or Symantec?

There is no easy answer to this problem. Of course, if you want to protect a computer you have the three basic rules, which are: running anti-virus, running a firewall and patching. Or, of course, you could just get rid of Windows and get Linux and forget all sorts of problems. Much of the problem is that home computer users are infecting corporate networks by accident.

CDM: It sounds like viruses hitting mobile devices could be the next big headache. How big an issue is this?

Hypponen: Such viruses really haven't appeared until this summer, with Cabir, the first proof-of-concept virus to hit Symbian-based Bluetooth phones. It's really interesting because it is the first virus that spreads based on proximity – if you are close to other Bluetooth devices you can spread the virus. Imagine someone with an infected phone getting on a crowded subway and transmitting the virus to hundreds of other phones. A couple of weeks ago, we found a proof-of-concept PocketPC virus (Duts) and the first backdoor for PocketPC devices (Brador).

PocketPC is a very open platform and it's very easy for developers to get their hands on code and port any desktop Windows software to PocketPC. The



fear is that such viruses eventually could be used to make phone calls, send text messages, delete phone numbers or even eavesdrop on your calls. Earlier this spring, we found a game for Symbian phones that was secretly sending messages to expensive toll numbers, creating invisible costs for the user.

The ease of infection makes this a very big and real problem. Mobile devices are more common, and as they become more widespread, they become a more attractive target for virus writers – which is important to keep in mind. The bigger the target, the better it looks to these people.

CDM: What's your overall take on the virus situation today?

Hypponen: It's been getting worse and worse. I entered the business in 1991. Looking back now, things were easy then. Almost all infected computers

were caused by boot viruses that were physically carried and spreading viruses ... so it would take a year for them to get around the world. Now with network worms like Slammer, Sasser and Blaster, viruses hit computers and networks all over the world in a matter of minutes. We can't react that fast, no matter how fast we are.

Of the 100,000 viruses seen over the last 18 years, we've cracked every single one. But it's not a given that will continue to be the case. We might very well see a virus some day that we can't crack.

CDM: What is the likelihood of an attack on major infrastructure or transportation such as planes and trains?

Hypponen: We've seen serious and successful attacks on transportation, trains, hospitals, nuclear power plants, airports, coast guards etc. But these have not been targeted attacks. The virus writer didn't try to stop planes and

Now with network worms like Slammer, Sasser and Blaster, viruses hit computers and networks all over the world in a matter of minutes. We can't react that fast, no matter how fast we are.

trains; it was just a side effect. Now, if somebody tried doing something like this on purpose, it actually isn't that simple.

Yes, the terrorists are using the Internet all the time. But they're mostly using it for spreading their propaganda via their websites or for communication. Doing directed attacks is possible,

and we know of several nightmare scenarios on what could happen ... but we believe groups like Al-Qaeda do not have the needed know-how in-house, and nowadays it's hard for Al-Qaeda to outsource things like this to "normal" hackers.

So I'd actually be much more worried about more realistic threats, such as

organized attacks from anarchists and activists. And of these, we already have real-world examples.

CDM: Is it possible we will ever witness the electronic equivalent of 9/11?

Hypponen: Ever? We might. In the next few years? No, I don't think so. **CDM**

