19 Key Essays on
**How Internet is
Changing our Lives**

CH@NGE

19 Key Essays on
How Internet Is Changing Our Lives

CH@NGE

Mikko Hypponen

Cyber Attacks

OpenMind
BBVA
bbvaopenmind.com

Mikko Hypponen
mikko.hypponen.com

Illustration
Pieter van Eenoge

Mikko Hypponen is the Chief Research Officer of F-Secure in Finland. He has been working with computer security for over 20 years and has fought the biggest virus outbreaks in the net, including LoveLetter, Conficker, and Stuxnet. His TED Talk on computer security has been seen by almost a million people and has been translated into over 35 languages. His columns have been published in the *New York Times*, *Wired*, CNN, and the BBC. Mr. Hypponen was selected among the 50 most important people on the web by *PC World* magazine. *Foreign Policy* magazine included him on the list of “Top 100 Global Thinkers.” Mr. Hypponen sits on the advisory boards of the ISF and the Lifeboat Foundation.

Sites and services that have changed my life

reddit.com
hxkcd.com
news.ycombinator.com

Cyber Attacks

Preface

The real world isn't like the online world.

In the real world, you only have to worry about the criminals who live in your city. But in the online world, you have to worry about criminals who could be on the other side of the planet. Online crime is always international because the Internet has no borders.

Today computer viruses and other malicious software are no longer written by hobbyist hackers seeking fame and glory among their peers. Most of them are written by professional criminals who are making millions with their attacks. These criminals want access to your computer, your PayPal passwords, and your credit card numbers.

I spend a big part of my life on the road, and I've visited many of the locations that are considered to be hotspots of online criminal activity. I've been to Moscow, São Paulo, Tartu, Vilnius, St. Petersburg, Beijing, and Bucharest.

I've met the underground and I've met the cops. And I've learned that things are never as simple as they seem from the surface. One would think that the epicenter for banking attacks, for example, would prioritize fighting them, right?

Right, but dig deeper and complications emerge. A good example is a discussion I had with a cybercrime investigator in Brazil. We spoke about the problems in Brazil and how São Paulo has become one of the largest sources of banking trojans in the world.

The investigator looked at me and said, "Yes. I understand that. But what you need to understand is that São Paulo is also one of the murder capitals of the world. People are regularly gunned down on the streets. So where exactly should we put our resources? To fight cybercrime? Or to fight crimes where people die?"

It's all a matter of balancing. When you balance the damage done by cybercrime and compare it to a loss of life, it's pretty obvious what's more important.

National police forces and legal systems are finding it extremely difficult to keep up with the rapid growth of online crime. They have limited resources and expertise to investigate online criminal activity. The victims, police, prosecutors, and judges rarely uncover the full scope of the crimes that often take place across international boundaries. Action against the criminals is too slow, the arrests are few and far between, and too often the penalties are very light, especially compared with those attached to real-world crimes.

Because of the low prioritization for prosecuting cybercriminals and the delays in launching effective cybercrime penalties, we are thereby sending the wrong message to the criminals and that's why online crime is growing so fast. Right now would-be online criminals can see that the likelihood of their getting caught and punished is vanishingly small, yet the profits are great.

The reality for those in positions like the São Paulo investigator is that they must balance both fiscal constraints and resource limitations. They simply cannot, organizationally, respond to every type of threat. If we are to keep up with the cybercriminals, the key is cooperation. The good news is that the computer security industry is quite unique in the way direct competitors help each other.

The Turning Point

If you were running Windows on your computer 10 years ago, you were running Windows XP. In fact, you were most likely running Windows XP SP1 (Service Pack 1). This is important, as Windows XP SP1 did not have a firewall enabled by default and did not feature automatic updates. So, if you were running Windows, you weren't running a firewall and you had to patch your system manually—by downloading the patches with Internet Explorer 6, which itself was ridden with security vulnerabilities.

No wonder, then, that worms and viruses were rampant in 2003. In fact, we saw some of the worst outbreaks in history in 2003: Slammer, Sasser, Blaster, Mydoom, Sobig, and so on. They went on to do some spectacular damage. Slammer infected a nuclear power plant in Ohio and shut down Bank of America's ATM systems. Blaster stopped trains in their tracks outside Washington, D.C., and shut down Air Canada check-in systems at Canadian airports. Sasser thoroughly infected several hospitals in Europe.

The problems with Windows security were so bad that Microsoft had to do something. And they did. In hindsight, they did a spectacular turnaround in their security processes. They started Trustworthy Computing. They stopped all new development for a while to go back and find and fix old vulnerabilities. Today, the difference in the default security level of 64-bit Windows 8 is so much ahead of Windows XP you can't even compare them.

We've seen other companies do similar turnarounds. When the Microsoft ship started to become tighter and harder to attack, the attackers started looking for easier targets. One favorite was Adobe Reader and Adobe Flash. For several years, one vulnerability after another was found in Adobe products, and most users were running badly outdated products as updating wasn't straightforward. Eventually Adobe got their act together. Today, the security level of, say, Adobe Reader, is so much ahead of older readers you can't even compare them.

The battle at hand right now is with Java and Oracle. It seems that Oracle hasn't gotten their act together yet. And maybe don't even have to: users are voting with their feet and Java is already disappearing from the web.

The overall security level of end-user systems is now better than ever before. The last decade has brought us great improvements. Unfortunately, the last decade has also completely changed who were fighting.

In 2003, all the malware was still being written by hobbyists, for fun. The hobbyists have been replaced by new attackers: not just organized criminals, but also hacktivists and governments. Criminals and especially governments can afford to invest in their attacks. As an end result, we're still not safe with our computers, even with all the great improvements.

But at least we don't see flights grounded and trains stopped by malware every other week, like we did in 2003.

Crypto Currencies

In 2008, a mathematician called Satoshi Nakamoto submitted a technical paper for a cryptography conference. The paper described a peer-to-peer network where participating systems would do complicated mathematical calculations on something called a *blockchain*. This system was designed to create a completely new currency: a crypto currency. In short, a currency that is based on math. The paper was titled "Bitcoin: A Peer-to-Peer Electronic Cash System."

Since Bitcoin is not linked to any existing currency, its value is purely based on the value people believe it's worth. And since it can be used to do instant transactions globally, it does have value. Sending Bitcoins around is very much like sending e-mail. If I have your address, I can send you money. I can send it to you instantly, anywhere, bypassing exchanges, banks, and the tax man. In fact, crypto currencies make banks unnecessary for moving money around—which is why banks hate the whole idea.

The beauty of the algorithm behind Bitcoin is solving two main problems of crypto currencies by joining them: how do you confirm transactions and how do you inject new units of currency into the system without causing inflation. Since there is no central bank in the system, the transactions need to be confirmed somehow—otherwise one could fabricate fake money. In Bitcoin, the confirmations are done by other members of the peer-to-peer network. At least six members of the peer-to-peer network have to confirm the transactions before they go through. But why would anybody confirm transactions for others? Because they get rewarded for it: the algorithm issues new Bitcoins as reward to users who have been participating in confirmations. This is called *mining*.

When Bitcoin was young, mining was easy and you could easily make dozens of Bitcoins on a home computer. However, as Bitcoin value grew, mining became harder since there were more people interested in doing it. Even though the dollar-to-BTC exchange rate has fluctuated, fact remains that in the beginning of 2013, the exchange rate for the U.S. dollar to a Bitcoin was $8 and by the fall it was $130. So Bitcoins now have very real real-world value.

When Bitcoins became valuable, people were more and more interested in Satoshi Nakamoto. He gave a few e-mail interviews, but eventually stopped correspondence altogether. Then he disappeared. When people went looking for him, they realized Satoshi Nakamoto didn't exist. Even today, nobody knows who invented Bitcoin. Indeed, however, Bitcoin fans have been spotted wearing T-shirts saying "Satoshi Nakamoto Died for Our Sins."

Today, there are massively large networks of computers mining Bitcoins and other competing crypto currencies (such as Litecoin). The basic idea behind mining is easy enough: if you have powerful computers, you can make money. Unfortunately, those computers don't have to be your own computers. Some of the largest botnets run by online criminals today are monetized by mining. So, you'd have an infected home computer of a grandmother in, say, Barcelona, running Windows XP at 100 percent utilization around the clock as it is mining coins worth tens of thousands of dollars a day for a Russian cybercrime gang. It's easy to see that such mining botnets will become very popular for online criminals in the future.

Even more importantly, such an attack does not require a user for the computers in order to make money. Most traditional botnet monetization mechanisms required a user's presence. For example, credit card keyloggers needed a user at the keyboard to type in his payment details or ransom trojans needed a user to pay a ransom in order to regain access to his computer or his data. Mining botnets just need processing power and a network connection.

Some of the upcoming crypto currencies do not need high-end GPUs to do the mining: a regular CPU will do. When you combine that with the fact that home automation and embedded devices are becoming more and more common, we can make an interesting forecast: there will be botnets that will be making money by mining on botnets created out of embedded devices. Think botnets of infected printers or set-top boxes or microwave ovens. Or toasters.

Whether it makes sense or not, toasters with embedded computers and Internet connectivity will be reality one day. Before crypto currencies existed, it would have been hard to come up with a sensible reason for why anybody would want to write malware to infect toasters. However, mining botnets of thousands of infected toasters could actually make enough money to justify such an operation. Sooner or later, this will happen.

Espionage

Spying is about collecting information. When information was still written on pieces of paper, a spy had to physically go and steal it. These days information is data on computers and networks, so modern spying is often carried out with the help of malware. The cyber spies use trojans and backdoors to infect their targets' computers, giving them access to the data even from the other side of the world.

Who spends money on spying? Companies and countries do. When companies do it, it's called industrial espionage. When countries do it, it's just espionage.

In the most typical case, the attack is made through e-mail to a few carefully selected people or even a single person in the organization. The target receives what seems like an ordinary e-mail with an attached document, often from a familiar person. In reality, the whole message is a forgery. The e-mail sender's details are forged and the seemingly harmless attached document contains the attack code. If the recipient does not realize the e-mail is a forgery, the whole case will probably go unnoticed, forever.

Program files like Windows EXE files do not get through firewalls and filters, so the attackers commonly use PDF, DOC, XLS, and PPT document files as the attachment. These are also more likely to be viewed as safe documents by the recipient. In their standard form these file types do not contain executable code, so the attackers use vulnerabilities in applications like Adobe Reader and Microsoft Word to infect the computer when the booby-trapped documents are opened.

The structure of these attack files has been deliberately broken so that it crashes the office application in use when opened, while simultaneously executing the binary code inside the document. This code usually creates two new files on the hard disk and executes them. The first is a clean document that opens up on the user's monitor and distracts the user from the crash.

The second new file is a backdoor program that starts immediately and hides itself in the system, often using rootkit techniques. It establishes a connection from the infected computer to a specific network address, anywhere in the world. With the help of the backdoor the attacker gains access to all the information on the target computer, as well as the information in the local network that the targeted person has access to.

The attacks often use backdoor programs like Gh0st RAT or Poison Ivy to remotely monitor their targets. With such tools, they can do anything they want on the target machine. This includes logging the keyboard to collect passwords and a remote file manager to search documents with interesting content. Sometimes the attackers can eavesdrop on their target by remotely controlling the microphone of the infected computer.

I've been tracking targeted spying attacks since they were first observed in 2005. Targets have included large companies, governments, ministries, embassies, and nonprofit organizations like those who campaign for the freedom of Tibet, support minorities in China, or represent the Falun Gong religion. It would be easy to point the finger at the government of China. But we don't have the smoking gun. Nobody can conclusively prove the origin of these attacks. In fact, we know with a high degree of certainty that several governments are engaging in similar attacks.

It's also clear that what we've seen so far is just the beginning. Online espionage and spying can only become a more important tool for intelligence purposes in the future. Protecting against such attacks can prove to be very difficult.

The most effective method to protect data against cyber spying is to process confidential information on dedicated computers that are not connected to the Internet. Critical infrastructure should be isolated from public networks.

And isolation does not mean a firewall: it means being disconnected. And being disconnected is painful, complicated, and expensive. But it's also safer.

Exploits

A very big part of criminal or governmental cyber attacks use exploits to infect the target computer.

Without a vulnerability, there is no exploit. And ultimately, vulnerabilities are just bugs: programming errors. And we have bugs because programs are written by human beings and human beings make errors. Software bugs have been a problem as long as we've had programmable computers, and they aren't going to disappear.

Before the Internet became widespread, bugs weren't very critical. You would be working on a word processor and would open a corrupted document file and your word processor would crash. While annoying, such a crash wasn't too big of a deal. You might lose any unsaved work in open documents, but that's it. But as soon as the Internet entered the picture, things changed. Suddenly bugs that used to be just a nuisance could suddenly be used to take over your computer.

We have different classes of vulnerabilities and their severity ranges from a nuisance to critical.

First, we have local and remote vulnerabilities. Local vulnerabilities can only be exploited by a local user who already has access to the system. But remote vulnerabilities are much more severe as they can be exploited from anywhere over a network connection.

Vulnerability types can then be divided by their actions on the target system: *denial-of-service*, *privilege escalation*, or *code execution*. Denial-of-service vulnerabilities allow the attacker to slow down or shut down the system. Privilege escalations can be used to gain additional rights on a system, and code execution allows running commands.

The most serious vulnerabilities are remote code execution vulnerabilities. And these are what the attackers need.

But even the most valuable vulnerabilities are worthless if the vulnerability gets patched. So the most valuable exploits are targeting vulnerabilities that are not known to the vendor behind the exploited product. This means that the vendor cannot fix the bug and issue a security patch to close the hole. If a security patch is available and the vulnerability starts to get exploited by the attackers five days after the patch came out, users had five days to react. If there is no patch available, they users had no time at all to secure themselves: literally zero days. This is where the term *zero-day vulnerability* comes from: users are vulnerable, even if they had applied all possible patches.

The knowledge of the vulnerabilities needed to create these exploits is gathered from several sources. Experienced professionals search for vulnerabilities systematically by using techniques like fuzzing or by reviewing the source code of open-source applications, looking for bugs. Specialist tools have been created to locate vulnerable code from compiled binaries. Less experienced attackers can find known vulnerabilities by reading security-themed mailing lists or by reverse engineering security patches as they are made available by the affected vendors. Exploits are valuable even if a patch is available, as there are targets that don't patch as quickly as they should.

Originally, only hobbyist malware writers were using exploits to do offensive attacks. Worms like Code Red, Sasser, and Blaster would spread around the world in minutes as they could remotely infect their target with exploits.

Things changed as organized criminal gangs started making serious money with keyloggers, banking trojans, and ransom trojans. As money entered the picture, the need for fresh exploits created an underground marketplace.

Things changed even more as governments entered the picture. As the infamous Stuxnet malware was discovered in July 2010, security companies were amazed to notice this unique piece of malware was using a total of four different zero-day exploits—which remains a record in its own field. Stuxnet was eventually linked to an operation launched by the governments of the United States and Israel to target various objects in the Middle East and to especially slow down the nuclear program of the Islamic Republic of Iran.

Other governments learned of Stuxnet and saw the three main takeaways of it: attacks like these are effective, they are cheap, and they are deniable. All of these qualities are highly sought after in espionage and military attacks. In effect, this started a cyber arms race that today is a reality in most of the technically advanced nations. These nations weren't just interested in running cyber defense programs to protect themselves against cyber attacks. They wanted to gain access to offensive capability and to be capable of launching offensive attacks themselves.

To have a credible offensive cyber program, a country will need a steady supply of new exploits. Exploits don't last forever. They get found out and patched. New versions of the vulnerable software might require new exploits, and these exploits have to be weaponized and reliable. To have a credible offensive cyber program, a country needs a steady supply of fresh exploits.

As finding the vulnerabilities and creating the weaponized exploits is hard, most governments would need to outsource this job to experts. Where can they find such expertise from? Security companies and antivirus experts are not providing attack code: they specialize in defense, not attacks. Intelligence agencies and militaries have always turned to defense contractors when they need technology they can't produce by themselves. This applies to exploits as well.

Simply by browsing the websites of the largest defense contractors in the world, you can easily find out that most of them advertise offensive capability to their customers. Northrop Grumman even runs radio ads claiming that they "provide governmental customers with both offensive and defensive solutions."

However, even the defense contractors might have a hard time building the specialized expertise to locate unknown vulnerabilities and to create attacks against them. Many of them seem to end up buying their exploits from one of the several boutique companies specializing in finding zero-day vulnerabilities. Such companies have popped up in various countries. These companies go out of their way to find bugs that can be exploited and turned into security holes. Once found, the exploits are weaponized. In this way, they can be abused effectively and reliably. These attackers also try to make sure that the company behind the targeted product will never learn about the vulnerability—because if they did, they would fix the bug. Consequently, the customers and the public at large would not be vulnerable any more. This would make the exploit code worthless to the vendor.

Companies specializing in selling exploits operate around the world. Some of the known companies reside in the United States, the United Kingdom, Germany, Italy, and France. Others operate from Asia. Many of them like to portray themselves as being part of the computer security industry. However, we must not mistake them for security companies, as these companies do not want to improve computer security. Quite the opposite, these companies go to great lengths to make sure the vulnerabilities they find do not get closed, making all of us more vulnerable.

In some cases, exploits can be used for good. For example, sanctioned penetration tests done with tools like Metasploit can improve the security of an organization. But that's not what we're discussing here. We're talking about creating zero-day vulnerabilities just to be used for secret offensive attacks.

The total size of the exploit export industry is hard to estimate. However, looking at public recruitment ads of the known actors as well as various defense contractors, it's easy to see there is much more recruitment happening right now for offensive positions than for defensive roles. As an example, some U.S.-based defense contractors have more than a hundred open positions for people with Top Secret/SCI clearance to create exploits. Some of these positions specifically mention the need to create offensive exploits targeting iPhones, iPads, and Android devices.

If we look for offensive cyber attacks that have been linked back to a known government, the best known examples link back to the governments of the United States and Israel. When the *New York Times* ran the story linking the U.S. Government and the Obama administration to Stuxnet, the White House started an investigation on who had leaked the information. Note that they never denied the story. They just wanted to know who leaked it.

As the U.S. is engaging in offensive cyber attacks on other countries, certainly other countries feel that they are free to do the same. This cyber arms race has created an increasing demand for exploits.

Government Surveillance

When the Internet became commonplace in the mid-1990s, the decision makers ignored it. They didn't see it as important or in any way relevant to them. As a direct result, global freedom flourished in the unrestricted online world. Suddenly people all over the world had in their reach something truly and really global. And suddenly, people weren't just consuming content; they were creating content for others to see.

But eventually politicians and leaders realized just how important the Internet is. And they realized how useful the Internet was for other purposes—especially for the purposes of doing surveillance on citizens.

The two arguably most important inventions of our generation, the Internet and mobile phones, changed the world. However, they both turned out to be perfect tools for the surveillance state. And in a surveillance state, everybody is assumed guilty.

Internet surveillance really become front-page material when Edward Snowden started leaking information on PRISM, XKeyscore, and other NSA programs in the summer of 2013.

But don't get me wrong. I do understand the need for doing both monitoring and surveillance. If somebody is suspected of running a drug ring, or planning a school shooting, or participating in a terror organization, he should be monitored, with a relevant court order.

However, that's not what PRISM is about. PRISM is not about monitoring suspicious people. PRISM is about monitoring everyone. It's about monitoring people that are known to be innocent. And it's about building dossiers on everyone, eventually going back decades. Such dossiers, based on our Internet activity, will build a thorough picture of us. And if the powers-that-be ever need to find a way to twist your hand, they would certainly find something suspicious or embarrassing on everyone, if they have enough of their Internet history recorded.

United States intelligence agencies have a full legal right to monitor foreigners. Which doesn't sound too bad—until your realize that most of us are foreigners to the Americans. In fact, 96 percent of the people on the planet turn out to be such *foreigners.* And when these people use U.S.-based services, they are legally under surveillance.

When the PRISM leaks started, U.S. intelligence tried to calm the rest of the world by explaining how there's no need to worry, and about how these programs were just about fighting terrorists. But then further leaks proved the U.S. was using their tools to monitor the European Commission and the United Nations as well. It's difficult for them to argue that they were trying to find terrorists at the European Union headquarters.

Another argument we've heard from the U.S. intelligence apparatus is that everyone else is doing Internet surveillance too. And indeed, most countries do have intelligence agencies, and most of them do monitor what other countries are doing. However, the U.S. has an unfair advantage. Almost all of the common Internet services, search engines, webmails, web browsers, and mobile operating systems come from the U.S. To put in another way: How many Spanish politicians and decision makers use American services? Answer: all of them. And how many American politicians and decision makers use Spanish services? Answer: none of them.

All this should make it obvious that we foreigners should not use U.S.-based services. They've proven to us that they are not trustworthy. Why would we voluntarily hand our data to a foreign intelligence agency?

But in practice, it's very hard to avoid using services like Google, Facebook, LinkedIn, Dropbox, Amazon, Skydrive, iCloud, Android, Windows, iOS, and so on. This is a clear example of the failure of Europe, Asia, and Africa to compete with the U.S. on Internet services. And when the rest of the world does produce a global hit—like Skype or Nokia—it typically ends up acquired by an American company, bringing it under U.S. control.

But if you're not doing anything wrong, why worry about this? Or, if you are worrying about this, what do you have to hide? My answer to this question is that I have nothing to hide... but I have nothing in particular that I'd want to share with an intelligence agency either. In particular, I have nothing to share with a foreign intelligence agency. If we really need a big brother, I'd much rather have a domestic big brother than a foreign big brother.

People have asked me if they really should worry about PRISM. I've told them that they should not be worried—they should be outraged instead. We should not just accept such blanket and wholesale surveillance from one country on the rest of the world.

Advancements in computing power and data storage have made wholesale surveillance possible. But they've also made leaking possible. That's how Edward Snowden could steal three laptops which contained so much information that, printed out, it would be a long row of trucks full of paper.

Leaking has become so easy that it will keep organizations worrying about getting caught over any wrongdoing. We might hope that this would force organizations to avoid unethical practices.

While governments are watching over us, they know we are watching over them.

Summary

We've seen massive shifts in cyber attacks over the last two decades: from simple viruses written by teenagers to multimillion-dollar cyber attacks launched by nation-states.

All this is happening right now, during our generation. We were the first generation that got online. We should do what we can to secure the net and keep it free so that it will be there for future generations to enjoy.

OpenMind

bbvaopenmind.com/en/article/cyber-attacks

About us

OpenMind

bbvaopenmind.com/en/what-is-openmind

Open Mind Channel

YouTube

youtube.com/user/bbvaopenmind

Share

Article

Cyber Attacks

About the Author

Mikko Hypponen

bbvaopenmind.com/en/author/mikko-hypponen-en

YouTube

youtu.be/UV9XxIeSP5g

Related Articles

- Technology and the Burden of Responsibility

- Cyberflow

- The Future of Global Cooperation: What is missing? What could be successful?

Read the full book

Other Books

- There's a Future: Visions for a Better World

- Values and Ethics for the 21st Century

- Innovation. Perspectives for the 21st Century

- The Multiple Faces of Globalization

- Frontiers of Knowledge