MAKING SENSE OF THREATS FOR SMBs

Cyberwar, hacktivism, DDoS attacks. They're are all over the news, but they only affect multinationals and governments - right?

F-Secure's **Esa Tornikoski** makes sense of the threat landscape for businesses.

The world of data security is complex and moving fast. Most companies have too much to do and too much variety on their plates to maintain a specialist's knowledge of security. But with Stuxnet and Flame in the news almost every day, we've received questions from several different kinds of organizations about how their businesses and data are at risk.

There's no single "kind" of threat, but an entire landscape

One of the most abstract things for businesses is to understand which cases make for great media stories and which represent a real danger to SMBs. How do you know what attacks are most likely to affect your business?

WHAT IN FACT AFFECTS SMBS MOST IS NOT ANY SINGLE "KIND" OF THREAT, THE CHANGING, EVER-PRESENT THREAT OF CYBERCRIME.

This is something that can't be pinned down to individual elements like "viruses" or "spam", and it certainly isn't documented thoroughly in the media. The business of cybercrime is as rich and complex as any other – and each individual "threat" is created by a different party, bought and sold and intertwined with many other elements. The result is a complex engine with many different forms – but one clear purpose, to steal data and money.

F-Secure

Zombie computers, fooled humans, and holes no one can see

There is a definite pattern forming in the ways attackers work. Foiled by ever-better technical security measures – anti-virus, spam filters, browsing protection, and so on – attackers seek different ways to gain access to data, and SMBs are particularly susceptible to certain forms: botnets (zombie computers), social engineering (the art of being tricked), and vulnerability exploits (being attacked through unknown security holes).

Botnets: Your company resources, at work for another "company"

A common problem for SMBs is called a **botnet**. A bot is an infected computer that can be controlled remotely, and a botnet is a whole network of those infected machines – it's like an army of zombies controlled by one person, doing whatever he/she bids. In these cases, a legitimate company's resources can be captured and controlled, and used to do dirty deeds like send out spam, steal data, even attack other sites – and it can take a long time before the company itself catches on.

The person who creates the botnet is usually not the one who uses it – he'll make a lot of money by selling the bot to the highest bidder. They'll even rent them out by the hour or week.

SMBs present an ideal environment for botnet use: there's a large number of machines networked together, and office workers typically don't turn them off when they leave for the night.

"A COMPROMISED CORPORATE NETWORK CREATES A POOL OF VIRTUALLY UNLIMITED RESOURCES FOR ATTACKERS", SAYS SEAN SULLIVAN, SECURITY ADVISOR AT F-SECURE LABS.

"It's a situation where a company's resources are actually doing the attackers' work."

Social engineering: We're only human. Attackers know that, too.

Advances in technical security have led attackers to seek other ways in to a system – and what better way than through the system's users? **Social engineering** refers to manipulating people into performing certain actions or providing information – for example, tricking them into installing a file, or giving up their password or credit card info. Attacks used to be obvious (remember the Nigerian prince who needed your bank account number?) but have become more creative and elegant, and oftentimes indistinguishable from legitimate sources.

Ransomware is an attack form becoming commonplace – an attacker locks down the user's computer, demanding they pay to release it. Usually it's done in the guise of a message from the police, saying that the user has to pay a fine due to possessing nasty, unlawful content. "People need to get in touch with the helpdesk", says Sullivan, "but they don't want to do that, because the malware creates an embarrassing situation for them".

Vulnerability exploits: Even trustworthy sources can wreak havoc

Perhaps the preferred way for attackers to gain access to a computer is through **vulnerability exploitation**. This is simply the art of finding a security hole in any software and using that as a way to infect the machine.

The most common culprit? Old, unpatched software.

"YOUR SOFTWARE IS LIKE THE FRONT DOOR TO YOUR PC", SAYS SULLIVAN.

"Out-of-date software is a wide-open door for all kinds of attacks, especially from innocuous places." Examples like banner ads – which run on sites such as newspapers that most people inherently trust – are specifically designed to take advantage of plugins like Java and Flash. They seek out any possible way to infect the machine, and install malware that steals data, turns it into a bot, or just locks it up and holds it for ransom.

In the future, exploits will move even faster

Sean Sullivan predicts a much more rapid turnaround of exploits, and far more of what are called "zero-day" exploits – something for which no patch or fix yet exists.

"Holes will be exploited so rapidly that software vendors won't be able to keep up", he says, "And the zero-day period is just beginning." Exploit detections made up 58% of F-Secure top ten detections during H1 2013, with 45% of those being Java related. All it takes is for a user to visit a compromised website – even with the latest versions of IE7, IE8, or IE9 – and control of their machine is ceded over to the attackers.

This is a good example of a threat that doesn't get widespread media coverage – mainly tech blogs, and it gets technical very fast. Most businesses likely don't hear anything about it. In cases like this, the first line of defense is to stop using the compromised product until a suitable fix is released.

Will cyberwarfare lead to collateral damage?

As mentioned, attacks like Flame are all over the news. In simple terms, Flame is an element in what appears to be a cyberwar between national governments. Flame itself, in the form we know it now, won't reach most normal users. But the techniques used certainly will. With Flame,

the coders used advanced methods of targeting individual computers, and tricked the OS into thinking that Microsoft had created the updates itself.

Right now most cybercriminals don't need to be that thorough. But when they discover that they can get a better return on investment, or nudge out the competition, they'll start to employ these techniques.

Like Sean told me, "Today's R&D is tomorrow's practical application." The hard work is now done, and so the methods used in the Flame case will eventually be picked up and adopted by crime syndicates. And we'll all have to be prepared.

Be vigilant. Don't panic.

So what are the main things to be aware of in such a rapidly changing landscape?

Naturally, be sure your organization has solid anti-virus, anti-spam, and browsing protection running on the whole environment, from laptops and desktops to servers and mobiles.

What is important particularly for SMBs is to be sure you're running the latest versions of all your software – yes, that's all your software, like operating systems, plugins such as Flash and Java, Microsoft Office and any browsers in use – not just security software.

Finally, be in touch with an expert who can guide you through security issues and knows the dangers out there.

In short, by making sure that all software in use is the latest version, and that security products cover all layers in your organization, you will be able to devote your time and resources to your own business priorities.

About the author

Esa Tornikoski is Product Manager at F-Secure. He specializes in building offerings to match IT security needs for SMBs.

About F-Secure

F-Secure is a global company with headquarters located in Helsinki, Finland. Founded in 1988, F-Secure is a pioneer in the security business and today operates in more than 100 countries. F-Secure has 18 branch offices and more than half of our employees are working outside Finland. We are a trusted service partner for over 200 operators as well as a preferred security provider for businesses worldwide through an extensive network of reseller partner.