EXPOSING THE SECURITY WEAKNESSES WE TEND TO OVERLOOK

As security analysts we often get asked the question: "*What threats and vulnerabilities do you expect we will see in the future?*" This is a very interesting question but also an indication that the way we think about and discuss IT security is fundamentally wrong. Let us tell you why.

As most people know, if you want to improve something you first need to know what you are doing wrong, so that you can focus on the things which are important for your progress. The same goes for IT security. By focusing only on the exciting and new technical forecasts from security evangelists, we often forget the really important things. In short, tomorrow we are most likely to see the errors and threats that we fail to solve today.

To analyze this in depth, Kaspersky researcher David Jacoby joined forces with Outpost24's CSO, Martin Jartelius, gaining access to unique statistics related to the technical risk exposures from the vulnerability management vendor. This statistical analysis, coupled with a few interesting research projects, led us to a few conclusions that we think are really important in our fight towards a more secure and healthy IT security environment.

David's daily job involves regularly analyzing trends and proactively fighting cybercrime. One important tool in doing so is to read a lot of articles, blogs and mail conversations on a daily basis. But when David started to analyze the discussions and topics, it became clear that the topics most discussed and commented on are about national security and APT attacks or advanced exploitation techniques. At this point, David reached out to Outpost24 to dig deeper. Together with Martin they asked themselves: *does it really take an APT with some advanced zero-day vulnerabilities to attack a country?* After a bit of digging, it became clear that the threats "of tomorrow" are those that are already with us today, yet remain unsolved.

If we look at some of the previous breaches, zero-day vulnerabilities have been the entry point for the attacker; but the number of attacks where zero-day vulnerabilities have been used are still quite low, even though this number is rising. What about all the other breaches that are happening out

there? What about critical infrastructure? When discussing critical infrastructure it seems that all focus is on PLC-based devices, energy plants with SCADA systems, factories with CNC robots and core networking appliances. But what about other governmental organizations and institutions, hospitals, schools, radio and TV stations, banks or other financial institutions? What systems are they using, and what is the security level of those systems? Many of these institutions and companies are linked together; there are multiple dependencies between them. And one general rule when talking about security is that security is only as good as the weakest link. So we asked ourselves: *how weak is the weakest link?*

There are many different ways to measure IT (in)security. We decided to perform tests and also collect data about patch management. Since David Jacoby and Martin Jartelius are both based in Sweden, we decided to use this region as our target group.

HOW WEAK IS THE WEAKEST LINK?

Attackers often have different approaches when trying to compromise a target. One common attack is to send specially crafted emails containing zero-day exploits, or to attempt a phishing attack. But another method is to break into external-facing machines. When reading about APT and targeted attacks, we often get detailed descriptions about new vulnerabilities and advanced phishing emails exploiting client-side vulnerabilities, and about malware bypassing security mechanisms and client-side exploitation. This is very important and a huge attack vector. But have we totally forgotten about all the attacks targeting our external machines? Or good old social engineering attacks?

To define the weakest link we also need to understand that there are logical flaws that the attacker can take advantage of, and to understand that those flaws also exist in security products. For example, when talking about patch and vulnerability management there are some risks that a lot of companies have not taken into consideration when using these services. One very common problem is that companies do not compensate for the critical time window during which they are actually vulnerable to something until the point when they actually know that they are vulnerable to it; as well as the timespan from when they become aware of the problem to when they resolve it.

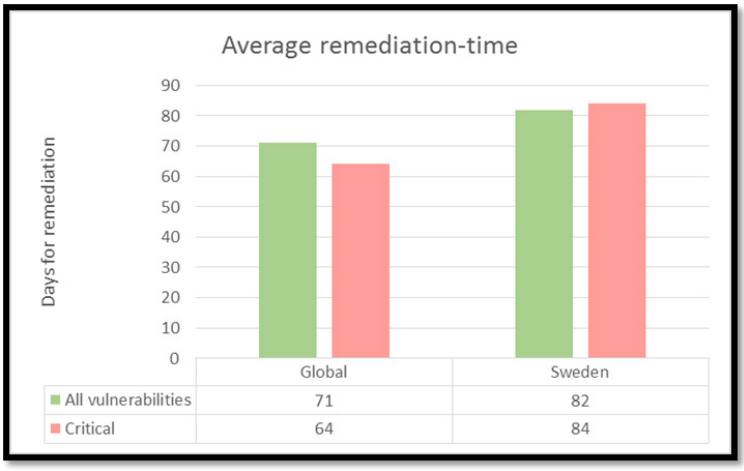
One example of what this time period may look like is this:

1. A vulnerability is discovered by a security researcher.
2. Security researcher notifies the vendor.
3. Vendor checks the vulnerability and develops a fix/patch.
4. Vendor + security researcher publically inform everyone about the problem and the patch.
5. Exploit developer at the security company implements a test for the vulnerability.
6. Customer of the security company performs a security scan of his machines.
7. Customer receives a report with guides on how to patch this vulnerability.
8. Customer patches the vulnerability.

As you can see in the example above, there is a time window from when the customer is informed about the existence of a vulnerability until the moment the vulnerability is fixed. This paper will not address the risks associated with a zero-day vulnerability, but only the risk with known attacks that are out there. We asked ourselves *"How many days does it take us to fix a vulnerability after we get informed about it?"*

Together with Outpost24's technical team, we categorized the vulnerabilities into two different groups - *"Critical"* and *"All vulnerabilities"*. A critical vulnerability may be, for example, remote command execution without authentication. We then started to analyze the critical time windows using this data.

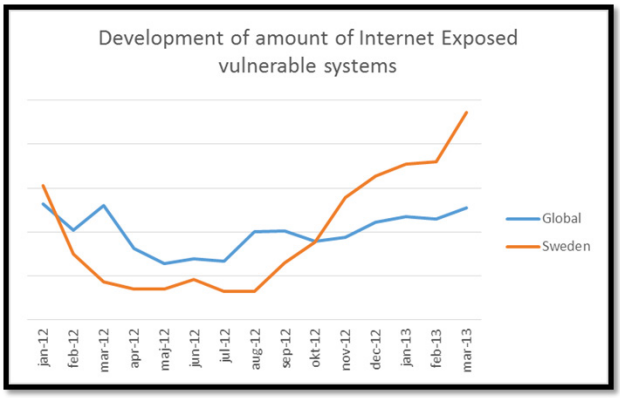
It did not take very long before our theory was confirmed. In general, it takes a company 60-70 days to fix a vulnerability. Critical vulnerabilities have a higher priority and are fixed before the non-critical ones. But in Swedish companies we see a different trend. Firstly Swedish companies are a little bit slower. What is quite interesting is that the critical vulnerabilities take about two days longer to get fixed than less critical ones vulnerabilities in Sweden. This might be because some of the critical vulnerabilities are also found on critical and important systems that can be tricky to patch. In general organizations in Sweden require about 10 to 20 days longer to patch a vulnerability than the rest of the world.



Source: Outpost24

Security maturity and awareness is increasing in most businesses, but the question arises, does this mean vulnerabilities are solved more quickly, and is the amount of internet-exposed vulnerable systems decreasing? We decided to look at a trend for the last year. This trend shows the ratio of

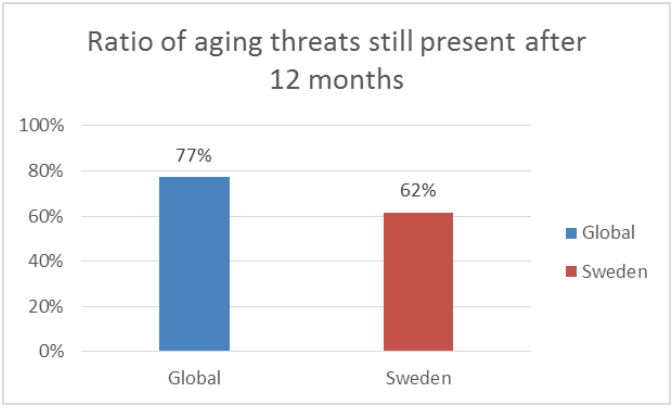
vulnerable systems in relation to all scanned systems, meaning that it compensates for an increase or decrease in sample size to get comparable results.



Source: Outpost24

It is a very bad sign when we look at the trends and we see that it is more common to encounter vulnerable systems in Sweden this year than it was during the same period last year. It should be noted that Sweden has a better baseline, with about half the rate of vulnerable systems compared to the global sample, but this advantage is starting to even out, and it is doing so fast.

So how can Sweden have a better baseline with few vulnerable systems, but still be slower at patching and slower at handling new vulnerable servers? The answer appears to lie mainly in a slow but grinding process. A common problem for both Swedish and international organizations is obviously that if someone drops the ball there is rarely someone there to pick it up.

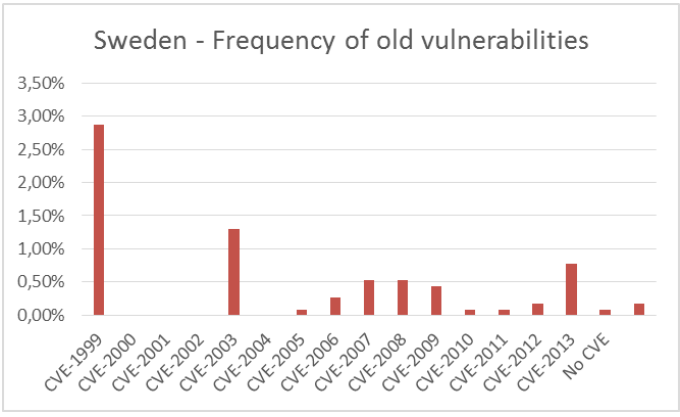


Source: Outpost24

A common baseline is that all critical threats should be resolved within a time span of three months at worst. If this is not done, it is time for action and re-action. The above graph shows that of the vulnerabilities that get past this three-month baseline, 77 % are still present after a full year on the global base, while the same number for Sweden is 62 %. This fits rather well with the general impression of Swedish organizations that work is not always swift, but it is thorough and process-oriented.

During the research we started to look into which vulnerabilities the machines were vulnerable to, and started to collect data from 2010. There are still systems that are vulnerable to vulnerabilities reported in 2010, and these vulnerabilities are also considered as critical due to the ease of exploitation and impact. We can only hope that any vulnerable system does not contain any critical data, or have connections to important networks.

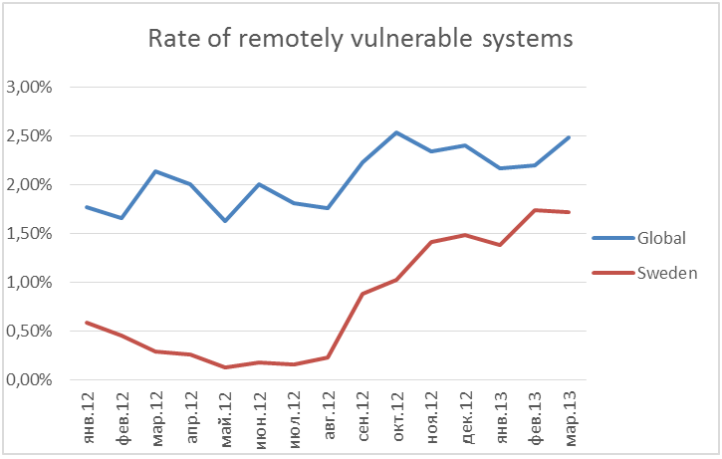
As a next step in the research we collected statistics on how many systems Outpost24 knows of that are still vulnerable to old vulnerabilities. Outpost24 provided with a statistical selection for more than 2,000 Internet-facing machines, which means that none of the machines used in this survey are workstations behind a firewall. The statistics provided by Outpost24 used in this section are calculated for the four first months of 2013.



Source: Outpost24

We were not expecting to see systems vulnerable to vulnerabilities older than 2010, but as it turns out, quite a high percentage of systems are still vulnerable to 10 year old vulnerabilities. Perhaps even more interesting, these are companies who are paying to keep track of their security. We can only wonder how much higher the numbers would be for a larger selection, including systems that are not actively monitored.

On the other hand, it is important to keep in mind that some of these systems might be embedded systems or systems that simply cannot be updated due to their configuration.



Source Outpost24

If we focus on how common it is to encounter a system that is remotely exploitable, on a global basis the statistics fluctuate between 2-2.5%, and for Sweden the numbers are on the level of between 0.5-1.5%.

In practice, this means that if you are at the level of an average organization that proactively manages your vulnerabilities, it is still likely to find 2-5 vulnerable servers in a single C-level internet-exposed network range.

WHAT IS “CRITICAL INFRASTRUCTURE”?

Critical Infrastructure - what is it? Most of the reports we read, especially concerning IT threats, are articles about power and energy plants. We also read about industries with certain “robotic” software such as SCADA systems and CNC robots.

But if you ask us, our perspective is that everyone tends to forget about transportation, financial systems and systems containing sensitive information about our citizens. There are also a lot of privately-owned companies who are contributing to the so called “critical infrastructure” and most likely have network connections to other companies. To put this in perspective, the power grid is probably a system critical to society. But so is the system processing work orders for the local power service company, as introducing changes here may lead to chaos. Don’t hack the system, hack the people who manage the system.

From another point of view, we should also consider hotels. When diplomats, politicians and C-level people travel, they typically stay at hotels. By getting access to the corporate network and front desk computers, you can probably get access to the room of any guest.

During David Jacoby’s recent travels he took the liberty of taking some photos of unprotected network outlets and computers. This is quite a common view at hotels around the world.

So we asked ourselves again, what is actually critical infrastructure and what are we trying to do to protect these systems?

THE USB CHALLENGE

David performed part of the study not at his computer, but using charm, wit and a nice suit. David explains: “As a security researcher it is my job to question things and try to find alternative conclusions. I’ve been looking at the statistics that were provided to me by Outpost24 and – Yes! Some numbers are pretty scary. But can I trust the numbers? Can you simply hack a machine with a vulnerability that’s more than ten years old? Or use any of the newer vulnerabilities within the 80 days the company takes to fix the vulnerability?”

Remembering that when we first heard about Stuxnet and how it exploited the Microsoft Windows Shell LNK vulnerability with a specially crafted USB stick, a plan was formed. That vulnerability was a zero-day, and a pretty nasty one. But how easy would it be to insert a USB stick into a computer when you have no permission to do it?

David decided to perform a small social engineering test by walking around for about three hours, dressed in a suit, with a USB stick in his pocket. The USB did not contain any vulnerabilities or exploits. It simply had a PDF of David’s CV on it, that’s it. The goal was to visit as many government institutions, hotels and large privately-owned companies as possible and ask them if they could help print the document because David had “left his papers at home and don’t want to arrive at his appointment unprepared”. The interview was not even with anyone from the same company he was visiting. The target list looked like this:

- **3** hotels within different chains.
- **6** governmental organizations or institutions.
- **2** large privately owned companies.

Before starting this experiment, the expectation was that maybe three quarters would fall for the trick, but the actual outcome was more interesting and nuanced than this.

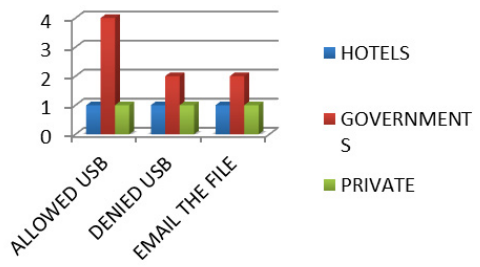
Let's start with the hotels. Only one hotel allowed David to insert the USB stick in their computer. However, even in this case the system administrator had actually disabled the USB port. Clever and a good protection against the human element. But service staff are there because they are service-minded and ready to help; and the receptionist told David to use another computer that was for guests and then to email her the PDF file. We don't know if this is considered as a "Win" or "Fail", but she did print the PDF, providing ample scope for any attack that exploits vulnerabilities in PDF software.

As mentioned earlier in this report, two of the hotels did not allow David to connect his USB stick to their computer, but they both had corporate ethernet ports placed around the hotel - and actually with DHCP enabled.

The privately-owned companies had the same security as the hotels. One of the two companies visited did put the USB stick in their computer, to find out that the USB port was disabled. At this point she did not ask David to email the file, but she actually went upstairs to insert the USB stick in another computer. Again, a success for technical security thwarted by the friendly front our organizations present to the world.

Now for the interesting part - the governmental institutions and organizations David visited. These types of organizations were varied. Some more or less kicked him out saying, "This is not a library". But some were very helpful. Out of the six organizations/institutions visited, four actually did help by inserting the USB stick in the computer. Two wanted to help, but the USB port was disabled so they asked David to send his CV via email instead.

We could go into much more detail about the different scenarios. But it is not necessary to go into detail on this aspect of our research, since the aim was to prove a point, not create instructions on how to break into government organisations.



What is really surprising is that the hotels and privately-owned companies had greater awareness and security than the governmental institutions/organizations. While David did visit fewer hotels and privately-owned companies, from this experience we think it's fair to say that we have a real problem.

"THE PENTEST CHALLENGE"

When doing research it's always important to get real facts, and one of the ways to do this is to get your hands dirty. During our research we also wanted to perform a practical challenge for a few companies from different industries. We would go out to the companies and perform a security audit with a pre-defined checklist based on the results from our research. We would check and see if they had any systems vulnerable to old threats, review their security routines and perform a lot of additional tests.

This challenge would be an eye-opener for the companies who wanted to participate in this challenge, and it would help us complete our research. The only problem was that only a handful of companies actually wanted to participate in this challenge.

Most of the companies were interested in testing a specific service, but not the entire network, and especially not their corporate network. They said that they were already aware of the risks and were not interested in testing this.

We both feel that this really is one of the key problems today; we spend more time on new exciting vulnerabilities and threats than actually looking into the real problems. We decided to perform the challenge anyway, and the results were pretty interesting. The challenge focused on getting as much network access as possible, without using any real exploits. We considered ourselves able to misuse the current configuration IF we were able to get network access. The company which agreed to participate in the challenge is quite large. It has about 1,500 active accounts in its Active Directory. The company has access to some extremely sensitive financial and political data; and also has access to infrastructure affecting the community, such as heating, power supply, Internet access and other things. The duration of the challenge was five hours, and we had no prior information about the target. During these five hours, the Kaspersky Lab and Outpost24 testers were able to:

> Walk into the building without anyone questioning us, gaining access to internal areas.

> Use an authenticated computer without anyone questioning us.

> Get corporate network access through several different locations, including printer room and halls.

> Convince two employees to allow use of their computers while they were authenticated.

- Extract usernames/passwords for important services via public network shares.
- Access extremely sensitive economic and political documents from an employee workstation.
- Connect a computer acting as a backdoor to their corporate network without anyone noticing.
- Collect usernames/passwords written on paper next to employees computers.
- Identify very poor patch levels on third party software such as Adobe Acrobat Reader, Java and Shockwave, in the standard configuration pushed to all users. Java was more than 9 months old.
- Enumerate over 300 accounts that had the setting “Password never expire” in the Active Directory.

In short, exploiting bad security practice, misconfigured security devices and a lack of staff security training, it was possible to gain full control of most parts of the organization, even though no new attacks or methods were used. To make a point regarding priorities, this specific organization was currently looking at implementing DNS-sec, but its current domains allowed zone transfer.

WHERE ARE WE GOING WRONG?

"If you always do what you've always done, you'll always get what you've always got."
-Henry Ford (1863-1947)

Whenever someone offers a simple, one-off solution, they do not understand the problem. Whenever someone offers to identify a single cause of a problem, they are probably treating the problem too simplistically.

Through this research, we have realized there are two key areas where the IT security mindsets of most organizations are going wrong:

> Security tools, or "solutions", are viewed as stand-alone solutions that add processes and logistics rather than as a supplement to existing business processes.

> Security efforts are aimed at checking compliance boxes.

TOOLS SUPPLEMENT BUSINESS PROCESSES

Over the years, IT has failed over and over again, because we think of solutions as a silver bullet. The solution to bad code was object orientation, the problem with documentation and design was UML and the problem with network intrusions was to buy the best available system and deploy it on your network. Those ideas are common, but sadly they are not true. They never have been, and never will be.

When a vendor shows up with a tool that will solve problems easily, or check boxes, beware! However, if the vendor talks about supporting your business processes, finding stakeholders, and providing metrics to improve existing solutions and processes, they might be worth listening to.

All security solutions, including our own, share one issue—no solution, whatever the quality of the technology, will make you safer as a stand-alone solution.

We need to evolve our way of thinking about security tools and solutions. We need to stop viewing them as tools that impose new logistical work on our organizations, and begin to understand that *they should support, measure, aid and improve our existing business processes*.

In the best case, new systems are procured based on their ability to improve or support the core

business. We should always identify our key stakeholders, risks and assets before we start a project. This way we will have systems that don't force specialists to write reports for other stakeholders; and our best technicians can focus on technology and systems that support the organization. We should require a review of changes to any sensitive infrastructure and systems. All these measures are free, but will increase security.

COMPLIANCE AND STANDARDS DON'T EQUAL SECURE

In the same way we can also see compliance as a threat to security. If compliance forces you to direct time and effort in a direction which does not fit the core business, it will be cumbersome. If it requires investments, it may move budgets away from areas that actually matter to the organization. Whenever an IT administrator loses the time to fix a vulnerability because he is writing a report to prove compliance, we lose security. Whenever it is more important to "perform regular vulnerability scanning", rather than to integrate the results of a mature scanner into the change- and quality-management processes, we fail. Being compliant does not mean you are secure, but generally being secure will aid efforts towards compliance.

To summarize, consider the following example:

In order to be compliant, an organization needs to inform all new staff about the risks of social engineering and IT security threats. This is commonly resolved by asking each new employee to sign a paper. Then, in practice, the IT department will still need to disable the USB port at the reception desk. Nevertheless, the staff is likeable and service-minded, so they will still ask customers to email the files, or go upstairs and insert the drive somewhere in your internal systems.

Despite our efforts, this is hardly a mature state of security.

IN CONCLUSION

With the experience gained from the weeks we've been working on this paper we have started to question the security industry. We, as security researchers, need to take our responsibility seriously, to both conduct research and then share relevant information that will actually help us and those we work with improve security.

If we only focus on the "cool" and "new" stuff, we will tend to forget the critical, everyday aspects of security. One goal of this research was to somehow try to restore the balance by publishing research that not only affects everyone, but also helps people improve their IT security. Rather than buying new tools and systems, if companies would take a second, more critical, look at their procedures and their culture and ask themselves "Are we providing the resources and processes necessary to actually address this?" it could be a major eye-opener.

For both of us, one of the most important insights was that almost all problems relate back to a "pay once" idea - provide training once, try and fix the threats of a vulnerability report once, setup the firewall properly once. The missing part is joining solutions and processes, something we will definitely bring home to our teams as this continues to be one of our main areas of focus: support existing processes, don't force new ones on the business.

Even with all the amazing new technology available, buying it without understanding the context of the problem is like driving your car without the belt on—simply the presence of a belt does not make you safe. Its proper use does.

We would like to thank everyone who made this possible, including all the "victims". We also want to send out a special thanks to the company who allowed us to perform the "Pentest Challenge".

Regards,

David and Martin