Redmond MAGAZINE

IT FACES TOO MANY THREATS AND NOT ENOUGH DEFENSES

This paper is based on a recent fireside chat webcast featuring Nick Cavalancia of Techvangelism and Michael Mimoso of Kaspersky Lab discussing the current level of security threats facing IT professionals.

KASPERSKY lab

usa.kaspersky.com

IT professionals face a daunting, some might say overwhelming task, in trying to protect their organization's systems from a perfect storm of malware.

Opening a discussion titled Too Many Threats, Not Enough Defenses, Nick Cavalancia of Techvangelism told a webcast audience: "There is not a day that goes by where we aren't hearing about some newly discovered vulnerability, maybe another variant of malware, new strain of ransomware, external attack, or insider threat."

Looking at it from an IT security perspective, he characterized the dilemma using an old phrase: It's enough to make your head spin.

"You're trying to figure out which way you're supposed to be watching," the Techvangelist said. "What threat are you supposed to be protecting your organization from, and it does make your head spin."

Never-before-seen threats keep emerging. Cavalancia points to a ransomware variation that uses a multi-step approach.

It begins with the familiar email with a PDF attachment.

"The PDF attachment has some kind of automatic coding to call out to a website to download a Word doc," Cavalancia explained. "I open up the Word doc that has a macro to call down the Trojan which then calls back home and pulls down the actual ransomware. That's a lot of steps. So, that means, if nothing else, in all of those steps you have different parts of the process that you have to protect against. Should you let macros run or not? You have to worry about whether PDFs should be able to go outside to the internet. Whether or not the email should even actually open up the PDF in the first place or should you have email scanning in place. Where are you scanning and detonating the attachment to see what it actually does when it gets executed."

DOING EVERYTHING AT ONCE

Schools of management and psychology may tell you not to try doing everything at once. But faced with threats constantly coming at you from every direction, searching for every possible vulnerability in your system, there isn't much choice.

Among the things you have to watch out for are:

- Malware
- Ransomware
- Phishing
- Trojans
- Rootkits
- SQL vulnerabilities
- JavaScript issues
- Flash vulnerabilities

Cover: Tippa Patt / Shutterstock.com

And, as we all know now from experience, the bad guys are innovative and likely to come up with something no one has ever heard of.

Ideally, you would focus on a specific threat to your system. In the old days, when there was one basic threat like spam, you could do that.

"A good place to start is focusing on what kind of threat should you be looking at," Cavalancia said. "What is the threat I need to be looking at? The first issue, is there a specific threat you should be looking at? And the reality is, there isn't. That's one of the big challenges here is that there isn't just one kind of threat that you have to worry about."

> "A GOOD PLACE TO START IS FOCUSING ON WHAT KIND OF THREAT SHOULD YOU BE LOOKING AT." —NICK CAVALANCIA

The past year and a half has seen an explosion in the number of malware threats, especially ransomware.

"I've been covering security for 10 years," Michael Mimoso of Kaspersky Lab told the webcast audience, "and I've never seen a threat evolve as quickly as ransomware did in the past eighteen months. Last year was dominated by ransomware and that's probably the biggest change we've seen in terms of malware is we've got this immediate opportunity for profit with a malware infection, which is something that really wasn't the case going back even two years. We went from attacks that would just lock down somebody's desktop. Then that quickly evolved into encrypto-ransomware where the malware was encrypting files and holding that for ransom. Then as backup became a good strategy against ransomware, these guys would target files that were in connected backup stores. They were looking for network access to infect other machines. There were ransomware variants that would try to brick your hardware, go after the bios on your machine."

HOW MALWARE METHODS EVOLVE

Kaspersky Lab's Mimoso said that in the constantly changing world of security threats, there's recently been a switch back to some old school malware methods.

"We've seen a lot of email based attacks recently," he explained. "That's a shift because they used to be almost exclusively web-based kinds of attacks. And we're seeing a switch back to spam and phishing pushing a lot of malware. That's kind of a real old school attack, where the malware is embedded inside a legitimate Office document, for example a Word document or a spreadsheet. That's a big shift that we've seen lately, kind of going back to these

email based attacks, requiring some user interaction; requiring the user to fall for a scam by using social engineering."

The good news is that security software vendors are constantly improving anti-malware technology and end users are becoming more malware aware, Mimoso said. End users understand what phishing is and what the risks are around phishing.

But phishing scams are still out there. They are often large scale campaigns and all they need to do is hit on the one user in your organization who isn't aware or doesn't care and the bad guys have a means of breaking into your system.

> THE GOOD NEWS IS THAT SECURITY SOFTWARE VENDORS ARE CONSTANTLY IMPROVING ANTI-MALWARE TECHNOLOGY AND END USERS ARE BECOMING MORE MALWARE AWARE.
>
> —MICHAEL MIMOSO

THE DANGER OF EXPLOIT KITS

Because finding vulnerabilities is the key to breaking into your system, criminals are buying and relying on exploit kits sold in the underground and black market on the dark web, Mimoso explained.

"These kits are used to find vulnerabilities in websites," he said. "To infect them with malware that takes advantage of vulnerabilities in browsers. So, if you surf to this website and you are using an older version of Internet Explorer, or an unpatched version of FireFox and there's an exploit for a particular vulnerability in your browser, you're going to get infected by one of these kits."

Some of these exploit kits are very sophisticated. They search for versions of IE and Firefox that have not been updated. This is one place where IT can make a difference by ensuring that end users are not working with older versions of browsers or unpatched versions that leave the door open for hackers.

"They're preying on IT departments being really swamped in terms of putting out day to day fires and maybe they're behind on their patching," Mimoso said. "They're preying on the thirst that consumers have for the latest and greatest mobile app. Especially in the Android ecosystem there's a lot of opportunity there to push malicious apps onto websites. It's really hard getting them into Google Play but given the way the ecosystem is you can grab an app for Android anywhere, so the risk is a lot higher to get infected that way."

THE DEFENSE CAN NEVER REST

In the current malware world, IT can never let down its guard. This requires a defense

in depth strategy, which is basically working to protect everything you have from anything a criminal organization might do. In reality this is impossible to do to the point that your system can never be hit by malware. But it is important to make your infrastructure as hard a target as possible.

So where do you start?

PATCHES

"Patching is super important," argues Kaspersky Lab's Mimoso. He points out that many of the vulnerabilities are in third-party apps that are running on almost every endpoint. So it is critical that you not only patch operating systems and web browsers but also apps using Adobe or Java software.

ATTACHMENTS

To protect against malware hidden in email attachments, Cavalancia suggests taking the attacker's perspective.

"Look at the attachments," he told the webcast audience. "See if the attachments are going to try and run on the endpoints. And follow that along and in reality you have to take a layered approach, a defense in depth approach. The reason for that is, again taking the attacker's perspective, thinking about this as a business, they can't test against a layered approach. Let's say you have a myriad of protections in place, they aren't going to put all that in place and then test their malware against that environment to see if they can get through. They don't bother. It's not worth the effort. It's better just to go, you know what, here's a wide range. Send an email out to everyone on a given list and see what hits. But they can't test against a layered approach."

BACKUPS

Backups are important but for true defense in depth you need to back up more than just the files on your servers and users' endpoints.

"I need to have a backup of Active Directory," Cavalancia said. "I need to be able to recover that. I mean backups of everything. Because at some point there may be such a breach you're not actually certain what's been screwed up. One of the tactics if someone gets access to Active Directory is to make tons of accounts, so that way they create persistence. If you delete one account, there's another one."

BACKUPS ARE IMPORTANT BUT FOR TRUE DEFENSE IN DEPTH YOU NEED TO BACK UP MORE THAN JUST THE FILES ON YOUR SERVERS AND USERS' ENDPOINTS. —**NICK CAVALANCIA**

ENCRYPTION

Make sure you add encryption to your defense in depth strategy.

"In all the discussion around privacy and keeping communications secure between parties, I think encryption is a

vital part of that," said Mimoso. "If you're firing up an ecommerce site and you're going to be taking in credit cards or personal information of any kind, if you are collecting personal information from customers, I think you're negligent these days if you're not encrypting that traffic. If you aren't encrypting the network channel that you're communicating over, between your customers and your infrastructure, I think you're negligent if you're not encrypting that. Do you want to encrypt email conversations? Do you want to provide secure messaging for your remote workforce? There are a lot of interesting secure messaging apps out there where there's end-to-end encryption across the whole communication channel between two parties. It's expensive, but it's not as hard as it used to be to implement. There's a lot to consider, there's key management, there's a lot that goes with it, but it's definitely not a luxury any more. It's going to be part of a ground floor, defense in depth conversation.

"IF YOU AREN'T ENCRYPTING THE NETWORK CHANNEL THAT YOU'RE COMMUNICATING OVER, BETWEEN YOUR CUSTOMERS AND YOUR INFRASTRUCTURE, I THINK YOU'RE NEGLIGENT." —**MICHAEL MIMOSO**

KASPERSKY LAB ENTERPRISE PROTECTION

To help you protect against the wide range of threats, Kaspersky Lab offers security solutions and services including:

- Kaspersky Endpoint Security for Business: Integrated protection against known, unknown and advanced threats
- Kaspersky Anti-Targeted Attack: Defending against targeted attacks and advanced threats
- Kaspersky Security for Data Centers: A perfectly balanced combination of protection and performance for hybrid data centers
- Kaspersky Virtualization Security: The only security solution you need -- whatever your virtual environment
- Kaspersky DDoS Protection: Total defense against all types of Distributed Denial of Service (DDoS) attacks
- Kaspersky Fraud Prevention: Reduction of fraud risk for online and mobile financial transactions
- Kaspersky Security for Mobile: Advanced security, management and control for smartphones and tablets
- Kaspersky Security Intelligence Services: World leading threat intelligence, expert services and security training.
- Kaspersky Industrial CyberSecurity: Specialized protection for industrial control systems

For more information, visit usa.kaspersky.com

KASPERSKY lab