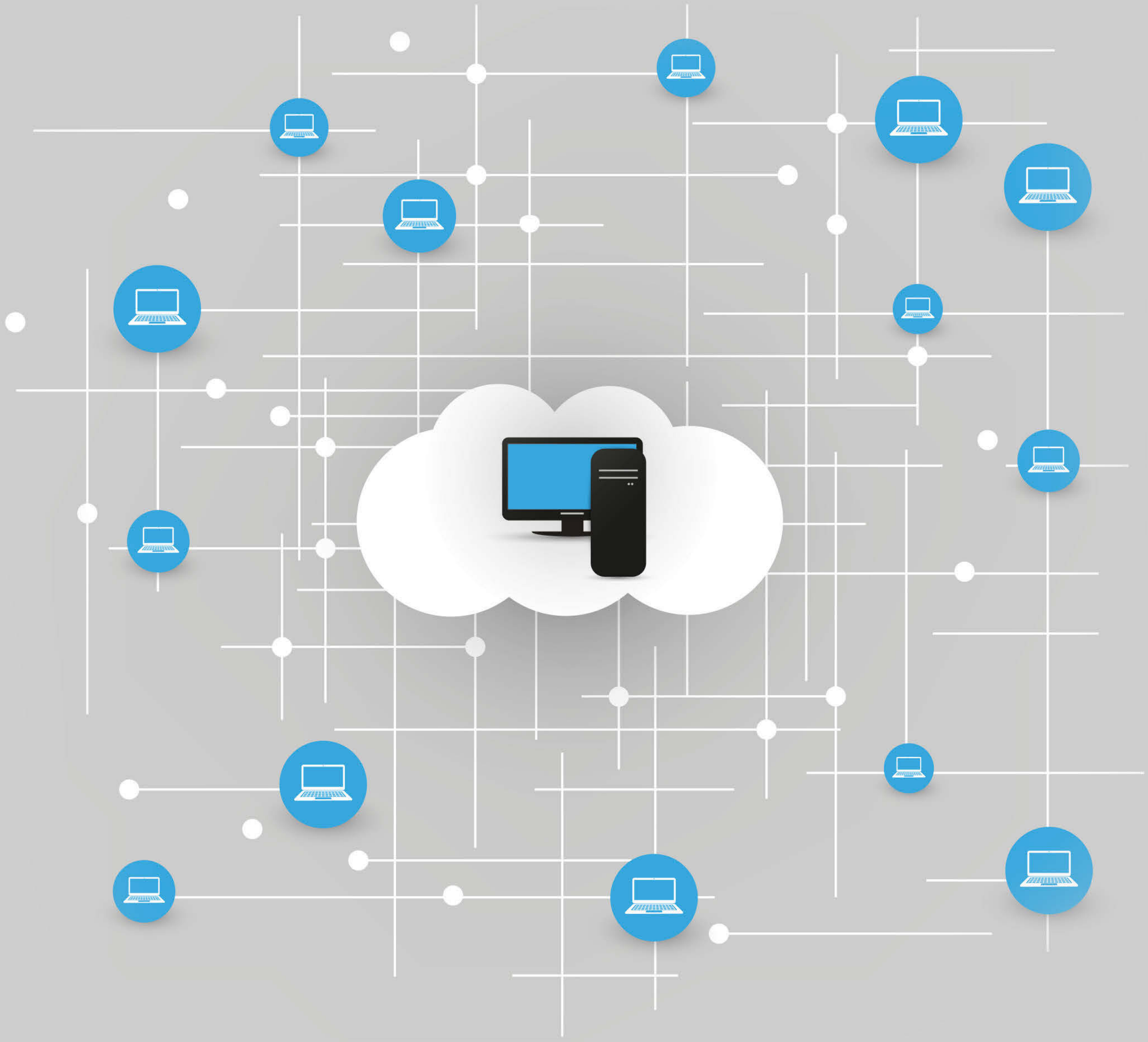
The Sorry State of Endpoint Security

Dan Schiappa of Sophos on Why Ransomware Defeats Current Defenses



iSMG
INFORMATION SECURITY
MEDIA GROUP

SOPHOS

Sophos X Intercept

Tom Field: Now, Dan, you've just released the results of a new state of endpoint security today's study. Can you share with me some of the highlights of that research?

Dan Schiappa: Yeah. It's a really fascinating piece of research. And to some degree you look at the stats and you just get wowed by them. The highlights are this simple. Companies are still getting hit by ransomware. It is still a very, very big issue. When you start to dig into the details of how they get hit [and] why they got hit, what you start to learn is that they don't really fully understand all the different approaches that hackers take to have successful ransomware attacks.

For example, 54 percent of all the organizations we polled were hit by ransomware. A vast majority were hit by ransomware twice. That's a pretty big number and it's a pretty telling stat.

And furthermore, when you dig in a little bit deeper – a lot of these ransomware attacks that we've seen – the entry points were exploits. So 54 percent of those organizations feel that they're really open to attack by way of exploit. And so they don't have the proper exploit protections in place. And that really makes a lot of sense when you hear the next stat, which is that 69 percent of organizations don't really understand anti-exploit technology and what the risks are. They don't understand the difference between a malware attack and an exploit attack. And that's one of the ways that leads them into this.

And when we talk further about that, 77 percent of them were actually using traditional end point companies, fully up-to-date, and they were still hacked and had successful ransomware attacks launched against them, because, primarily, those were through exploits and they didn't have proper protection.

Ransomware: Myths and Realities

Field: Dan, let's focus for a moment on ransomware. What are some of the myths and realities that you've uncovered?

Schiappa: So I think that the myth is that people are protected with some of the off-the-shelf technology they've been using for many years, regardless of how up-to-date it may be. What's happening is these ransomware attacks are very sophisticated – they're leveraging exploits. Many of them are coming from these ransomware services. And what happens with entrepreneurial hackers is they have to have effective technology in perpetrating an attack, or the people aren't going to pay those subscription fees to get access to that technology.

So you're getting a lot of polymorphic, high-entropy, exploit-based ransomware attacks. And some of those traditional technologies just don't protect against them. Yet some of these companies sit back and think that they're in pretty good shape and have the right protective measures.

Endpoint Security Controls

Field: Dan, specifically, what did you learn about the endpoint security controls that many organizations are employing now?

Schiappa: I think they're not as effective as they hope. When you have 54 percent of people being attacked by ransomware, and a big chunk of that being attacked twice, they just don't have the effective technology. And part of it is the lack of understanding of things like exploits and how to protect against exploits. And so I think what we've learned is you have to really go out with a solution that's going to provide broad coverage against the various types of attacks.

And [it is] something that is much more predictive than reactive. In the previous world of security, you had reactive technologies. You saw an attack somewhere, you built a defense to hope that you could block it should that same attack happen again.

That doesn't happen anymore, and you have to be predictive. You have to build technologies that are out in front of what the hackers may do next – so understanding what types of techniques hackers would use to exploit a vulnerability. Understanding what types of malware may come your way by using things like artificial intelligence and deep learning. That's really what customers need to be focused on.

Concerns About Endpoint Security Defenses

Field: Dan, giving what you've shared with me, what most concerns you about endpoint security defenses as we proceed in 2018?

Schiappa: I think the key thing is, as an industry, and as a person who would buy from a vendor, you have to find companies who are doing relentless innovation. Innovation is super critical, because what we're up against now is capitalistic hackers. Right? With these servers ... And, obviously, just ransomware in and of itself is hacking for profit.

And that changes the game completely. When you're doing hacking for profit, you're only going to make profit if you're effective. And so whether I'm offering a service to other hackers or I'm a hacker myself, if I have something that's not effective, then I'm not going to make money. And so as a result, they're going to do lots and lots of innovation. And they're taking that innovation and putting it in the hands of lots and lots of hackers.

So as an industry, we have to be in this relentless innovation mode where we just have to keep moving forward and moving forward. And we have to do it in a way that's building technologies that are focused on predictive measures and not reactive [measures].

Anti-Ransomware, Anti-Exploit, Deep Learning

Field: Now what concerns do you have about organizations' understanding of anti-ransomware, anti-exploit, and deep learning technology?

Schiappa: I think the biggest fear I have is that people don't understand how best to test and ensure that what they're using and what they're buying matches the marketing. And it's a very, very difficult thing. Every endpoint vendor out there is going to talk about how they're super effective against ransomware and all these advanced attacks. But the proof has to be in the pudding. You have to be able to prove it in the real world. And that's a very difficult thing for a lot of vendors to do.

So we recommend several things. One is look at the public tests. I think that's a very good way to gauge the effectiveness of products. And we won't see all the vendors in the community in those public tests, but I think it's still a good measuring stick to do that.

There's also ways to test these things yourself in a safe environment. So pretty shortly we'll be publishing a cookbook where we actually walk you through the various steps of how to do this testing in your own environment in a safe way.

And then, in the worst case, reach out to some of the testing organizations who will do a private test for you. If you have some specific needs or you want to test some very specific things that are maybe unique to your environment, then they're more than happy to go out and do these tests for you.

So for me, it's really go out and make sure that what you're seeing on the marketing side is married to what goes in the real world.

New Features of Sophos X Intercept

Field: Dan, you're introducing a new version of Sophos Intercept X. How will the new features help organizations to get a better handle on exploits and ransomware [and] at the same time improve endpoint protection overall?

Schiappa: So we focused primarily on the predictive, so we wanted to cover three key areas.

One is protection – specifically against ransomware. So we look at the behaviors of malicious code that is executing a ransomware attack. And we try and predict what type of behaviors they would provide and jump in front of [them]. So, for example, when the WannaCry outbreak happened, we blocked all the ransomware attacks for any customer using Intercept X – same with Petya. In that case, we blocked the exploit, which was a boot loader exploit.

And so that's the next step. There are about 27 different techniques that hackers can use to exploit any vulnerability in any product. There are things like stack pivots and code. What we saw with WannaCry were the asynchronous procedures called exploits. And so what we do is we build protections against those techniques. So we don't scan malware, we don't ever have to have seen a piece of code or an exploit ever before. We just know that those are the different types of techniques that hackers use to exploit a vulnerability.

And then the last piece – the introduction of deep learning - neural networking. So this is the form of machine learning that's really the most advanced form out there in the cybersecurity space, where we're actually using a collection of independent neurons that, frankly, operate a lot like the human brain. And so that makes it much, much smarter and gives it a larger opportunity to train with large data sets, which is really important with any machine learning, to be able to train data sets. And so that gives us the opportunity now when we see a malicious portable executable file to be predictive and not have to have seen that file, even that family, of attacks before. And we can kind of build a model that will work out for things that, frankly, haven't been written yet.

And so that's what we're focused on, is this predictive nature across ransomware, exploit protection and deep learning.