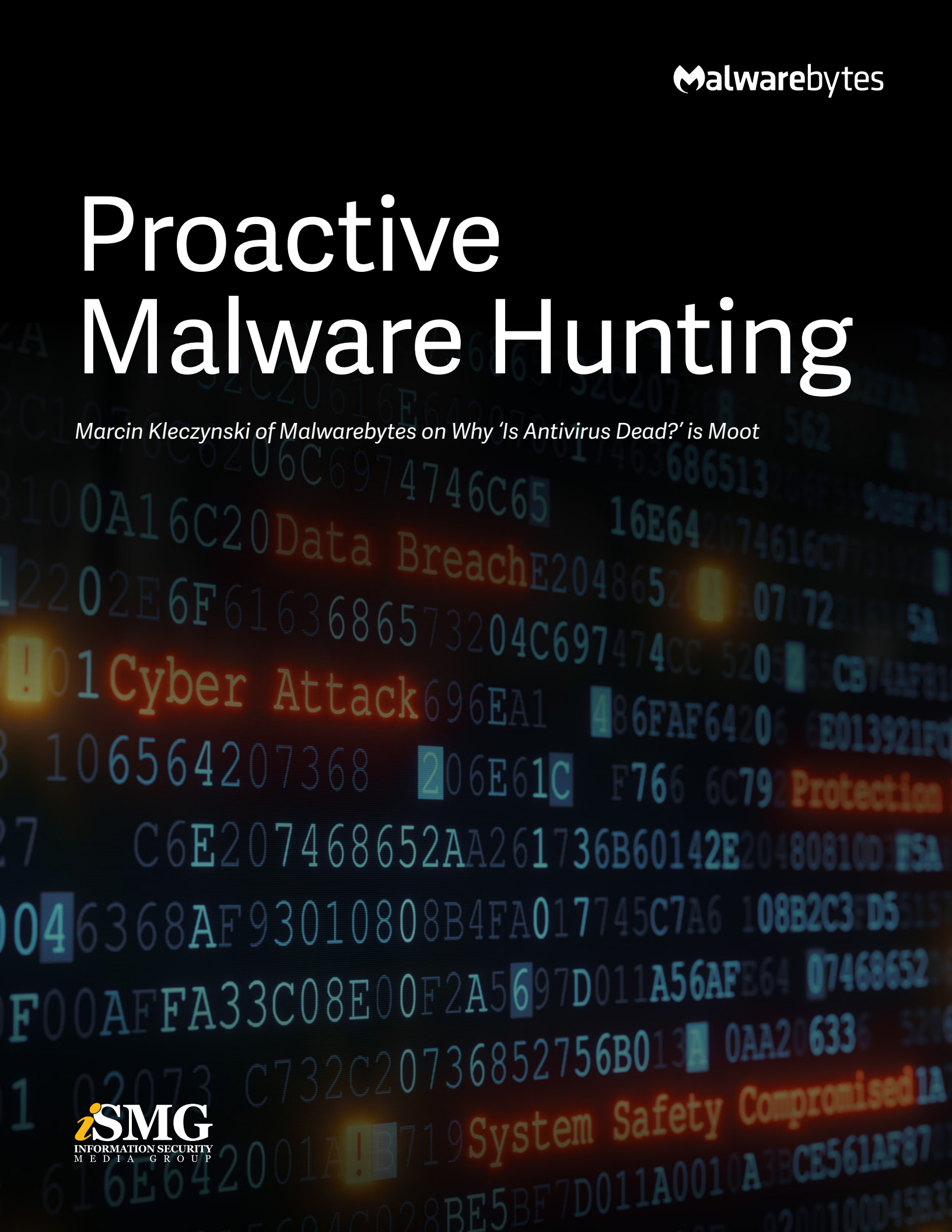
Malwarebytes

Proactive Malware Hunting

Marcin Kleczynski of Malwarebytes on Why 'Is Antivirus Dead?' is Moot

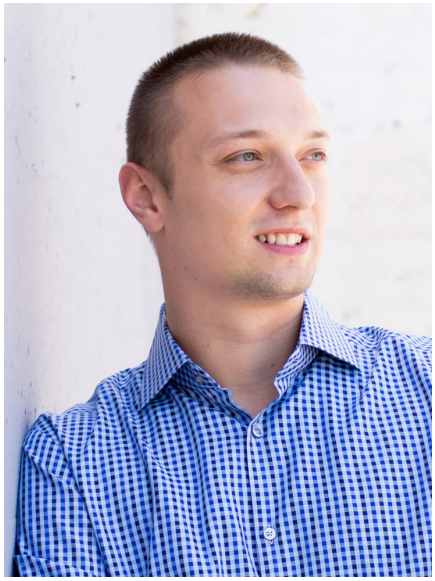


ISMG
INFORMATION SECURITY
MEDIA GROUP

Malwarebytes

Malwarebytes *provides anti-malware and anti-exploit software designed to protect businesses and consumers against malicious threats that consistently escape detection by traditional antivirus solutions. Founded in 2008, the company is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts.*

For more information, please visit us at www.malwarebytes.org.



Marcin Lleczynski

If malware infections and data breaches are inevitable, then why should organizations even try to be proactive? Isn't a reactive stance more appropriate? Not so, says Marcin Kleczynski, CEO of Malwarebytes.

"Just being reactive gives the attackers many opportunities to steal data from your environment," says Kleczynski, who also is the founder of Malwarebytes. "If you are at least somewhat proactive, you can mitigate a lot of the damage that some of these low-hanging-fruit threats can do to you."

A lot of critics - and even some security vendors - have taken to claiming "Antivirus is dead." But Kleczynski won't go quite that far.

"This is a controversial topic for me because I actually don't think 'antivirus is dead' is the right thing to be talking about," he says. "It's really: 'What kind of solutions do you need on the endpoint?' Whether it's next-generation or it's called antivirus, I don't think the typical organization cares. In the end, I think an IT administrator looking to deploy something in their environment needs to look at efficacy and efficacy alone."

In an interview about proactive malware detection, Kleczynski discusses:

- Why it's not enough to react to malware;
- The evolution of endpoint malware detection;
- Why risks of the Internet of Things are overhyped.

Kleczynski is the CEO and founder of Malwarebytes. He wrote the first piece of software for Malwarebytes in 2004 and launched the company four years later. Malwarebytes products have been downloaded over 500 million times and have removed over five billion pieces of malware. Today, Marcin leads more than 250 employees in 14 countries, overseeing the strategic expansion of the business, as well as the long-term vision for the research and development teams. Marcin is recognized as one of the leading authorities on cybersecurity and is a regular speaker at conferences around the world. In 2011, he earned his pilot's license and trains regularly to bolster his flight skills. He earned a degree in computer science from the University of Illinois at Urbana - Champaign, received the Ernst and Young Entrepreneur of the Year award in 2014, and was named to the Forbes 30 Under 30.

Why Be Proactive?

TOM FIELD: So, Marcin, if breach is inevitable, then why should organizations even attempt to be proactive? Shouldn't they just focus on being reactive to this inevitability?

MARCIN KLECZYNSKI: I think there are two sides of the coin there. The first is: Just being reactive gives many opportunities for the attacker to steal data from the environment. If you are at least somewhat proactive, you can mitigate a lot of the damage that some of these low-hanging fruit threats can do to you. So if you're able to block 99 percent of threats, you're not remediating the 99 percent of those threats that are coming in. If you're just remediating all of the time and being reactive, it's not a good story for the organization.

Is Antivirus Dead?

FIELD: Marcin, given the evolution and success of malware, especially over the past few years, is antivirus as we have defined it and as we traditionally know it effectively dead?

KLECZYNSKI: This is a very controversial topic, especially now with companies coming out and saying antivirus is dead. Even Symantec [is] saying antivirus is dead, and their biggest product is an antivirus. I think the term itself, as traditionally defined, is definitely dead. And there are

"Just being reactive gives many opportunities for the attacker to steal data from the environment."

a lot of these antivirus companies just not innovating for many years, actually. So there's been a need for advanced input protection, which I think is kind of the next term of input protection.

This is a controversial topic for me because I actually don't think that "antivirus is dead" is the right thing to be talking about. It's really "what kind of solution do you need on the endpoint?" - whether it's called next generation, whether it's called antivirus. I don't think a typical organization cares. In the end, I think an IT administrator looking to deploy something in their environment needs to look at efficacy and efficacy alone. If it's called antivirus, that's fine. If it's called next-generation input protection or antimalware, that works as well. Let's not really define terms around it, but rather "I have this product, it does its job for me, I don't have many breaches, I'm happy as an organization."

Distracted by the Headlines?

FIELD: We're constantly seeing hacks - I'm thinking of Ashley Madison, OPM. Are we as security professionals being distracted by what you might call the headline hacks and perhaps overlooking low-profile exploits that truly matter but aren't necessarily making the news?

KLECZYNSKI: I think the media does a pretty good job of covering threats. Maybe they over-blow certain types of threats - internet of things and so on. But I think they do a pretty good job, and the reason is it's a game of publicity. Of course, the first thing we do is turn to the media and say," look, we found this threat or this hack or this breach and we want you to write about it."

Now, that's really the external view. The internal view is when a company like Target or Home Depot gets hacked, the time to discovery of that hack for them traditionally has been several hundred days. In the case of certain of these companies, it's 200-plus days before they actually discover an attack that's happening on their network and maybe kind of already been stolen. So these companies have been historically pretty bad at warning the public that their information has been stolen. So there's kind of, again, two sides of the coin here. It's really who discovered the threat = was it the organization itself that was breached, or maybe they might be a little

"I actually don't think that 'antivirus is dead' is the right thing to be talking about. It's really 'what kind of solution do you need on the endpoint?'"

slow to tell the media about, you know, what happened, and of course they don't want to admit such a breach. But a security company like ours, after we responsibly disclose it, we try to gain publicity and awareness around that topic. That's the important part, awareness that your credit card was stolen.

Proactive Malware Hunting

FIELD: I want to get back to this topic of proactive malware hunting. If you take a look at the definition of it, who is actually doing the proactive hunting? And I guess not so much why are they doing it, but how are they doing it? And what are the results of this proactive hunt?

KLECZYNSKI: Well, when I started the company several years ago, remediation was a huge problem for organizations, meaning they were not able to scan their environment to see if there was malware on those computers, on those endpoints. And even today when you read the Verizon data breach report, the average time on some of these environments is 200 days. So, 200 days ago, somebody was infected in my environment - a computer in my organization was infected = and 200 days later I finally discovered it. Wow, that drill pattern is not very good, right? In 200 days, there's an attack, right? I've pretty much done my job. So there's this concept of proactive malware hunting, which is basically checking every computer in my environment as frequently as I can. Are you infected? And so with Malwarebytes, for example, we provide a malware hunting tool where you can go to every computer and look at the malware and tell if it's infected. We're really trying to bring that drill time down, which is a problem for a lot of these organizations. If the attacker has more time, they're able to do more damage. And so IT administrators are turning from this proactive mode to this reactive mode, and I think there needs to be a balance. I think there needs to be a balance in that you filter out as many threats as possible on the site and then go after the threats that may be on the reactive side. So a lot of these IT administrators are trying to figure out what's the right balance for them.

Measuring Success

FIELD: So Marcin, how do you measure the success of this? Have you been able to quantify with some of your customers if you can reduce that time to discovery?

KLECZYNSKI: There are a lot of metrics across the board that we actually look at. Of course, customer satisfaction is a big one. With a lot of the threats that we detect, it's really a positive identification. We have either, A, seen this before, we've seen this behavior before, we've seen the characteristics before. So we're able to positively identify. We don't really

identify something and say we think this is maybe malware. We really bring it kind of to them and say this is malware..

One other metric that's interesting, last year we actually cleaned up 250 million computers worldwide. Now, that's an impressive statistic because that's a lot of computers. That's also an unfortunate statistic because that's how many computers are getting infected that we see each year. So we do track our telemetry and our detection rates. We do some third-party testing as well. We look at other companies and how they do remediation and detection. A lot of them recording of the device and what's going on on that device. We actually try to identify positively a piece of malware or a threat running on a computer.

Endpoint's Changing Needs

FIELD: A few minutes ago we actually talked about the whole notion of AV is dead and how you wanted to get people thinking more about endpoint protection. In what ways do you see organizations starting to respond to changing needs in endpoint malware detection? Are they falling for the hype of AV is dead or do you see a significant and thoughtful mind shift?

KLECZYNSKI: It's a little bit of both. I definitely see companies moving to a layered security approach, a defense. So they understand that the days of trusting one antivirus provider such as Symantec or McAfee, those days are over. I don't talk to any chief internet security officers today that say all we run in our environment is Symantec; they've got 40 to 50 different tools that are used for various purposes. And I think that's where the direction of security is heading and very rapidly. The problem with this approach is a lot of these companies have gotten information overload. So they do have 30 to 40 tools, but they may not be employing those tools correctly, meaning, they haven't spent the time to actually set them up properly and configure them, which a lot of these security products need. They don't have the staff.

There's a huge type of security shortage. They don't have the staff to actually monitor a lot of these tools.

Evolution of Staff

FIELD: Marcin, you bring up a good point here. We talk about the evolution of the security tools, but we don't talk nearly enough about the evolution of security staff. In your perspective, what are some of the skills that security professionals have to bring to the table today to be effective in endpoint malware detection?

KLECZYNSKI: You know, it's very difficult to gauge that. You have somebody fresh out of college and a lot of these colleges and universities unfortunately don't have any cyber security programs. You know, when I went to the University of Illinois, didn't you have a cybersecurity program? Absolutely not. I compare the shortage of these people similar to the engineering shortage that the world faced several years ago. It took universities many years to actually build a curriculum and then another four years to bring that out. And if you're a large organization looking to hire cybersecurity staff, you're talking about hiring somebody with experience. Well, if there are no new graduates coming out of college, you're basically poaching talent. And that's why I hear some of these chief internet security officers that I talk to, they're just going back and forth with the same talent and, you know, providing higher compensation plans. So I think unfortunately because of the nature of the problem, you're looking for somebody with some type of security experience, and that's very difficult to find unless you're poaching that talent from somebody else in that same position, so it's really an endless circle. And today is the day to be a cybersecurity professional. I mean, there are just great companies to join, great pay for the job. But I think ultimately it comes down to do they have any type of security experience? You know, managing a security platform or security program in an organization in the past, I think that's what I would look for if I were to hire somebody in my organization where we need, you know, a security professional.

"I think a lot of it is still over hyped. Is my Nest thermostat looking to kill me today? Probably not."

FIELD: You make a good point there, Marcin, that there's no better time to enter the security profession. And I feel like over the past few years that security vendors, analysts, certainly the media have built this up as a place to go; there are opportunities there. I don't think we can promote this any better. Where are we falling short in bringing appropriate in to fill these positions that we have open?

KLECZYNSKI: Yeah, I wish I knew the answer to that question so I could solve some world problems here. I think a lot of the universities really do need to just sit down and put together a curriculum for security. I just reached out to my university and I said 'let me help you to do this,' you know, and they fully admit that a security program at the University of Illinois is short. They don't have professors that have security experience. And if they try to find one, another university is poaching that talent. It's very similar in the corporate world, where you have a chief finance security officer that's being actively hunted for because they've got a ton of experience and can keep their organization safe. It really -- it's not a matter of tools to keep an organization safe; that's a factor, but it's the people. You need professionals or you need people that know what they're doing and can keep the data safe in the organization.

AV Endpoint Protection

FIELD: Now, you go to the same events I do, whether it's RSA or DEFCON or Black Hat, and if you got a silver dollar for every time that someone gets up on stage and says "There are no silver bullets," you'd never need to start up another IT security company. Everyone says that: There are no silver bullets. So why do we put our trust in a single AV or endpoint protection solution?

"If you're not hunting for malware in your environment, it's hunting for you."

KLECZYNSKI: I think it's just what we were taught, right? And in 1995 or the year 2000, when you had this computer that you paid thousands of dollars for an antivirus solution, that was enough. And even today when you talk to a lot of consumers - if you talk to my mother, for example, she would think antivirus is enough. And I think that's a little bit -- you've got to learn that it's not, right? And it takes a breach to show you that it's not. A lot of these companies with their old ways are so -- their antivirus solutions fail right in front of their eyes, and they turn to an aggressive expansion where they buy several tools, never deploy half of them, and get a little lost. So I think it really takes a good security leader to come into an organization, understanding that antivirus is just not enough or one single endpoint solution is no longer enough. Just like you have several network solutions, a firewall, an IDS, you need the same on the endpoint. And in the end, the endpoint is what's getting accepted, right?

So the perimeter is falling apart. People are taking their laptops and going to coffee shops and working, and that laptop is the endpoint that gets infected. You should be putting all of your resources into that laptop, that endpoint, and subsequently that endpoint solution is what's going to need to fail to get infected. And that's really what people need to start thinking about.

IoT

FIELD: So, Marcin, the definition of endpoint has changed considerably in the past several years. A few minutes ago you mentioned the internet of things, and I think I know which side you're going to come down on this but I'm going to ask it anyway. hat about IOT? Is it over hyped or is it underestimated?

KLECZYNSKI: I think a lot of it is still over hyped. Is my Nest thermostat looking to kill me today? Probably not, right? And if an attacker gained access to it, that's concerning, but data is not getting stolen that's sensitive to me. Maybe the wi-fi password, and that's a bigger concern, but in general I think Internet of things is being a little bit over hyped. It's getting the same coverage as some of the breaches in the news that are definitely affecting people today.

You know, my mother's car is connected to the internet. Am I going to tell her to stop driving it today? Absolutely not. Will I tell her, 'hey, you need to be careful about this site and that site and, you know, deploy some kind of security solution with Malwarebytes?' Yeah, absolutely. You know, on one hand you see a [car] being hacked and a proof of concept that they were able to slow the car down or stop it at a very low speed. And then you look on the news the week before and Yahoo! was able to infect tens of millions of people

because their advertising platform was breached. So which one is really top of mind, you know? I still think that exploits and mal-advertising and visiting just a website like CNN, not having to put down anything to get infected, that's really the scary stuff for me.

Evolution of Security

FIELD: Marcin, this space has changed so much since the time that you entered the field back in 2008. How would you say that Malwarebytes is most different today than when you launched the company?

KLECZYNSKI: We've matured. We've hired a ton of staff; we're very focused on R&D, so we're spending the majority of our operating expenses on just keeping technology evolving. But what's changed the most I think is the space. When we came on the scene, we said we are going to be a layer of secure endpoints. So if you've already got security solution in your environment, that's great; we're going to work with every security solution under the sun. The perception of layered security back in 2008 was "OK, that's great, I just can't afford it. I don't need it, I've got my single antivirus, and that's going to be great." I think that perception has changed dramatically. We were a little bit ahead of our time providing a layered security. Today that is almost universally accepted as the only way to mitigate getting infected. And more so, I consider remediation or the malware hunting a layer as well because that's the layer that gets you cleaned up if something gets through, right. And if you're not hunting for malware in your environment, it's hunting for you. ■

Listen online
http://www.inforisktoday.com/interviews/proactive-malware-hunting-i-2866

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com