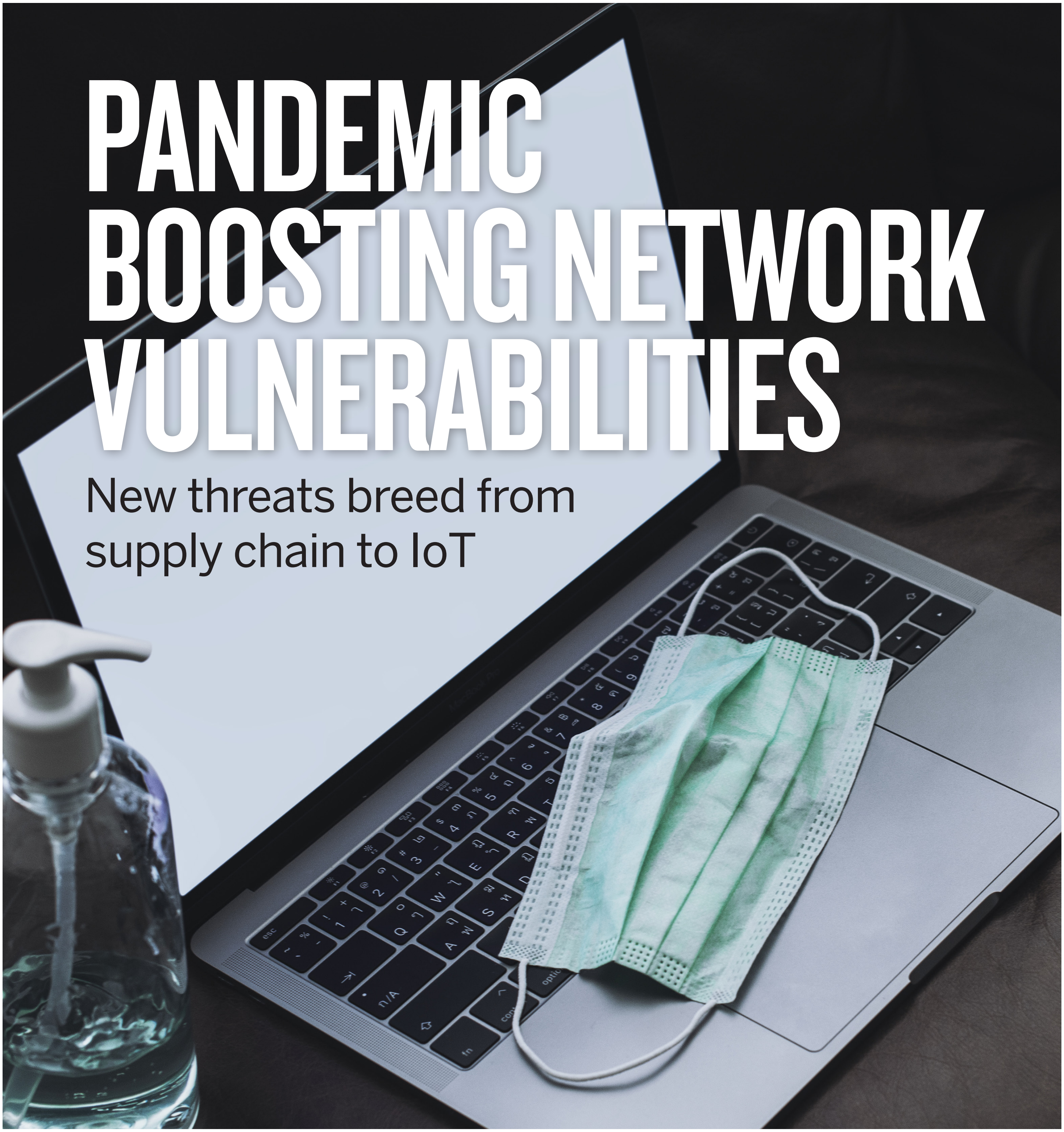

PANDEMIC BOOSTING NETWORK VULNERABILITIES

New threats breed from supply chain to IoT

ebook
An SC Media publication

Sponsored by
VULCAN™

Data, supply chain drives hidden network threats

Proper cyber hygiene is not enough today to stop new threats. Esther Shein unveils how to find the hidden network vulnerabilities.

In a perfect, world, cybersecurity would be easy to manage. Find a problem, then fix it. Once it is fixed, it is no longer a problem. Yet, finding and fixing security problems seems to vex so many information security pros. They get bogged down with patches then wonder if fixes will break something else. On top of that, there are faulty systems, cloud configurations and compliance regulations to consider.

Networks have all kinds of hidden vulnerabilities and sometimes even small ones can turn into disasters. The trick is knowing how to locate and fix them, even if all the obvious check boxes are ticked and you think you are secure.

That can be a tall order. Defending against hidden network vulnerabilities is a difficult job — but organizations often make it even harder when they neglect to manage their overall attack surface in a coordinated way, observes Andrew Douglas, a managing director in Deloitte's cyber and strategic risk practice based in Park City, Utah.

OUR EXPERTS: Network vulnerabilities

Doug Barbin, principal, Schellman & Co.

Kevin Bong, director of cybersecurity, Sikich LLP

Andrew Douglas, managing director cyber and strategic risk practice, Deloitte

Patricia Luxton, senior vice president of engineering services, Kelser Corp.

Patricia Titus, chief privacy and information security officer, Markel

While managing operational tasks — such as patching — it can be nearly impossible for IT professionals to identify and address vulnerabilities, Douglas says.

Additionally, adds Doug Barbin, principal of Schellman & Co., a Tampa-based independent cybersecurity and compliance firm, "There's inertia on the patching side and the same applies to network configuration and management."

Windows, cloud woes

Lack of rigorous firewalls and VPN appliance patch management is a greater risk than most organizations realize, says Kevin Bong, director of cybersecurity for Sikich LLP, an accounting firm in Naperville, IL. "While IT teams are often diligent with Windows patches, it is common for teams to only apply firewall patches for new features or performance issues, or when a firewall vulnerability is so bad it makes the news," he says.

Even if your Windows environment is fully patched, there are a lot of built-in weaknesses in Microsoft operating systems and networking protocols that put your network always at risk, Bong says.

Attacks against other built-in weaknesses have recently emerged. Kerberoasting attacks, where the attackers abuse traits of the Kerberos protocol to steal password hashes for Active Directory and service account passwords, make use of weaknesses in Windows encryption algorithms and authentication protocols, he says. Golden ticket attacks allow an attacker to retain complete administrative control over a Windows domain even if all domain admin passwords are changed, he adds.

"Once they've authenticated to a system, attackers don't need to use malware or viruses to perform successful attacks," he says. Instead, to bypass antivirus programs, attackers often deploy a technique called "living off the land," where they use "trusted binaries, scripting languages and other

86%

Percentage of companies using tape that believe it is critical or important to meet compliance requirements

– ESG

tools already built into default Windows installations to create backdoors, log keystrokes, steal secrets from system memory and establish command and control channels."

There are other issues at play, such as an attack surface that much broader than before, with complex applications that could be residing in more than one cloud surface, Barbin says. "It's not enough to put something in a cloud service and say, 'It's in Amazon, I don't have to worry anymore,'" when in fact, "you have full [security] control over what you put [in the cloud]."

Doug Barbin, principal, Schellman & Co.

Amazon Web Services (AWS) has responsibility for its own security, he says, but it is the customer who puts the passwords on the servers and sets up the network and authentication to secure cloud-based data.

As far as Barbin is concerned, cloud sprawl is the top cause of undetected network vulnerabilities. "Due to the nature of cloud services, it's easy for anyone in the organization" to procure them, he says. Even when a cloud service is being used in a legitimate manner, it is not being tracked by IT.

Pandemic pressures

When the pandemic forced organizations' employees to start working remotely in March 2020, that increased networks' footprints also left many of them more vulnerable due to the increased surface attack area and exponentially greater potential threats.

"You used to have everyone contained in the office and able to easily transfer information, and that was protected by a firewall … and now, all of a sudden, the entire workforce in many cases, is working from home," says Patty Luxton, senior vice president of engineering services at Kelser Corp., an IT managed services provider based in Glastonbury, CT. "So now you have introduced new endpoints in environments that can be exposed to home networks."

A child who might be playing games in the basement innocently is now potentially an unwitting hacker, she says. The initial reaction IT had was to get employees set up on VPNs and use multifactor authentication (MFA) to have them sign in, Luxton says.

"Sometimes, that's as far as it goes. Now, anything that goes on on the home network has unfettered access to the office environment." Couple that with layoffs and fewer network administrators, and sometimes corners get cut, she says. "It's a lot for … corporations to manage."

Stress and the pressure to perform under a COVID lockdown creates errors, agrees Patricia Titus, chief privacy and information security officer at Markel Corp., in Richmond, Va.

"Plus, there are less 'water cooler' conversations happening so you can't bounce your ideas or deployments in a casual setting, like at a bar with your engineering buddies," Titus says. "They used to be able to help you see all sides of the equation, but now we are more single-threaded, which equals single point of failure."

> "You have full [security] control over what you put [in the cloud]."
>
> – *Doug Barbin, principal, Schellman & Co.*

These days, everyone is also deluged with emails and meetings, so the communications team mainly issues company emails "for only vital corporate communications, shooing

28%

Insider threat cyberattacks accounted for 28% of DDoS attacks in 2020

– Verizon

away the security team," Titus adds. "Even the coveted intranet site is under close hold for more mental health messaging or positive messaging, and let's face it, security is not a feel-good message all the time."

Douglas echoes the sentiment that critical communication is lacking. "The assumption of [having] strategic coordination across IT is a frequent blind spot for CISOs," he says. "Although most IT professionals within any organization share information on things like cyber vulnerabilities, that communication alone doesn't always lead to the type of collaborative, proactive improvements and overall governance that truly reduce attack surface risk."

Patricia Titus, chief privacy and information security officer, Markel

IT might focus more on "large volumes of low-priority issues instead of fixing basic cyber hygiene measures that can offer big wins later," Douglas says.

Dark shadows

Another hidden vulnerability is shadow IT, or perhaps today, it is shadow IT 3.0. And it is getting easier to implement the technology, Titus says. Employees working from home often do not think twice about buying a Software-as-a-Service (SaaS) product they think will help them do something better, but instead of going through global procurement, they put it on their credit card. Such a service could include cloud storage, cloud security or a cloud-based application.

"Part of the problem is wrangling in people … who are actually creating network vulnerabilities and issues; people who want to connect in through a remote desktop protocol," Titus says, noting that the remote desktop protocol (RDP) was how the water company in Florida was breached.

"The shadow IT piece is fundamental and it's hard, especially now in a world with APIs (application programming interfaces) where they're connecting to your environment," she says. "You have to know where the APIs are and that can create hidden vulnerabilities if you're not securing them."

For example, if an API is reverse engineered, she says, "I could figure out how to get in via a backdoor. So, there's so much complexity to network vulnerabilities. The more simplified our technologies are the more complicated it becomes to secure them because you don't know all the tools your people are using."

Schellman's Barbin concurs, saying "cloudy, shadow IT" is an increasing problem. Collaboration has become more important than ever in a remote world, and someone might download a project management tool and start uploading attachments. "The next thing you know, you could be sharing sensitive documents in this collaborative app," he says. "Now, company data is sitting in this other cloud service."

> "The assumption of [having] strategic coordination across IT is a frequent blind spot for CISOs."
>
> *– Andrew Douglas, managing director cyber and strategic risk practice, Deloitte*

Whereas people used to go to a website and download software and run it locally, now that software sits elsewhere, he says, "and by nature of that, any data that interacts with that software is potentially shared elsewhere, too."

Analytics is often touted as the be all end all,

20B

An estimated 20.4 billion IoT devices were expected to exist by the end of 2020

– Gartner

and IT executives tend to think more is better when it comes to collecting data on network traffic and users. But collecting that data without some care and foresight can create new vulnerabilities, and crash the network, says Luxton.

Kevin Bong, director of cybersecurity, Sikich LLP

Data a double-edged sword

"I encountered a network not too long ago that had an SNMP with the settings cranked up so high the network performance was horrendous," Luxton recalls. "The network had wireless controllers managing thousands of access points and these controllers would fail with the CPU running up to 100 percent."

IT would reboot them, and they would be okay at first, but fail again before long, she says. "Like many Fortune 500 companies, those in charge of network management and analytics were on a different team from those that run the infrastructure, and communication wasn't as good as it should have been," Luxton says. "Eventually, we learned there were probes set up that were requesting gobs of data once per minute. These one-minute increments were compounding, and the controllers just couldn't keep up."

> "The more simplified our technologies are the more complicated it becomes to secure them because you don't know all the tools your people are using."
>
> *– Patricia Titus, chief privacy and information security officer, Markel*

A full report every single minute from your gateways is not required to achieve adequate network data for cybersecurity monitoring, she says.

The more granular you get with the data you're harvesting, the more stress it puts on the network.

While this might be perceived as more of a major bottleneck issue than a hidden vulnerability, Luxton says that when you are not paying attention to performance issues, hackers can swoop in.

"One of the things hackers can do to wreak havoc on a network is make it not available," she says. That can create a vulnerability as well. "Our main objective is to keep networks [protected] whether vulnerabilities come from hackers or inside, due to poor configuration."

Another potential CISO blind spot for hidden network vulnerabilities is in cyber risk assessment, according to Deloitte's Douglas. "When leaders outside of IT mistrust in the data, analyses or updates CISOs provide, enterprise risk exposures may be lurking."

As such, CISOs who develop, monitor and remediate against a "living" list of cyberrisks that changes as the threat landscape or bad actors do, are often viewed more favorably by their other peers in leadership positions, Douglas says.

"Just as strategic coordination across IT can be a blind spot for some CISOs, improper engagement with teams outside of tech can also result in hidden network vulnerabilities," he notes.

Asset management, cloud security, endpoint security, patching, traditional vulnerability management, application security and operational technology (OT) should be coordinated so that all users are providing feedback to identify vulnerabilities, Douglas says.

Building reference architectures and attack surface service models that encompass these capabilities can help CISOs effectively crowdsource the identification, monitoring and remediation of cyber threats, he says.

16

Some 16 DDoS attacks took place every 60 seconds in 2020 with rates reaching 622 Gbps

– ZDNet

Is your supply chain a risk?

Since it can be tricky to configure controls manually, you might be tempted to outsource data collection, Luxton says. If that is the case, be sure to vet a network analytics vendor "extremely well" because you must provide them with full network access, she advises.

"I have absolutely seen environments where an analytics vendor led to a third-party data breach," she says. "Often, the analytics vendor was added without too much thought." IT might be thinking, "'Oh, we'll get more data? More data is good. Let's do it,'" she says. In reality, "there wasn't any thought given to the increased risk of a new vendor in the network."

Patricia Luxton, senior vice president of engineering services, Kelser Corp.

Sometimes IT executives are not clear about the problem they are solving and rush into a potential situation without fulling understanding it, Luxton says. If you think more network data can be useful to you and your team, there are several questions to consider before your team acts, she says. Among them is one of the most important when it comes to hidden network vulnerabilities: Is the value of the data we are going to get outweighed by the potential risk of adding an analytics vendor?

> "It's great you got it set up, but did you put in proper security access controls to only give specific access? Otherwise, by default, it will be left open."
>
> *– Patricia Luxton, senior vice president of engineering services, Kelser Corp.*

Luxton makes no bones about her wariness of third-party vendors. "I think we're becoming such an outsourced and cloud-sourced industry," for reasons including cost and staffing, that IT sometimes acts too quickly, she says.

"We don't think about the fact that, every time we add a third-party tool, we give [them] access to our network and that creates a threat vector. So, I'm wary."

An effective vetting includes getting recommendations from peers, as well as references, and asking pointed questions such as how the vendor's infrastructure is set up, what have they done to ensure it is secure, are they security operations center (SOC) compliant and do they have clients in highly regulated industries, she says.

"If a vendor is held to compliance-driven standards, they're more likely to have security best practices in their environment," she explains.

Luxton also advises making sure third parties are confined to only the network area to which they need access. It is also a good idea for IT to ask what specific network data the vendors need to solve the challenge the organization is facing or to accomplish a specific objective, she adds.

You do that by being very precise about your requirements and the problem you are trying to solve, Luxton says. For example, if you are trying to solve a capacity issue, there are specific analytics that address network capacity, she says.

"Many third-party companies have so much data and it can be mind-numbing, and you can get really lost in it," she says. "I've seen people sitting in a meeting with a vendor and the vendor is doing their dog-and-pony show and it looks really good." IT hears about "all the shiny things we can do when really, we haven't taken a step back

67%

U.K. respondents who said they were more worried about cyber-related losses in 2020 than they were in 2017

– Mactavish

and asked what do we want to collect? If you don’t know, it’s a little scary having the vendor tell you.”

What you must do

Luxton believes a more diligence can go a long way. Often, she will see a network engineer get a server set up or a cloud app working and then stop there.

Andrew Douglas, managing director cyber and strategic risk practice, Deloitte

“I would like to see a little more diligence beyond that because it’s not enough that it’s working, but that it’s secure,” she says. That means taking some extra steps to figure out how an app is used, or what access do people need on the VPN, or how IT should configure a server.

“We need to tighten access,” Luxton says. “It’s great you got it set up, but did you put in proper security access controls to only give specific access? Otherwise, by default, it will be left open.”

Data visualization tools also need to be implemented more frequently, security experts say. Use of them can provide insights such as detection and visualization of thread injections, correlation of network activities and the causing processes and activity timelines.

> “While IT teams are often diligent with Windows patches, it is common for teams to only apply firewall patches for new features or performance issues, or when a firewall vulnerability is so bad it makes the news.”
>
> *– Kevin Bong, director of cybersecurity, Sikich LLP*

Without proper visualization of data from multiple sources of threat intelligence, even the savviest of defenders are missing critical vulnerabilities and attack vectors in their environments, experts say. A top-view-down approach to network and security data visualization, through automated tool integration, can only strengthen an organization’s secure identity by quickly discovering critical information.

Titus believes some vulnerabilities can be alleviated simply by tightening up contracts and ensuring they have right language. If a contract includes language like “I have DDoS security,” a CISO might assume the provider is offering it up, unless they ask enough detailed follow-up questions to be sure.

“That’s when you get a distributed denial of service attack usually coming out of one or two IP locations, and you can sinkhole it,” but if the DDoS is coming at you from multiple places, your sinkhole cannot keep up with it, Titus notes.

Today, DDoS and ransomware attacks are starting to come together, she says. “First, you get the DDoS that distracts everyone, but it has already been in your environment and encrypting all your data. And then you get an email saying, ‘Send me bitcoin and I’ll unencrypt your data.’ It’s the age-old attack from one side but they’re attacking from behind. It’s the art of warfare.”

Titus finds herself concerned that sometimes she is too trusting and “I may not have done a good job of the verification piece. That’s the part most CISOs come to — I asked a question and was told the answer, and I believed the answer, but I didn’t go back and ask more detailed questions.”

Everyone is busy and wants to believe the person they are asking questions to is competent and knows the answers, she says.

78%

Respondent firms now report using some form of public cloud infrastructure, up from 67% in 2020

– ESG

"But often, when we're in a rush, we're not using our best communication skills and asking the question we think we're asking."

IT and security officials must take time to focus and block out an hour or two to catch up and do some reading, she says. In today's Zoom-crazed world, meetings can be back-to-back and there is no time for that. "You have to create time to do it and teach people to respect your schedule."

It is also important to challenge the status quo and be inquisitive, Titus says. "Oftentimes, as CISOs, we get complacent that our team knows everything, and our job is to continue to challenge them and stretch their thinking.

"As a CISO, it's in how you ask questions so you're not putting a person on the defensive," she says. One way to ask is "Why aren't we looking at this data? Where is all the telemetry coming from? Help me understand better where our gaps are."

If the questions are not asked, typically, people will not offer up the information, she says, especially because security people tend to be introverted to begin with. "At the end of the day," Titus says, "all the tech you throw at the network isn't going to solve the fact that there are humans at the other end." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

10 yrs

Nigerian (not a prince) national's U.S. prison sentence in for at least $11 million in victim losses in BEC attacks

– FBI

Sponsor

VULCAN™

At Vulcan Cyber we're changing the way businesses reduce cyber risk through vulnerability remediation orchestration. We help security and IT teams go beyond remedial vulnerability management to help them drive vulnerability remediation outcomes. From scan to fix, Vulcan Cyber delivers the unique ability to orchestrate the entire vulnerability remediation process to GET FIX DONE at scale.

More information is available at vulcan.io

Masthead

EDITORIAL
SPECIAL PROJECTS EDITORIAL DIRECTOR
Stephen Lawton
stephen.lawton@cyberriskalliance.com
SPECIAL PROJECTS COORDINATOR
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*

So many vulnerabilities. So little time.

Get fix done.

VULCAN CYBER VULNERABILITY REMEDIATION ORCHESTRATION.

VULCAN™