Inspired eLearning
November 2021 Newsletter

Photo by Jopwell from Pexels

Have You Read the 2021 PhishProof Report?

With 2022 upon us, we're still considering the lessons learned in 2019 and 2020. The game hasn't changed, but the players are getting smarter. If you haven't yet read Phishing Prevention 2021, now's the time! Take advantage of phishing prevention tips you can implement today!

LEARN MORE

Review Our Course Catalog and Plan Your 2022 Schedule

Inspired eLearning's award-winning courses will help your team to gain confidence in their ability to detect and avoid malicious threats through the Security Awareness Training Program. That's not all we offer, though. Contact sales to learn more about our full catalog!

LEARN MORE

IRANIAN HACKERS EXPLOITING MICROSOFT, FORTINET VULNERABILITIES: FEDS

'The FBI and CISA have observed Iranian government-sponsored APT actors leverage Microsoft Exchange and Fortinet vulnerabilities to target a broad range of victims across multiple critical infrastructure sectors,' officials said Wednesday. By Michael Novinson

Iranian hackers have exploited Fortinet and Microsoft Exchange ProxyShell vulnerabilities to gain initial access to systems in advance of follow-on attacks like ransomware, officials said.
An advanced persistent threat (APT) group associated with the government of Iran has been capitalizing on the Fortinet flaws since at least March and the Microsoft flaw since at least October, according to a joint cybersecurity advisory from the FBI, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre, and the United Kingdom's National Cyber Security Centre.

"Since at least March 2021, the FBI and CISA have observed Iranian government-sponsored APT actors leverage Microsoft Exchange and Fortinet vulnerabilities to target a broad range of victims across multiple critical infrastructure sectors in furtherance of malicious activities," officials wrote in a 10-page advisory issued Wednesday.
Neither Fortinet nor Microsoft immediately responded to CRN requests for comment.
The APT group has targeted victims across the U.S. transportation, healthcare and public health sectors as well as Australian organizations, though officials said the hackers are more focused on

exploiting known vulnerabilities than targeting specific sectors. Access gained via Microsoft or Fortinet can be leveraged for follow-on operations like data exfiltration, data encryption, ransomware, or extortion.

Iranian hackers were observed in March scanning devices and ports for three different Fortinet FortiOS vulnerabilities, which officials said were likely exploited to gain access to vulnerable networks. Then in May, officials said the APT group exploited a FortiGate firewall to access a webserver hosting the domain for a U.S. municipal government, creating an account to further enable malicious activity.

Then in June, officials said the hackers took advantage of a FortiGate firewall to access environmental control networks associated with a U.S.-based hospital specializing in healthcare for children. The APT group likely leveraged a server associated with the Iranian government to enable further malicious activity against the hospital's network, according to the joint cybersecurity advisory.

The Microsoft Exchange ProxyShell vulnerability, meanwhile, was leveraged in the U.S. in October 2021 and in Australia at an unspecified time to gain initial access to systems. The hackers used a combination of malicious and legitimate tools to carry out the attack, including Mimikatz for credential theft, WinPEAS for privilege escalation, WinRAR for archiving collected data, and FileZilla for transferring files.

The APT group also established new user accounts on domain controllers, servers, workstations, and active directories, some of which were intentionally created to look similar to other existing accounts on the network, officials said. Hackers forced BitLocker activation on host networks to encrypt data, and threatening notes with ransom demands were sent to the victim or left on their network as a .txt file.

Officials encouraged organizations to investigate exposed Microsoft Exchange servers for compromise regardless of patching status and probe changes to remote desktop protocol, firewall, and Windows remote management configurations that might have allowed attackers to maintain persistent access. Antivirus logs should be examined for indications they were unexpectedly turned off, officials said.

The joint cybersecurity advisory also urged organizations to review domain controllers, servers, workstations and active directories for new or unrecognized user accounts. Finally, organizations were directed to review task scheduler for unrecognized scheduled tasks as well as manually review operating-system defined or recognized scheduled tasks for unrecognized actions.

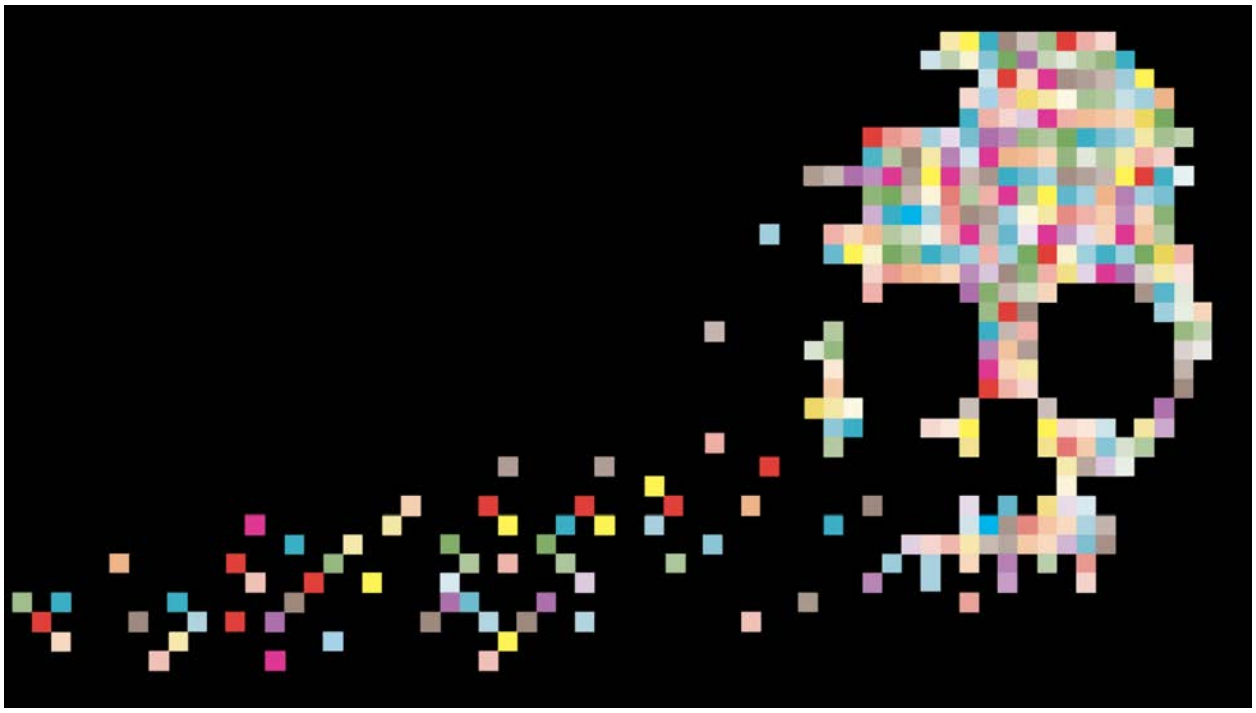
More broadly, officials said organizations not using Fortinet's FortiOS should blacklist the key artifact files used by FortiOS to ensure that any attempts to install or run FortiOS and its associated files are prevented. Businesses are also urged to immediately patch software affected by the three Fortinet and one Microsoft vulnerability identified in Wednesday's joint cybersecurity advisory.

This article was originally posted by CRN.com. Read the full article here.

HOW TO PROTECT YOURSELF FROM RANSOMWARE ATTACKS, ACCORDING TO CYBERSECURITY EXPERTS AND VICTIMS

If the hackers can get to your data, they can destroy your business. Here's how not to become a victim.

Every 11 seconds, business servers--even small-business servers--are infiltrated by hackers who encrypt their data and hold it hostage, according to Cybersecurity Ventures. Victims have few good options: You can pay the ransom, which might run into millions of dollars, but your data--and your reputation--might be beyond repair. Backups may save you, but you could lose weeks rebuilding, and your attackers may leak sensitive information in the meantime. Here, founders who have been hacked, along with a slew of cybersecurity experts, explain what you need to know to keep yourself from joining their ranks. --As told to Rebecca Deczynski, Kevin Ryan, and Brit Morse.



Infographic by Pop Chart Lab

Contain the Damage

Nathan Thompson, CEO of data- storage company Spectra Logic

My heart dropped when we found the ransom note last May. The attackers wanted $3.6 million in bitcoin within five days. An employee had opened an email on their laptop. And because they were VPN'd into our network, the malware attached to one of our servers and spread from there. The virus had spread to 150 of our 600 servers before we physically disconnected everything.

We hired a cybersecurity firm to help us. We had people working around the clock for four days, sleeping in shifts. A few hours before the ransom deadline, we determined we had all our data in

backups, so we decided we wouldn't pay it. We could rebuild everything--it would just take time. We have 400 employees around the world and customers in 50 or 60 countries. All of a sudden, we had to go from a pretty sophisticated system to having to text one another. That went on for two weeks while we rebuilt everything. It was a huge disruption to our business.

They hadn't just encrypted our files. They'd also tried to steal our customers' data. It took another six weeks to determine that nothing had been released to the dark web. Since then, we've built more moats and drawbridges within our system. It's all about limiting the blast radius. We know it will happen to us again someday. But we're darn well going to have as much protection as possible when it does.

Know Your Options

Ryan Olson, vice president of threat intelligence at cybersecurity firm Palo Alto Networks

We are always better off if people don't pay ransom, because it encourages more attacks. However, it is a calculation that each organization has to make in the moment. If you're a hospital, and you're shut down and can't provide care, you may be making literal life-or-death decisions based on whether you pay this ransom. Or maybe you could recover from your backups in two weeks, but that amount of time will cost you way more than if you pay the ransom. Never assume that you don't have another option but to pay. And never assume that the ransom demand is nonnegotiable, because bad guys like to negotiate as well.

Bring in a Backstop

Sid Berry, creative director of web design and marketing agency 71Three

We're rapidly growing--since March 2020, our agency has seen a 40 percent increase in revenue and we've brought on 11 new employees. So in June 2021, we planned to move to a higher floor in our Houston office, where we'd have more space. We keep most of our data offline, but our IT team had to disable certain components of our security for the move. There was so much hustle and bustle the Friday before the move. That's when it happened: The hackers locked and encrypted our systems, and sent a message asking for around $10,000 in bitcoin.

Because we work with highly sensitive data for our clients, we keep the majority of our backups offline and make new backups every single hour--that's literally what saved us. That data can't be stolen unless someone physically comes to our office with a gun.

The attack added 10 extra days to our move and probably cost us about $25,000 in productivity loss. But paying the ransom wasn't an option for us: We saw it as unethical, and it wouldn't have guaranteed recovery of our data. Now, we use an additional link inspector software called Barracuda Sentinel and make sure employees, especially interns, know: Do not click on any links in

unknown emails and definitely don't download any files. Our software has filtered out a few links since we installed it, so it seems like someone was trying to hack us again. At least we know it's working.

Untangle Your Network

Jaya Baloo, chief information security officer at antivirus software maker Avast

If you're spending money on laptops, network equipment, etc., you should reserve 10 percent of that for your cybersecurity costs. It's not a crazy thing to ask, 10 percent of IT spend. Most attacks are preventable through relatively straightforward measures you can take care of before an attack. These are things like patching your environment, using two-factor authentication, educating your staff about phishing, and trying to catch everything on your servers.

The problem is, the majority of companies today have a really hard time trying to identify their assets. They have no idea anymore what their network looks like, because it has grown organically and they cannot tell you all the software that's being used in their corporate environment, the data flows, the critical points. And these are the places where I think we're going to see quite a bit of pain.

Know You're a Target

Kerry Siggins, CEO of waterblast equipment maker StoneAge

This was one of the most intense, challenging experiences I've gone through as a CEO, and it happened back-to-back during Covid. I've run StoneAge for 12 years, and I'd never paid that much attention to cybersecurity. I was always under the impression that we're a small company in a niche industry in Durango, Colorado. I thought, how is anybody going to find us? I assumed we weren't a target. That came back to bite us in the pants.

On a cold, snowy Saturday morning in February 2020, I got a call from my IT manager that our enterprise resource planning system, which we use to run our business, was down. I rushed to the office. After hours of digging, we found the ransomware note, which first asked for $240,000, but eventually went up to $350,000 when we didn't pay right away. I asked about 25 employees to come into work Sunday morning. At 8 a.m., we all sat at a conference room table, and they looked at me with fear in their eyes. I was afraid too. I hired negotiators on the recommendation of our attorney, which was a game-changer. They advised us through the process.

We discovered that the hackers were manually deleting our backups, but they had missed our most recent two, so we were able to restore most of our data up to 12 hours before the hack. That's what made it possible to not pay the ransom and rebuild what we had lost.

Meanwhile, for four weeks my employees had to manually track, pack, and ship orders during our busiest time of year. We estimate the hack cost us about $250,000--more than the initial ransom. But even if you do get the encryption key back from your attackers, you likely will get only about 70 percent of your data returned.

The biggest thing we did to improve our security was get a 24-hour monitoring service, which has caught all kinds of things since the hack. We still have employee education, too--we always tell people to never be afraid to speak up if you click on something and feel like, "Oh, my gosh, I shouldn't have done that."

Don't Feed the System

Lou Steinberg, founder and CEO of cybersecurity research lab CTM Insights

There's an entire ecosystem of providers that come together to do these attacks. Paying the ransom is bad for everybody. The more money the hackers make, the more they're incentivized to do this again. You're proving their business model. You're trusting somebody who just put a gun to your head to do the right thing and give you back your systems. They can just walk away, and sometimes they do. In that case, you've not only lost your data--you've now been robbed on top of it.

Level Up Your Backup Game

Chad Ogden, president of flooring software-maker QFloors

I remember the exact day we were hacked, in May 2021. I mean, it was probably the worst day of my life. I felt so hopeless. We work with 400 flooring businesses all through the U.S. and Canada--there are thousands of users depending on me to keep them safe and help them run their businesses. Usually, with ransomware, the first thing they take out is your backup. About a year ago, we had implemented a backup system that was hidden. We got some comfort from that. We could rebuild everything we lost from scratch and avoid contacting the hackers, who we estimate would have asked for a ransom between $300,000 and $500,000.

Within 24 hours, we got our biggest customer back up, and the rest of our customers were back up within four days. It all hinged on these disconnected backups. We estimate each client lost at least $5,000. Our own business lost $50,000. We've implemented tons of other security measures since, but the truth is, no matter what you do, no one is 100 percent safe.

Report the Crime

Rahul Telang, professor of information systems at Carnegie Mellon University

Ethically, paying ransom makes no sense. When you start doing that, you're basically feeding the future of the ecosystem. But, at the same time, the easiest way to solve the issue is to pay, even though there's no guarantee that the hackers will play nice. It's the more instantaneous option.
What we know about ransomware is only what's been publicly disclosed. When a firm pays the actor and moves on, that stays undercover. Whatever statistics we have, the actual number is significantly higher. Unless someone discloses that info, we won't know the extent of the issue.

Drill the Basics

Stuart Madnick, professor emeritus of information technologies and founder of cybersecurity at MIT Sloan School of Management

If your company is shut down and losing $15 million a day, and recovering hacked data on your own might take a couple of weeks, you're talking about losing a couple hundred million dollars, or you could pay a ransom of $10 million. If you report to stockholders that you decided to be ethical and spend $100 million, how many lawsuits do you think you'll be facing? Most companies want to do it quietly and quickly. I've seen companies lose billions of stock value from these attacks.

Most focus on the protection aspect--and you need good passwords, the latest software. The trouble is that a determined attacker will find a way in. That doesn't mean you should give up and leave the doors wide open, but you need to be realistic. The analogy I use is fire drills. You should know where the staircases are, where you're supposed to gather so people know who's lost, and so on. You need cyber fire drills so you know that if a ransomware attack happens, you're prepared.

Think Like a Hacker

Kevin Johnson, CEO of penetration testing firm Secure Ideas

My colleague recently got an email that looked like it was from me asking him to approve a credit card charge. He didn't fall for it--we're security nerds, after all. But social engineering tricks are hard to detect. Most people don't realize how much information is available to somebody outside of their organization.
I can look up any company on LinkedIn, read employees' job descriptions, and get a good idea of the infrastructure and processes. You might use a third-party app that lets people outside your organization book time on your calendar. We use one too. But someone could see that you're booked all day Wednesday, Thursday, and Friday and presume you're out of town.

Then they send an email to an employee on one of those days: "I'm on a plane--you have to do this for me right now." And now you're the victim of a ransomware attack.

With every new process or piece of software your company adopts, think of what a bad person could do with it. I'm not trying to scare you. I just want you to think about it.

This article was originally posted on Inc.com. Read the full article here.

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

User Provisioning Documentation Updated

LEARN MORE

PhishProof: Microsoft ATP Bypass Rules Documentation Updated

LEARN MORE

CONNECT WITH US

info@inspiredelearning.com | 800.631.2078