Ransomware vs WFH: How remote working is making cyberattacks easier to pull off

zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off

Danny Palmer

How remote working is making life easier for hackers

The unique conditions of 2020 mean businesses are more reliant on being digitally connected than ever before. Cyber criminals know this, which is why ransomware attacks have become even more pervasive – and effective during the course of this year.

Hackers are breaking into networks of organisations ranging from tech companies to local governments and almost every other sector; encrypting servers, services and files with ransomware before demanding a bitcoin ransom that can be measured in hundreds of thousands or even millions of dollars.

Part of the reason for the upswing in successful ransomware attacks is the huge growth of remote working as a result of the pandemic.

While employees and their PCs were once safely behind the office firewall, now they're trying perched at a makeshift workstation in their kitchen or bedrooms, using all manner of cobbled-together technologies to get the job done.

"You have a much bigger attack surface; not necessarily because you have more employees, but because they're all in different locations, operating from different networks, not working with the organisation's perimeter network on multiple types of devices. The complexity of the attack surface grows dramatically," says Shimon Oren, VP of research and deep learning at security company Deep Instinct.

For many employees, the pandemic could have been the first time that they've ever worked remotely. And being isolated from the corporate environment – a place where they might see or hear warnings over cybersecurity and staying safe online on a daily basis, as well as being able to directly ask for advice in person, makes it harder to make good decisions about security.

"That background noise of security is kind of gone and that makes it a lot harder and security teams have to do a lot more on messaging now. People working at home are more insular, they can't lean over and ask 'did you get a weird link?' – you don't have anyone do to that with, and you're making choices yourself," says Sherrod DeGrippo, senior director of threat research at Proofpoint.

"And the threat actors know it and love it. We've created a better environment for them," she adds.

Remote working means a lot more of our daily workplace activity is being done over email and that's providing hackers with a smoother pathway for infiltrating networks in the first place via phishing attacks.

It's not hard for crooks to customise a phishing email to target employees of a particular organisation and direct them towards a link that requires their Microsoft Office 365 username and password, providing the attackers with initial entry into the network.

"We're now working from behind residential internet infrastructure whereas before we were behind enterprise-grade infrastructure. Now we're behind a cable modem that's not only intended for residential use, but also you've got your kids on the same network, people streaming TV," DeGrippo explains. "It's a change and a mix from better secured and controlled environments to chaos with no control."

Another WFH security issue; for some people, their work laptop might be their only computer, which means they're using these devices for personal activities too like shopping, social media or watching shows. That means that that cyber criminals can launch phishing attacks against personal email addresses, which if opened on the right device, can provide access to a corporate network.

"In the past, if a threat actor wanted to compromise a corporate asset, they'd typically have to email people on their corporate email accounts. But now they can either target corporate emails or personal accounts – and there are going to be less controls on personal accounts," says Charles Carmakal, SVP and CTO at security company FireEye Mandiant.

He said he had seen a number of attacks that started because somebody opened up an email from their personal account on their corporate computer. "The frequency seeing the personal email address as an attack target feels a little bit higher than it has been," he says.

"If an attacker is able to phish you and get a backdoor installed on your computer, it may not be connected to your company all day everyday but you will connect at some point," Carmakal explained.

Once an attacker has successfully compromised a home user, they'll wait for the user to be connected to the corporate VPN and take it from there like they would if they'd connected to a machine inside the walls of an office.

The attacker will attempt to move laterally around the network, gain access to additional credentials and escalate privileges – preferably by gaining administrator level rights – to be able to deploy ransomware as far and wide across the network as possible.

And with employees spread out by remote working – and in many cases, working irregular hours to fit work around home responsibilities – it can be harder for information security teams to identify unusual or suspicious activity by intruders on the network. That's especially the case if the information security team didn't have previous experience of defending remote workers prior to this year.

"They can go undetected because it's not a situation that organisations have prepared for in terms of their security posture," says Oren. "So it becomes harder for the defenders and on the other hand there's much more opportunity and more touch points for the attackers."

While the rise in remote working has provided cyber criminals with a potential new route into compromising networks with ransomware, it is still possible for an organisation to move to remote work while also keeping its staff and servers protected from a cyberattack.

Some of this comes from the human level, by training and engaging with staff, even while they're WFH, so they know what to look for in a phishing email or other suspicious online activity. But it's probably impossible – and unfair – to expect employees to carry the weight of defending the organisation from cyberattacks.

"A technical defence followed by a really well educated user base, who know what to do if they encounter something, if they seem unsafe, is the best way to go for most organisations," says DeGrippo.

One of the reasons ransomware has become so successful is because many organisations don't have offline backups of their data. Regularly backing up the network helps provide a fail-safe against ransomware attacks because it provides the ability to restore the network with relative ease without having to line the pockets of cyber criminals.

Multi-factor authentication is a must when it comes to helping to protect the network from cyberattacks, so if a user does fall victim to a phishing attack and gives away their password by accident – or if attackers simply manage to guess a weak password of an internet-facing port – a second layer of protection prevents them from easily being able to use that compromise as a gateway to the rest of the network.

If possible, it's also useful to separate the network so that it isn't flat throughout the entire structure of the organisation, something that doesn't have any real negative impact on the business, but can go a long way to making it harder for cyber criminals to move around the place if they get in. In the worst case scenario, that means if there is a successful ransomware attack, it can be restricted to a small part of the network.

"If you minimize the ability to move laterally across the network by instigating network segmentation it'll slow down the spread of ransomware," said Carmakal. "This is all security basics, but we find a lot of companies still struggle with the basics."

Regularly applying security patches can also prevent ransomware attacks from being effective as it means they're unable to take advantage of known vulnerabilities to spread around networks.

However, while ransomware remains a large problem for organisations, with cyber attackers getting more ingenious with their schemes and demanding higher ransoms, the battle isn't lost.

Other kinds of cyberattacks – that have previously been the flavour of the month for cyber criminals – have successfully been countered, so it isn't impossible that ransomware could go the same way if organisations – be they on premises, remote, or a mixture of the two – follow the correct security protocols.

"I don't think that it's all bleak; we've seen a significant reduction in software vulnerabilities over the past two or three years. Browser vulnerabilities are almost non-existent and much of that resulted in the reduction of the exploit kit landscape – exploit kits today are quite rare," says DeGrippo.

"Continuing to fight this fight could go the same way. If we continue to work on the problem, eventually it won't be as lucrative," she adds.

The reason ransomware remains lucrative is because victims pay the ransom, opting to do so because they perceive it as the best way to restore the network. But paying the ransom means attacks will just continue.

"Never ever recommend paying the ransom. I understand the considerations behind doing it, but I'd never say it should be done because it's very obvious that it perpetuates that kind of attack," says Oren.