RAVENii Report

BACK TO THE OFFICE

Hi ho, hi ho, it's back to the office we go. Are you ready?

For months now we have been talking about the pandemic; about the risks of contracting the virus and about the dangers of how quickly it spreads to infect other unsuspecting victims. As we are witnessing with the outbreaks in New York or here locally with the outbreak in St. Joseph, the virus can take down a community or a business in a matter of days. It's swift, it's quiet, it's dangerous.

Consequently, for months now we have been talking about the dangers of having an unprotected and unprepared remote workforce. We've been discussing the many avenues hackers are taking to exploit you and the billion other people out their trying to make work work at home.

According to a recent survey by Check Point and Dimensional Research, these are the most popular methods hackers are using to take advantage of remote workers during the pandemic:

Phishing - 55%
Malicious Covid 19 Websites - 32%
Malware - 28%
Ransomware - 19%

The study also reports that some of their favorite malicious acts are:

Remote User Credential Theft: Malicious logins are not being detected by security teams because the massive amount of remote connections are concealing them.

Phishing Emails with Malware: Hackers are creative and are using the coronavirus to lure us into falling for their tricks. For example, what if you got an email from Chipotle and it said, "During this difficult time, Chipotle wants to give you a free burrito. Just click on this link....."

Malicious Websites: Everyone should beware of any websites with Coronavirus or COVID-19 in the URL or title. Many are malicious sites and clicking on a link could invite malware into your device.

Zero-Day-Attacks: The coronavirus creates a natural distraction as security teams scramble to keep up. Consequently, hackers have no better time than the present to launch an attack to steal your data.

As stay at home orders begin to lift and people start going back to the office, are you prepared for the possible security issues that this migration may cause? What are the chances that someone at your business has an infected device? Are you comfortable allowing your employees to bring their devices back to the office and connect to the network?

RAVENii Report

We have all been doing the best we can to keep the coronavirus out of our homes. Make sure you are as diligent about keeping viruses out of your infrastructure when your organization comes back to the office.

“Just like the coronavirus, all it takes is one infected asset to bring down a business,” says RAVENii’s Chief Network Engineer, Eric Helm. “We don’t know how many devices are out there fostering infections. Security teams need to be prepared to protect their networks.”

RAVENii strongly recommends that you get a plan in place before you allow remote workers and their devices back into the office.

“Now is the time to lean on your policies and leverage your security tool stacks,” says Helm. “You should also dust off your Incident Response plan and make sure it is up-to-date.”

The coronavirus has robbed us of enough, don’t let it steal your critical business data and your reputation too.

If you need help coming up with your re-entrance plan, let us know. The RAVENii team is here to assist.

Stay safe and be well.