ISSUE 28 SPRING 2020

RJ2 TECHNOLOGIES

Newsletter

What's Inside

How Hackers are Exploiting the Coronavirus..and How to Protect Yourself

We all have new worries because of the current coronavirus pandemic, but the old worries haven't gone anyway. Among them: malicious hackers, some of whom are trying to use the outbreak to steal or ransom victims' data.

Several recent attacks have attempted to leverage the coronavirus by getting people to click on links in messages about the illness, according to a report by cybersecurity firm Nocturnus in March. Hackers have also tried to use the influx of people working at home because of the virus to their advantage. As with many other phishing efforts, the hackers' goal is to get a user to click on an emailed link that downloads malicious 'malware,' which can be used to steal victims' personal data or freeze their computers.

Nocturnus said the emails have tried to bait users into clicking with subject lines such as "Coronavirus: Important information on precautions" (in this case, in Italian). Other phishing emails spotted by a second security firm, Nuspire, include messages about a coronavirus vaccine (which doesn't exist yet), deals on medical equipment, and investment opportunities related to the outbreak.

Coronavirus-themed 'ransomware,' which can encrypt a computer's hard drive and let hackers demand payment to unlock it, has also been used. One malware spotted warns victims: "Just because you're home doesn't mean you're safe," before demanding payment to unlock files, according to Nocturnus.

How to avoid malware

Broadly, avoiding most of these risks means following the same advice as during more normal times. Don't click on links from unknown people. Only download or install software from trusted sources. And verify that the URL of any website that asks users to enter a password is accurate: hackers often set up URLs that are similar to real websites to harvest passwords.

Remote-work vulnerabilities

The sudden increase in remote work that many companies have instituted over the past week introduces a new set of cybersecurity risks to organizations. The fundamental problem: communication that is entirely online makes it much easier for bad actors to use to use deception to gain access to systems. This type of 'hack,' generally known as social engineering, relies on con artistry rather than code.
Hackers may "call into a department and pretend to be another department" of an organization, says Marty Puranik, president and CEO of cloud computing provider Atlantic.net. Chris Wysopal, co-founder and chief technology officer of security firm Veracode, warns that hackers may pretend to be employees having remote access problems and trick IT staff into giving them access.

Hackers impersonating government agents may have goals well beyond stealing bank account information, or even infiltrating corporate systems. An attempted hack of the U.S. Health and Human Services agency website on Sunday appears to have been aimed at slowing emergency information systems and spreading false information through text messages.

At their most extreme, hacks could even interfere with systems vital in the fight against the virus. A Czech hospital appears to have been hit by a ransomware attack, in which hackers ask for money to eliminate the problem, that shut down its information systems, though there is no evidence that attack was state-backed.

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

Hackers Come in All Shapes and Sizes

Hackers are known by the general public as cybercriminals, especially with so much news about nude celebrity photos beings released to the cloud, millions of customer information being stolen across many industries, and government agencies paying the ransoms hackers demand so that the former can regain access and control of their systems. However, did you know that not all hackers are bad guys? Read on to learn more about them.

A complicated history

In the 1950s, the term "hacker" was vaguely defined. As computers became more accessible, the word was used to describe someone who explored the details and limits of computer technology by testing them from a variety of angles.

But by the 1980s, hackers became associated with teenagers who were caught breaking into government computer systems — partially because that is what they called themselves, and partially because the word hacker has an inherently aggressive ring to it.

Today, several of those pioneering hackers run multimillion-dollar cybersecurity consulting businesses, while countless others run amok online, hoping to make a quick buck off of hapless victims.

"Black hat" hackers

Closer to the definition that most people outside the IT world know and use, black hat hackers create programs and campaigns to commit all sorts of malicious acts. Crimes such as identity theft, credit card fraud, and extortion are for their sole benefit, but they can also work under the auspices of a corporation or a state and commit espionage and cyberterrorism.

During the 1990s, Kevin Mitnick was a prime example of a black hat hacker. Mitnick went on a two-and-half-year hacking spree wherein he committed wire fraud and stole millions of dollars of data from telecom companies and the National Defense warning system.

After paying his debt to society by spending five years in prison, he set up his own eponymous cybersecurity firm and became its CEO and Chief White Hat Hacker.

"White hat" hackers

Sometimes referred to as ethical hackers or plain old network security specialists, these are the good guys. Whether it's selling what they find to hardware and software vendors in "bug bounty" programs or working as full-time technicians, white hat hackers are just interested in making an honest buck.

Linus Torvalds is a great example of a white hat hacker. After years of experimenting with the Sinclair QDOS operating system on his Sinclair QL, he released Linux, a secure open-source operating system.

"Gray hat" hackers

Whether someone is a security specialist or a cybercriminal, the majority of their work is usually conducted over the internet. This anonymity affords them opportunities to try their hands at both white hat and black hat hacking.

For example, Marcus Hutchins is a known gray hat hacker. He's most famous for testing the WannaCry ransomware until he found a way to stop it.

During the day, Hutchins works for the Kryptos Logic cybersecurity firm, but the US government believes he spent his free time creating the Kronos banking malware. He was arrested in 2017 and branded as a "gray hat" hacker.

RJ2 SPOTLIGHT

Connor Griffin

Support Engineer

Connor Griffin has been working in the IT field since 2017. Early in his career, he developed entrepreneurial skills by operating his own small business from home with contracts to fix computers and maintain network infrastructures which helped pay for his tuition at Elgin Community College. Post studies at ECC, Connor joined Serving Intel in South Elgin, IL as an Assistant Relationship Manager, equivalent System Admin. He then took a contract for Lenovo and Amedisys as a Migration Engineer. Once his contract was complete, he found his new home at RJ2 Technologies in the Client Support Center.

Fun fact: Connor had originally studied to be a Mechanical Engineer and he's a drummer in his free time.

BUSINESS PRESENCE

Should You Use UPS For Your Network Gear?

Smart business owners use an uninterruptible power supply (UPS) for emergency situations like a storm, fire, or other disasters. Often, a UPS is deployed for desktop computers to give employees ample time to save their work and prevent losing unsaved work. An even better power-saving strategy in emergency situations, however, is to use UPS for networking equipment.

UPS for network equipment

UPS systems provide backup power in case of outages and protect against power surges, which don't just damage computers but also make you lose unsaved work. Deploying them for Wi-Fi routers and modems allows you to stay connected to the internet in what is typically a chaotic time.

Moreover, it makes sense not to just keep your PCs powered up, but to also have internet access during a disaster. This strategy works relatively well if your staff are predominantly laptop users, as that means you only need power for your Wi-Fi gear.

Better than generators

Although generators are indispensable for certain businesses, they also require greater upkeep. Small- and mid-sized businesses (SMBs) may not have enough capacity to maintain them because they typically require a utility crew who can manage high-maintenance equipment.

What's more, extreme mishaps when misused or mishandled could result in generator-related fatalities. On the other hand, misusing a UPS unit could result in the loss of a day's work, but it's unlikely to lead to anything as extreme.

Why internet access is important during a disaster

UPS-supported modems or routers help you stay online for as much as 90 minutes, which should be enough time to get your bearings before power finally runs out. Internet service providers (ISPs) are usually prepared for catastrophes and would normally have an emergency power source to stay operational. And if you can stay online via Wi-Fi during an emergency, you get the following benefits:

Internet speed that's faster than cellular access
No extra telecom costs resulting from overreliance on cellular data
All devices stay online using a stable Wi-Fi connection
Devices don't have to rely on cellular data-equipped phones for internet connection

Plug in your network gear now

Businesses that aren't located in disaster-prone areas probably don't give much thought to installing UPSs for their computers, let alone their modems. But accidents and emergencies are inevitable. And when they happen, you'll find that having internet access is one of the most important things you need to ensure business continuity.

Think of an emergency power supply source like a UPS as an investment that not just protects your systems from data loss but also keeps your Wi-Fi equipment functioning in emergency scenarios. Call us today!

Feature Partner Product: Mimecast: Email Security

Email is the #1 attack vector. Protect your organization against spam, malware, phishing, and targeted attacks with a 100% cloud-based service.

Mimecast's cloud-based Secure Email Gateway protects organizations and employees using any cloud or on-premises email platform. It defends against inbound spear-phishing, malware, spam and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds.

Your information, and ultimately your business' reputation, is protected by outbound scanning of all emails to block threats and prevent malicious or unintentional loss of sensitive or confidential information.

April

"It's supposed to be automatic, but actually you have to push this button. "
- John Brunner

TECH TIPS OF THE MONTH

Data Backup Checklist:

1. **Determine the Data Storage Requirements**
2. **Schedule regular times and frequency of performing backup**
3. **Create a local backup solution that also syncs to an offsite cloud backup solution for reduncdancy**
4. **Test your solution that it is accurately backing up the data. No Corruption**
5. **Test your ability to recover your data should there be an issue both locally and form the cloud**