HACKER PERSONAS

A Deeper Look Into Cybercrime

CARBONITE an opentext company | WEBROOT an opentext company

THE OPPORTUNIST

Opportunists capitalize on unpreparedness, often exploiting common human traits such as trust and familiarity. They rely on targeted or focused attacks, and carry out their crimes against specific businesses or individuals. They are usually well planned, with hackers thoroughly researching their victims and running tests before performing an actual attack. What's more, opportunists look for existing weaknesses or vulnerabilities they can exploit en masse to pull as many victims as possible into their nets. In fact, by August 2020, the FBI saw a 300% increase in cybercrime related to attacks of opportunity.[1]

Opportunists Are a Threat to Everyone

Hackers use any opportunity to abuse victims by leveraging humanitarian crises and current events. For example, the global pandemic has led to a monumental rise in digital connectivity, creating a hotbed for cybercrime. These are just a few of their tricks of the trade:

Fake Covid-19 Trackers
Coronavirus trackers, which seem legitimate, can be hosts for malware and bots. In roughly the first half of 2020, more than 136,000 new domains were registered that reference the COVID-19 outbreak. A large portion of these sites distribute phishing campaigns and include a number of pandemic buzzwords.[2]

Ryuk and Conti Ransomware Attacks
An increasingly common tactic for big ransomware groups is to create "leak sites" where they upload and leak sensitive documents from companies that refuse to pay a ransomware decryption fee. Cybercrime group Conti and their predecessor Ryuk are known for using leak sites to launch opportunistic attacks.[3]

Fake Charity Websites and Phishing
No matter if it is a forest fire, hurricane or earthquake, cybercriminals are locked and loaded, and ready to take advantage of compassionate individuals. And many of these well-meaning victims never realize their donation failed to support their cause.[4]

> "The increase in remote work makes it easier than ever for cybercriminals to trick people into going to malicious websites because they're not protecting every endpoint and device."
>
> **Kelvin Murray,** Webroot

THE RISE OF MISINFORMATION

Cybercriminals have not only taken advantage of the pandemic to make a profit through malware and phishing, they have used it to spread misinformation. In mid-March 2020, hackers used bogus text messages to spread false details of an impending national quarantine owing to COVID-19.[5]

What's more, in a one-month period, one country reported 290 fake online postings about the pandemic with the majority containing both false information and concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities.[6]

Even the World Health Organization (WHO) and the U.S. Health and Human Services Department (HHS) were targeted by nation-state phishers said to be involved in an attempted hijack of the personal email accounts of WHO staffers.

Work From Home Adds New Risks

The surge in remote work has heightened cyber risks for both individual employees and organizations. The biggest security challenges to telework include an increase in phishing attacks, enhanced risk of cyberattack on the company network, and potential disruption to business continuity. Because remote workers are not on the organization's network, the IT team can't be in control of every device. This essentially expands the attack surface, creating new vulnerabilities that hackers can exploit. As a result, IT teams have an increasingly difficult time ensuring uniform cybersecurity practices, leaving the business open to attack.

With so many people working from home, hackers are finding new ways to attack businesses. Video conferencing has become a critical tool for many users who need to connect virtually. Unfortunately, vulnerabilities in popular platforms can be open doors to cybercriminals. The FBI warned users about "Zoombombing," in which uninvited people hijack video meetings to cause disruption. In one such example, users hijacked a city meeting to harass users with slurs and profanities.[7] However, these attacks can also lead to more serious repercussions. Earlier in 2020, one video conferencing platform was found to be routing internet traffic through a foreign state, raising concerns about privacy.[8]

Of course, even with new threats emerging daily, remote workers are still vulnerable to the age-old tricks of the trade. Remote Desktop Protocol (RDP), for example, is still a major threat to every business. Cybercriminals can easily find and target organizations by scanning for open RPD connections on TCP ports and then brute-forcing the credentials. Even lesser-skilled criminals can simply buy RDP access to already-hacked machines on the dark web.

Opportunists Will Target Any Business

While some cybercriminals specialize in targeting large enterprises or governments, opportunists will target anyone – whenever the opportunity arises! This means every business is at risk of attack, and business leaders need to ensure that every employee is properly protected, both from a technology standpoint and through continued security awareness training.

HOW TO PROTECT YOUR BUSINESS

- Warn employees to follow security best practices when opening or downloading COVID-19 related emails, links, or mobile apps
- Ensure every employee installs robust endpoint security on all devices
- Make sure to use RDP solutions that encrypt the data and use two-factor authentication and VPNs to connect to corporate networks
- Empower employees to become a strong line of defense by educating them about cybersecurity and data safety risks

Protect your business against opportunists with end-to-end security!

START MY FREE TRIAL

1 Entrepreneur, "FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak."
2 Webroot, "Cyber News Rundown: Malicious COVID-19 Websites Surge."
3 Security Intelligence, "Conti Ransomware Identified as Ryuk's Potential Successor."
4 FBI, "Charity and Disaster Fraud."
5 CNN, "Beware of these fake text messages and robocalls going around about the coronavirus."
6 INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19."
7 Michigan Live, "Internet trolls spew profanity, racial slurs during first virtual Kalamazoo city meeting."
8 Security World Expo, "Zoom Traffic Through China: Company Apologizes, Announces You Can Control Data Routing."

About Carbonite and Webroot
Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to help protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.