CYBERCRIME
IN VETERINARY MEDICINE

BY CLINT LATHAM, JD
DIRECTOR OF VETERINARY DATA SECURITY, LUCCA VETERINARY DATA SECURITY
WWW.LUCCA.VET

Extortion, identity theft and international data heists. This sounds like a plot for the next Hollywood blockbuster. Unfortunately, this is all too common reality for veterinary hospitals. Using the anonymity of the internet, hackers can hide behind computers, stealing millions of dollars from unsuspecting veterinary practice owners all over the world. What is cybercrime? How are the crimes committed? Is there anything we can do to protect our hospital?

WHAT IS CYBERCRIME?

According to The Legal Dictionary, cybercrime is "A crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs."

Cybercriminals cast a wide net looking for easy targets to pull ashore. Most veterinary practice owners don't think that they are swimming in the sea of cybercriminals. What they don't understand is that cybercriminals don't care where you are, what your business is or how small you are. All they care is that you are easy to catch in their net.

According to TechJury, every 39 seconds a business is attacked by a cybercriminal in the U.S.; 64% of businesses worldwide experienced a cyberattack last year. To make matters worse, the FBI reported a 363% increase in ransomware attacks to small businesses in 2020.[1]

Even with these staggering statistics, the broad term of *cybercrime* is not very helpful when trying to understand the complicated network of this criminal enterprise. Let's take a look at some of the specific tactics, tools and intentions of the modern cybercriminal.

MALWARE DELIVERY AND INFECTION

While the term *malware* is also a broad term, it is a great way to start narrowing our focus to understand the tactics of the cybercriminal and how we can protect our veterinary practice. Malware is simply an unwanted piece of software used to perform actions that you do not want or approve of on your workstations. If an attacker exploits a weakness in an operating system, spies on a user's keystrokes, or remotely hijacks a device, they're probably using malware.

Cybercriminals use the waterfall approach to attack veterinary hospitals. Cybercriminals deploy tools that look for the path of least resistance, much like a river. Most veterinary practices have aging equipment that lacks security patches, along with bad password management, open network connections and bad security practices implemented by software support vendors, making them the path of least resistance. Couple that with terms widely used in the healthcare industry – hospital, practice, medical, etc. – and they are squarely in the biggest target for cybercrime: healthcare.

Most people are mistaken in thinking that healthcare is a target because of the HIPAA regulations. Wrong! As an IBM cybersecurity example stated, "The healthcare industry is a leaky vessel in a stormy sea."[2] Veterinary medicine shares the same issues as human health care when it comes to leaky technology – thus making them ripe for attack.

How is malware deployed on your workstations?

- **Phishing links**
  As a malware delivery method, phishing makes use of social engineering and deception. Disguising themselves as a trusted contact or a legitimate business, the attacker will send an email containing a malicious download link.

- **Infectious websites**
  A website can be used as a malware host, infecting any visitors who view the page. To this end, perpetrators design their own domains, building a malicious download function directly into the site. To reach more victims, criminals may send page links in phishing emails, or use a similar domain name to a popular website.

- **Malvertising**
  Malvertising uses online ads, coded to install malware or redirect users to infectious websites. Cybercriminals try to sneak their pop-ups and banner ads onto legitimate sites, and even if people don't click on them, some can run automatically as soon as the page loads. A victim may not notice they've been targeted; the malvertisement can quietly install its malware and users will continue to browse on their devices, unaware of the infection.

The infection of malware on your workstations or server is just the start. The end result almost always results in the cybercriminal taking money, data or both as part of their catch.

FINANCIAL THEFT

Cybercriminals use every tool in their toolbox when it comes to stealing your money. For example, they may install a keylogger, a form of malware, that secretly records all of your keystrokes, allowing the cybercriminal to learn all of your banking information.

One way we see keyloggers deployed is to steal practice management software login info and email usernames and passwords. Then they use this information to create fake invoices and send them to all of your clients, not only stealing money from your client base but also ruining your reputation. This unfortunately is all too common in the veterinary industry. However, because your hospital is not a Sony, Garmin or Merck, it goes unreported and no one talks about it.

DATA THEFT

If you have followed my work for any length of time you may have heard me say that my life goal is "to help veterinary practice owners realize the value of their data and help them take the necessary steps to protect it."

For most cybercriminals it's not enough to just steal your money or scam your clients out of money. Once I'm on your network I might as well steal your data. If I've used a keylogger, that means I can steal your data even if you use a cloud-based practice management system.

Here the cybercriminal knows that they can easily sell your client lists, financial information and anything related to how you run your practice. Have you ever gotten one of those scam emails offering to sell you a list of pet owners in your area? How do you think they got that data?

The average veterinary staff member has access to around 1,000 sensitive files. With the pandemic forcing many CSRs, techs and associate DVMs to work from home, where cybersecurity

Continued

protocols are not properly enforced, it is very easy for a cybercriminal to compromise a single device. From that one device the criminal has access to a treasure trove of data.

RANSOMWARE

Targeting both individuals and, increasingly, veterinary hospitals, some criminals use ransomware, a type of malware that locks the user's access to a device or database. Once access has been restricted, the perpetrator demands a ransom. With business owners paying an average of $370,000 per attack, the global cost of ransomware crime is expected to reach $20 billion next year.

A couple of examples of how ransomware hit veterinary medicine: In late 2019 NVA had over 400 hospitals attacked by ransomware. In 2017 Merck Animal Health was hit by ransomware, costing them over $670 million to recover from the attack. The AVMA stated in a 2020 presentation that their average claim for a cyberattack was $133,000. After a cybercriminal has stolen your money, scammed your clients out of money, or stolen your data to be sold on the black market, the final step is to prevent you from accessing your own data.

References

1. Bulao J. How many cyber attacks happen per day in 2021? TechJury. May 11, 2021. https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref
2. Osborne C. IBM calls healthcare industry a 'leaky vessel in a stormy sea.' ZDNet. January 31, 2017. https://www.zdnet.com/article/ibm-calls-healthcare-industry-a-leaky-vessel-in-a-stormy-sea/

5 SIMPLE STEPS TO PROTECT YOUR HOSPITAL FROM CYBERCRIME

1. **Protect your passwords.** Ensure that you're using a long, complex password without any detectable patterns or words. Combine characters, numbers, and symbols to protect yourself against brute-forcing software. Avoid using the same login credentials across multiple accounts and find a password manager to simplify the process. Some of our favorites include 1Password, Bitwarden and LastPass.
2. **Be wary of email links.** Emails and social media messages may contain infectious links, even if the sender seems trustworthy. The best way to guard against these scams is to exercise caution whenever you're asked to click something online. Before engaging with an email, confirm the sender's authenticity: call the company's helpline, or search online for news of similar scams. Human caution is a strong defense against phishing tactics. There are great AI-based email protection tools that can help to better protect you from email scams. They will either flat-out block the email or warn you when an email looks suspicious, allowing you to easily flag the email to be added to the block list with a simple click of a button.
3. **Update your software.** Out-of-date software can provide the weak spots that malware takes advantage of. Anything from a browser extension to your operating system could be the target. You should regularly check for new software patches or set systems to update automatically. This includes mobile devices as well. There are also great ways to automate this process to push operating system updates as well as third-party software updates (Java, Chrome, Adobe, Firefox, etc.). All are done after hours, not interrupting your workflow and always keeping you protected.
4. **Use these free tools.** There are some great free online tools to help keep you protected. An extra 30 seconds could save you hundreds of thousands of dollars.

   a) **Blacklight** (themarkup.org/blacklight) – Blacklight helps you verify if a website is scanning your PC with any malvertising. Got a weird link in an email? Simply copy and paste it into Blacklight before visiting it to see what's behind the curtain.

   b) **Have I been PWNED** (haveibeenpwned.com) – Run your email addresses, passwords or usernames through this website every six months to see if you've been compromised. If you have an account that's been compromised, update it and make sure you have taken the appropriate steps outlined in step 1.

   c) **VirusTotal** (virustotal.com) – Before you open any resume you get from a potential employee, always run that document through VirusTotal. I can't tell you the number of times a veterinary practice gets compromised through fake resumes. Simply taking 15 seconds to upload it to VirusTotal first again could save you countless hours and dollars trying to recover.
5. **Provide staff training.** The weakest link in any cybersecurity defense is the human element. Take the time to get your staff the appropriate training at least once a year on the latest threats and what to look out for. The second and most important is to make sure you create an environment where your staff feel comfortable to come to you if they feel that they have been compromised. Once an attack starts, we have seconds to mitigate the damages. If a staff member tries to hide it under the rug, it's only going to compound your problems. ■