By Merle Windler, Thoroughbred Systems, Inc.

Computer Corner

What Monsters Are Lurking on The Dark Web?

The year 2017 was a banner year for the cyber bad guys! The press was loaded with dramatic demonstrations of just how dangerous and vulnerable data placed on the Internet has become. It was a record year of continuous announcements of compromised data, hacker attacks, scams, and ransomware, costing business and personal financial losses in the Billions of Dollars. The data that has fallen into the wrong hands over the last few years puts most of the population of the United States at risk.

In one of the biggest breaches, according to a CBS news report in October, Equifax, reportedly compromised approximately 145 million Americans, or nearly half of the U.S. population. Personal information, including Social Security numbers, exposes nearly half of all Americans to identity theft for years to come.

Yahoo recently announced hacker attacks in 2013, 2014 and 2016 were worse than originally believed, and in fact, every one of the more than three billion Yahoo accounts had been compromised.

An anonymous group of Internet hackers calling themselves the "Shadow Brokers" released a suite of extremely dangerous Internet hacking tools reportedly stolen from our own Central Intelligence Agency and National Security Agency. These hacking tools are now available on the "Dark Web" for use by others with potentially bad objectives.

The "Dark Web" was started by the U.S. Government years ago as an anonymous network unseen by search engines like Google, Yahoo, and others. It was designed with good intentions to be used for the military, law enforcement investigators, intelligence agents, researchers and others wishing to keep their online activities anonymous. However, over the years its very anonymity, combined with the introduction of new untraceable electronic currencies like Bitcoin, have made it a dark underworld of international illegal and illicit activities.

Criminals buy and sell Social Security numbers, birth dates and other personal information like addresses, credit card numbers, emails and passwords on underground, i.e., "Dark Web", Internet websites at bargain prices. Once data is compromised, there is a continuous threat of identity theft, credit card crime and other financial or even tax return theft.

> **Once data is compromised, there is a continuous threat of identity theft, credit card crime and other financial or even tax return theft.**

There is often confusion between the terms "Dark Web" and "Deep Web". The Dark Web, also sometimes referred to as the "Black Net", is a virtual world of intrigue and danger. The phrase Deep Web refers to the vast part of the Internet that is not as readily attainable by the typical search engines. While the casual user may believe that Google, Yahoo, Bing or ASK (all common search engines) puts the world at one's fingertips, in truth, those searches only pay attention to a small percentage of what is actually out there. There are hundreds of times more information on the Web than what is indexed by those search engines.

Most of the information that comprises the Deep Web is harmless data that is simply not bothered with by the typical search engine because it is not part of the mainstream. For example, anyone may set up a blog (a site on the Internet designed to share information), on the subject of rusty water, but just because the blog exists, doesn't mean that someone researching rusty water will find it on their search. This makes it a part of what is referred to as the Deep Web. On the other hand, if that same information is placed on a well known and widely used site like Facebook, most search engines will check it out and make it known.

While the majority of this less accessed information on the Internet, call the Deep Web, is harmless, tucked away in some obscure forum, chat room, or other less known source, the Deep Web is also where danger lurks in the form of the Dark Web.

While the ordinary person surfing the Internet is unlikely to stumble onto a Dark Web site or even access information from other parts of the Deep Web, the user doesn't need any special tools to access the Deep Web; one just needs to know where to look. Specialized search engines, directories, and wikis can help users locate the data they're looking for. The Internet is almost unimaginably vast. Once something is on the Web, it's out there, there's no getting it back or undoing it. Google, Bing, Yahoo or ASK, common search engines, may not find it, but it's still out there. (Think about that when the kids or grandkids are laughing about those wild party pics posted on the Web.) Trying to guarantee something is cleaned off of the Internet for good would be like spilling salt on a sandy beach and trying to retrieve it.

Any person perched at the computer doesn't have to be searching for trouble to find it. A person can be engaging in what seems like the most innocent of activities on the Internet and suddenly find themselves in trouble. Simply opening an email attachment, downloading a software program or visiting what turns out to be a malicious website, can land the person in hot water.

Ransomware, malicious software

Ransomware attacks were rampant this past year. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. WannaCry and BadRabbit are two that have separated many Internet users from their money, and their data. People are always taken by surprise when suddenly a frightening warning pops up informing the user that their security has been compromised and directing them NOT to turn their computer off and to immediately call the number on the screen for assistance. The wording and the display is designed to create panic. They don't want their victims thinking clearly. If the victim grants the hacker access to their computer the culprit now has a clear path to "lock" the computer files so that they can

demand money in order to unlock the files. As with kidnapping, payment may or may NOT result in retrieval. The FBI estimated U.S. ransomware loss to be in the billions of dollars in 2017.

Nothing is sacred. Even hospitals in California and Britain came under attack of these Ransomware hackers. Hospital computer equipment shut down halting health care due to facilities no longer controlling their own computerized equipment. The *New York Times* reported that the Department of Homeland Security and the Federal Bureau of Investigation concluded that hackers had targeted nuclear facilities, including the Wolf Creek nuclear facility near Burlington, Kansas, in Coffey County, in May. Westar Energy reported that the facility's nuclear reactor operational computer systems are separate from the corporate network and are NOT connected to the company business networks or the Internet. Therefore, despite hacker's compromise of the internal network, "...The plant continued to operate safely..."

One of the latest in a string of Amazon Cloud Server breaches occurred when an Amazon Cloud Storage Service was attacked in June, resulting in compromise of nearly 200 million voter records after a security setting was set incorrectly.

Perhaps one of the most distressing items revealed this year was the announcement that nearly ALL, not some, or merely a particular brand, but almost ALL modern computer processing chips, i.e. the main brain of nearly EVERY computer and electronic device, has two problems that actually aid hackers. The scary names given to these two recently identified vulnerabilities are Meltdown and Spectre. The weakness in their design could allow hackers to steal the entire memory contents of computers, including mobile phones and other mobile devices, and computer servers running in Internet 'cloud' computer networks. Ironically, it is the continued quest for more and more speed of processing that has created this vulnerability. This speed is what allows the hacker to make a clean sweep of their crime in the blink of an eye.

Experts say there is no easy fix for Spectre. The only guaranteed fix would be to scrap the current generation of processors, operating all over the world at this moment, and start from scratch. Not practical! So... meanwhile... the industry is attempting to create software patches that may be as troublesome as the original problem.

As for Meltdown, the software patch needed to fix the issue could slow down computer performance by as much as thirty percent. Microsoft and many others have already released software patches to address the issue. However, all Internet capable devices using these processor chips will need to be patched, not just Personal Computers and Mobile Phones.

The good news is, even though personal computers are vulnerable to this Meltdown design flaw, to exploit this particular weakness, hackers would have to first find a way to run software on the computer or device they are targeting before they could gain access to information on the machine. Attackers would need the user to download a software program, open or download an email attachment or visit an infected website.

In addition, a vulnerability discovered by security researches called 'Krack' compromises the WPA2 encryption protocol used by the vast majority of wireless Internet wifi connections. WPA2 has long been considered the "go to" secure encryption method of a safe wireless wifi network. But now that "Krack" has been uncovered, long trusted security standards are now considered broken making virtually all wifi networks vulnerable to hacking. The United States Computer Emergency Readiness Team (CERT) issued a warning that attackers can now read information that was previously assumed to be safely encrypted. As the exact quote of their warning is so filled with industry technical terms, not necessarily familiar to most people, a definition of terms directly follows the quote by CERT...

In addition, a vulnerability discovered by security researches called 'Krack' compromises the WPA2 encryption protocol used by the vast majority of wireless Internet wifi connections.

"The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection and others . . . "

- Decryption: The process of converting encrypted data back into its original form, so it can be understood.
- Packet Replay: A form of network attack in which a valid data transmission maliciously or fraudulently is repeated over and over to tie up the network to slow it down and keep it from working correctly

- TCP: Transmission Controlled Protocol - A standard that defines how to establish and maintain a network conversation via which application programs can exchange data.
- Connection hijacking: The commandeering/misdirecting of a computer transmission
- HTTP content injection: (i.e. virtual defacement) An attack targeting a user made possible by an injection vulnerability in a Web application.

So... The upshot of all this... Virtually ALL wireless systems and devices using the formerly safe WPA2 encryption method are now at risk within the range of the wireless signal.

The good news is that attackers would have to be physically close, within the wireless wifi range of the target. And, the potential weakness would not compromise connections to secure websites that use an additional encryption over and above the less secure WPA2, such as banking services or online shopping.

As most wifi signals have a range of only a block or two, with the maximum at around ten miles, the hacker in Russia, China, North Korea, Iran, or other locations of government sponsored attacks, will NOT be able to exploit this weakness here in the States. They would need to travel to within the limited signal range of their intended victim. Therefore, the risk is most likely limited to the local misbehaving teenager, disgruntled worker, or others that are within a close physical range of their target.

This basically means, the bad guy has to be close, in the parking lot, or close enough to get on the wifi, to be able to inject and manipulate data, inject ransomware or other malware into the network or website.

Connections to secure websites and encrypted connections such as virtual private networks (VPN) and secure socket shell (SSH) communications are still safe. *Or as safe as anything can be predicted to be in the world we live in today!*

However, insecure connections to websites – those which do not display a padlock icon in the address bar, indicating their support for HTTPS – should be considered public, and viewable to any other user on the network, until the vulnerability is fixed.

Even if someone fixes their own mobile phone or computer, they could still be connecting to an unfixed and unsecured router. Just the same, as many devices as can be fixed, should be, to ensure security on other networks. And... we haven't even talked about all the Smart TVs, Baby Cams, Web Cams, Security Alarm Systems, Alexa and Echo Voice Activated Assistant Devices, and basically any device that is attached to the Internet being used against the unsuspecting victim, to collect data and spy.

Some food for thought

If our government security agencies, the CIA and NSA, can't protect themselves from attacks and data theft, would it not be wise for the small town or water district to thoroughly explore the best possible course for protecting confidential data and vital systems from the wide range of possible threats that exist today? Automation is a wonderful thing, but every new technology implemented may also carry with it certain risks that should be considered. Despite what the salesman says, fully research any online application, Internet Data Backup Service, Online Bill Payment Service, Remote Access Telemetry System and all the rest that might potentially be a liability rather than an asset if targeted by an expert hacker.

Even if someone fixes their own mobile phone or computer, they could still be connecting to an unfixed and unsecured router. Just the same, as many devices as can be fixed, should be, to ensure security on other networks.

For recommendations for dealing with security threats watch for Part 2 of this article in the next issue of *The Kansas Lifeline* magazine Computer Corner "Guarding Against the Monsters of the Dark Web" or, for a preview of some of that information, go to the KRWA website for a listing of Recommendations for Guarding Against the Monsters of the Dark Web.

Also, for a recent and extensive publication on these problems assembled from Computer Security Experts all over the world check out the *Time Life* publication "Time Cyber Security Special Edition Magazine".

Time magazine just released a "Special Edition" magazine called "Cyber Security Hacking, the Dark Web and You" with an eleven page chapter on "How to Protect Yourself".

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Inc., Topeka. The company specializes in utility billing for cities and rural districts, computer networking and associated training. Contact: merlewindler@yahoo.com