'NETWORKINGS

A PUBLICATION OF LOCKNET MANAGED IT SERVICES

HARDWARE SOLUTIONS

DETAILS INSIDE

PICTURED ABOVE >> AARON FOGLIA, LOCKNET SECURITY ENGINEER

QUARTER 2 » 2019

A Message from Peter Kujawa, Locknet Division President

I hope your summer is off to a great start! At Locknet – An EO Johnson Company, there is no "summer slowdown" as you will read in this Newsletter.

Peter Kujawa

It's official! Our **social media** channels are back online as of May 1! See details on page 2 on how you can find and follow us on **Facebook**, **Twitter** and **LinkedIn**. In addition to our social media channels, we are also bringing you brand new **blog** articles every week! These articles provide the latest technical trends, best practices and additional Locknet news. Please visit our website, **locknetmanagedit.com** and click **blogs** at the top of the page.

In addition to social media, we will continue to bring you our quarterly newsletter so you'll always know what's happening behind the scenes at Locknet. In this edition, we're sharing some background and an update regarding a recent significant vendor change that impacted our **Netxuspro™** and **Keysuite™** products as well as some simple tips and a little education surrounding IT security. We're also sharing insights on an easy solution that can keep your business current with the latest hardware technology with a predictable monthly fee, also known as **Hardware as a Service** or **HaaS**.

I'm going to completely shift gears and talk to you about a scary topic that you may not heard of; **The Dark Web**. The Dark Web is an underground marketplace where hackers and other criminals conduct business with complete anonymity. We share awareness on how your user name and password are a hot commodity and the measures you can take to keep your information safe. Read more about this on page 3.

Enjoy the rest of your summer!

WHAT'S INSIDE

LOCKNET

AN EOJOHNSON COMPANY

>> SOCIAL MEDIA Come Follow Us

As part of our exciting new brand transformation that began late last year, we are pleased to announce the relaunch of our social media platforms to better align with our new image. Go to each site today and sign up to follow us to stay current on all things Locknet!

Locknetmanagedit.com
Twitter.com/LocknetInc
Fb.com/Locknet
Linkedin.com/company/locknetmanagedit

CRN, a brand of The Channel Company, named Locknet – An EO Johnson Company – to its 2019 Tech Elite 250 and MSP 500 lists.

CRN Tech Elite 250. This annual list honors a select group of North American IT solution providers that have earned the highest number of advanced technical certifications from leading technology suppliers, scaled to their company size. These companies have distinguished themselves with multiple, top-level IT certifications, specializations, and partner program designations from the industry's most prestigious technology providers. www.CRN.com/TechElite250

> *CRN's Tech Elite 250 list recognizes solution providers with extensive technical knowledge and premier certifications," said Bob Skelley, CEO of The Channel Company. "Pursuit of vendor certifications and broader skill sets in a wide range of technologies and IT practices, proves a solution provider is committed to delivering maximum business value from those technologies and giving their customers the highest level of service.*

CRN MSP 500. This annual list recognizes North American solution providers with innovative approaches to managed services. These services help customers improve operational efficiencies, maximize return on IT investments, and continuously help them navigate the complexities of IT solutions. www.CRN.com/msp500.

> *Capable MSPs enable companies to take their cloud computing to the next level, streamline spending, effectively allocate limited resources and navigate the vast field of available technologies," said Skelley. "The companies on CRN's 2019 MSP 500 list stand out for their innovative services, excellence in adapting to customers' changing needs and demonstrate ability to help businesses get the most of out of their IT investments.*

ARE YOUR CREDENTIALS FOR SALE

>> ON THE DARK WEB?

Digital Credentials, such as usernames and passwords, connect you and your employees to critical business applications, as well as online services. Unfortunately, criminals know this—and that's why digital credentials are among the most valuable assets found on the Dark Web.

What is the Dark Web?

The Dark Web is a sublayer of the Internet that is hidden from conventional search engines such as Google, Bing and Yahoo. These search engines have the ability to only search .04% of the indexed or "surface" Internet. The other 99.96% of the Web is not searchable and consists of databases, private academic and government networks, and the Dark Web.

The Dark Web is estimated at 550 times larger than the surface Web and growing. Because you can operate anonymously, the Dark Web holds a wealth of stolen user names and passwords, also known as credentials. Criminals dealing with stolen credentials can make thousands of dollars by selling them to multiple buyers. A breach using one stolen set of credentials could potentially come from dozens of attackers.

How your work credentials can lead to a breach.

76% of people will use the same password for most, if not all, websites for the sake of personal convenience. Often times these passwords are weak and guessable so this common practice can make someone an easy target to a hacker. When employees use their work email credentials on websites such as social media sites, travel sites, free email services sites, etc., it can make your business vulnerable to a breach.

Small businesses are at greater risk.

According to the Federal Trade Commission, "information available for sale on the Dark Web is up to 20 times more likely to come from an entity whose breach wasn't reported in the media. Many of these are smaller retailers, restaurant chains, medical practices, school districts, etc. In fact, most of these breaches the U.S. Secret Service investigates involve small businesses. Data stolen from these businesses ends up on the Dark Web where criminals buy and sell it to commit fraud, get fake identity documents, or fund their criminal organizations."

How to identify if your credentials are residing on the Dark Web.

Locknet offers **Dark Web Monitoring** to help safeguard organizations against stolen user credentials. **Dark Web Monitoring** scours millions of sources including botnets, criminal chat rooms, peer-to-peer networks, malicious websites and blogs, illegal black market sites as well as other private and public forums to see if your business' email addresses and domains have been compromised and exposed. This service includes continuous searching and 24/7/365 monitoring. In addition, Locknet will notify you if your business' credentials have been found on the Dark Web so that you can take action quickly to change the affected login password(s) before they are used to compromise your network and data.

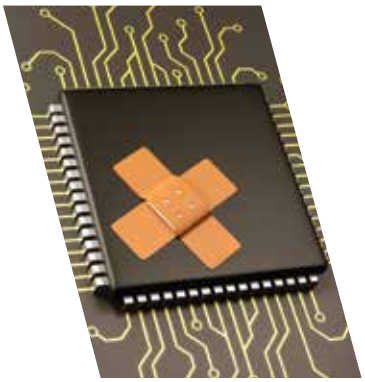
There are also other ways to stay proactive.

By taking some simple, yet effective precautions, businesses can help protect themselves by instituting stronger password guidelines. This includes creating passwords that make it more difficult for hackers to crack while steering clear from using obvious passwords, such as Password1 or personal information such as birth dates or childrens' names. Some other best practices include using phrases that are unique yet easy to remember or creating passwords using 8 characters or more in length that comprise of upper case and lower case letters as well as a combination of symbols and numbers.

continued on page 4

Remote Monitoring & Patch Management Vendor Conversion

Locknet is committed to providing client partners with world class, state-of-the-art products and services. For that reason, we continually reevaluate our vendor partnerships as well as their products and services to ensure they continue to be best-in-class products.



In Q4 of 2018, after a nearly two-year investigative process, we selected a **new Remote Monitoring and Management vendor** whose product and service excellence lined up strategically with our own. This tool offered several advantages for client support, such as full integration into our Support Center ticketing system to provide faster and more accurate ticket documentation. As a result, in Q1 we began to convert our monitoring and patch management tools over to our new vendor and migrate our **Netxuspro™** and **Keysuite™** clients to the new platform one at a time. We are pleased to announce that this conversion and client migration was fully completed on schedule on April 15!

The end result of this conversion has allowed the Locknet Support team to become more nimble from an operational standpoint. The new tools have empowered our team members to and deliver better service in a more timely manner to our client partners. In addition, this product will include several longer term improvements for our clients in terms of services provided and we will provide further updates on these in future editions. **While technology continues to evolve, you can always rest assure, Locknet continues to keep pace, to keep you safe!**

Contact the Locknet Support Center should you have any questions on this new tool or require additional training.

DARK WEB

continued from page 3

While there is always a risk that attackers will compromise a company's systems through advanced attacks, the fact is that most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees.

Implementing a suite of tools such as Blockade™ (managed firewall), Vulnerability Management, SIEM (Security Information and Event Management) as well as Locknet's Security Education and Awareness Training (employee training) and others can help businesses protect themselves and other assets from seeping into the Dark Web.

Learn more about Locknet's Dark Web Monitoring service or any other defense in depth security strategy offerings, contact a Locknet Account Executive at 844-365-4968.

BLACKLIST VS. WHITELIST. *WHAT'S THE DIFFERENCE?*

As a Managed Security Service Provider (MSSP), one of our most common questions from new clients is "What's the difference between blacklist and whitelist?" Understandably, this can be confusing.

Blacklisting means using a web content filter to allow all website/resources to be accessed, except those that the web content filter is told to explicitly deny access to. So, unless the filter is told to block access, it won't. Blacklisting can increase your risk of virus/malware infections and can impact system performance.

Whitelisting is the opposite, meaning that you start with an assumption that by default, all access to websites/resources is going to be blocked, unless a decision has been made to allow all or some users to have access to specific sites. With this approach you use a list of approved apps, software, emails, domains, etc.

Which is best? Locknet recommends that while it is usually more work to set up, from a security perspective most businesses should consider a whitelisting approach. The whitelisting option makes it easier to take control over end-user web activity and give them what they need for their job, without causing a security risk.

Transform Your Outdated Computer Fleet With a Cost Effective, State-of-the-Art, Agile Solution

In light of the rapid advancements in technology, businesses need to stay current with the latest technology and be able to scale to size quickly without dramatic spikes in cost.

Software updates and newer applications require more robust equipment to run. The Windows 7 End of Life (EOL) is a good reminder that newer operating systems, such as Windows 10, can be unable to perform efficiently on computers as new as two years old. If you're a business who suffered the consequences from this, you're not alone.

Chances are technology is not your primary business.

Windows 7 EOL is just one recent dilemma businesses face when maintaining a computer fleet. We all know that keeping up with all of the technology advancements can sometimes feel like a never ending battle and although your business may run on technology, chances are you're not in the technology business. You're likely throwing away valuable time and money into procuring, depreciating and maintaining computer hardware. Or worse yet, running your business on obsolete hardware.

Technology advances may actually hurt your business.

Keeping outdated hardware past its useful life typically leads to lower productivity, reduced revenue, and potentially much worse -- a security liability to your business! If you don't keep up with the technology lifecycle it could become a ticking time bomb. Before no time, you may be mopping up from an expensive security nightmare and being forced to make a rapid and sizable cash outlay for more new equipment.

Hardware as a Service (HaaS) is an easy, yet affordable solution.

The experts at Locknet have a solution to help solve this dilemma. Much like Locknet's bundled managed service solutions such as Keysuite™, Blockade™, Netxuspro™ and Reinforce™, Locknet also provides an option to change this process into a predictable monthly payment through Hardware as a Service (HaaS). HaaS is a complete hardware lifecycle solution that bundles hardware procurement, software subscriptions, delivery, and setup designed specifically to meet the needs of your unique business. Here are some of benefits:

- **Capex vs. Opex**. IT Hardware spending has traditionally been an upfront Capital expense for most businesses. There was a time that it made sense to make a large upfront investment so you could take advantage of amoritization and depreciation over time. However today that can be risky and it can tie up cash needed for other areas of the business. In light of the rapid advancement of technology, businesses are adopting the Opex approach so they can be nimble and keep current with technological advancements and scale to size quickly without the upfront capital.

- **Predictable Cash Management**. You can free up your money to be spent on other parts of your business. Instead, you pay a fixed monthly fee just as you do with Locknet's other managed services.

- **Flexibility**. As your IT needs evolve due to organization growth and changes, HaaS makes it easier for you to add or decommission hardware when your operation grows or scales down.

- **Current technology.** Locknet provides you with cutting edge hardware and ensures you get the most recent technology so you can be reassured you can continue to run and update your applications and work efficiently throughout the lifecycle of your hardware.

- **Robust security.** Hardware can be a cybersecurity soft spot. With so much attention focused on software and networks, hardware tends to get overlooked. As software and cyber threats continue to evolve, so do the advances in computer hardware. Keeping hardware current ensures that you can continue to run your security tools and receive critical security updates for both your operating system and applications.

- **Expert technologists.** From selecting equipment to fit the needs of your business and your budget to imaging and installation, Locknet has a team of experts who can guide you through the process and remove the burden of setup and installation.

Learn more about HaaS by contacting your Locknet® Account Executive at 844.365.4968.

LOCKNET
AN EOJOHNSON COMPANY

>> locknetmanagedit.com

844.365.4968

IOWA
- 129 Plaza Circle **Waterloo** IA 50701

MINNESOTA
- 7550 Market Place Dr., Ste C **Eden Prairie** MN 55344
- 2477 Clare Lane NE **Rochester** MN 55906

WISCONSIN
- 1505 Prairie Lane **Eau Claire** WI 54703
- 3310 S. Kinney Coulee Rd. **Onalaska** WI 54650
- 505 S. 24th Ave., Suite 204 **Wausau** WI 54401
- 8400 Stewart Ave. **Wausau** WI 54401

>> WINDOWS 7

TIME IS RUNNING OUT!

After January 14, 2020, Microsoft will no longer provide security updates or support for PCs running Windows 7.

It's still not too late! Contact your Locknet Account Executive at 844.365.4968 to help you devise a plan to move to Windows 10.

Work Smarter. Not Harder.

EOJOHNSON
BUSINESS TECHNOLOGIES

Document Scanning & Conversion by EO Johnson

Do you have boxes or file cabinets full of documents? Would you like to free up office space, or, do you want to be able to secure and search for documents electronically? Do you want to be able to retrieve these document in case of a disaster? If so, EO Johnson can make this easy for you! EO Johnson has full service Document Scanning & Conversion Services for customers looking to move away from paper files and convert them to electronic documents.

EO Johnson scanning services handles paper based documents, microfiche, microfilm and even wide format documents. EOJ has also worked with all types of businesses, including: FFIEC examined financial institutions, HIPAA regulated health care facilities, educational organizations and governmental offices. Documents including medical records, HR information, accounting, loan files, student records, maps, insurance documents are a small sampling of the types of documents we have worked with previously.

EO Johnson Document Scanning & Conversion Services are UCS/SOC2 Certified and conducted in an office monitored with 24 hour security. EOJ's team of experts will provide a smooth, user friendly process and best of all, the process is very affordable.

For more information, contact your Locknet® Account Executive today.