As the COVID-19 outbreak has ramped up, so, too, has cybercrime, including ransomware. The medical sector has long been a favorite target of cybercriminals and now, with the increased need for uninterrupted care during the COVID-19 outbreak, ruthless criminals continue to hammer the healthcare industry despite promises to the contrary. Though some criminal organizations have claimed to no longer be targeting health care and have even offered free decryption software for organizations affected by malware, any interruption in patients’ care could prove fatal when every second counts. It’s not just hospitals that are under attack, as life sciences firm 10X Genomics reported “an attempted ransomware attack”. Though they were able to quickly recover, there may have been a breach in their data.

“The company isolated the source of the attack and restored normal operations with no material day-to-day impact to the company or the company’s ability to access its data,” according to the filing. “The company’s investigation of the attack is ongoing with assistance from outside experts, and the company is also working with law enforcement officials on their ongoing criminal investigation of this matter.”

Israeli security researcher Under the Breach reported that on March 13th, 1 TB of data was stolen from 10x Genomics by prolific ransomware operator Sodinokibi, aka REvil and Sodin.

“It is particularly disappointing that we would be attacked at a time when our products are being used widely by researchers around the world to understand and fight COVID-19,” 10x Genomics commented in a statement provided to Cyberscoop.

Jürgen Stock, Secretary General of international crime-fighting agency Interpol stated, “As hospitals and medical organizations around the world are working non-stop to preserve the well-being of individuals stricken with the coronavirus, they have become targets for ruthless cybercriminals who are looking to make a profit at the expense of sick patients.”
I pondered what to write in this edition. The world has changed so much since our last publication. The COVID-19 pandemic is at the front of everything we do and think about, it seems. And while it should, because this is not a virus to be messed with, there are other things looming out there as well, so I thought I would take some time to mention them here.

The IT Conference is currently scheduled for October 21st. We really do not believe that anyone in the United States will be attending large indoor events until there is a cure for this virus. So, we are looking to present a virtual event, which is exciting, new and different. As soon as we have all the details, we will be sure you know about it. If you have already registered, great. You need to do nothing. If you have not, let us know that, too! Like many other businesses, the IT Project relies on attendance at these events to support our programming. The fears are that a virtual event may not be as interactive or fun to attend. But, I can tell you we will make this event as much fun as one can have in a virtual environment!

As if this virus wasn’t scary enough, please read through this edition of Bits & Bytes because it is not just the virus that is looking to attack you. Scammers are using this pandemic in the most notorious ways by preying on those who are already vulnerable or working from home. In the past three weeks alone, I have received multiple e-mails from my “boss” asking that I wire money to some bank account. Really? My staff has put a tag line at “EXTERNAL” on every e-mail that is generated outside our association. So, even if it actually looks like my boss sent me an e-mail, as soon as I see the word “EXTERNAL” in the subject line, it is a dead giveaway that this e-mail wasn’t from her.

Remember, please educate your staff not to give out personal information, bank information or other private information to anyone without first checking to see if the person or organization is legitimate. Call the person on the telephone from your own contact list. If you are contacted by a third party, do not use the number they give you to contact them, but rather, do an internet search and use the number shown on the website.

Since mid-March, the IT Project has worked diligently to support agencies quickly transitioning to a remote workforce with tele-mental health. All of the agencies we support were well positioned already, due to prior recommendations of the IT Project. While some agencies were not quite as ready as others, the IT Project engineers and help desk team have been actively supporting providers throughout the state with remote management and maintenance on their systems.

I wish everyone the best of health during these times. Please do whatever you can to stay safe, both in person and online!

Peace,

June Noto
June Noto
Vice President
IT Project

---

**New Updates to Microsoft Browser Edge Offer Unique Features and Benefits**

The discontinuation of Windows 7 signifies the end of the long-standing browser option of Internet Explorer. However, many users and organizations have been choosing to use better and sleeker browser options. The vast majority of computer users have been using Google Chrome, Mozilla Firefox or Safari as their browser of choice, and this has been our recommendation for a long time now. Microsoft’s release of Microsoft Edge, the most recent iteration of Explorer, has had the same success as its older browser for many reasons. Its shortcomings include a lack of app support, native connection to Bing as a search browser, and an overall clunky feeling. However, this has changed, as Microsoft has been working on a new browser for the past two years or so. Microsoft decided to rebuild Edge from scratch, but this time used the open source Chromium as a base. Chromium is the base that Google Chrome is built from, which has given Edge some new unique properties. The biggest improvement to Edge with this change is the large number of add-ons uniquely made for Chrome and Chromium. Coupled with the speed of the browser itself, Edge took a huge step forward as a strong alternative to becoming the go-to web browser in the future months. With Edge getting all these new tools and improvements, it doesn’t lose one of its greatest default features. Edge retains its native Internet Explorer compatibility mode, which allows those older Internet Explorer only sites to be useable with Edge’s sleek new upgrade. In addition, there is still one large pressing advantage Edge Chromium has over its competition and your other options. Edge Chromium will come pre-installed on all Windows machines in the near future, meaning no more downloading other browsers out of necessity, getting the world closer to computers that will be ready right away. We urge you to give Edge Chromium a try before it’s pushed to all Windows machines through a future Windows update. For more information on the Edge updates, visit microsoft.com/en-us/edge.

---

**No COVID-19 Respite: Ransomware Keeps Pummeling Health Care**

Continued from page 1

“The attacks are as prevalent as ever. There has been no abatement, empathy or free decryptor granted by cybercriminals,” claims Bill Siegel, CEO of ransomware incident response firm Coveware.

“Ransomware attacks on healthcare providers are occurring with the same frequency as this time last year. There is no ceasefire,” says Brett Callow, a threat analyst at cybersecurity firm Emsisoft, adding, “It’s not only attacks on healthcare providers that are concerning; attacks on the medical supply chain could prove problematic, too. In recent weeks, we’ve seen attacks on research labs, medical device manufacturers and logistics companies and all of these have the potential to indirectly impact patient care and result in the loss of life.”

Malware is primarily spread through e-mails disguised as coronavirus correspondence, and Interpol is working with countries targeted by these cybercriminals to help block these attacks, which are largely infecting systems with ransomware. The e-mails are falsely claiming to contain coronavirus information or advice regarding the coronavirus from a government agency, which encourages recipients of the e-mails to click on infected links or attachments, which then encrypt their data.
Sodinokibi Scans for Vulnerable VPNs

In the worldwide campaign to “flatten the curve” of COVID-19 infections, a number of businesses are instructing their employees to work remotely in accordance with social distancing measures. This is leading to an uptick in cybercrime organizations attacking vulnerable Virtual Private Network (VPN) systems.

While there are numerous ransomware operators at work, one of the most prolific is Sodinokibi, also known as REvil and Sodin. Created in April 2019, Sodinokibi operates as one of the most prolific ransomware-as-a-service organizations. REvil ransomware configurations point to more than 1,000 controllers. Interestingly, the live domains we verified all were WordPress websites, so it is probable they might be compromised by the operators or purchased from other cybercriminals,” says Cybercrime intelligence firm Intel 471.

It is critical for organizations to make sure they have installed the latest patches that have been released to fight vulnerabilities and increase cybersecurity. Many organizations have failed to install these critical patches in a timely manner. For example, ransomware victims Finastra and Travelex appear to have been hacked via unpatched VPN infrastructure - unpatched Citrix gateway servers and unpatched Pulse Secure VPN servers, respectively. Among the organizations that have failed to patch critical flaws in their VPN systems are “several dozens of hospitals with vulnerable gateway and VPN appliances in their infrastructure,” says Microsoft, adding that it has alerted them to the flaws.

“REvil ransomware configurations point to more than 1,000 controllers. Interestingly, the live domains we verified all were WordPress websites, so it is probable they might be compromised by the operators or purchased from other cybercriminals,” says Cybercrime intelligence firm Intel 471.

It is critical for organizations to make sure they have installed the latest patches that have been released to fight vulnerabilities and increase cybersecurity. Many organizations have failed to install these critical patches in a timely manner. For example, ransomware victims Finastra and Travelex appear to have been hacked via unpatched VPN infrastructure - unpatched Citrix gateway servers and unpatched Pulse Secure VPN servers, respectively. Among the organizations that have failed to patch critical flaws in their VPN systems are “several dozens of hospitals with vulnerable gateway and VPN appliances in their infrastructure,” says Microsoft, adding that it has alerted them to the flaws.

“REvil ransomware configurations point to more than 1,000 controllers. Interestingly, the live domains we verified all were WordPress websites, so it is probable they might be compromised by the operators or purchased from other cybercriminals,” says Cybercrime intelligence firm Intel 471.

It is critical for organizations to make sure they have installed the latest patches that have been released to fight vulnerabilities and increase cybersecurity. Many organizations have failed to install these critical patches in a timely manner. For example, ransomware victims Finastra and Travelex appear to have been hacked via unpatched VPN infrastructure - unpatched Citrix gateway servers and unpatched Pulse Secure VPN servers, respectively. Among the organizations that have failed to patch critical flaws in their VPN systems are “several dozens of hospitals with vulnerable gateway and VPN appliances in their infrastructure,” says Microsoft, adding that it has alerted them to the flaws.

“When we sent a targeted notification with important information about the vulnerabilities, how attackers can take advantage of them, and a strong recommendation to apply security updates that will protect them from exploits of these particular vulnerabilities and others,” Microsoft reported.

Amid the chaos of the COVID-19 pandemic, and many hospitals struggling to manage massive caseloads, did these alerts help - and were they even noticed? Microsoft has not yet responded to requests for comment about how many hospitals it alerted, via what channels or how many hospitals confirmed receipt of the alerts and have now applied the patches.

Prevention and education remain paramount in the fight against cybercrime, and it is especially important that organizations remain vigilant as the war against coronavirus continues.
Microsoft’s Power BI: A Powerful yet Easy-to-Use Tool

The digital age continues to decrease the time and effort required to do the busy work of today’s assignments. While in the past, info graphs would require multiple pages and an excessive amount of time to formulate, modern programs such as Microsoft’s Excel have made the process more streamlined, even allowing templates and quick data changes to view different scenarios. The natural evolution of productivity continues through Microsoft’s Power BI.

Microsoft’s Power BI is a currently available and very valuable tool able to be brought to any business environment. The piece of software is Microsoft’s answer to a growing need for Business Intelligence (BI) programs, which have recently been changed to more accessible Business Analytics. The powerful piece of software is designed to offer ease-of-use, allowing all information to be seen at a glance in one easy-to-use package. While tools like Microsoft Excel offer powerful solutions to data storage and algorithmic logic, it does a terrible job of displaying the information in an easily digestible way. Power BI will allow any grouping of information to be displayed in a quick, at-a-glance kind of way, taking significantly less at the users’ and corporations’ time to understand information.

This program has a multitude of accessibility features to allow seamless visuals in response to a need for data. Using features such as downloadable custom visuals and their story mode, you can create and view excellent representations of data to be very digestible. Point-Interval graphs that change on a year-by-year basis are then able to transition that data into bar graphs seamlessly, importing that data from a plethora of sources. It also includes features to move forward in time as well, allowing visuals on projection into the future to see how the data will change based on prior movements. Regardless of your specific use case, there will be a very beneficial way to incorporate Power BI into your work environment.

For more information on Power BI, please visit powerbi.microsoft.com/en-us/desktop/

IoT raises Privacy and Security Concerns

By Kenneth Romer, Certified Ethical Hacker, GIAC Certified Penetration Tester, CIO, ITMS LLC

If you are not familiar with the term IoT, let’s start with some background. IoT is an abbreviation to describe the Internet of Things. Well, that still may not be much help to all readers. An easier way to think of it is anything connected to the Internet that may not be considered a traditional computer or networking device. A few examples are lightbulbs, door locks, appliances and yes, those devices offered by Amazon, Google and others that are in your home waiting for you to command them.

As you may have surmised from the title of this article, I am very cautious and skeptical about these devices. Most of these items are built for ease of use. This is done by the manufacturers, so the average person can set them up without the need for a lot of computer or network security skill. Unfortunately, when you increase ease of use, privacy and security are lowered. Many of these devices come with built-in usernames and passwords that the average user never changes, and some arrive with pre-loaded usernames and passwords you could not alter even if you wanted to change them. There are stories of in-home video systems exposed to the Internet for all to view with no knowledge of the owners. People have purchased IoT front door locks that others have sold online second hand; however, the original owners and any individuals they gave access to can still use the devices and know where you live.

OK, let’s move onto privacy. Many of these devices are now being subpoenaed by the courts and law enforcement to be used as evidence against the owners of IoT devices. A man’s pacemaker records helped prove he set fire to his own home. An Amazon Alexa-enabled item was perused in a murder trial. Yes, I have heard these devices only are listening when the trigger word is used, but in some form, they must still always be listening. The authorities wanted all recordings this device may have captured during a time at which they believed a murder occurred. In the collection of evidence for this same case, police also subpoenaed his IoT water meter, which proved he was not accurate with his statement to the authorities.

The stories go on and on, so what to do? I am not saying to never use an IoT item; however, do your research and understand the conveniences versus the risk. After that, you will be able to make a better educated decision if this is something you want in your home or business. Also, there are ways to make these devices safer on your networks.

I will be covering how to use these devices to better protect your networks, as well many other topics at the NJAMHAA IT Project’s conference. No Fooling! IT is Critical. On October 21st.

qualifacts

Tracy Deep
Senior Account Executive
tracy.deep@qualifacts.com
330.310.7744

Abs

Traverise

OSA

Ramirez

Biostatistician

Summer 2020
NJAMHAA’s 2020 IT Project Conference:
No Fooling - IT Is Critical!
10.21.20

Sandra Rocha-Bucco
Client Development Executive
908.347.1317
srocha@ntst.com

Kevin Vitale
Sales
keinv@go-domain.com
Domain Computer Services

Erica James
Sales Executive
eljames@nextgen.com

Dawn Buck
Director of Sales
dawn@nextstepsolutionsinc.com

Netsmart Technologies

Domain Computer Services

nextgen healthcare