News from Wednesday, September 18, 2019. Reported on Thursday, September 19, 2019.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

Source: Information Security Media Group

Victim Total Soars in County Health Data Breach

A Minnesota county that originally reported last December that a hacking incident affected about 600 individuals now says about 118,000 may have had healthcare data exposed. What's behind the huge spike?

Final breach victim counts can sometimes jump significantly because preliminary investigations "may be too narrow in scope or not performed with sufficient expertise," says Kate Borten, president of privacy and security consulting firm The Marblehead Group.

"It is not uncommon at all to find that the number of victims impacted by a breach grows over time," says former healthcare CIO David Finn, executive vice president at security consulting firm CynergisTek. Attackers can penetrate a target and remain invisible to the organization for weeks, months or even years, he adds.

When the victim count in a health data breach changes substantially from the time it was first reported to HHS, entities need to provide government agencies and individuals affected with updated reports.

"Especially if the victim count exceeds 500, HIPAA breaches require public notice, and a significantly larger number could mean media notices need to be more widespread," say Kate Borten, president of privacy and security consulting firm The Marblehead Group.

"If significant details change, then covered entities must update HHS with that information. And, of course, newly identified victims must be notified individually - typically through the mail - no later than 60 days from discovery."

"Sometimes there are legitimate challenges in meeting the 60-day reporting time limit" under HIPAA for breaches affecting 500 or more individuals, Borten says. "But often it appears that some organizations treat the reporting timeframe as a desirable goal, but [one that is] not enforced."

Lumin PDF Leak Exposed Data on 24 Million Users

Ignoring a breach disclosure can have ugly consequences. Case in point: Lumin PDF, a PDF editing tool, which saw data for much of its user base - about 24.3 million - published in an online forum late Monday. Lumin PDF, a product of NitroLabs of New Zealand, is free PDF editing tool that offers tiered subscriptions for more advanced features and storage.

The published data includes users' full names, Google profiles, email addresses, locales and in some cases, Google access tokens and hashed passwords.

The person who says he found the data, who asked not to be named, tells Information Security Media Group that his team found a MongoDB database belonging to Lumin PDF accessible online around mid-April. He says he reached out to NitroLabs, including its founder and CEO Max Ferguson, on his personal email, but did not receive a response.

Efforts to reach Ferguson, a native New Zealander whose LinkedIn profile says he is a research assistant at Stanford University in California, and NitroLabs, were unsuccessful.

A sensitive aspect of the breach is the leak of Google account access tokens. Lumin PDF allows users to use either their Google or Dropbox credentials to sign into the service. That allows Lumin to have access to, for example, a person's Google Drive storage and email.

Capturing those access tokens is valuable to cybercriminals, because it could provide access to someone's Dropbox or Google Drive account. One of the comments posted following the leak on the hacker forum says: "Data looks good and it's not 'that' old. So you might be able to reuse some of these Google tokens since they usually don't expire that quickly."

The person who found the data says he held off posting it sooner due to the access tokens, saying that the four-month delay should have allowed most of the tokens to expire.

Adoption of AI Surveillance Technology Surges

Governments are rapidly adopting AI surveillance technology to advance political goals, according to a new report from the Carnegie Endowment for International Peace. While Chinese suppliers dominate, liberal democracies and authoritarian regimes alike are developing and procuring such technology.

Source: Bleeping Computer

Windows Defender Antivirus Scans Broken After New Update

Microsoft has released a new update for Windows Defender that has broken both the Quick and Full antivirus scans. When users use these scan options, Windows Defender will only scan approximately 40 files. This issue is now resolved in "Security Intelligence Update for Windows Defender Antivirus - KB2267602 (Version 1.301.1684.0)" definitions.

Amadey Botnet Targets U.S. Taxpayers with Tax Refund Notice

A phishing campaign has been spotted recently delivering Amadey botnet malware to taxpayers in the U.S. through fake income tax refund emails.

Security researchers at Cofense noticed this phishing campaign bypassing a secure email gateway (SEG) solution and dropping emails with malicious attachments.

The infection chain starts with a message pretending to be from the Internal Revenue Service (IRS), informing the recipient that they're eligible for a tax refund. The trick is pretty clever, as the attacker does not ask for credentials

but instead provides a temporary username and password to log into the fake IRS portal, linked to in the message body.

Victims are deceived that they can get the refund after filling in some details in a document available from the fraudulent site. The file is a ZIP archive that contains a Visual Basic script dropper.

Smominru Mining Botnet In Cyber Turf War With Rival Malware

The Smominru mining botnet continues to wreck havoc on corporate machines by not only installing cryptominers, but also stealing credentials, installing backdoors, and making system configuration modifications that could affect the proper operation of an infected machine.

Smominru is a wormable malware that spreads using the EternalBlue exploit and by brute forcing RDP, MSSQL, Telnet and other exposed services. Once the botnet gains access to a machine, it will attempt to remove rival malware, secure the box from further infections, and then install cryptomining software, steal login credentials, install backdoors, and spread laterally to other machines.

As this worm uses the EternalBlue exploit, the researchers note that most of the infected operating systems are Windows 7 and Windows Server 2008, which include working exploits for this vulnerability.

New TortoiseShell Group Hacks 11 IT Providers to Reach Their Customers

A newly discovered threat group that security researchers call TortoiseShell is compromising IT providers in what seems to be supply-chain attacks intended to reach the network of specific customers.

Security researchers at Symantec identified 11 organizations that had been hit by TortoiseShell. Most of the targets are based in Saudi Arabia and in at least two cases there are enough clues to conclude that the attacker had privileges of a domain administrator, which come with access to all systems on the network.

Source: Krebs on Security

Before He Spammed You, this Sly Prince Stalked Your Mailbox

A reader forwarded what he briefly imagined might be a bold, if potentially costly, innovation on the old Nigerian prince scam that asks for help squirreling away millions in unclaimed fortune: It was sent via the U.S. Postal Service, with a postmarked stamp and everything.

In truth these old fashioned “advance fee” or “419” scams predate email and have circulated via postal mail in various forms and countries over the years.

The recent one (pictured in Krebs’s article) asks for help in laundering some $11.6 million from an important dead person that anyway has access to a secret stash of cash. Any suckers who bite are strung along for weeks while imaginary extortionists or crooked employees at these bureaucratic institutions demand licenses, bribes or other payments before disbursing any funds. Those funds never arrive, no matter how much money the sucker gives up.

It's easy to laugh at this letter, because it's sometimes funny when scammers try so hard. But then again, maybe the joke's on us because sending these scams via USPS makes them even more appealing to the people most vulnerable: Older individuals with access to cash but maybe not all their marbles.

The losses from these types of scams are sometimes hard to track because so many go unreported. But they are often perpetrated by the same people involved in romance scams online and in so-called 'business email compromise" or BEC fraud, wherein the scammers try to spoof the boss at a major company in a bid to get wire payment for an "urgent" (read: fraudulent) invoice.

These scam letters are sometimes called 419 scams in reference to the penal code for dealing with such crimes in Nigeria, a perennial source of 419 letter schemes. A recent bust of a Nigerian gang targeted by the FBI gives some perspective on the money-making abilities of a $10 million ring that was running these scams all day long.

Source: arstechnica.com

Protocol found in webcams and DVRs is fueling a new round of big DDoSes

WSD is supposed to be confined to local networks. It's not, and researchers are concerned.

Hackers have found a new way to amplify the crippling effects of denial-of-service techniques by abusing an improperly implemented tool found in almost 1 million network-connected cameras, DVRs, and other Internet-of-things devices.

The technique abuses WS-Discovery, a protocol that a wide array of network devices use to automatically connect to one another. Often abbreviated as WSD, the protocol lets devices send user datagram protocol packets that describe the device capabilities and requirements over port 3702. Devices that receive the probes can respond with replies that can be tens to hundreds of times bigger. WSD has shipped with Windows since Vista and is one of the ways the operating system automatically finds network-based printers.

The WSD specification calls for probes and responses to be restricted to local networks, but over the past few months, researchers and attackers have started to realize that many Internet-of-things devices allow devices to send probes and responses over the Internet at large. The result: these improperly designed devices have become a vehicle capable of converting modest amounts of malicious bandwidth into crippling torrents that take down websites. Depending on the device, responses can be anywhere from seven to 153 times bigger, an amplification that puts WSD among the most powerful techniques for amplifying distributed denial of service attacks.

Source: govtech.com

Stolen Computers in Atlanta Hold Statewide Voter Data

Two computers that are used to check in voters were stolen from a west Atlanta precinct hours before polls opened for a recent school board election, and those computers hold statewide voter data.

Officials replaced the computers before voters arrived, and the election wasn't disrupted, according to the Georgia Secretary of State's Office.

The express poll computers contain names, addresses, birth dates and driver's license information for every voter in the state, said Richard Barron, Fulton County's elections director. They don't include Social Security numbers. They are password-protected, and the password changes for every election.

The computers, which were in a locked and sealed case, haven't been recovered.

Georgia Secretary of State Brad Raffensperger said he's concerned about the stolen election equipment. "They may not have realized what they were stealing. They may have just thought they were stealing computer hardware of some sort, but they stole a whole lot more than they thought," Raffensperger said. "They're in a whole lot of trouble. There will be a thorough investigation."

Barron said the machines don't connect to the internet and can't be used for other purposes. He said they can't be tracked. "I'm sure whoever took them had no idea what was in that case," he said. "A Palm Pilot from 2000 is probably more sophisticated than those things. They're pretty primitive pieces of equipment."

Source: NIST

Transport Layer Security (TLS) Server Certificate Management Industry Day Is Next Week

There's still time to register for TLS Server Certificate Management Industry Day on **September 26, 2019**, at the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE).

The project team will discuss their contributions to NIST's Special Publication 1800-16 *Securing Web Transactions: TLS Server Certificate Management* draft practice guide which can benefit executives, chief information security officers, system administrators, or anyone who has a stake in protecting his or her organization's data and overall operational security.

What you'll learn. During this half-day event, members of the project team will:

- Share why having a TLS management plan can protect your organization's data, information technology operations, reputation and bottom line
- Explain the risks organizations face by not having a TLS management plan
- Demonstrate an example implementation of TLS certificate management in a typical enterprise organization using commercial off-the-shelf technologies
- Show how the practice guide can aid your organization's TLS management efforts

This event is free, but you must register in advance to attend.

Location: The NCCoE, 9700 Great Seneca Highway, Rockville, Maryland 20850

Time: Check-in begins at 8:30 a.m. EST. The formal programs begins at 9:00 a.m. and conclude at noon.

Questions? Please send an email to tls-cert-mgmt-nccoe@nist.gov.

Long Form Article Source: ZD-Net by Steve Ranger (11-13 minutes)

Ransomware: 11 steps you should take to protect against disaster

Ransomware continues to be one of the biggest menaces on the internet. Clicking on the wrong link could be enough to set off a sequence of events that ends with all your data being encrypted by crooks, who will only unlock it in return for a hefty ransom -- usually in bitcoin or another hard-to-trace cryptocurrency.

Criminal ransomware gangs are well financed (thanks to all those bitcoin ransoms) and employ increasingly sophisticated tactics. Only low-level crooks are interested in encrypting PCs one-by-one: the big gangs seek backdoors into corporate networks and then explore until they are ready to cause maximum chaos (and a big payday) by encrypting as many devices as possible in one go.

It's not just criminal gangs that have noticed the power of ransomware: state-backed hacking groups have also used ransomware to create both chaos and profit for their backers.

What we're seeing is an arms race between the crooks looking for new ways to compromise systems and businesses trying to plug every gap in their defenses.

This level of threat means there's no way to absolutely protect yourself or your business from ransomware, or indeed any other kind of malware. But there are a number of steps you can take to minimize your attack surface.

11. MAKE SURE YOUR ANTIVIRUS SOFTWARE IS UP TO DATE

This seems obvious, but is occasionally neglected by smaller organizations. Many antivirus packages now offer ransomware-spotting features or add-ons that try to spot the suspicious behavior that's common to all ransomware: file encryption. These apps monitor your files for unexpected behavior -- like a strange new piece of software trying to encrypt them all -- and aim to prevent it. Some security packages will even make copies of the files that are threatened by ransomware.

10. UNDERSTAND WHAT'S HAPPENING ACROSS THE NETWORK

There's an array of related security tools -- from intrusion prevention and detection systems to security information and event management (SIEM) packages -- that can give you an insight into the traffic on your network. These products can give you an up-to-date view of your network, and should help you spot the sort of traffic anomalies that might suggest you've been breached by hackers, whether they are intent on infecting your systems with ransomware or have something else in mind. If you can't see what's happening on the network, there's no way you can stop an attack.

9. SCAN AND FILTER EMAILS BEFORE THEY REACH YOUR USERS

The easiest way to stop staff clicking on a ransomware link in an email is for the email never to arrive in their inbox. This means using content scanning and email filtering, which ought to take care of many phishing and ransomware scams before they actually reach staff.

8. HAVE A PLAN FOR HOW TO RESPOND TO A RANSOMWARE ATTACK, AND TEST IT

A recovery plan that covers all types of tech disaster should be a standard part of business planning, and should include a ransomware response. That's not just the technical response -- cleaning the PCs and reinstalling data from backups -- but also the broader business response that might be needed. Things to consider include how to explain the situation to customers, suppliers and the press. Consider whether regulators need to be notified, or if you should call in police or insurers. Having a document is not enough: you also need to test out the assumptions you have made, because some of them will be wrong.

7. THINK VERY LONG AND HARD BEFORE YOU PAY A RANSOM

Ransomware crooks have found their way through your defenses and now every PC across the business is encrypted. You could restore from backups, but it will take days and the criminals only want a few thousand dollars. Time to pay up?

For some, that may be the obvious conclusion. If the attackers only want a relatively small amount then it might, in the short term, make business sense to pay up because it means the business can be up and running again quickly. However there are reasons why you might not want to pay.

First, there's no guarantee that the criminals will hand over the encryption key when you pay up -- they are crooks, after all. If your organization is seen to be willing to pay, that will probably encourage more attacks, either by the same group or others. There's also the broader impact to consider. Paying a ransom, either from your own funds or via cyber insurance, is to reward these gangs for their behavior. It will mean that they are even better funded and able to run even more sophisticated campaigns against you or other organizations. It might save you some pain in the short term, but paying the ransom only fuels the ransomware epidemic.

6. UNDERSTAND WHAT YOUR MOST IMPORTANT DATA IS AND CREATE AN EFFECTIVE BACKUP STRATEGY

Having secure and up-to-date backups of all business-critical information is a vital defense, particularly against ransomware. In the event that ransomware does compromise some devices, having a recent backup means you can restore that data and be operational again fast. But it's vital to understand where that business-critical data is actually being held. Is the CFO's vital data in a spreadsheet on their desktop, and not backed up in the cloud as you thought? It's no good having a backup if you're backing up the wrong stuff, or backing it up so infrequently that it's useless.

5. UNDERSTAND WHAT'S CONNECTED TO YOUR NETWORK

PCs and servers might be where your data resides, but they aren't the only devices you have to worry about. Thanks to the office wi-fi, the Internet of Things and working from home, there's now a wide variety of devices connecting to the company network, many of which will lack the kind of built-in security you'd expect from a corporate device. The more devices, the greater the risk that one will offer hackers a backdoor into your network, and then use that access to move through your systems to more lucrative targets than a badly secured printer or a smart vending machine. Also, think about who else has access to your systems: are your suppliers aware of the potential risk of ransomware and other malware?

4. MAKE IT HARDER TO ROAM ACROSS YOUR NETWORKS

Ransomware gangs are increasingly looking for the biggest possible payday. Encrypting the data on one PC isn't going to make them rich, so they are likely to gain access to a network and then explore widely in order to spread their malware as far as possible before pulling the trigger and encrypting everything. Make this harder by

segmenting networks, and also by limiting and securing the number of administrator accounts, which have wide-ranging access. Phishing attacks have been known to target developers simply because they have broad access across multiple systems.

3. TRAIN STAFF TO RECOGNISE SUSPICIOUS EMAILS

One of the classic routes for ransomware to enter your organization is via email. That's because spamming out malware to thousands of email addresses is a cheap and easy way for ransomware gangs to try and spread malware. Despite the basic nature of these tactics, it's still depressingly effective.

Training staff to recognize suspicious emails can help protect against ransomware and other email-borne risks like phishing. The basic rule: don't open emails from senders you don't recognize. And don't click on the links in an email if you aren't absolutely sure it is legitimate. Avoid attachments whenever possible and beware of attachments that ask you to enable macros, as this is a classic route to a malware infection. Consider using two-factor authentication as an additional layer of security.

2. CHANGE DEFAULT PASSWORDS ACROSS ALL ACCESS POINTS

Clicking on a bad link in an email is probably the best-known way of getting infected with malware, but it's far from the only way. Nearly a third of ransomware was distributed via brute force and remote desktop protocol (RDP) attacks, according to research by F-Secure. Brute force attacks are attempts by hackers to access servers and other devices by trying as many passwords as possible, usually with the aid of bots, in the hopes of hitting the jackpot.

As many companies fail to change default passwords or use easily-guessed combinations, brute force attacks are regularly effective. RDP allows remote control of PCs, and is another common ransomware attack avenue. There are steps you take to reduce the risk of an attack via RDP, ranging from ensuring strong passwords are used, to changing the RDP port, to limiting its availability to only the devices that really need it.

1. APPLY SOFTWARE PATCHES TO KEEP SYSTEMS UP TO DATE

Patching software flaws is a painful, time-consuming and tedious job. It's also vital to your security. Malware gangs will seize on any software vulnerabilities and attempt to use them as a way into networks before businesses have had time to test and deploy patches. The classic example of what happens if you don't patch fast enough is WannaCry. This ransomware caused chaos in the summer of 2017, including significantly disrupting the NHS in the UK. A patch for the underlying Windows Server Message Block protocol exploit that allowed WannaCry to spread so far had actually been released several months before the ransomware hit. But not enough organizations had applied the fix to their infrastructure, and over 300,000 PCs were infected. It's a lesson many organizations are still to learn: one in three IT professionals admitted that their organization had been breached as a result of an unpatched vulnerability, according to a survey by security company Tripwire.

BONUS TIP: DON'T PLUG IN THAT RANDOM USB STICK...

...you know, the one you found in the street by the office.