trinity times

December 2019

Christmas Fun Facts

1. "Jingle Bells" was written for Thanksgiving, not Christmas
2. Rudolph's red nose is probably the result of a parasitic infection of his respiratory system.
3. The "X" in "Xmas" doesn't take "Christ" out of "Christmas". In fact, in the Greek alphabet, the letter X ("chi") is the first letter of the Greek word for Christ or Christos.
4. The first artificial Christmas Tree wasn't a tree at all. It was created out of goose feathers that were dyed green.

This monthly publication is provided courtesy of Lance Reichenberger, President of Trinity Networx, LLC

Give us a call and let us show you what fast, friendly and highly responsive outsourced IT services should be for your small to medium business: 951-479-1727

Crippling Ransomware attacks targeting US Cities on the rise

New York (CNN) Kevin Collier
Updated May 10, 2019

Targeted ransomware attacks on local US government entities -- cities, police stations and schools -- are on the rise, costing localities millions as some pay off the perpetrators in an effort to untangle themselves and restore vital systems.

The tally by cybersecurity firm Recorded Future -- one of the first efforts to measure the breadth of the assaults -- found that at least 170 county, city or state government systems have been attacked since 2013, including at least 45 police and sheriff's offices.

The firm compiled all known instances of ransomware infections of local government systems, a type of cyberattack that encrypts a computer's files, where the attacker demands payment --usually in bitcoin -- for a key to unlock them.

The federal government and the FBI do not track the attacks nationwide.

22 known attacks this year

There have been 22 known public-sector attacks so far in 2019, which would outpace 2018, and that does not take into account that attacks often aren't reported until months or years after they're discovered.

The latest major city to be hit is Baltimore, which was infected with ransomware Tuesday. It has quarantined its networks and been forced to provide most of its municipal services manually.

"It's frustrating. It's unfortunate. But we're working through it," Baltimore City Council President Brandon Scott said in a news conference Friday.

At the end of March, New York's state capital, Albany, quietly admitted it had

Continued on pg.2

Continued from pg.1

been hit with ransomware, on a Saturday -- a typical choice, as hackers calculate attacks can do more damage when IT staff aren't working.

The city announced the attack the day it was discovered but downplayed its severity, announcing only that it had affected a handful of city services including the issuing of marriage licenses and birth certificates. Many of those problems were cleared up by the beginning of the workweek.

However, City Hall didn't mention that the Albany Police Department's systems had been significantly impacted.

"We were crippled, essentially, for a whole day," Gregory McGee, a patrolman who is vice president of the Albany Police Department's union, told CNN at the time.

"All of our incident reports, all of our crime reports, that's all digitized," McGee said, which meant cops had to write down everything that happened on paper. They showed up to work and had no access to staff schedules. "We were like, who's working today?" McGee said. "We have no idea what our manpower is, who's supposed to be here."

The Albany mayor's office didn't respond to multiple requests for a status update on the attack, though a spokesperson had previously said the city would make an announcement once it had been cleaned up.

First attack in 2013

The first known small government ransomware infection hit the small town of Greenland, New Hampshire, in 2013 but the number of attacks didn't explode until 2016, when there were 46.

The number dropped to 38 in 2017 -- indicative of a temporary worldwide reduction in ransomware infections -- before rising to 53 last year. Industry estimates suggest ransomware attacks cost billions of dollars each year, though it's hard to put a precise number on the costs because there's no comprehensive record of attacks across the globe and not all of them are reported. The number of victims who have self-reported to the FBI's Internet Complaint Center has decreased in recent years. There were 2,673 cases in 2016; 1,783 in 2017; and 1,493 last year. Those numbers don't reflect all the cases the FBI is aware of through field office reports.

This suggests hackers are being more discerning about who they decide to target, to maximize the amount of money they can make, according to Supervisory Special Agent Adam Lawson of the FBI's Major Cyber Crimes Unit. "It's less of an individual user, and it's more targeting towards private sector, businesses, or public sector, municipalities, police departments, etc. Those attacks are going up, while attacks on individual users are going down," Lawson told CNN.

"I think our assessment is that (who gets targeted is) who's got more money. An individual user, if their computer is impacted by ransomware, it's kind of a cost-benefit analysis: 'I've had this computer for five years. I'm not going to pay you $300 to unlock my computer; I'll just go get another one.' Whereas for a business network, if you lock up the main controller or some vital records, it's much more complicated for them. So it's probably based on who's paying the money."

Perpetrators

Attacks are carried out by a wide variety of actors, ranging from criminal gangs to people allegedly working at least tangentially with their countries' governments. There are likely other suspects the FBI has identified but the agency is waiting for them to travel to countries where the US is able to coordinate arrests."We are aware of who some of these people are," Lawson said. "Just because we don't come out and say it doesn't mean that we're not waiting for them to perhaps travel somewhere, where we can get them."

Shiny New Gadget Of The Month:

Holiday tech gifts under $25 that wow!

Courtesy of Amazon this neat little gadget is sure to get your tech friends to smile.

ONXE USB LED Clock Fan with Real Time Display Function,USB Clock Fans,Silver,1 Year Warranty

Price: $13.99 FREE Shipping on orders over $25.00 shipped by Amazon or get Fast, Free Shipping with Amazon Prime & FREE Returns

PVC soft fan blades for safety, mental flexible neck.

Simply plug into any USB port on notebook or PC to create a gentle refreshing breeze.

Keep cool and display cool messages at your office or on the go with the USB LED Message Fan.USB FAN 1 year warranty,Fan only through ONE TWO brand stores sales, other stores selling fake, do not enjoy 1 year warranty service

Inspirational Leadership Spotlight Michael S. Hyatt

Michael S. Hyatt is an American author, podcaster, blogger, speaker, and the former chairman and CEO of Thomas Nelson. He has written several books about leadership, planning, and goal setting. Courtesy Wikipedia

5 MARKS OF AUTHENTIC LEADERS
Courtesy michaelhyatt.com

1. AUTHENTIC LEADERS HAVE *INSIGHT*

Sometimes we refer to this as *vision*, but that usually has exclusive reference to the future. While leaders must have vision, they need more.

Leaders need wisdom and discernment for the present. They need to be able to look at complex situations, gain clarity, and determine a course of action.

Steve Jobs stands as one of the best examples of this in recent decades. When he returned as CEO of Apple, Jobs inherited a mess. But he had the necessary insight to reboot the business and dominate the industry.

2. AUTHENTIC LEADERS DEMONSTRATE *INITIATIVE*

Leaders go first. They don't sit on the sidelines. They don't ask others to do what they are unwilling to do themselves. Instead, they lead by example. This is what distinguishes leaders from theoreticians and armchair quarterbacks.

When I think of a leader that really took initiative, I think of Lt. Col. Hal Moore. Famously depicted by Mel Gibson in the movie, *We Were Soldiers* Moore told his troops, before leaving for Vietnam, "We are going into battle against a tough and determined enemy. I can't promise you that I will bring you all home alive. But this I swear, before you and before Almighty God: that when we go into battle, I will be the first to set foot on the field, and I'll be the last to step off. And I will leave no one behind. Dead or alive, we will all come home together, so help me God."

3. AUTHENTIC LEADERS EXERT *INFLUENCE*

It's no coincidence
that influence and influenza come from the same root word. Real leaders are contagious. People "catch" what they have.
People are drawn to their vision and their values. They are able to gather a following and move people to act.

4. **AUTHENTIC LEADERS HAVE *IMPACT***

The measure of leadership cannot be found in the leader. It's found in the impact the leader has on his or her followers.

At the end of the day, leaders make a difference. They're either instrumental in creating real and lasting change, or they're not leaders. They're just entertainers.

5. **AUTHENTIC LEADERS EXERCISE *INTEGRITY***

Not every leader is benevolent. We can all think of leaders in business, politics, or ministry that have insight, initiative, influence, and impact. But when we look at their lives and legacies, we can see something is still missing—something big.

What is it? Their lives are
not integrated with the highest values. Integrity—or the lack thereof—ultimately determines the quality of a person's impact. In a sense, this is the foundation of authentic leadership.

QuikSilver and Billabong Affected by Ransomware Attack

Action sports giant Boardriders was hit by a ransomware attack that affected some of its subsidiaries, including QuikSilver and Billabong, and forced the company to shut down computing systems all over the world. Boardriders has around 10,000 employees from all over the world and its Quiksilver, Billabong, ROXY, RVCA, DC Shoes, and Element brands are sold in over 110 countries. Following the attack, the company's e-commerce stores displayed messages offering customers 20% off promotions and stating that Boardriders is experiencing shipping delays.

Global-scale ransomware attack

Following the incident, Boardriders said in a statement to ShopEatSurf that the attack impacted multiple systems, from several regions around the world.

"Our IT teams have been working to quickly restore our systems to support our operations, which are now largely transacting and shipping normally," Boardriders also said.

"We are proud of how our teams have responded to this challenge, and we are incredibly grateful for their hard work," the company added. "We also greatly appreciate our customers' and vendors' patience and support during this brief interruption."

While BoardRiders' statement does not detail the type of cyberattack they experienced, sources familiar with the matter told BleepingComputer that they were affected by ransomware. We were further told that this attack occurred during the last week of October 2019.

"They have been in a world of pain. Staff haven't even been able to turn on their com-put-ers and have been banned from us-ing them un-til the whole IT sys-tem is cleaned," an in-dus-try source told pressreader. "There have been ma-jor de-lays in get -ting stock to re-tail-ers and on-line cus-tomers."

BleepingComputer reached out to Boardriders for more details regarding the incident but did not hear back at the time of publication.

Courtesy~
Bleeping Computer
By Sergiu Gatlan
November 8, 2019

iOS App Tries to Warn You of iPhone Hacking Attempts

iVerify will periodically scan your iPhone to sniff out certain 'side effects' that exploited iOS vulnerabilities tend to generate.

A new iOS app launching today promises to detect whether your iPhone has been secretly hacked. The iVerify app comes from security firm Trail of Bits, and it's been designed to periodically scan your device for "security anomalies" that can indicate whether it's been tampered with. If an abnormality is found, the app will show you how you can secure your device.

The $4.99 app addresses a gap in iOS's security: Previously, consumers had no tool to detect whether an iPhone was hacked. As Motherboard notes, Apple has generally locked down all access to iOS's internal processes, making it hard for security researchers to examine the software for bugs. (It was only in August when Apple began issuing special developer iPhones to select security experts to find flaws.)

The company also bans antivirus products on the App Store. Apple has a strict rule against one app scanning

another; all third-party programs have to be "sandboxed" from each other, which effectively bars antivirus scanning.

However, the iVerify app is no antivirus program, according to Trail of Bits. Instead, the product tries to sniff out the "side effects" that exploited iPhone vulnerabilities tend to generate, the company told Motherboard.

The iVerify app offers a potential safeguard against such attacks. To detect the side effects from exploited iPhone vulnerabilities, Trail of Bits studied all past public iPhone jailbreaks. These hacks involve exploiting old flaws to gain root access to iOS, which can allow you to install unauthorized third-party apps, including malware.

Specifically, the iVerify app will scan from a set of indicators, "about 30 or 300, depending on how you count," Dan Guido, CEO of Trail of Bits, told PCMag in an email. He went on to describe the app as a "security multitool," given that the product will come with a whole suite of features, including instructional guides to keep your iPhone activities private.

For example, the app includes a section on preventing data leakage. It'll then advise what settings on iOS you need to modify in order to limit ad tracking, disable location-based ads or stop data sharing with Apple's Siri voice assistant. Expect more guides and security features to be added to the app over time.

Courtesy~ PCMag
By Michael Kan Nov. 14, 2019.