January 2020

TechTidbit.com

brought to you by Tech Experts

10 Most Important CyberAttacks Of The Last Decade

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

The only way to keep history from repeating itself is to learn from the mistakes of the past. The following is a list of the most significant cyberyattacks from the last decade, as compiled by TechTarget:

Yahoo - 2013

With the unfortunate legacy of being the largest breach in the history of the internet, all three billion Yahoo accounts were compromised. The organization took 3 years to notify the public of the breach and that every account's name, email address, password, birthdate, phone numbers, and security answers had been sold on the dark web.

Equifax - 2017

Probably the most damaging attack occurred just 3 years ago with the hack of Equifax. The hackers were successful in gaining access to 143 million Equifax customers and information vital to the lives of all.

The data stolen from Equifax included customer's names, birthdates, social security numbers, driver's license numbers, and addresses, and the hackers released over 200,000 credit card numbers and more than 182,000 documents containing personal identifying information.

Sony Pictures - 2014

Hackers were successful in wreaking havoc on Sony Pictures by releasing damaging emails sent between Sony employees and discussing what they really felt about some of the world's top film stars. The hack was in retaliation for Sony's production of a Seth Rogen film, The Interview, and featured an attempt to assassinate the North Korean leader, and propelled North Korea into international prominence.

Marriott Hotels - 2018

This attack has gained notoriety because the malicious actors behind the scenes had an unprecedented four years with which to move around the Starwood system. The hackers gained access to the names, credit cards, passport numbers, and addresses of millions of people who stayed at the hotel between 2014 and 2018 and no Starwood hotel was left untouched.

Starwood Hotels operate under the brand names of Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Méridien, Tribute, Design Hotels, Element, and the Luxury Collection.

Ashley Madison - 2015

While this attack was not financially significant, the damage it caused was devastating. When hackers breached Ashley Madison, the "discreet extramarital dating website" in 2015, more than 30 million email addresses and hundreds of credit cards were leaked. The company was sued in 2017 for $11 million as a result of the breach, but the ramifications for some were life-altering.

Target - 2013

Affecting more than 40 million Target customers, cybercriminals were successful in obtaining payment card details. In the years following, Target ultimately admitted the number was even larger, and estimated that the impact reached 110 million of their consumers, resulting in the ousting of Target's then CIO.

Capital One - 2019

One of the most recent breaches occurred in July when Capital One bank acknowledged that for almost 14 years (2005 to 2019), hackers gained access to the financial information of 100 million Americans and six million Canadians.

The United States Office of Personnel Management - 2015

Perpetuated by the Chinese government, the attack on the US Office of Personnel Management is considered one of the most significant to ever hit the government in the history of the country.

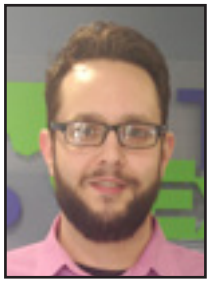
The hackers gained access to 21 million records of current and former government workers, even including information from background checks of individuals

Continued on Page 4

One of the most recent breaches occurred in July when Capital One bank acknowledged that for almost 14 years (2005 to 2019), hackers gained access to the financial information of 100 million Americans and six million Canadians.

Microsoft Starts Forcing November 2019 Update On Users

"The November 2019 update is being pushed out to users, whether you want it or not. While it sounds deceitful, there is – as always with Microsoft – more to it."



Jason Cooley is Support Services Manager at Tech Experts.

The Windows 10 November 2019 update (also known as Version 1909) is live and many users have moved to Microsoft's latest feature update.

As an IT professional here at Tech Experts, it seems like these feature updates happen one right after another.

Although this is not the case as Microsoft only releases feature updates twice a year, the issues we encounter during each feature update's life cycle make it seem that way. The only notable updates between these feature updates are ones that may fix an issue, which may or may not have been caused by the last feature update.

So what are updates like for someone who is not one of the Tech Experts?

As a user, you may or may not notice updates a lot more frequently, but those are smaller updates and may not fix anything at all. There are regular security updates made during each cycle, updates to Microsoft applications, important system files, drivers, and numerous other things.

The larger 'feature updates', while not intending to do so, are the most likely to cause system issues. Many users who are more tech savvy avoid installing these until they are certain it is stable. In some cases, users will try to avoid installing them at all.

Many people live under the "if it isn't broke, don't fix it" mentality. Minus security updates, I can see a strong case for this line of thinking.

For years, many users (myself included) could selectively manage their updates. I could avoid installing many updates and keep installing only security updates.

While there is still some ability to manage updates in Windows 10, it is also more limited. One way Windows 10 has made managing updates easier for everyday users is by having the option to pause updates altogether. There is even an option specifically allowing you to stop those feature updates, which is great if your system is running well and you don't want to cause any issues.

There are also times where you may have a specific piece of software that is not compatible with the newest feature update and you need to avoid software incompatibility. That is when you are probably most grateful for the pause feature updates option.

Well, the time has come for Microsoft to go against your choices and decide that it knows what is best for you!

The November 2019 update is being pushed out to users, whether you want it or not. While it sounds deceitful, there is – as always with Microsoft – more to it.

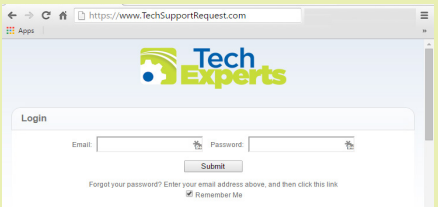
Users who are currently on Version 1809, which is now two versions behind, are being pushed to the November update. There are new security updates for Version 1909, and they cannot be applied to 1809.

Microsoft is taking this precaution to make sure users stay protected. In the past, Microsoft typically reserved forced rollouts for Windows Home version, but these forced updates will also apply to all computers running Windows 10 Professional.

If you are on Version 1809 and want to avoid being updated to 1909, you may be able to delay the process by manually moving to Version 1903 instead. Just remember, Microsoft is prioritizing your security, not comfort.

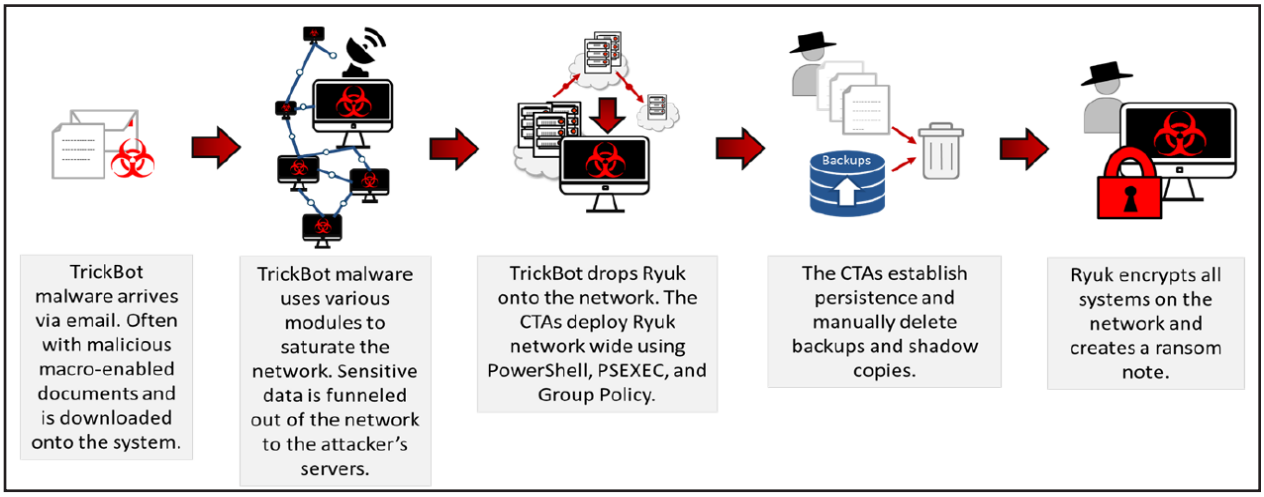
Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



Why Is Ryuk The Most Dangerous Ransomware?

Ryuk is one of the most prevalent ransomware variants in the threat landscape, with infections doubling from the second to the third quarter in 2019.



Ransomware infections continue to increase in tandem with overall impact and monetary demands.

Furthermore, Ryuk's ability to delete shadow copies and backups makes Ryuk extremely costly and almost impossible to remediate.

For instance, Ryuk operators demanded nearly $600,000 from one government agency after successfully encrypting nearly all files on the network.

Ryuk uses encryption to block access to a system, device, or file until a ransom is paid. It is often dropped on a system by other malware (e.g., TrickBot) or delivered by cyber threat actors (CTAs) after gaining access to the system through compromising Remote Desktop Services.

Once on a system, CTAs deploy Ryuk through the network using PowerShell, PsExec, or Group Policy, with aim to infect as many systems as possible. The number of infected systems depends upon how the malware is deployed as well as the CTA's access and privileges.

This may be a local subnet, the list of computers in active directory, or the entire organization depending on the variability and process specific nature of spreading the malware.

Once the malware is pushed out to the network, it targets backups and begins the encryption process.

Researchers have observed an increase in Emotet or TrickBot infections leading to a Ryuk infection.

For example, TrickBot disabled the organization's endpoint antivirus application and spread throughout the network, infecting hundreds of endpoints and multiple servers.

Since TrickBot is a banking trojan, it likely harvested and exfiltrated financial and other sensitive information prior to deploying Ryuk.

Once Ryuk is deployed network-wide, the CTAs encrypted the organization's data and backups, and left ransom notes on the machines.

Ryuk ransom notes once contained a message and a ransom amount, but have since evolved over time.

Throughout most of 2019, the ransom note did not list a ransom amount and only contained a message and email address.

However, now Ryuk ransom notes are very simplistic, with no price or message, only containing an email address, the ransomware's name, and the statement "balance of shadow universe."

The CTAs demands payment via Bitcoin cryptocurrency and direct victims to deposit the ransom into specific Bitcoin wallets.

The ransom demand is typically between $100,000-$600,000, which as of 12/19/19 is 14-84 Bitcoins. Notably the ransom demand is determined by the organizations' assessed ability to pay and the sensitivity of the data affected.

It is highly likely the CTAs account for characteristics like industry, solvency, subscription to cyber insurance, and network saturation when calculating ransom demands. Furthermore, the CTAs have been known to negotiate with victims and adjust the initial ransom amount.

Ryuk's main infection method is to be dropped on a system by other malware. The file will have a five-letter random name that is

Continued on page 4

Why Is Ryuk The Most Dangerous Ransomware, continued

usually generated by the srand1 and GetTickCount2 functions.

Persistence

Once executed, the main payload attempts to stop antivirus related processes and services. It uses a preconfigured list to kill more than 40 specific processes and 180 services with taskkill and net stop commands.

This preconfigured list includes antivirus processes, databases, backups, and document editing software. Additionally, the main payload establishes persistence in the registry and injects malicious payloads into several running processes.

To increase persistence, Ryuk makes changes to the registry allowing it to run the payload every time the user logs on.

Ryuk's anti-recovery techniques are more extensive and sophisticated than most types of ransomware, making recovery almost impossible without restoring from clean external offline backups.

Ryuk's process injection allows the malware to gain access to the volume shadow service and delete all shadow copies, including those used by third-party applications.

Encryption

Ryuk uses unbreakable RSA and AES encryption algorithms with three keys. The CTAs use a private global RSA key as their base encryption model. The second RSA key is delivered to the system via the main payload and is encrypted with the CTA's private global RSA key.

Once the malware is ready for encryption, the final key is created in their three-key encryption model.

Ryuk scans the infected systems and encrypts almost every file, directory, drive, network share, and network resource.

Ryuk attempts to encrypt all mounted network drives. As long as the drives are not CD-ROM types, the files will be encrypted.

Finally, once the malware is finished with the encryption process, it will create the ransom note, "RyukReadMe.txt", placing it in every folder on the system.

10 Most Important CyberAttacks, Continued

who were not even hired by the government.

First American Financial - 2019

For over 15 years, real estate title insurance company First American Financial was the victim of a breach that exposed over 800 million financial, real estate deeds, loans and other real estate specific files.

Stuxnet - 2010

Formed in collaboration with the United States and Israel, the Stuxnet worm was the first example of government-led cyberattacks on third parties causing infrastructure damage to an opposing force. The worm destroyed over 900 of Iran's uranium enrichment centrifuges and ruined most of the nuclear program.

The biggest challenge for businesses like yours with cybersecurity is the simple fact that users are unaware of the risks.

Keep in mind that 90% of cyberattacks are a result of human error.

Employees are the weakest link in the chain when it comes to your cybersecurity. Have you taken the time to evaluate your internal policies and security?

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com