Q-News

A Quanexus Publication

March 2016

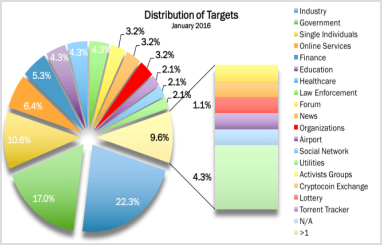
The Quanexus Newsletter

by Jack Gerbs

We have now been in our new building for almost two months and things are going great! Everything is back to normal. We continue to grow our Office 365 skill set and have migrated several more clients to the Office 365 platform. In fact, we now have more than enough clients on the platform to qualify for Microsoft's Small and Midmarket Cloud Partner Competency. There is some good news out there for the home user. A recent study shows that home users are now the third most targeted group for cyber-threats, down from number two. Last year, 13% of cyber-threats were targeting individuals, but it is now down to 10%. Windows 8 and Windows 10 include a new file backup solution called "File History". It allows users to automatically backup their files every 10 minutes and keep up to two years' worth of version history. This means that if you delete or make a change to a file, you can recover a previous version of the document. Password reuse is a bad practice. This month, I explain why companies should not let employees use passwords that they use for personal accounts. We have recently partnered with TrendMicro to provide their complete endpoint solution. The TrendMicro solution lets us take network protection to a whole new level. A lot of exciting things are going on at Quanexus, including Q-Works for Home, and I look forward to sharing them with you in upcoming newsletters.

Cyber-Threats Top Targets

It appears there is some good news for the home user and bad news for the government, according to hackmageddon.com. In February 2015, 13% of the cyber-attacks were targeted against the individual, which put this group in the number two threat position. In the latest research by hackmageddon.com, the threats against individuals dropped to 10%, putting them in the number three spot and moving governments into the number two spot, with 17% of all cyber-threats.



Inside Q-News

File History in Windows 8 and 10

Windows 8 & 10 both include a very nice backup feature that is great for use on workstations. We primarily suggest and implement Storagecraft's backup solution for our clients because of its superior image backup capability and management features. However, if you are interested in backing up less critical computers at the office or at home, Windows File History is a great solution. Windows File History has been designed to be easy to use and supports desktops and laptops. A key feature, specifically designed for laptops, is when they are not plugged into the backup drive or network, the backups will be cached on the laptop. Then, when the device is plugged back in, it will sync the cached data with the backup device.

Windows File History allows a user to recover a file or folder from a particular point in time with a maximum of two years of data retention. This means if you accidently delete or make a change to a file, you can recover from the previous version. With the risk of ransomeware, this is one way to assure you will be able to recover from that threat. Windows File History takes a snapshot of your file system every 60 minutes, and this can be adjusted to as little as 10 minute intervals.

(Continued on page 2)

Ransomeware Hits Mac

It was just a matter of time before the Mac became a target of a ransomeware. On March 4th, Claud Xiao and Jin Chen detected that "The Transmission BitTorrent client installer for OS X was infected with ransomeware, just a few hours after installers initially posted it". They named the ransomeware "KeRanger". According to the post, they believe KeRanger is the first, fully functional ransomeware seen on OS X. They also believe that "Transmission's official website was compromised and the files were replaced by re-compiled malicious versions," but they were unable to confirm this.

Apple validates programs before they can be installed on a system running OS X. This is done with certificate signing. Infected files were signed with a legitimate certificate, which allowed it to get around Apple's security. Apple has revoked the abused certificate after they learned of the issue.

Once a system is infected by KeRanger, the application will sit dormant for 3 days. After 3 days, the application will encrypt the most common file extensions. In order to unencrypt the files, the victim is provided with instructions on how to pay the $400 ransom. As of the writing of this article, approximately 6,500 systems had been infected.

While this threat is limited in scope, it should serve as a warning for Apple fans that they are quickly becoming a target. Many believe that Apple is more secure by design. I am sure that many may not agree with the following statement, but "the fact is that with its limited market share, Apple has not been worth the hackers' time to attack that platform".

(Continued on page 4)

File History in Windows 8 and 10

(Continued from page 1)

Before you setup Windows File History, you will need an external hard drive or a network attached storage device, such as a ReadyNas, Synology NAS or a Western Digital MyCloud device.

To setup File History follow these steps:

- Open the control panel.
- Click on System and Security.
- Click on File History which opens your setting panel.
- On the right hand side, click on select drive.
- If you are using a USB drive, select the letter of the drive.
  - This should automatically turn on File History, if not, on the bottom right of the display, click "turn on".
- If you are using a network location such as a NAS or shared network drive:
  - Click on the "Add network location" and browse to location.

While Windows File History works well, there are a few things you should be aware of. When you backup to a USB drive, that device is in the same location and is attached to your computer. If something very wrong happens to the computer, there is a chance it could affect the backup drive. So, having a NAS device in a different part of the office or house is recommended.

Your backup data is not encrypted, which means if someone takes the USB drive, they will be able to access your files by plugging it into another computer. Most modern NAS devices offer drive encryption, but this option needs to be enabled first. If you are going to use a USB drive, you should consider encrypting that drive with BitLocker, but be aware, BitLocker is only supported on Windows Pro and Enterprise editions, not the Home Edition of Windows.

Password Reuse – What is it and Why is it Important?

A topic that I always cover in Security Awareness training sessions is the scary term "password reuse". This term refers to using the same password for multiple accounts. Time Warner was the first to experience a major breach in 2016. They had 320,000 user IDs and passwords compromised. It is unclear if this was an actual breach of a Time Warner system or the result of a phishing scheme, targeting Time Warner clients or something else. If the credentials were acquired by a phishing attack, targeted directly against Time Warner clients, it strongly highlights the important issue of password reuse and the reason you must always check every link that is embedded in an email.

To check embedded links, you should put your mouse over the link and a small popup will indicate where that link is going to take you. Make sure you look at the whole link. Often times, the first part of the link will look legitimate, but the last part is the most important. Look at the part of the link before

(Continued to page 3)

Password Reuse

(Continued from page 2)

and after the last period in the domain name. If you get an email from timewarnercable.com, it might look like timewarenercable.com, or it may look like timewanercable.com.yourhacked.net /xx.html. Note that the part before and after the period in the domain name is "yourhacked.net". This is the site you will be taken to, and a phony page that looks legitimate will be displayed. When you log into this site, you are giving the bad guys your user ID and password.

The bad guys are always trying to steal credential information. They know that most of us are lazy, and we tend to use the same passwords over and over again. It is likely that the password used for your Time Warner account is the same password for your bank, online shopping and work. Once they have a set of credentials, the user becomes a person of interest. Through information that we voluntarily share through social media, it is not hard for the bad guys to learn a lot about us, and use the newly acquired credentials to place fraudulent purchases or raid our bank account.

If you are a business owner, you should also be concerned because often time, employees will use the same passwords they use for personal accounts at work, and now the bad guys are just a half a step away from breaching your network. Business owners should have a policy and employees should be trained not to use personal passwords on work computers.

One way to manage many passwords is with a password manager. One of the better password managers out there is keepass, which can be downloaded at keepass.info. It is available for Windows, Mac, Android and iPhones. A very effective way to manage multiple keepass information is to keep the database in a cloud solution such as OneDrive, DropBox, Box, etc. While many fear keeping all your passwords in one file and then saving that file in the cloud is dangerous, I suggest that "this is a better solution than password reuse". I also strongly suggest that you use a very strong passphrase to protect your keepass file. It should be at least 20 characters long, and don't use this password for anything else. After all, that is why you are using a password manager.

Smartwatch Attack

What's next? Tony Beltramelli's Masters Thesis from the IT University of Copenhagen titled "Deep-Spying: Spying using Smartwatch and Deep Learning" shows a new form of hacking credit card PIN and ATM codes. While this is not a real threat today, it does demonstrate what we can look forward to as technology and wearables continue to be developed. Tony's thesis states "wristband and armband devices such as smartwatches and fitness trackers already took an important place in the consumer electronics market and are becoming ubiquitous. By their very nature of being wearable, these devices, however provide a new pervasive attack surface threatening users privacy".

Tony has developed an algorithm that performs touch logging on 12-key keypads with above average accuracy when confronted with raw unprocessed data. This means "his algorithm can track your wearable device and determine your PIN codes.

Frustrated with your Home Computer?

We have had many inquiries about providing IT support for home users. Consumers become frustrated with attempting to call an 800 number somewhere in the world, hanging on the phone for long periods of time and still not getting the help that they need.

Quanexus has come up with a solution for home users that want to deal with a trusted local company - **Q-Works for Home**.

Whether you are looking to set up, secure or repair your computer, Quanexus has the know-how to help. With 24 years in business and an A+ rating with BBB, you can trust and count on our knowledgeable IT technicians for in-home service.

- Computer Set-up
- Data Backup or Transfer
- Email/Printer Set-up
- Wireless Set-up
- Hardware installation or repair
- Data Recovery
- Virus/Spyware removal

If you prefer ongoing support, for a low monthly fee **Q-Works for Home** offers an option that includes:

- Remote Support by phone
- AVG Anti-Virus
- Unlimited monthly updates
- Discounted in-home service

Give us a call at **937 885-7272** to discuss pricing or schedule a visit.

Trend Micro

With TrendMicro's complete end point protection, we can now secure workstations at a whole new level. Because of all the features in this type of product, we have to work closely with our clients not to make the network too restrictive to not impede users from accomplishing their job functions. Key features in the solution are:

- Host Based Firewall: A host based firewall allows us to closely monitor a workstation's network activity. For example, it is normal for a workstation to communicate with servers and printers, but they typically should not have to communicate with another workstation on the network. If a workstation attempts to communicate with another workstation on the network, it may be an indication that the workstation is infected with malware. This activity would be blocked and the network admin would be notified of this type of activity.
- Application White Listing: This feature determines if an application is permitted to run on a workstation. If an application is not white listed, it won't run. This is an excellent way to prevent malware from running on a workstation. If an unauthorized program attempts execution, the activity is blocked, logged and an alert is sent.
- Input/Output (IO) Device Control: IO control allows the organization to determine if users can remove company information on removable media such as USB devices.
- Data Leak Prevention: This feature monitors the contents of files and can detect if personal or protected information is attempting to leave the network in an unencrypted or unauthorized manner.
- Intrusion Prevention: This feature monitors applications on the individual workstations. If there are known vulnerabilities in an installed application, the IPS feature will build a filter to block the known exploit from getting to the system.

TrendMicro's end-point solution adds an additional layer of protection for our clients and I'm excited to be partnering with TrendMicro.

For a fixed monthly fee, we are revolutionizing the IT industry with our Q-Works program. Quanexus' complete "managed services" package means that you will see increased performance, security, and reliability immediately, at an affordable price.

Your business success depends on your IT infrastructure. You need Quanexus to deliver proactive services that not only keep your network up and running, but running effectively and efficiently.

Ransomeware Hits Mac

(Continued from page 2)

As Macs become more popular, we can expect more attacks. The Mac operating system (OS) is not as mature as Windows OS. Apple has not had to deal with the issues that Microsoft has faced for a long time, keeping the OS secure. However, as Macs grow in popularity, Apple will have to step up their game. As a side note, I am typing this article on a Mac and I am a Mac fan.

Here is an example of a ransomeware message:

README_FOR_DECRYPT.txt — Edited

```
Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to ( IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN
THIS LINK: http://fiwf4kwysm4dpw5l.onion )
2. Use 1PGAUBqHNcwSHYKnpHqzCrPkyxNxvsmEof as your ID for authentication
3. Pay 1 BTC (~407.47$) for decryption pack using bitcoins (wallet is your ID for authentication -
1PGAUBqHNcwSHYKnpHqzCrPkyxNxvsmEof)
4. Download decrypt pack and run


---> Also at https://fiwf4kwysm4dpw5l.onion.to  you can decrypt 1 file for FREE to make sure
decryption is working.


Also we have ticket system inside, so if you have any questions - you are  welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```