# Q-News

A Quanexus
Publication

August 2016

## Pokémon Go

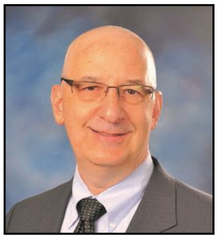
If you haven't heard about Pokémon Go, you must be on another planet! This newly released app has some benefits, but as with many apps, there is good reason to be concerned. Within 4 days of Pokémon Go's release, there was a counterfeit version created, that could be downloaded from unofficial sites. Unofficial sites are sites that have the application or a hacked version of the application. The sites typically have a slightly misspelled domain name to trick the user into thinking they are downloading the application

*(Continued to next column)*

## Inside Q-News

## The Quanexus Newsletter

*by Jack Gerbs*



Since my first newsletter, my goal was to share information about the IT industry. It was never a goal to try to push product and services. This newsletter is a little different from the typical newsletter. Quanexus partners with some great companies and there is a reason we chose the vendors included in our technology stack. In this edition, I am going to share some brief information about our key vendors and highlight how, when combined, they provide a total solution to create a stable and secure network environment. With all the news about Pokémon Go, there are some potential issues that you should be aware of. More big mergers in the news- Microsoft buys LinkedIn and AVAST buys AVG. Also, the MXLOGIC/McAfee SASS email filtering platform will be shutting down.

## Pokémon Go – cont.

from an official site. Often times, users do not pay attention to the source of where they get their applications. The recently released, counterfeit version contains the DroidJack malware, which gives unauthorized access to everything on the user's cell phone (email, contacts, photos, videos and text messages).

Even if you download the software from an official site, you should still be concerned about how quickly Pokémon Go was released and what vulnerabilities may be in the code. The original user agreement gave the developer, Niantic, full access to the user's Google accounts. Niantic has since updated the user agreement making it more reasonable.

Some businesses have suffered as players have swarmed a business's parking lot, looking to collect the digital monsters. Niantic has worked with those companies to remove their facilities from the game. On the plus side, I have heard from neighbors and friends that some of their family members are actually going outside and getting some exercise, and dogs are getting walked more frequently. Pokémon's augmented reality appears to be a huge success, so we can expect more applications like this in the near future.

One final thought of caution, "Situational Awareness". Players of this game become so engrossed in it that they become unaware of their surroundings. The game may lead them to secluded parts of a park or an alley, which could make them vulnerable to an attack. Players need to be aware of where they are going in their attempt to capture the digital monsters. Party on Garth!

# Quanexus' Services and Our Partner's Solutions

For years, I have talked about different companies that we partner with and how each brings a key component to keeping our clients' networks secure and stable. Here is the rundown of our technology stack:

**Q-Works Platform:** Our Q-Works platform is the central component to monitor and manage our clients' networks. The platform includes these capabilities:

- Monitor and alert on the health of servers and workstations.
- Monitor and alert on the status of the backup solution.
- Provide remote access for support.
- Automate patch management.
- Report on the status of patch updates.
- Report on the status of anti-virus updates.
- Provide monthly reports to clients.
- Provide on-demand hardware and software inventory reports.

**Microsoft's Hyper-V Virtualization:** Virtualization allows a physical server to run multiple virtual servers. This allows the separation of specific functions between different virtual machines. Depending on the environment, we often suggest having a minimum of two servers, if it's within the budget. With the Hyper-V replication feature, we are able to keep replicas (copies) of virtual machines on the primary production server and store them on the second server. Should the main server fail, we can quickly spin up the replica on the second server and the client can resume operations very quickly. Understanding the client's need and the critical functions of the organization, allows us to craft a business continuity and disaster recovery plan. Business continuity and disaster recovery is discussed more in the "Backup" section.

**Anti-virus/Malware:** We partner with two anti-virus vendors – AVG and TrendMicro. AVG is included in our Q-Works platform, while TrendMicro's solution is an additional cost. We chose two vendors because they offer different solutions. AVG is a full-featured anti-virus/malware solution and TrendMicro is a full-featured end-point solution.

AVG is a centrally managed solution that provides all of the basic services. TrendMicro includes the basic features of AVG, but adds many more tools. Some of the tools help our clients meet regulatory requirements based on their industry. Below are just some of the key features in TrendMicro's solution:

- **Host Based Firewalls:** A host based firewall allows very granular control of what a workstation can and cannot do on your network. For example, workstations can talk to servers, printers and the Internet, but it is not normal behavior for a workstation to communicate with another workstation. Typically, if workstations communicate between each other, that is a sign that a system may have been breached. We need to block that traffic and send an alert based on suspicious traffic.

- **Locking Down USB Ports:** Information can be stolen or improperly transferred to unsecure devices via USB. With the ability to not let storage devices connect to computers, we mitigate this exposure. The USB ports are still available for peripheral devices such as keyboards, mice, microphones, etc.

- **Application Whitelisting:** This is an excellent way to protect your network from malware, especially ransomware. Each application that a user needs to access is put into a whitelist (permit list). If any application attempts to run/execute that is not on the whitelist, it is blocked. While application whitelisting is an excellent solution, it is very difficult to manage. We consider the goal of IT is to make the organization more efficient. Application whitelisting is a complex operation and can actually inhibit the organization from running smoothly.

- **Data Leak Prevention (DLP):** DLP is used to monitor and provide alerts if there is an attempt to remove protected data from the network. This requires proper configuration to determine what protected data is. Examples of protected data are: credit card numbers, social security numbers, medical record numbers, financial statements, personal identification information (PII) and much more.

- **Intrusion Detection and Protection (IDS/IPS):** IDS and IPS are signature-based technologies. If the TrendMicro agent detects that there is an unpatched or older, vulnerable application on a workstation or server, the agent will monitor, block and alert if there is an attempt to exploit the known vulnerability.

*(Continued to page 3)*

# Quanexus' Services and our Partner's Solutions

*(Continued from page 2)*

**Firewall:** Our firewall vendor is Fortinet. Fortigate firewalls are rock solid and offer many features that protect the network. Business class firewalls are 86% effective at keeping threats from entering the network. The firewall monitors, blocks and sends alerts if the firewall detects network traffic that attempts to violate a network rule. The key features of a Fortigate firewall are:

- **Anti-virus Protection:** This is not a replacement for server and workstation anti-virus programs. Files are scanned at the network edge (where the local network connects to the Internet) for malicious programs. This adds an additional layer of protection to the network. Additionally, the firewall can block known control and command centers for botnets and ransomware.

- **Web Content Filtering:** This feature prevents the accidental or intentional access to inappropriate sites. A very important feature of the web content module is the ability to block advertising. There are many banner ads that contain malicious code.

- **Intrusion Detection and Prevention (IDS/IPS):** IDS/IPS on the firewall monitors for known vulnerabilities that are attempting to exploit devices that may be vulnerable on the network.

- **Data Leak Prevention:** DLP monitors, blocks and sends alerts on traffic that contains information that should not leave the network.

- **Network Segmentation:** Network segmentation is the ability to separate the network. A segmented network typically would have the servers, workstations, and printers each on their own, separate segment. A segment is a separate IP network. A firewall can only monitor traffic that passes from one interface on the firewall to another interface. If servers, workstations and printers are all on the same segment, traffic cannot be easily monitored. Segmenting a network provides visibility into the traffic between devices and can help detect a potential breach. If there are network connectivity issues, segmentation can also make troubleshooting the network easier. While all Fortigate firewalls support network segmentation, it is not always wise to enable this feature. The lower end firewalls have limited throughput and can create network performance issues. Caution should be taken before implementing segmentation.

If you have read this article and have gotten to this point, you may be asking what is the difference between a full end-point solution and a firewall? You may also be asking if you need both. The answer is, at minimum, you need the firewall and a basic anti-virus solution. The addition of the end-point solution provides an additional layer of security to your network. The firewall provides protection at the network edge and between segments and the end-point solution (host based) protects the workstations and servers.

**Backup – StorageCraft:** StorageCraft is an image based backup technology. There are two basic backup solutions- image based and file based. File based solutions only backup files. If a server crashes and you have a file-based solution, it could take days to a week to recover a crashed file server. An image based file server with bare metal recovery allows for quick recovery of a crashed server. Once the hardware is repaired or replaced, a file server can typically be recovered within a day.

Where should you store backups- local, cloud or removable devices? Our solution typically involves the installation of a Network Attached Storage (NAS) device. All servers are backed up to the NAS device. Our NAS devices have USB ports and an internal backup utility that we use to backup the NAS to external USB hard drives, which can be rotated and taken off-site. While we do monitor the backup status, it is the client's responsibility to rotate the backup media. As an additional feature, the backup images can be backed up to a cloud solution. We have equipment in a data center and offer remote backup. If the data needs to be backed up out of state or across the country, we do offer that feature, as well.

A remote/cloud backup solution does not replace the need to have local backups. Local backups let us quickly recover lost files

*(Continued to page 4)*

# Quanexus' Services and Our Partner's Solutions

*(Continued from page 3)*

or a failed server. Remote backups are used for the rare occurrence of a catastrophic event, that destroys the server and the local backup media. Creating a business continuity and disaster recovery plan requires an understanding of the client's needs. There is no one solution that fits all.

**Server Monitoring – Netwrix:** Netwrix is an application that we use for server and workstation auditing. It integrates with system events and can monitor, alert and report on events such as:

- Changes of permissions granted to users (privilege escalation).
- Unauthorized attempt to access files that a user does not have rights to.
- Unauthorized login attempts.
- Who changed what and when.

Netwrix has the capability of taking screen shots when changes are made. We have had clients catch auditors snooping around their network and they were able to show snapshots of the auditor's activities.

**Security Awareness Training - KnowBe4 & Quanexus:** KnowBe4 brings a unique model to security awareness training. It is a series of on-line training modules that focus on social engineering. Their product comes with a tool to run social engineering tests on your users. It provides the framework to create and send spam email messages to your users to determine who is susceptible to clicking on links, and then provide feedback to the user and the administrator, suggesting additional training for that user. This is an ongoing subscription-training model.

**The BIG QUESTON?** Do I need to implement everything? The answer is no. There are a few key components that everyone should implement and then based on your industry, the sensitivity of your data and your risk tolerance, you can make informed decisions on what appropriate solutions should be installed.

*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.*

**If you have any suggestions or topics you would like to see covered, please contact us with an email at info@quanexus.com or give us a call at 937-885-7272. We would love to hear from you.**

# Giant Mergers

Last month, Microsoft announced they were going to acquire LinkedIn for $26.2 billion. According to Mike Propero, Tom's Guide review editor, this an important acquisition to accelerate Microsoft's cloud strategy. LinkedIn has a strategy for growth and bringing additional benefits to their clients. LinkedIn also recently purchased Lynda, an online training company (lynda.com).

Another acquisition last month was Avast purchasing AVG for $1.3 billion. After the merger, Avast will have over 400 million endpoints. The purchase price comes out to $25 per share of AVG, which is a 33 percent premium to the shareholders. Quanexus has partnered with AVG for over 6 years, so we'll be keeping a close eye on the transition and what this might mean to our clients and us.

Linked in

Quanexus™
We make *IT* easy.

571 Congress Park Dr.
Dayton, OH 45459
937 885-7272
info@quanexus.com