Talk Nerdy To Me

Inside the Amazon Warehouse - Humans and Machines Working Together

If you haven't heard yet, or driven west on US 30, Fort Wayne is getting our very own Amazon fulfillment center. The Fort Wayne facility will be Amazon's first fulfillment center in Indiana to use innovative and advanced robotics technology and the company's 10th fulfillment center in the Hoosier state.

Workers grab a flat package, hold its barcode under a red laser dot, and place it on a small orange robot. They hit a button to the left and off zips the robot to do their bidding, bound for one of more than 300 rectangular holes in the floor corresponding to zip codes. When it gets there, the bot engages its own little conveyor belt, sliding the package off its back and down a chute to the floor below, where it can be loaded onto a truck for delivery. It's a symphony of electric whirring, with robots pausing for one another at intersections and delivering their packages to the slides. After each "mission," they form a neat queue at stations along the periphery, waiting for humans to scan a new package, load the robots once again, and dispatch them on another mission.

Amazon needs this robotic system to supercharge its order fulfillment process and make same-day delivery a widespread reality. But the implications strike at the very nature of modern labor: Humans and robots are fusing into a cohesive workforce, one that promises to harness the unique skills of both parties. A system in the cloud, sort of like air traffic control, coordinates the route of every robot across the floor, with an eye to potential interference from other drives on other routes. That coordination system also decides when a robot should peel off to the side and dock in a charger, and when it should return to work. Sometimes the route selection can get even more complicated, because particularly populous zip codes have more than one chute, so the system needs to factor in traffic patterns in deciding which portal a robot should visit. The end goal is to minimize congestion through an even distribution of traffic across the field. So on top of tweaking the robots' routes, the system can actually switch the chute assignments around to match demand, so that neither the robots nor the human sorters they work with hit any bottlenecks.

Although the system is automated, humans still monitor the robots on flatscreens below the field, where the packages come down the chutes, and respond to crises. Amazon runs simulations to figure out how to keep their human workers comfortable when loading robots with packages. This includes their range of movement from an ergonomics standpoint and their safety. Or such questions as how best for a human to grab a parcel, scan it, place it, and reach over to hit the button that sends the robot on its way.

Source: https://www.wired.com/ and https://wpta21.com/

2

June 2021

Ransomware As A Service

What is Ransomware as a Service (RaaS)?

Ransomware as a service (RaaS) is a subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks. Affiliates earn a percentage of each successful ransom payment.

Ransomware as a Service (RaaS) is an adoption of the Software as a Service (SaaS) business model. Like all SaaS solutions, RaaS users don't need to be skilled or even experienced, to proficiently use the tool. RaaS solutions, therefore, empower even the most novel hackers to execute highly sophisticated cyberattacks. RaaS solutions pay their affiliates very high dividends, with some affiliates earning up to 80% of each ransom payment.

How does the RaaS model work?

For the RaaS model to work, you need to start with expertly coded ransomware developed by skillful ransomware operators. The ransomware developers need to be reputable to compel affiliates to sign up and distribute their malware. Reputable RaaS developers create software with a high chance of penetration success and a low chance of discovery.

Once the ransomware is developed, it's modified to a multi-end user infrastructure. The software is then ready to be licensed to multiple affiliates. The revenue model for RaaS solutions mirrors SaaS products, affiliates can either sign up with a one-time fee or a monthly subscription. Some RaaS solutions, don't have monetary entry requirements and affiliates can sign up on a commission basis.

Ransomware affiliates are supported with onboarding documentation containing a step-by-step guide for launching ransomware attacks with the software. Some RaaS distributors even provide affiliates with a dashboard solution to help them monitor the status of each ransomware infection attempt.

To recruit affiliates, RaaS post affiliate opening on forums on the dark web. Some ransomware gangs, like Circus Spider, only recruit affiliates with specific technical skills, due to their higher chances of claiming prestigious victims. Other ransomware gangs are purely interested in rapid distribution and have very soft affiliate requirements.

How do RaaS attacks work?

Most ransomware victims are breached through phishing attacks. Phishing is a method of stealing sensitive data, such as passwords and payment details, through a seemingly innocuous source. Phishing emails is the most common category of phishing attacks. Victims are presented with an email that seems legitimate, but when they click on a link, they're unknowingly activating a cyber threat.

RaaS affiliates present victims with a very convincing phishing email. When a link is clicked, victims are directed to the exploit site where the ransomware is clandestinely downloaded.

Since the pandemic, Covid-19 themed phishing emails have been flooding inboxes. These emails seem very convincing, especially to a panic-stricken victim with fragile reservations.

Once downloaded, the ransomware moves throughout the infected system, disabling firewalls and all antivirus software. After these defenses are comprised, the ransomware may trigger the autonomous download of additional remote access components.

If a vulnerable endpoint is discovered, such as a desktop, laptop, or even IoT device, it could serve as a gateway to the complete internal network of business. Ransomware that surpasses this depth of penetration is capable of holding an entire business hostage.

With the ransomware now free to progress without detection, the victim's files are encrypted to the point of being inaccessible. Most ransomware operates beneath authorized processes, so victims are unaware of any data breaches occurring.

After the attack is complete, the extortion game begins. Some ransomware gangs, such as cybercrime group Maze, operate on a double-extortion model. They demand a ransom payment in exchange for a description key and also threaten to published the breached data on the dark web if payment isn't made before the deadline.

The dark web is a criminal-infested network, so any leaked information on the platform will give multiple cybercriminal groups free access to your sensitive data and those of your customers. The fear of further exploitation compels many ransomware victims to comply with cybercriminal demands.

To make the ransom payment, victims are instructed to download a dark web browser and pay through a dedicated payment gateway. Most ransomware payments are made with cryptocurrency, usually Bitcoin, due to their untraceable nature. Each ransom payment is sent to a money launderer that obfuscates the trajectory of the funds so that it cannot be traced to the ransomware developer or the RaaS affiliate.

Is your business at risk of a ransomware attack?

Contact Preferred IT Group today for a FREE network security risk assessment and find out how we can help you protect your business.

Source: https://www.upguard.com/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

We Love Our Interns!

For the last 10 years, Preferred IT Group has worked with local high schools to facilitate internships throughout the school year. Most of our interns throughout the years have gone to school for jobs in the IT industry.

This year, we had two amazing seniors, Ian Scott and Mark Myers.

Ian got a wrestling scholarship to Marian University in Indianapolis and will be studying business.

Mark will be attending Purdue University to study engineering.

We wish them all the success in the years to come!

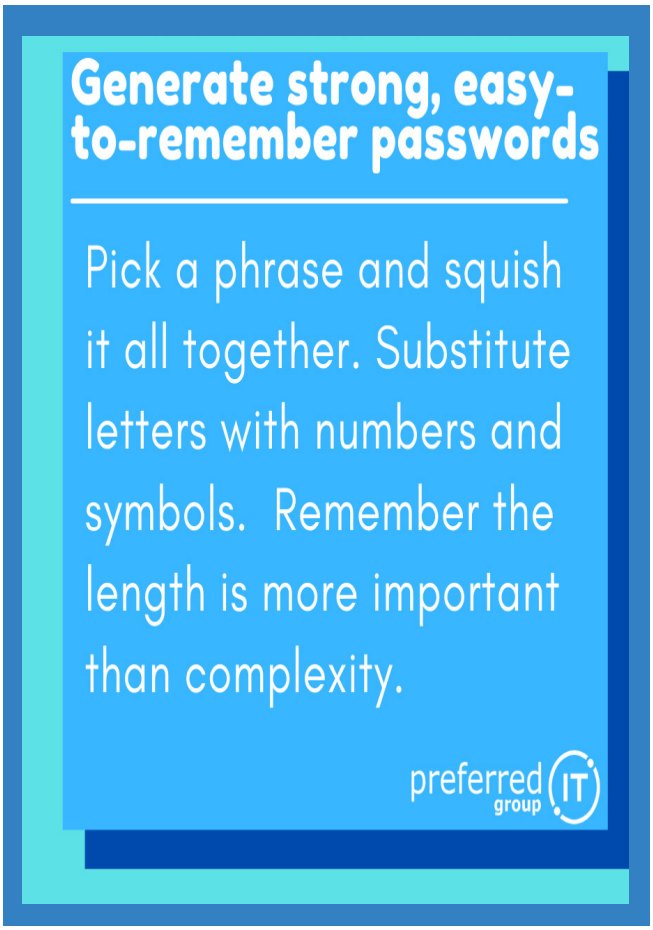
PITG Birthday Boys!

May was a BIG month for Preferred IT Group birthdays!

Huge happy birthday to our technicians Jordan Marks and Trevor Curry, our senior engineer Scott Diehl, and our Director of Operations Matt Carpenter!

You guys ROCK!

FUN FACT!



preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.