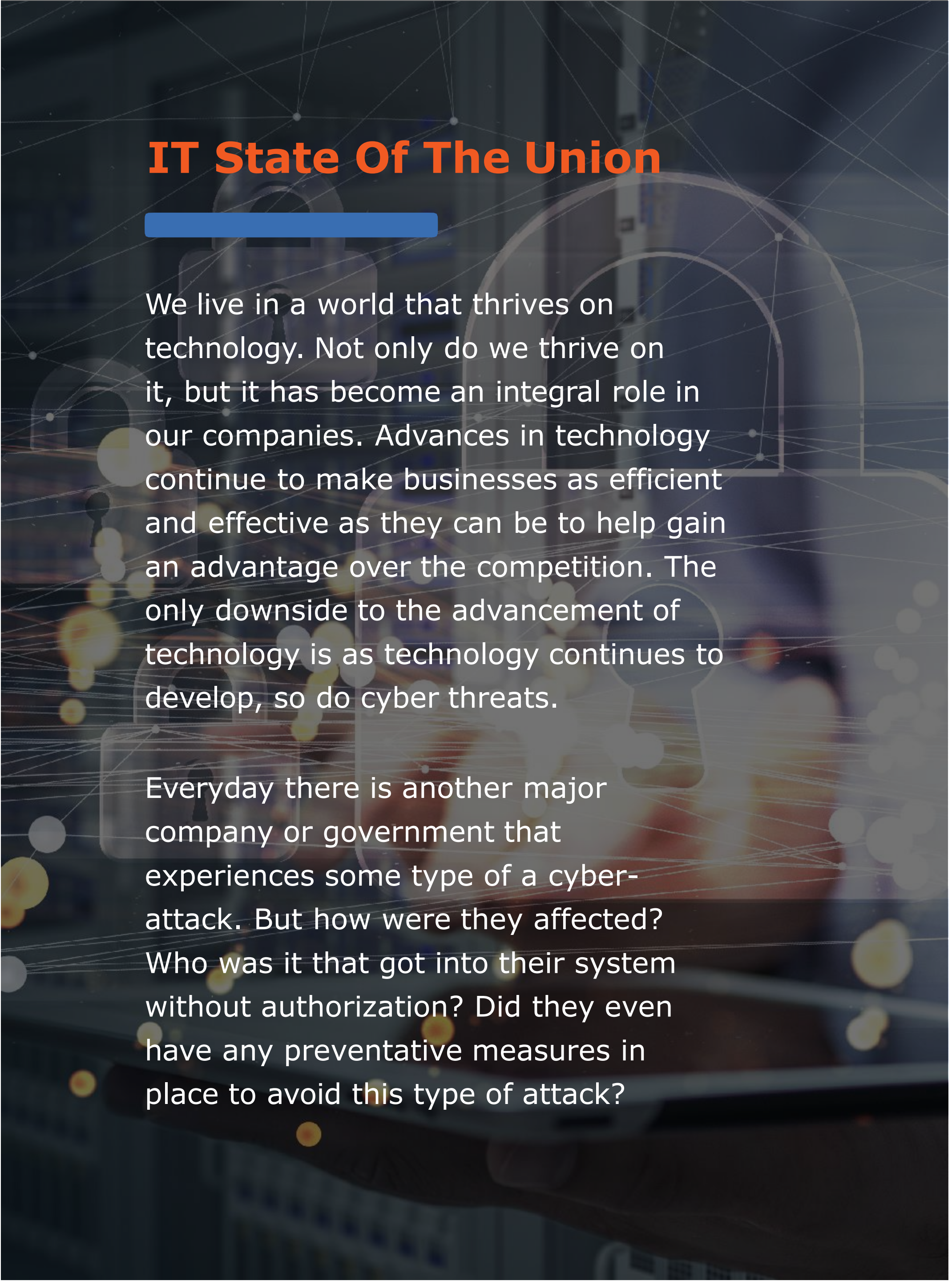
completecloud
POWERED BY AVATARA

It’s Time to Rethink Security

AT&T Partner Exchange®
Platinum Solution Provider



IT State Of The Union

We live in a world that thrives on technology. Not only do we thrive on it, but it has become an integral role in our companies. Advances in technology continue to make businesses as efficient and effective as they can be to help gain an advantage over the competition. The only downside to the advancement of technology is as technology continues to develop, so do cyber threats.

Everyday there is another major company or government that experiences some type of a cyber-attack. But how were they affected? Who was it that got into their system without authorization? Did they even have any preventative measures in place to avoid this type of attack?

THE US NAVY RECEIVES 110,000 CYBER-ATTACKS EVERY HOUR.

68% OF FUNDS LOST AS A RESULT OF CYBER-ATTACKS WERE DECLARED UNRECOVERABLE

99% OF COMPUTERS ARE VULNERABLE TO EXPLOIT KITS TARGETING JAVA, ADOBE READER, OR ADOBE FLASH

59% OF EMPLOYEES STEAL PROPRIETARY CORPORATE DATA WHEN THEY QUIT OR ARE FIRED

MYDOOM IS CONSIDERED TO BE THE MOST EXPENSIVE VIRUS IN THE WORLD AND IN CYBER SECURITY HISTORY, HAVING CAUSED AN ESTIMATED FINANCIAL DAMAGE OF $38 BILLION.

Usual Suspects

Theodore Thief

Some call him old school, but he is still making a killing from laptops and even servers left unguarded.

Betty Bad Bots

Known for years to release the nastiest bots, know to target those neglected open ports.

Ronda Ransomware

She plays in Bitcoins, setting her malware loose and watches the money come in.

Mr. Crime as a Service

Successful CEO builds his second great company with Ransomware software as a service.

Philip Phishing

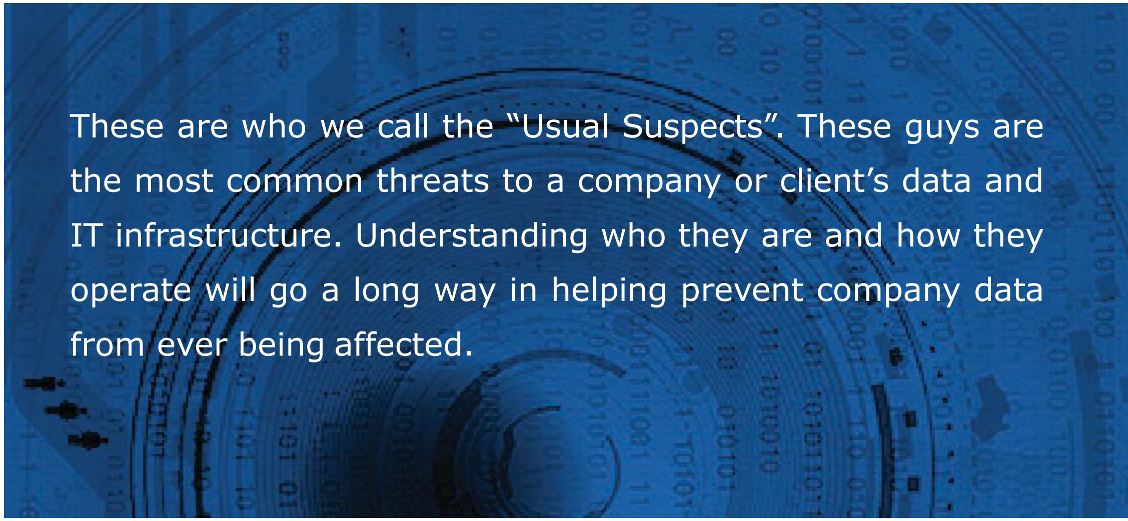
Known for grabbing passwords from midair.

Tina Trojan

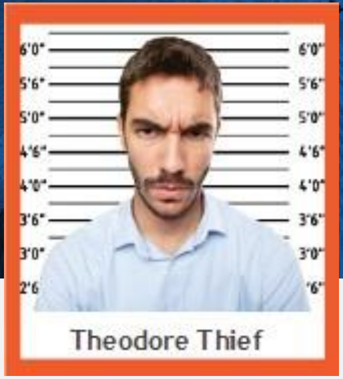
Known to use HTTP injection to spoof bank websites, stealing credentials from oblivious users.

C.J. Hacker

Code Name FUD, Fully UnDetectable. C.J. has been avoiding top AV for over 3 years.



These are who we call the "Usual Suspects". These guys are the most common threats to a company or client's data and IT infrastructure. Understanding who they are and how they operate will go a long way in helping prevent company data from ever being affected.



Theodore Thief

Theodore is an everyday, typical thief. His goal is to swipe hardware while his victim isn't looking.

He'll go after unattended laptops at coffee shops or sneak into office buildings and take as much as he can.

He's no hacker, but he can still walk off with any company or customer data on that equipment.

Stolen laptops, smartphones, and tablets continues to be one of the primary ways that patient's protected health information is being compromised.

Betty Bad Bots

"Bots" is short for "robots" which are automated programs that function through and over the internet. Betty Bad Bots operates the same way that a human user would operate, but with malicious intent. This can make her hard to detect and prevent from affecting a user or company's data.

According to Incapsula's annual Bot Traffic Report, bad bots made up 28.9% of website traffic.* With almost 30% of site traffic consisting of bad bots, how do these bots operate? There are numerous types of bots, but these are some of the most common bad bots.

Click Bots:
Click on paid advertisements so that a company's market research is skewed and their pay-per-click funding is wasted on robots and not their actual human target audience.

Scraper Bots:
Searches the internet for information and data it can steal and use elsewhere without the owners permission or knowledge.

Imposter Bots:
Their goal is to sneak around a company's security measures. They often are linked to "Denial-of-Service" attacks which block legitimate users from a site, network, or server.

Spam Bot:
The most common known bot that delivers spam like content through email, website comments, and social media.

*** "Bot Traffic Report 2016." *Incapsula.com*. InCapsula, n.d. Web. 06 May 2017.**

Ronda Ransomware

Ronda Ransomware

Ransomware is malicious software that will prevent users access to their files and data until a sum of money is paid.

Typically Ronda requires payment in bitcoin, which is an untraceable source of digital currency. Making it impossible to find her and halt her sinister "business".

Most ransomware villains attack by tricking users to visit their site though emails or web advertisements. These attacks are becoming more common and people continue to pay the ransom, which is causing the ransom price to increasing every year as well.

The FBI predicts that payments for ransomware will reach $1 billion from 2016; compared to $24 million in 2015.

The United States Justice Department found that there were 4,000 ransomware attacks per day in 2016.*

* "How to Protect Your Networks for Ransomware." The United States Justice Department, n.d. Web. 6 May 2017. SECURITY

Mr. Crime as a Service

Mr. Crime As Service

Ransomware attacks have accelerated due to a budding Crime as a service (CAAS) industry.

Software criminals are not only exploiting for themselves, but selling their software or undetected positions (droppers) within an infrastructure to others.

These mercenary's attacks aren't just focused on induvial users anymore. They'll target small businesses, major corporations, non-profits, or government entities. Mr. Crime as a Service is available for hire for whatever the job and whatever the target.

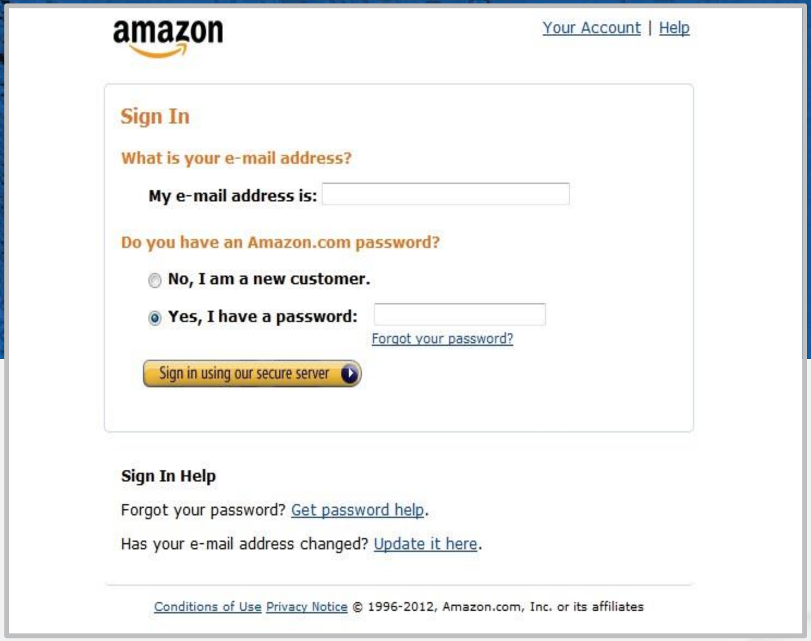
The recent worldwide ransomware attack,"WannaCry", affected tens of thousands of companies, shut down hospital operations in The United Kingdom, and crippled companies in Russia and China for more than a day. The aftermath cost of this attack has been estimated from the hundreds of thousands to $4 billion according to Cyence.

Philip Phishing

Philip Phishing uses fraudulent emails that are designed to trick employees and individuals to reveal personal information ranging from passwords and credit card info.

These emails are becoming extremely sophisticated and can be challenging to determine if it is actually a legitimate email or a phishing attempt.

These Amazon emails are a great example at how sophisticated phishing attempts look today. There are subtle differences, such as incorrect URLs or spelling errors that reveal their fraudulent intent. People that frequently shop on Amazon and are used to seeing similar messaging could accidently fall right into Philip Phishing's hands, giving him free access to their information.



amazon

Your Account | Help

Sign In

What is your e-mail address?

My e-mail address is:

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password:

Forgot your password?

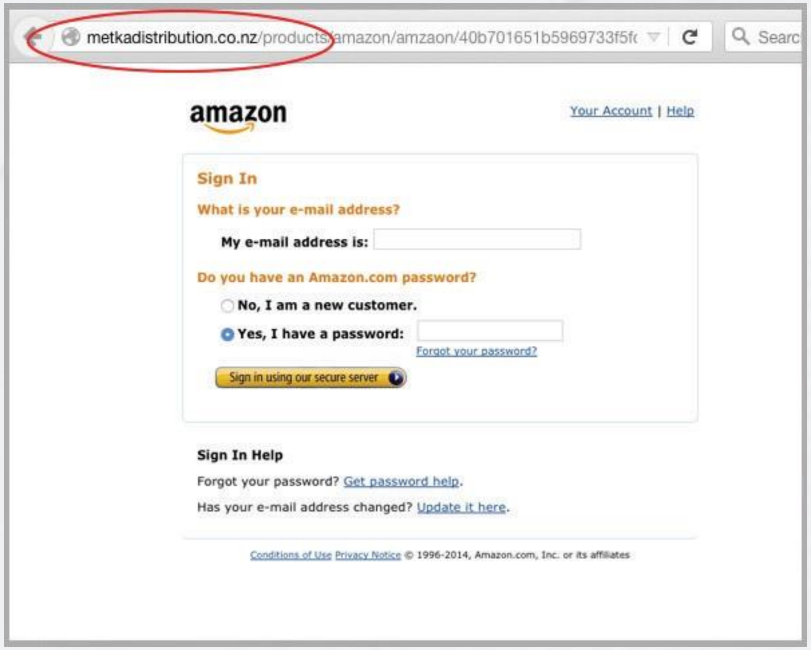
Sign in using our secure server

Sign In Help

Forgot your password? Get password help.

Has your e-mail address changed? Update it here.

Conditions of Use Privacy Notice © 1996-2012, Amazon.com, Inc. or its affiliates



metkadistribution.co.nz/products/amazon/amzaon/40b701651b5969733f5fc

Searc

amazon

Your Account | Help

Sign In

What is your e-mail address?

My e-mail address is:

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password:

Forgot your password?

Sign in using our secure server

Sign In Help

Forgot your password? Get password help.

Has your e-mail address changed? Update it here.

Conditions of Use Privacy Notice © 1996-2014, Amazon.com, Inc. or its affiliates

Tina Trojan

Tina is dangerous malware that is often hidden or disguised as an innocent tool or legitimate software. Sometimes the Trojan itself is the malicious villain and in other cases it is just the one that opens the doors for others to come in.

Trojans like Tina cannot self replicate like computer viruses, but they still can delete, copy, modify, block, or interfere with the abilities of an individual computer or network.

Backdoor:
This allows the hacker to "open the door" to the infected computer. Once the door is open the hacker can control the computer, access all its data, and even deliver additional malware.

Ransom:
When a Ransom Trojan makes its way into a computer it will disrupt how a computer operates or deny access to certain data until Tina's ransom is paid.

Downloader:
These Trojans download and install additional malware onto the infected computer and will even update to new versions to ensure they're as effective as possible.

Spy:
A Trojan Spy will spy on how a computer is used, taking snapshots of passwords, logins, and running applications.

C.J. Hacker

C.J. Hacker

Using whatever means possible, some hackers target specific companies with specific aggressive attacks.

C.J. is the guy sitting in a basement scanning the internet looking for open ports that he can get into. But what is an open port and why does he need to scan for them?

A port is a way for servers to identify the type of information and requests that are being made to and from that server.

A Hacker's Typical Attack Looks Something Like This:

A Port Scan reveals which public ports run services.

Once they know which ports are publically accessible they can fingerprint all those services (rattling a door knob to check if the door is open).

By fingerprinting they can find where vulnerabilities reside.

Once the vulnerabilities are determined C.J. can begin his exploitations.

Compliance Reporting

Mr. Auditor

Ms. Regulator

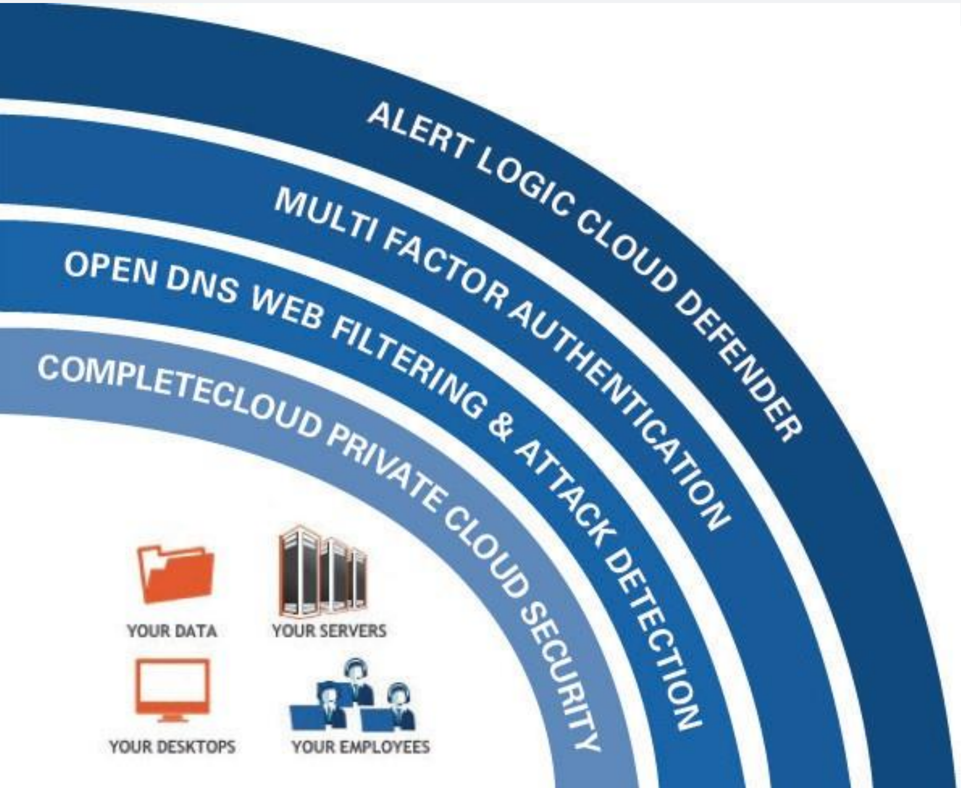
Mr. Customer

Even with a perfectly defended infrastructure some businesses have to deal with various compliance and regulations.

The National Institute of Standards and Technology (NIST) is an agency that develops the standards, processes, and cyber security practices for all government agencies and various other industries. NIST recently raised their standard for cyber security and reporting, which affects a lot of organizations. Two major players that have been affected by this are Defense Federal Acquisition Regulation Supplement (DFARS) and the Health Insurance Portability and Accountability Act (HIPAA), since they are dealing with highly classified military contracts for the government and personal health information (PHI). IT audits are even starting to be layered into regular corporate financial audits as well.

With these compliance standards businesses need to be able to provide quarterly compliance reports and third party penetration testing to show Mr. Auditor and Ms. Regulator that their data is secure.

What's the Solution? CompleteCloud.



ALERT LOGIC CLOUD DEFENDER
MULTI FACTOR AUTHENTICATION
OPEN DNS WEB FILTERING & ATTACK DETECTION
COMPLETECLOUD PRIVATE CLOUD SECURITY
YOUR DATA
YOUR SERVERS
YOUR DESKTOPS
YOUR EMPLOYEES

The Most Secure Private Cloud Environment In The Market

CompleteCloud utilizes a 24/7 Security Operations Center and some of the biggest names in cyber security, like Cisco Umbrella (OpenDNS) and Alert Logic, to help reduce the chances of your business being affected by malware.

If you're concerned about meeting industry standards like HIPAA, you're covered. We will provide the reports to show your auditors that your systems are secure. CompleteCloud allows you to operate with the peace of mind that your business is safe, data secure, and industry standards meet regardless of the cyber threat.

A Multi-Layered Approach

Private Cloud

With CompleteCloud all your data gets transitioned into the data centers, which will remove the opportunity for bots to enter your company's infrastructure by getting rid of any unneeded open ports. Server and edge firewalls, along with intrusion detection software, help to continually protect your data.

Cisco Umbrella (OpenDNS)

Predictive cloud based security that leverages the internet to take in millions of data points per second to identify suspected threat origins. Not only does OpenDNS block threats and run analytics, but it is completely automated and always searching. OpenDNS prevents malware and blocks phishing attempts and inappropriate content, while containing any botnets.

Multi Factor Authentication

Helps provide additional security for remote user logins so when a laptop is lost, or left unattended with a sticky note on it that just so happens to have the username and password, no one but you can get in. In addition to a user login there is a quick cell phone call to substantiate your identity is correct and will then grant you access.

Alert Logic Cloud Defender

Alert Logic continually monitors network traffic for any unknown threats and analyzes all the data it collects to better identify potential risks later on. These non-stop assessments help find and identify any vulnerabilities and exposures that your system may have which will allow you to rest assured your information is protected. All of this is coupled with Alert Logic's Security Operations Center (SOC) that provides 24/7 monitoring by GIAC-certified analysts. This level of security and threat analysis helps meet rigorous PCI DSS, HIPAA, and Sarbanes-Oxley requirements.

Compliance Reporting

CompleteCloud also provides quarterly comprehensive compliance reports to your customers, regulators, or auditors so they can sufficiently inspect your infrastructure. Regardless if you're getting assessed by HIPAA or DFARS, you're covered.

completecloud
POWERED BY AVATARA

If you would like more information on the most secure private cloud environment in the country, contact us at sales@avataracloud.com or 888-943-5606.