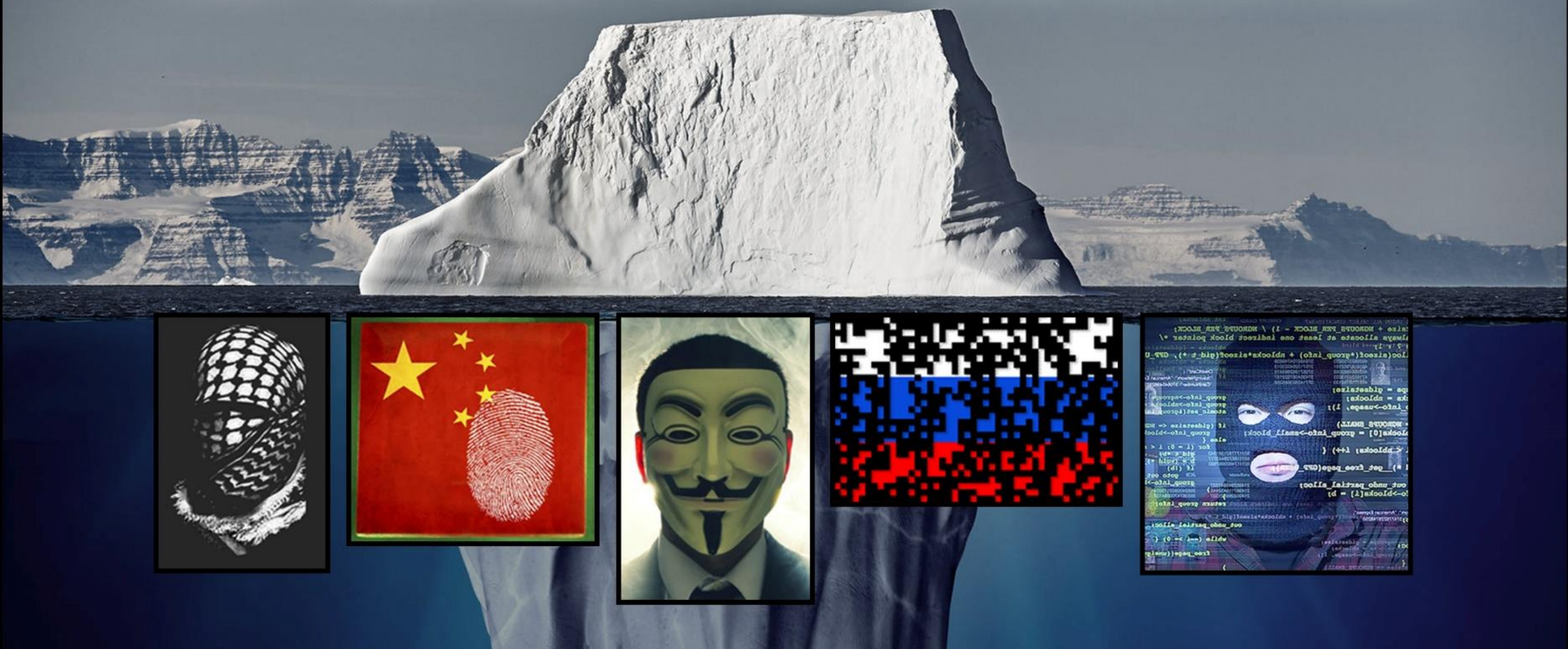
IN 2017, THE INSIDER THREAT EPIDEMIC BEGINS



AUTHORS:

JAMES SCOTT (ICIT SENIOR FELLOW – INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

DREW SPANIEL (RESEARCHER AT THE INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

ICIT | Institute for Critical Infrastructure Technology

In 2017, The Insider Threat Epidemic Begins

February 2017

Authors

James Scott, Sr. Fellow, ICIT
Drew Spaniel, Researcher, ICIT

Expert Contributions From

- Travis Farral, ICIT Contributor & Director of Security Strategy, Anomali
- David McNeely, ICIT Fellow & V.P. Product Strategy, Centrify
- Don MacLean, ICIT Fellow & Chief Cybersecurity Strategist, DLT
- David Rubal, ICIT Fellow & Chief Technologist, DLT
- Michael Seguinot, ICIT Fellow & Director of Federal, Exabeam
- Michael Crouse, ICIT Fellow & Director Federal Technical Sales, Forcepoint
- Josh Salmanson, ICIT Fellow & CTO, Converged Cyber and Physical Security Defense and Security Division, Parsons Corporation
- Igor Baikalov, ICIT Fellow & Chief Scientist, Securonix
- Robert Lord, ICIT Fellow & CEO, Protenus
- Stan Wisseman, ICIT Fellow & Security Strategist, HPE
- Rob Roy, ICIT Fellow & Federal CTO, HPE

ICIT Briefing: In 2017, The Insider Threat Epidemic Begins

February 23, 2017 – Washington D.C.

Join ICIT as we discuss the findings of this paper and hear from leading insider threat experts.

http://icitech.org/event/icit-monthly-briefing-insider-threat/

ICIT Critical Infrastructure Forum
June 7, 2017
Washington D.C.

The 2017
Critical Infrastructure Forum
Rise of The Machines
June 7, 2017
The Four Seasons - Washington D.C.

www.ICITForum.org

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

`

Table of Contents

Introduction

Just as American and European critical infrastructure executives were beginning to wrap their minds around the devastation of the Office of Personnel Management, ransomware erupted onto the scene. We then experienced concentrated DDoS attacks such as the Mirai botnet attack on Dyn, which enabled a quantum leap for cyber criminals of even the most novice of technical aptitude to wreak havoc on targeted organizations at the click of a button or for less than one bitcoin. Unfortunately, adversaries continue to evolve, and cyber defense remains a reactionary culture. Numerous, persistent and adaptive, cyber-adversaries can more easily, remotely and locally besiege critical infrastructure systems, than information security personnel can repel the incessant barrage of multi-vector attacks.

Now, all techno-forensic indicators suggest that an under-discussed cyber-kinetic attack vector will ubiquitously permeate all critical infrastructure sectors due to a dearth of layered bleeding-edge military grade cybersecurity solutions. Unless organizations act immediately, in 2017 The Insider Threat Epidemic Begins.

The act of espionage, to the unsuspecting pawn, is the ultimate betrayal. Michael Crouse, Forcepoint Director Federal Technical Sales and an ICIT Fellow, opines that “Insider Threat is still fairly new to organizations and the awareness of the problem is just emerging today.” Cyberespionage is trivial when organizations render little to no resistance to modern threats. The amalgamation of digital exploitation of network vulnerabilities and the manipulation of psychological weakness empower numerous unknown adversaries to persist on vital systems and to compete amongst each other for dominance over our critical infrastructure.

The cold war has been replaced by the “New Global War” that is virtually absent of munitions; instead cyber-kinetic attacks and information warfare that destabilizes socio-political structures and that weaponizes social media for expedited malicious payload delivery. Government surveillance has been supplanted by corporate dragnet surveillance profiteers who operate without restraint. China’s 13th Five-Year Plan continues to be an all hands on deck national initiative. The Russian/American chess match exchanges nukes for technological stealth and sophistication and 0-day exploits. And in the end, American and European industry and citizens absorb the impact from all sides, while government agencies struggle to stave off endless waves of cyber assaults against their Frankensteined antiquated legacy systems and their haphazard IoT microcosms. All these attacks are facilitated and exasperated by non-malicious and malicious insider threats that poison critical infrastructures from within by subverting their cyber-defenses, by exfiltrating treasure troves of sensitive data, and by infecting vital systems with sophisticated espionage and cyber-kinetic malware.

The Insider Threat Epidemic

America's critical infrastructure organizations are perpetually infiltrated by insider threat actors who ignore cyber-hygiene measures and who bypass cybersecurity controls; thereby, enabling cybercriminals, nation-state advanced persistent threat (APT) actors, and other threats to besiege critical infrastructure systems, to launch cyber-kinetic attacks on the United States, and to exfiltrate treasure troves of sensitive PII, PHI, and IP. According to IBM, of all the 2014 cybersecurity incidents, 31.5% were perpetrated by malicious insiders, and 23.5% resulted from the activities of non-malicious insider threats [1]. These incidents have become so prevalent that Americans have become desensitized to the cycle of alarm, dismay, and reassurance that follows each and every breach in the interminable series of cybersecurity incidents that leave sensitive data in the hands of cyber-adversaries. Shock and public outcry have transformed into disregard and apathy as a new generation of desensitized Americans, who are also conditioned by social media and the internet to openly share information, enter the critical infrastructure workforce. As a result, the policies, procedures, guidelines, and technical security controls protecting sensitive systems, databases, and intellectual properties, are no longer sufficient to protect critical infrastructure organizations from the users that threaten their security from within the network perimeter. Exabeam Director of Federal and ICIT Fellow Michael Seguinot comments, "The long history of IT security has been focused on hardening the perimeter, so inertia and familiarity are the likely culprits. You'd be surprised how often a senior security architect responds by stating that his organization is not at risk because they've deployed next-gen firewalls and two-factor authentication. The notion that these are useless against many insider threats simply doesn't register." Malicious and non-malicious insider threat actors seek to compromise network security, breach databases, disable security controls, install malware, exfiltrate data, or aid adversarial multi-vector information warfare and cyber-kinetic campaigns because they are motivated by ignorance, apathy, mistaken ideals, personal greed, loyalty to a foreign power, etc. HPE Security Strategist and ICIT Fellow Stan Wisseman states, "Change does not come easy. The cyber security budget is limited - generally less than 8% of the IT budget - the availability of high-quality cyber security professionals is limited, making a fundamental change challenging. Additionally, senior business management/Board of Directors tend to run cyber security by "reading a magazine on an airplane" or via business magazine article. This does not lend itself to well-rounded defense in depth security programs." Companies continue to invest in obsolete security strategies focused around external-facing network defenses which do nothing to detect, deter, prevent, or mitigate insider threats. Protenus CEO and ICIT Fellow Robert Lord reasons, "External threats are easier to understand and detect than internal ones, making it easier to explain the case for investing in solutions to combat external threats to decision-makers. While the signs that point to incidents of hackers breaking down firewalls and gaining access to patient records are well-known, the signs that point to incidents of insider threats are more subtle, relying on detailed patterns in EHR accesses that only advanced technologies can recognize.” Further, the discussion surrounding insider threats has stagnated and resulted in a scarcity of actionable intelligence. Additionally, many industry tools and guidance that do mention insider threats, such as the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool, remain vague and brief [2]. Other coverage of the topic devolves into techno-babble that is of little utility to small-to-medium businesses or corporate CISOs.

At their core, organizations depend on trusted personnel to access critical systems, to make pivotal decisions, and to carry out vital operations. Despite all the technological innovation of the digital age, humans remain the strongest and the weakest link in every organization’s cybersecurity. Personnel are the most vital and the most vulnerable operational resource. Cybersecurity resiliency depends on detecting, deterring, and mitigating insider threats because, with just a few minutes of access to the right system, a single insider threat can jeopardize decades of work, can inflict millions or billions of dollars of harm, and can impact millions of lives. Cyber-adversaries from across the globe depend on insider threats to bypass or disable technical and non-technical cybersecurity controls in order to facilitate critical infrastructure breaches. Anomali Director of Security Strategy and ICIT Contributor Travis Farral notes, ”It can be assumed, based on public knowledge of attacks on critical infrastructure, that these targets are chosen for a handful of key reasons. Namely, the asymmetric value in launching attacks on foreign critical infrastructure from relative safety outside of that nation and the level of impact these attacks can have for relatively little cost. From a geopolitical perspective, this is an enticing capability to leverage. A focused phishing campaign can turn unsuspecting insiders into vehicles of mayhem or worse inside a critical infrastructure organization.” Eighty-nine percent of organizations surveyed by the Information Security Forum in 2014 believe that they are vulnerable to insider threats [3]. Due to the sheer number of “trusted employees”, large organizations struggle to identify insider threats or to implement necessary controls before incidents occur; meanwhile, small and medium organizations often lack the resources necessary to detect, deter, or mitigate insider threats. In 2015, only 17 % of security professionals were aware of an insider threat on their network; although, anomalous activity may indicate that insider threats operated in 85% of organizations in 2015 [4]. False alerts, information overload, and an increasingly complex cyber threat environment make detecting the increasing number of insider threats, proportionately difficult. Rather than continue to promote the same antiquated and obsolete perimeter cyber-security solutions, critical infrastructure organizations need to adopt bleeding-edge defense-grade insider threat solutions that seamlessly detect, deter, and mitigate the harmful activities of malicious and non-malicious insider threat actors.

Characterizing Insiders Threats

CERT's "Common Sense Guide to Mitigating Insider Threats," defines an insider as a current or former employee, contractor, or business partner who meets the following criteria:

- Has or had authorized access to an organization's network, system, or data
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

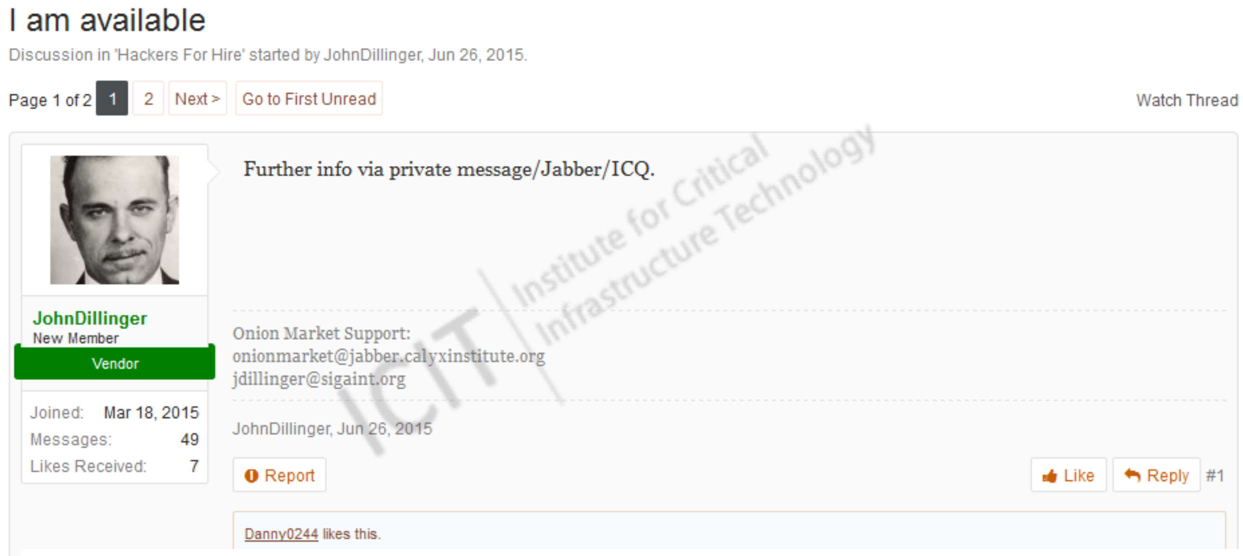
Insider threat occurs in three varieties, of decreasing frequency:

1. Careless or uninformed users who unintentionally violate security requirements and policies due to a lack of cybersecurity awareness, training, or foundational cyber-hygiene.
2. Negligent users who intentionally evade security measure out of convenience, neglect, or misguided attempts to increase productivity.
3. Malicious users who intentionally evade security measures in attempts to profit financially, gain revenge, or seek to unmask corruption or other malfeasance, based on a misguided sense of idealism

According to DLT Chief Cyber Security Technologist and ICIT Fellow Don Maclean, "All of these users leave digital evidence behind, and bleeding-edge technologies can use that evidence to identify the perpetrator. The convergence of data analytics and cybersecurity, in the form of threat-hunting tools gaining traction in the market, is particularly interesting in this area. These tools ingest security data from a huge variety of sources, both external and internal to the organization. They can correlate and analyze that data to identify anomalous behaviors and to flush out insider threats." ICIT Fellow and Chief Technologist at DLT David Rubal continues, "The growing intersection of cybersecurity and data analytics is driving the evolution of defense-in-depth strategies. Data science-derived technologies like big data analytics, machine learning, deep learning and artificial intelligence move visibility, modeling and prediction of cyber-related events to the next level. The effective collection and batch analysis of large amounts of structured (i.e. databases) and unstructured data (i.e. log/machine data, social media data, metadata) are leveraged to create situational awareness and support ongoing insider threat detection, analysis, incident response, and mitigation. Use of a combination of analytics, visualization, and learning algorithms are used to determine classification and pattern detection to result in effective time-series predictions. This outcome-oriented approach and process helps agencies proactively determine risk, what action to take, and in which priority to act."

The Insider Threat Cyber "Kill Chain"

Figure 1: Deepweb Hacker for Hire Can Assist Insider Threats with Technical Attacks Layers



I am available

Discussion in 'Hackers For Hire' started by JohnDillinger, Jun 26, 2015.

Further info via private message/Jabber/ICQ.

Onion Market Support:
onionmarket@jabber.calyxinstitute.org
jdillinger@sigaint.org

JohnDillinger, Jun 26, 2015

JohnDillinger
New Member
Vendor

Joined:	Mar 18, 2015
Messages:	49
Likes Received:	7

Danny0244 likes this.

Figure 1 depicts a Alphabay Deepweb forum listing for a hacker –for-hire. An unsophisticated insider could outsource cyber-technical operations to a hacker-for-hire for a percent commission.

Everyone operating in critical infrastructure sectors has heard of insider threats ranging from Julius and Ethel Rosenberg to Robert Hanssen; however, insiders develop and operate differently in the digital age. Insider threats do not have to be well-positioned, hackers, or technologically sophisticated to inflict catastrophic harm on critical infrastructures or average Americans. No matter how many organizational resources are exerted, humans remain the one data container that employers cannot secure. ICIT Fellow Josh Salmanson of the Parsons Corporation Converged Cyber and Physical Security Defense and Security Division, clarifies, "Many businesses are simply overwhelmed by the duality of having a business presence on the internet and protecting themselves in cyberspace. There are not enough competent defenders available right now to prevent accidental exposures caused by poor computer hygiene practices. Organizationally, a response can only mirror the time and effort invested in end-user training, policy and process adherence, and application of best practices. It is very difficult to punish a naïve end user when the organization hasn't taken all the appropriate steps to protect themselves. Therefore, more training vs. punishment is an important choice related to issues of accidental insider threats. However, data suggests that even large organizations that spend significant resources, people, training time and money end up with only slight improvements in end user behavior and that smart adversaries will always find a path to compromise if they are so inclined." Insider threats often start as trusted employees who are radicalized, polarized, or recruited. Their transformation begins as minor disobedience and deviations from expected behaviors, such as hiding communications from external parties. They flourish in high bustle and high-stress settings; which, inconveniently includes many critical infrastructure environments. The decision to turn is often toyed with before it is acted upon. It might begin as the curiosity about where their access boundaries lie or whether they can access pieces of information that are not relevant to their position. The actor might ask coworkers vague questions, might search for data, or might delegate the aggregation of data to another. Next the insider begins to hoard data. They might even obfuscate it through cryptography or by renaming files or extensions. Eventually, the adversary exfiltrates the data through an egress medium (email, USB, cloud, print, disk, network transfer, etc.). This can often be recognized through uncharacteristic traffic or by off-hour activity; though the insider threat may spread the transfer over multiple sessions. Finally, the adversary exfiltrates the data and attempts to monetize it, transfer it, exploit it, or publically disclose it. Combating insider threats requires a multidisciplinary approach that combines non-technical and technical controls [5].

Non-Malicious Insider Threats

Non-malicious insider threats unintentionally compromise the cybersecurity of the organization through lack of cyber-hygiene or lack of cybersecurity training and awareness. The actions of this category of insider threats are often described as “human error”; however, these mistakes circumvent the cybersecurity of the organization and invite adversaries onto network systems. The impact of non-malicious insider threats should not be dismissed or discounted. The Department of Health and Human Services Office for Civil Rights’ asserts that the Top 5 breaches in Q1 2016 were the result of theft, loss, improper data and account disposal, unauthorized email access, and unauthorized data disclosure [6][7]. Centrify Vice President of Product Strategy David McNeely, an ICIT Fellow, explicates, “The successful attacks that I have seen typically exploit careless users who unknowingly open malicious email attachments or websites which execute malware to steal the user’s credentials and leverage that user’s legitimate access rights in order to move around the network looking for privileged accounts and access to sensitive systems using existing legitimate accounts. External threats are typically addressed with perimeter defenses which have now been rendered useless against these new attack methods which leverage existing communication paths and user accounts. A new model for protecting organizations is required.” Information security teams have difficulty detecting non-malicious insider threats because their unintentionally malicious activity often overlaps with the conventional activity, traffic, and responsibility of their position within the organization. Further, cross-sector trends related to non-malicious insider threat activity are inconclusive or incomplete because activity does not always result in security incidents. Consequently, actions that could allow adversaries access to the network are often not monitored due to a lack of foresight and are not self-reported due to fear of repercussions.

Michael Crouse of Forcepoint agrees that “Efforts to estimate how often companies face attacks from within are difficult to make. It has been suggested that insider attacks are under-reported to law enforcement and prosecutors. Reasons for such under-reporting include an insufficient level of damage to warrant prosecution, a lack of evidence or insufficient information to prosecute, and concerns about negative publicity.”

In some cases, the actions of non-malicious insiders may not lead to incidents or breaches. For instance, most users who mistakenly receive a spreadsheet containing financial or healthcare data, may not know how to monetize the data, may ignore it, or may possess the scruples to contact the sender and inform them of the error. However, in other instances, the actions of the non-malicious insider, such as the aforementioned unauthorized disclosure, can result in a significant impact to the organization or to millions of customers. Non-malicious insider threats are best mitigated by comprehensive cybersecurity policies that do not compromise employee privacy and by a robust cyber-hygiene program that does not hinder employee productivity.

Undertrained Staff

Many critical infrastructure personnel began their careers before the advent of the internet, while others failed to receive cybersecurity awareness and training. In either case, an undertrained individual’s lack of basic cyber-hygiene (i.e. the failure to adhere to cybersecurity policies, procedures, guidelines, and best practices) or the disregard and circumvention of technical controls, leaves the organization vulnerable to compromise by internal or external threat actors. In many cases, a trusted employee becomes an unintentional insider through a seemingly run-of-the mill action (such as taking files home to complete additional work) due to the lack of clear policies to dictate acceptable (and security conscious) actions. This category of insider often includes elderly personnel who fail to receive or retain cybersecurity awareness training and recently onboarded hires that do not receive proper guidance and training.

Employees deficient in sufficient cyber-hygiene and in cybersecurity training and awareness are susceptible to social engineering campaigns and to otherwise undermining the cybersecurity of the organization [8]. According to the Verizon 2016 Data Breach Incident Report, accidents attributed to un-cyber-hygienic personnel accounted for 30% of all security incidents in 2015 [9]. Undertrained staff may also make poor decisions that at best leave the organization legally liable and at worst expose sensitive data to a plethora of cyber-adversaries. For instance, an employee who uploads data to social media, to email clients, to storage sites (Google Drive, ZippyShare, etc.) or to development sites (CodeHaus, SourceForge, etc.) may not be aware of the terms and conditions, privacy policies, or security controls, of those sites [4]. As a result, data ownership may transfer to the site in question or the data may be unintentionally exposed to other insider threats or cyber-adversaries.

Accident-Prone Employees

Accident-prone insider threats are personnel whose unintentional actions compromise the organization despite receiving cyber-hygiene and cybersecurity training and awareness information. Every time a device is lost, an email is sent to the wrong recipient, or a sensitive system is left logged-in, data is unintentionally disclosed and the organization suffers an incident. If an investigation reveals that an adversary obtained even a single datum, then a breach has occurred; though, breach laws, such as the HITECH Act (section 13402(e)(4)), define breaches slightly differently and require at least 500 records to have been compromised before mandating public disclosure [7]. Robert Lord from Protenus states, “In healthcare, we frequently see guidelines that reflect key challenges currently facing the industry. For example, amidst a spike in ransomware activity, the Department of Health and Human Services issued guidelines describing actions healthcare providers can take to prevent ransomware attacks. One unintended consequence of mandates that arise in direct response to big-time privacy breaches is that they serve as Band-Aid solutions rather than long-term ones that will have systemic implications, leaving institutions unknowingly still vulnerable to threats. After all, cybersecurity is a marathon, not a sprint. The hope is that these major events will serve as a wake-up call that inspires forward-looking technologies rather than the tired FTE models of security and privacy. If the old approaches clearly fail to keep data safe, it’s a major sign that it’s time to pay attention to new models.” Every time an employee clicks a malicious link, visits a watering-hole site, opens a malicious attachment, etc., they subvert the organizational cybersecurity and invite adversaries to infiltrate, compromise, and infect the network.

Consider that despite years of cybersecurity awareness and training, most staff’s kneejerk reaction to finding a “lost” USB drive is to plug it into a corporate PC in order to read through the files or to identify the owner. Social engineering attacks such as these can be used by sophisticated nation-state advanced persistent threats, and other adversaries, to infect critical infrastructure systems via an un-cyber-hygienic employee. This methodology was used in 2008 in order to spread the Agent.BTZ malware through the Department of Defense and other critical infrastructure facilities. At the time, it was hailed as the “worst breach of U.S. military computers in history”. Agent.BTZ may have been spread by the Russian state-sponsored Uroburos APT. The Uroburos malware, which appeared in 2011 (or earlier) and was discovered in 2014, scans for the presence of Agent.BTZ on target systems and remains inactive if Agent.BTZ is installed. The two malware also share some file names, encryption keys, and other technical indicators [10].

The APT currently relies on targeting inadvertent insiders with spear phishing campaigns, drive-by-infections, watering hole attacks, and social engineering to push their malware onto target networks. The Uroburos malware is a sophisticated, flexible, and modular cyberespionage platform that is designed to spread throughout an entire compromised network and to exfiltrate sensitive data back to its operators. The malware can even infect air-gapped systems by infecting removable media and transient host systems [10].

Negligent Workers

When not efficiently implemented, some personnel may feel that technical and non-technical cybersecurity and cyber-hygiene controls hinder their performance and the execution of their duties. As a result, these insiders intentionally ignore or circumvent the essential security policies and controls for convenience, for the sake of increasing their personal performance, or (they often erroneously believe) for the sake of the organization [8]. For example, a negligent employee might connect an unapproved third-party device to the network, they might use email or cloud applications to transfer files outside the network in order to work from home, or they might access sensitive network assets from an insecure connection (such as public Wi-Fi or a BYOD device), etc. For instance, if a negligent worker takes works from their personal computer and they connect to the Wi-Fi at a foreign hotel. Then they may become compromised by DarkHotel, or similar APTs, who specifically target negligent insiders [11].

In one exemplary 2013 illustration of employee negligence, an American software developer outsourced his programming job to a consulting firm in Shenyang, China for approximately $50,000 while he continued to collect a salary of several hundred thousand dollars. Meanwhile, the negligent insider spent his workdays surfing social media and reading emails. The insider activity was detected when an investigation into anomalous activity discovered that the employee's credentials were being used to remotely access the company systems. The employee had mailed his multi-factor authentication key to the Chinese consultant via Fed-Ex. For the potential years that the employee outsourced his job, he received excellent marks in his performance reviews and the clean and functional code that he submitted was considered some of the best in the organization [12].

Though the negligent employee's scheme was clever and though the organization may have used and praised the outsourced code for years, the actions of the employee make him an insider threat because the data and systems of the organization were accessible by a foreign agent who could have themselves been a malicious threat actor. If nothing else, the Chinese government requires that every organization operating within its borders have a liaison to the Chinese government [13]. The liaison possesses full administrative privileges and could easily coerce the contractor into exfiltrating data or provide access for a Chinese APT.

APT1, Axiom, and numerous other Chinese nation-state sponsored APTs may receive information from embedded liaisons. Some information may be monetized or exploited, while other data is repurposed to facilitate cascading breaches.

Mismanaged Third-party Contractors

Third-party contractors, who are placed within an organization without being briefed on the organization's cybersecurity policies, procedures, guidelines, practices, and controls, may become a non-malicious insider threat when they act in any manner that exposes the network or its data to compromise.

Critical infrastructure depends on numerous third-parties in order to operate within a reasonable budget. However, not all contractors are reliable or can be trusted to automatically prioritize the cybersecurity of client systems. Consider that the 2013 breach that cost Target an estimated $1 billion was the result a spear-phishing attack campaign that compromised the HVAC, Fazio Mechanical Services. Fazio was responsible for a small portion of Target's electronic billing, contract submission, and project management. Target was the only client for whom Fazio provided remote process management. Despite a claim of "full [IT and Security] compliance with industry practices", the perpetrators of the attack were not detected on Fazio's system because the firm's only protection was the free version of an anti-malware application. Fazio had remote access to: Ariba external billing systems, Target's Project Management software, a contract submission portal called Partners Online, and Target's Property Development Zone portal. Ariba was used for the ticket submission and payment collection of external vendors. Contractors, such as Fazio, accessed the front end of the application, while Target Administrators used the back end access to maintain the system and to pass credentials. Target relied upon Active Directory for most internal credential processes. Once the attackers accessed Ariba from Fazio's credentials, the group laterally navigated to Target's internal servers by superseding administrator privileges. Despite claims of PCI compliance, Target failed to meet the requirement that merchants incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties. An inside source says that Target only rarely met this requirement by using a one-time token or other means of secondary authentication. In fact, the anonymous source claimed that:

> "Only the vendors in the highest security group — those required to directly access confidential information — would be given a token and instructions on how to access that portion of the network. Target would have paid very little attention to vendors like Fazio, and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target."

The hackers uploaded a fully un-detectible (FUD) malware, similar to the known BlackPoS code, onto a small number of Target's point of sale terminals between November 15 - 28, 2013. Despite the use of over 40 commercial antivirus, antimalware, and firewall applications on each terminal, the malware remained unnoticed. The code was tested for approximately two weeks, before it launched nationwide and it began to store the information from magnetic CAD strips processed at infected terminals. The magnetic signatures (credit card numbers and cardholder information) of the cards were parsed from internal memory the instant after the card was swiped. The information of ~40 million cards was transmitted to a hijacked internal server where it was aggregated with the stolen personal information (name, mailing address, email address, phone number, etc.) of ~70 million customers on a shared S: drive. The internal server, made by BMC software, may have been hijacked using backdoor administrator credentials used for batch jobs or it may have been infected with "Blade Logic" malware to facilitate lateral network movements. The data remained inactive for six days, before transfer to an external FTP server. Beginning on December 2, 2013 the server transmitted the payloads to the FTP server of a hijacked website several times a day, for a two week period. A Russian virtual private server (VPS) began downloading the data. Some of the data was also exported to zombie dump PCs in Miami and Brazil. Approximately 11 GB of stolen data was transmitted over the two week period. The card information can be used to produce counterfeit cards by replicating the magnetic strip. The cards and some of the personal information were sold on popular underground sites such as rescator[.]la for payments of $18-$35.70. [14][15]. Perhaps if Target better communicated its cybersecurity expectations to its contractor or if it better restricted the connection to Fazio systems based on the access due to their HVAC role, the breach could have been prevented.

Overwhelmed Personnel

Overwhelmed or fatigued personnel may be the largest category of critical infrastructure insider threats because America's critical infrastructure is acutely under-resourced in certain areas. For instance, in 2016, there were an estimated 1 million critical infrastructure cybersecurity job vacancies, and that number is expected to increase to 1.5 million by 2019 [16]. These positions are vacant because current personnel are either incapable of performing cybersecurity duties or already dedicated elsewhere. Consequently, the inability to fill these positions with qualified personnel or actions such as hiring freezes, which prevent the hiring of vital personnel, shift cybersecurity or other duties onto unfit or overburdened critical infrastructure personnel [17]. These overexerted personnel become inadvertent insider threats the moment that they take shortcuts, cut corners, or circumvent policies and controls in any attempt to balance their disproportionate workloads. Additionally, the disproportionate workload can cause frustration and resentment to build, and the overwhelmed employee may develop into a malicious insider. Stan Wisseman from HPE explains, "When employees are stressed and working fast, they tend to be more susceptible to social engineering attempts. Organizational leaders need to examine whether they are creating a stressful environment or one that fosters a natural workflow. For example, one aspect of a plan to minimize stress could involve allocating time for employees to fulfill information security compliance requirements."

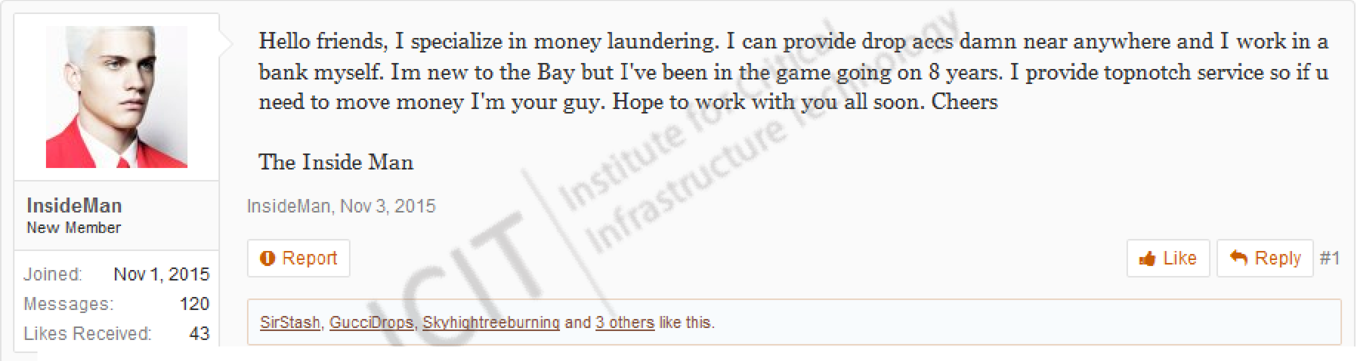
Malicious Insider Threats

Organizations often fail to predict or detect the activity of malicious insiders because cybersecurity strategies tend to focus solely on external third-party adversaries. These organizations discount the possibility that any of their personnel could be enticed to act against the organization. In reality, a fraction of every organization's workforce can be motivated by internal or external incentives to intentionally subvert the cybersecurity of the organization [8].

Disgruntled Employee

Trusted employees develop into malicious insider threats due to distrust of the organization, due to perceived inequality, or due to perceived harm. These threat actors often seek to disrupt operations, to delete data, or to harm the organization. For example, a disenfranchised or disgruntled employee might exfiltrate sensitive data with the intention to later sell, exploit, or publically release the information to inflict reputational harm on the organization [8]. Disgruntled employees are dangerous because they blend into the background. Without bleeding-edge technical solutions, the threat is often unrecognized until a cyber or physical event occurs. Could you look at the janitorial or support staff and know with full confidence that they harbor no ill-will towards the organization?

Figure 2: Alphabay Forum Listing of Financial



InsideMan
New Member

Joined: Nov 1, 2015
Messages: 120
Likes Received: 43

Hello friends, I specialize in money laundering. I can provide drop accs damn near anywhere and I work in a bank myself. Im new to the Bay but I've been in the game going on 8 years. I provide topnotch service so if u need to move money I'm your guy. Hope to work with you all soon. Cheers

The Inside Man

InsideMan, Nov 3, 2015

SirStash, GucciDrops, Skyhightreeburning and 3 others like this.

The self-proclaimed insider in Figure 2 claims to work in a bank and offers money laundering services to Deepweb users.

Disgruntled employees are organizational vulnerabilities waiting to be exploited by an opportunistic adversary. In many cases, their privileged positions as support staff (who often feel used or under compensated) or as mid-level management (jealous of the advancement of their peers) make them valuable intelligence assets to external attackers. Imagine how much harm an enemy nation state could inflict if they knew the daily schedule or account credentials, of say, the President or a Fortune 50 CEO. Hail-mary threat actors such as ISIS or North Korea, lack the sophisticated technical acumen necessary to severely impact United States critical infrastructure; however, a disgruntled employee can be recruited through ideological propaganda or financial gain to launch cyber-kinetic attacks on an employer’s critical infrastructure systems. After all, it is cheaper to pay a disgruntled employee to disable layers of security controls than it is to hire an APT team to launch attacks and search for vulnerabilities.

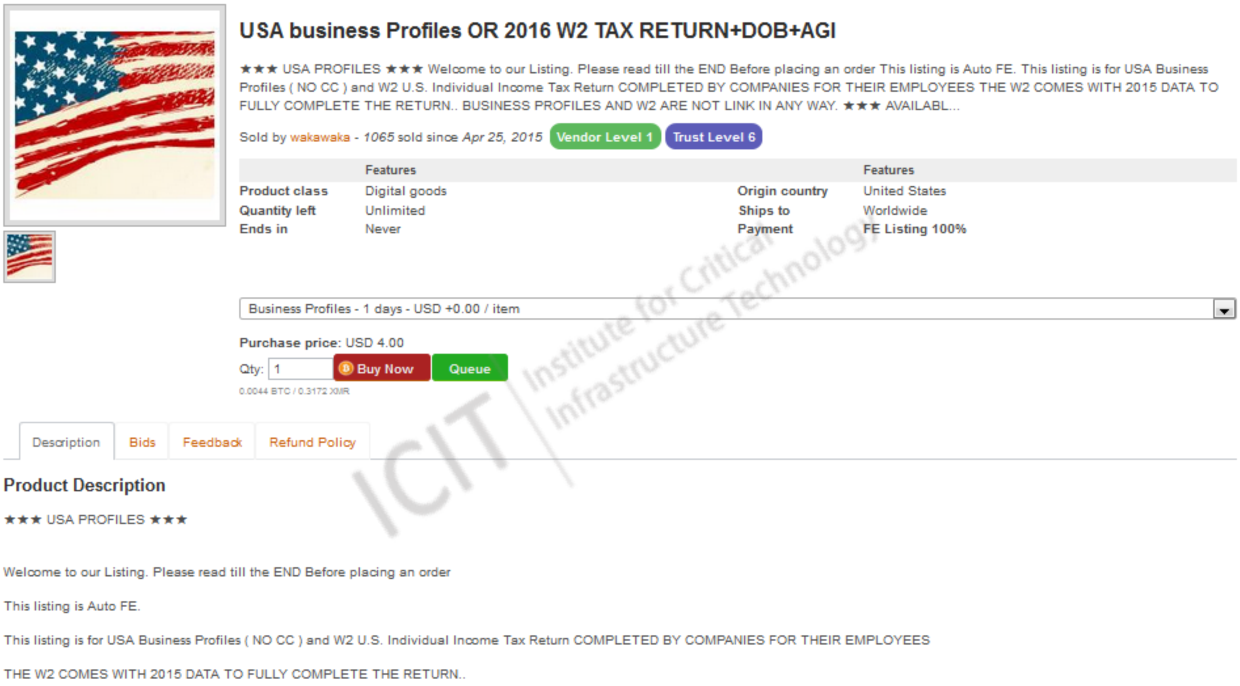
Cyber-Jihadist

Cyber-jihadists, whether self-radicalized or recruited seek to infiltrate Western critical infrastructure in order to conduct multi-vector cyber-physical attacks, to exfiltrate sensitive intelligence, or to pre-position future campaigns.

In May 2016, the Islamic State Hacking Division claimed to have an insider threat in the British Ministry of Defense. While this claim was unsubstantiated, it may be worth noting that 15.6% of ISIS recruits have completed one or more years of college. Active college students brainwashed by the Daesh ideology could be persuaded to apply for an entry level position at a target company as pre-positioning for a cyber-kinetic campaign. These low-tier recruits could physically harm critical infrastructure personnel or systems. Moreover, their actions within an organization could be synchronized with unsophisticated or outsourced layered attacks, such as a DDoS attack, for a compounded impact.

Departing Executive

Figure 3: Deepweb W-2 Database Sale



USA business Profiles OR 2016 W2 TAX RETURN+DOB+AGI

★★★ USA PROFILES ★★★ Welcome to our Listing. Please read till the END Before placing an order This listing is Auto FE. This listing is for USA Business Profiles (NO CC) and W2 U.S. Individual Income Tax Return COMPLETED BY COMPANIES FOR THEIR EMPLOYEES THE W2 COMES WITH 2015 DATA TO FULLY COMPLETE THE RETURN.. BUSINESS PROFILES AND W2 ARE NOT LINK IN ANY WAY. ★★★ AVAILABL...

Sold by wakawaka - *1065* sold since *Apr 25, 2015* Vendor Level 1 Trust Level 6

	Features		Features
Product class	Digital goods	Origin country	United States
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Business Profiles - 1 days - USD +0.00 / item

Purchase price: USD 4.00

Qty: 1

0.0044 BTC / 0.3172 XMR

Product Description

★★★ USA PROFILES ★★★

Welcome to our Listing. Please read till the END Before placing an order

This listing is Auto FE.

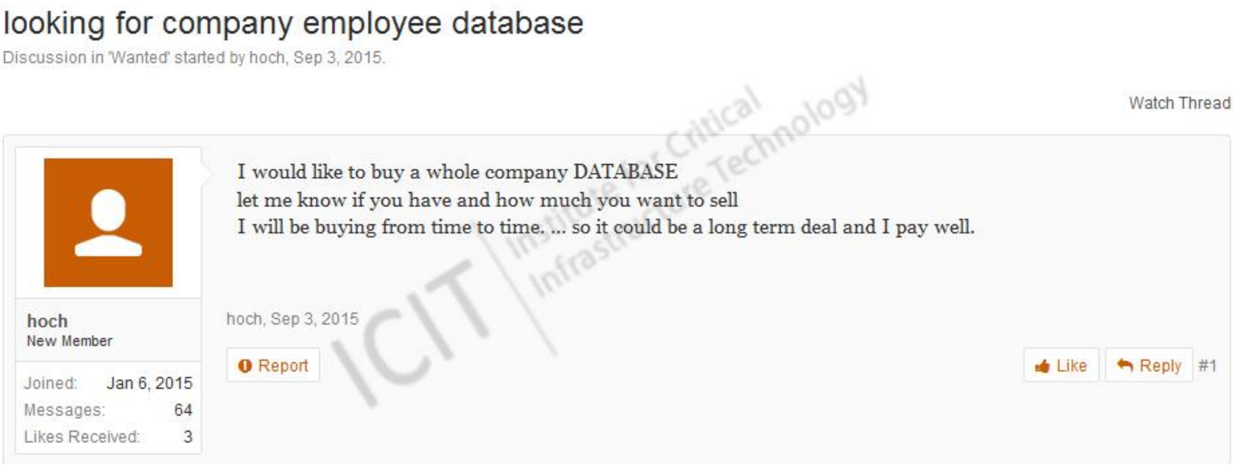
This listing is for USA Business Profiles (NO CC) and W2 U.S. Individual Income Tax Return COMPLETED BY COMPANIES FOR THEIR EMPLOYEES

THE W2 COMES WITH 2015 DATA TO FULLY COMPLETE THE RETURN..

A departing executive could leave the company with intellectual property, trade secrets, financial information, PII, etc. For instance, someone with access to payroll could exfiltrate and later sell employee tax information.

Concern that data may be exfiltrated by departing personnel is a concern independent of organization size or sector. Whenever an executive or other high-ranking personnel leaves an organization, there is the risk that the individual will steal confidential data, client lists, or intellectual property, and take the information to a competitor. The theft of customer or sales data may be difficult to detect because it may be known to the individual (people are information vessels too) or it may be contained in a proprietary corporate database or application that is inadequately integrated into the cybersecurity environment. User Activity Monitoring can help detect whether an employee is browsing competitor sites, communicating with parties outside the organization, or applying to external job listings from the corporate network. Psychographic big data analytics of the Salesforce traffic on cloud services or of the traffic logs can also help identify anomalous user behavior [4].

Figure 4: Solicitation of Company Databases



looking for company employee database

Discussion in 'Wanted' started by hoch, Sep 3, 2015.

hoch
New Member

Joined:	Jan 6, 2015
Messages:	64
Likes Received:	3

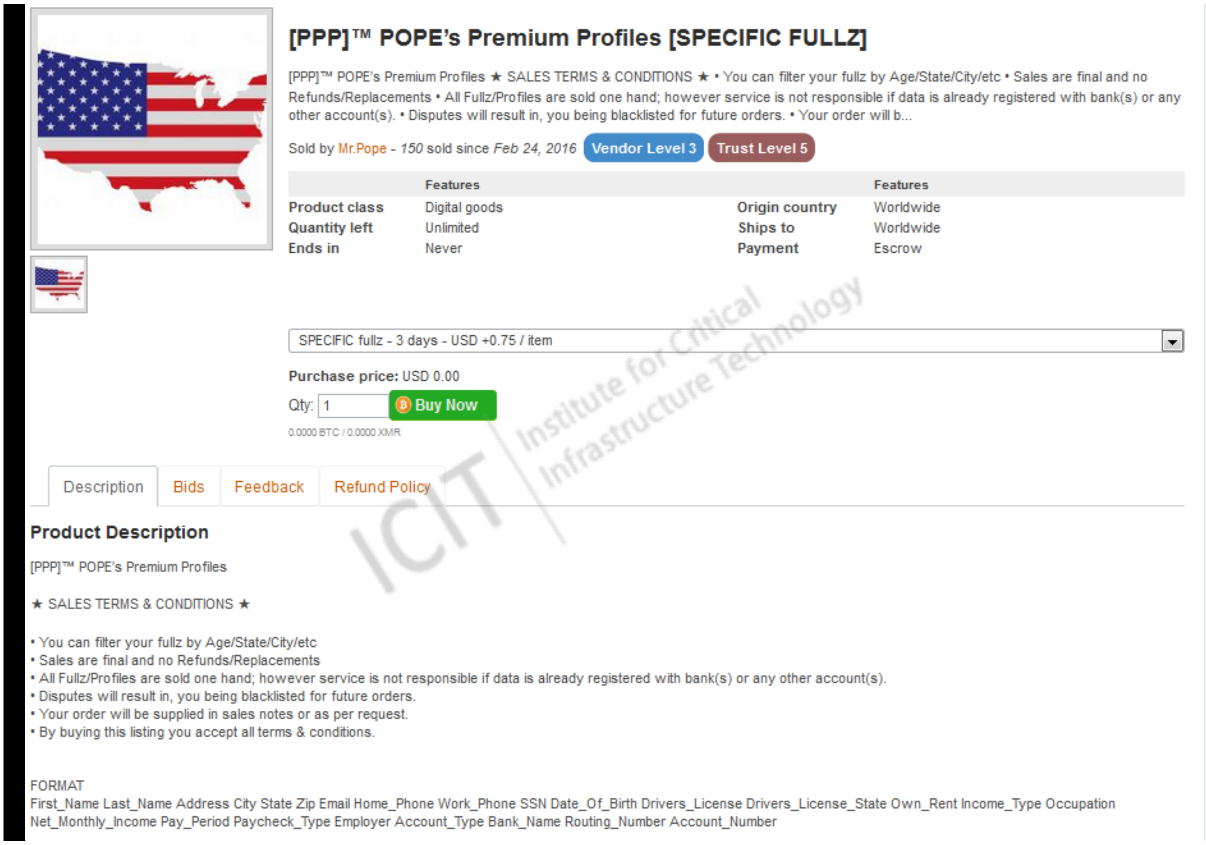
I would like to buy a whole company DATABASE
let me know if you have and how much you want to sell
I will be buying from time to time. ... so it could be a long term deal and I pay well.

hoch, Sep 3, 2015

Cybercriminals exchange company databases and other PII on Deepweb markets and forums. A departing executive could easily exfiltrate and sell massive treasure troves of employee data.

Cyber-criminal

Figure 5: Specific Fullz Sale



[PPP]™ POPE's Premium Profiles [SPECIFIC FULLZ]

[PPP]™ POPE's Premium Profiles ★ SALES TERMS & CONDITIONS ★ • You can filter your fullz by Age/State/City/etc • Sales are final and no Refunds/Replacements • All Fullz/Profiles are sold one hand; however service is not responsible if data is already registered with bank(s) or any other account(s). • Disputes will result in, you being blacklisted for future orders. • Your order will b...

Sold by Mr.Pope - 150 sold since Feb 24, 2016 Vendor Level 3 Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

SPECIFIC fullz - 3 days - USD +0.75 / item

Purchase price: USD 0.00

Qty: 1

0.0000 BTC / 0.0000 XMR

Product Description

[PPP]™ POPE's Premium Profiles

★ SALES TERMS & CONDITIONS ★

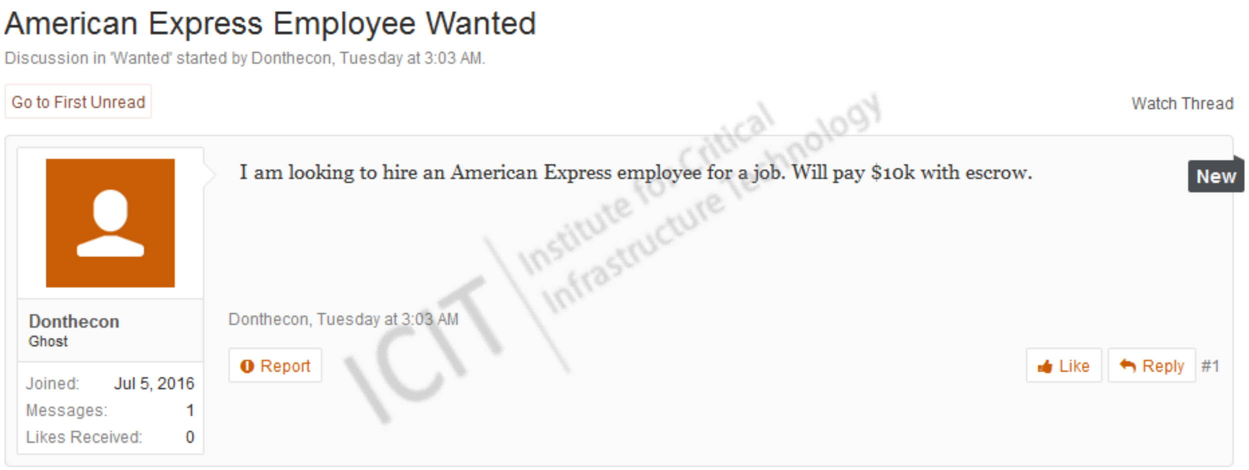
- You can filter your fullz by Age/State/City/etc
- Sales are final and no Refunds/Replacements
- All Fullz/Profiles are sold one hand; however service is not responsible if data is already registered with bank(s) or any other account(s).
- Disputes will result in, you being blacklisted for future orders.
- Your order will be supplied in sales notes or as per request.
- By buying this listing you accept all terms & conditions.

FORMAT
First_Name Last_Name Address City State Zip Email Home_Phone Work_Phone SSN Date_Of_Birth Drivers_License Drivers_License_State Own_Rent Income_Type Occupation Net_Monthly_Income Pay_Period Paycheck_Type Employer Account_Type Bank_Name Routing_Number Account_Number

The Alphabay listing in Figure 5 enables a cyber-criminal to target and exploit the PII of a specific individual.

Stolen personal identifiable information (PII) has generated Deep Web markets worth over an estimated $120 billion [6]. Cybercrime is common wherever cyber hygiene is lacking. Some enterprising personnel, who are dissatisfied by their salary or are overwhelmed by greed, may be compelled to exfiltrate sensitive information from the organization in order to sell it on Deep Web markets such as Alphabay. Information on high-profile individuals could also be sold to tabloids, geopolitical adversaries, etc. Healthcare organizations, which are subject to massive personnel throughput, are at particular risk to the exfiltration of sensitive information by insider cyber-criminals [18].

Figure 6: Disgruntled Employee Solicitation



American Express Employee Wanted

Discussion in 'Wanted' started by Donthecon, Tuesday at 3:03 AM.

I am looking to hire an American Express employee for a job. Will pay $10k with escrow.

Donthecon, Tuesday at 3:03 AM

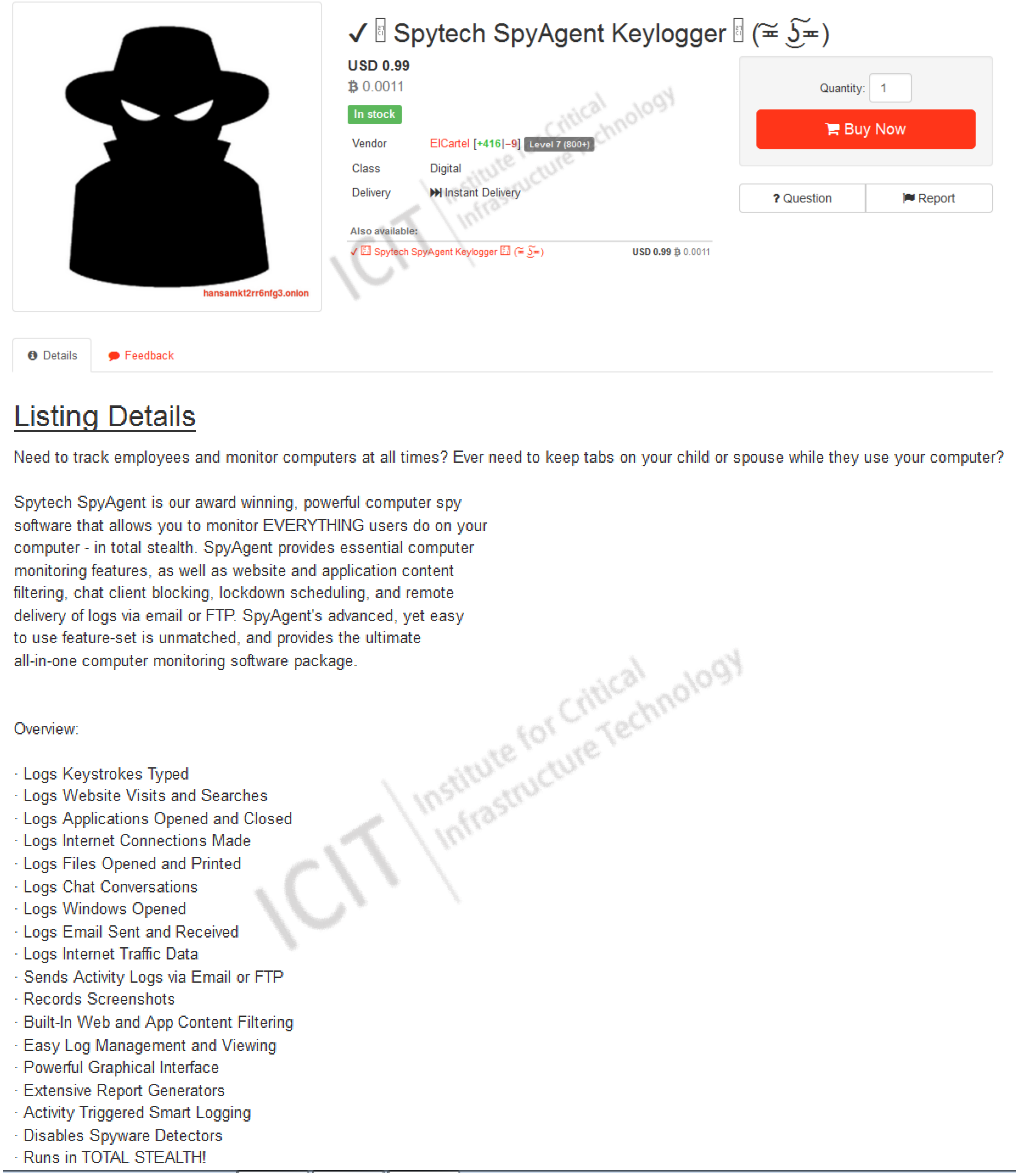
Donthecon
Ghost

Joined:	Jul 5, 2016
Messages:	1
Likes Received:	0

Cybercriminal or APT threat actors solicit disgruntled employees to aid in their operations in order to ease the compromise and decrease the resource input.

The Carbanak group are a criminal advanced persistent threat group whose attacks against dozens (potentially hundreds) of global financial institutions resulted in an estimated $1 billion in losses in the first half of 2014. Their custom backdoor targets the intranet of the victim organization so that the adversaries can locate systems with financial data, credentials, classified emails, manuals, cryptographic keys, or financial applications. In the latter case, the attacker uses keyloggers, video capture plugins, and screen capture tools to ascertain an operational picture of typical workflow, tool usage, and practices.

Figure 7: HansaMarket Listing for the Spytech SpyAgent Keylogger



✓ □ Spytech SpyAgent Keylogger □ (≆ ʖ≆)

USD 0.99
฿ 0.0011

In stock

Vendor ElCartel [+416|-9] Level 7 (800+)
Class Digital
Delivery ⏭ Instant Delivery

Also available:

✓ □ Spytech SpyAgent Keylogger □ (≆ ʖ≆) USD 0.99 ฿ 0.0011

Listing Details

Need to track employees and monitor computers at all times? Ever need to keep tabs on your child or spouse while they use your computer?

Spytech SpyAgent is our award winning, powerful computer spy software that allows you to monitor EVERYTHING users do on your computer - in total stealth. SpyAgent provides essential computer monitoring features, as well as website and application content filtering, chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP. SpyAgent's advanced, yet easy to use feature-set is unmatched, and provides the ultimate all-in-one computer monitoring software package.

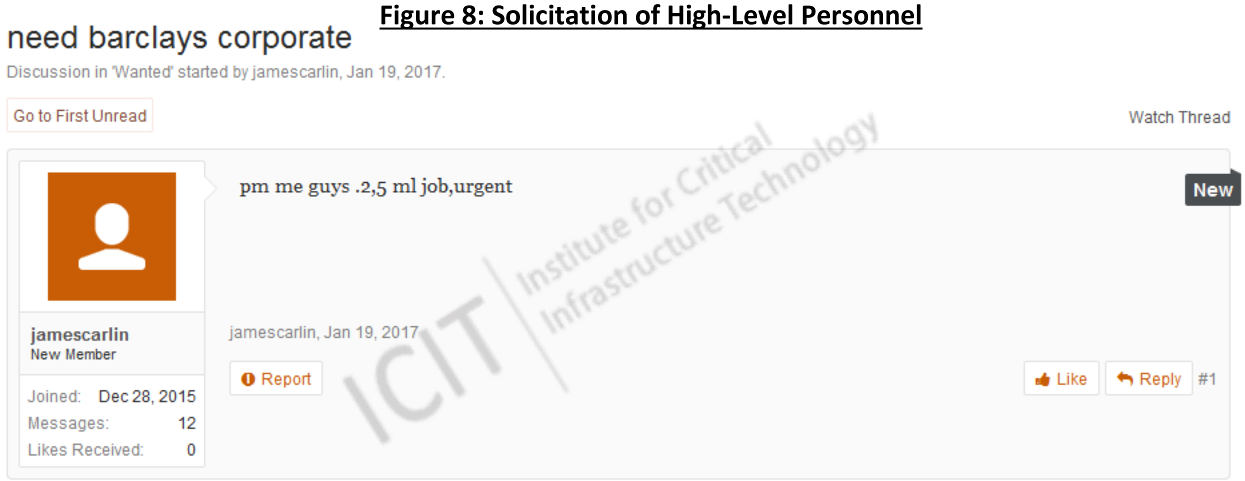
Overview:

· Logs Keystrokes Typed
· Logs Website Visits and Searches
· Logs Applications Opened and Closed
· Logs Internet Connections Made
· Logs Files Opened and Printed
· Logs Chat Conversations
· Logs Windows Opened
· Logs Email Sent and Received
· Logs Internet Traffic Data
· Sends Activity Logs via Email or FTP
· Records Screenshots
· Built-In Web and App Content Filtering
· Easy Log Management and Viewing
· Powerful Graphical Interface
· Extensive Report Generators
· Activity Triggered Smart Logging
· Disables Spyware Detectors
· Runs in TOTAL STEALTH!

Insider threat actors might load a keylogger on behalf of an external threat actor or to facilitate privilege escalation and data capture.

Once the adversary knows how to use the most powerful host applications, they would withdraw or transfer significant sums, via fraudulent online banking transfers, electronic cash transfers to banks in China and the United States, SWIFT transfers to compromised bank accounts, and remote commands to ATMs to spew cash onto the street at a specific date and time, depending on the system, situation, and available resources (time, people, etc.). Carbanak is hindered by their reliance on a non-malicious insider to unintentionally download the malware, and by their unfamiliarity with each target's financial system. If they were able to hire or embed a malicious insider in the financial institution, then their attack lifecycle might be reduced from months to days [19] [20].

Figure 8: Solicitation of High-Level Personnel



need barclays corporate

Discussion in 'Wanted' started by jamescarlin, Jan 19, 2017.

pm me guys .2,5 ml job,urgent

jamescarlin
New Member

Joined:	Dec 28, 2015
Messages:	12
Likes Received:	0

jamescarlin, Jan 19, 2017

External cyber threat actors seek partnerships with high-level insider threats in hopes that the position of the will facilitate data exfiltration.

Rogue System Administrator

Privileged users, such as system administrators, have specific knowledge, unique authority and unparalleled access to sensitive data and systems. When system administrators turn into malicious adversaries, the consequences are severe. For example, in 2008, Terry Childs, a San Francisco network administrator, locked the city out of its FiberWAN network by creating his own passwords. The network served as the infrastructure connecting hundreds of departments and buildings to each other and to a central data center, FiberWAN governed email, payroll, police records, inmate information, and city hall systems. Childs locked the system after becoming disgruntled that his job was in jeopardy [21]. Rogue system administrators can lock systems, delete data, alter user privileges, exfiltrate data, install malware, or compromise systems.

Malware has advanced significantly since 2008. Imagine if a rogue system administrator, with full knowledge and access to critical infrastructure systems, intentionally deployed sophisticated malware, such as BlackEnergy, an IoT worm, or ransomware. On December 23, 2015, the BlackEnergy malware systematically caused a severe outage at three Ukrainian power plants in, what was likely, a global demonstration of Russian APT cyber-kinetic capabilities. The attackers targeted IT staff and system administrators with a phishing email that loaded malware onto Ukrainian power company systems and enabled external adversaries to harvest credentials and gain insider access and control of electricity systems. The adversaries were able to systematically disable controls, systems, and failsafes as they laterally navigated upstream within the network architecture.

A less sophisticated attacker could intentionally cripple a network in order to cause chaos. System administrators tend to know the single points of failure of their networks. A targeted IoT DDoS attack, such as the Mirai attacks on Dyn, could result in a devastating impact. Alternately, the attacker could target vulnerabilities in the sector as a whole. For instance, the energy sector is increasingly dependent on insufficiently secured IoT devices. An attacker could launch a self-propagating worm to “brick” or neutralize infected routers, IP cameras, DVRs, sensors, or other IoT devices. Security researchers Eyal Ronen, Colin O’Flynn, Adi Shamir, and Achi-Or Weingarten, demonstrated in their paper “IoT Goes Nuclear: Creating a ZigBee Chain Reaction,” that an IoT worm could infect adjacent IoT devices through networked connectivity in an attack capable of spreading throughout a city within minutes.

Malicious Third-Party Insider

Insider threats are typically considered to be within the enterprise network; however, an insider within a lateral third-party network may prove equally or exponentially more dangerous to an organization because their distance from the target makes their activities more difficult to deter or detect. For instance, a malicious insider at a cloud service provider may be able to access all of an organization’s data without being subject to the technical cybersecurity controls or non-technical policies, procedures, guidelines, and culture that insulate that organization from insider threats. Unless the data is encrypted with customer-managed keys, the attacker can exfiltrate or manipulate the data, they can sell credentials or access, or they can steal intellectual property. If the service provider is not subject to a service level agreement (SLA) that directly addresses cybersecurity and liability, the enterprise customer may bear the entire impact of the breach. This example demonstrates the necessity of only relying on reputable service providers, and of requiring a comprehensive service level agreement (SLA) that clearly defines expected cybersecurity policies, procedures, controls, responsibilities, standards, and liabilities.

David McNeely of Centrify advises, “Assume the contractor is an Insider Threat and minimize access rights and privileges. It is too common for outsourced support contractors to request both VPN access as well as rights to checkout Break Glass accounts for all systems they are contracted to support. However both of these are very bad and should never be used by any employee much less a contractor. Instead, contractors should only be given application layer access to specific systems they require access to for specific work tasks. Further they should only be granted specific privileges to accomplish the task at hand, even if that may require them to come back and ask for additional privileges. Break Glass accounts can do anything to a system and should never be used, unless you really have a system down and need to actually break glass.”

Activist

Self-radicalized lone-wolf activists, such as Edward Snowden, may infiltrate organizations with the express intent of compromising systems, of conducting a cyber-kinetic attack, or of exfiltrating data. The actor often believes that their actions benefit the greater good. These malicious insiders can be detected in the background check process and can be deterred by strong access controls, such as Identify and Access Management solutions, and through sophisticated detection mechanisms, such as User Activity Monitoring (UAM).

Corporate Spy

A corporate spy either infiltrates an organization in order to exfiltrate data or is coerced into stealing data for a third-party or in service to an external motivation. The impact of corporate spies can be minimized by limiting employee privileges and access, by segmenting networks and responsibilities, and by monitoring attempts to access, alter, or exfiltrate treasure troves of valuable data.

In April 2013, Huajun Zhao, an associate cancer researcher at the Medical College of Wisconsin, stole three bottles of an anti-cancer compound with the intent of transporting them back to China. Zhao had been disciplined months earlier for storing sensitive research data on his personal computer. Upon further investigation, Zhou’s computer was found to contain 384 items related to the anti-cancer research, additional research from the Hematology/Oncology department, and a grant application addressed to the Chinese government that claimed that he had discovered the compound and that requested funding for additional research. College security also discovered that after his suspension and while the investigation was pending, Zhou had remotely accessed the Medical College servers and deleted the primary researcher’s raw data [46]. Similarly, from February 2013 to June 2014, Chinese engineer Jun Xie stole 2.4 million files (~1.4 terabytes) from GE Healthcare. The data consisted of engineering designs, testing data, business strategy and source code for magnetic resonance systems. Xie was not authorized to access most of the data, and the information was not pertinent to his work. Xie copied the data to separate storage devices and sent them to his wife and brother in China. Xie intended to return to China and join a firm that directly competes with GE in the MRI field. In court documents, GE stated that it would have suffered "irreparable harm" if the trade secrets were disclosed [22].

Nation-State Sponsored Threat

The most dangerous and the most elusive insider threat is a malicious nation-state sponsored APT proxy that infiltrates an organization in order to facilitate the compromise of sensitive systems as part of multi-vector cyber-kinetic warfare campaigns. The threat actor may seek just to plug in a USB or open a malicious email attachment, rather than directly exfiltrating data. Securonix Chief Scientist Igor Baikalov, an ICIT Fellow, asserts, “We do see quite a bit of employees offering their corporate credentials for sale advertised on the dark web - is a lot cheaper and faster than hacking your way into a corporate network and then looking for the right level of access. Besides willing insiders, coercion in the form of blackmail, extortion, and other threats has been made easy by the availability of massive amounts of very sensitive information from the breaches at OPM, Anthem, Yahoo and others. Nation-states possessing this data can build fairly complete profiles and screens for potential targets.”

The Chinese state-sponsored Deep Panda APT exfiltrated 22.1 million granular, detailed SF-86 forms in the 2015 OPM breach. The SF-86 is 127 pages of granular demographic and psychographic information about United States critical infrastructure personnel and clearance applicants. Further, Deep Panda breached Anthem, United Airlines, and other critical infrastructure organizations in the last few years. The information stolen in OPM and healthcare breaches can be aggregated in a custom database of American critical infrastructure personnel; meanwhile, travel logs and SF-86 information can be used to profile and track specific personnel. As a result, China already can single out personnel who can be coerced into acting as malicious insiders. Alternately, Deep Panda can assist in the Chinese infiltration of American critical infrastructure through identities stolen in the OPM or cascading breaches or by leveraging any false information added to OPM databases during the extended breach. These threats can be deterred through the layering of thorough background checks, a cyber-hygienic employee culture, data loss and spillage prevention mechanisms, identity and access management solutions, virtualization, and user activity monitoring.

The Insider Threat Debate

Conventional, and often ineffective, strategies to combat insider threat focus entirely on protecting endpoints and mobile devices. More efficacious modern approaches focus on either securing data or monitoring users. HPE's Stan Wisseman explains that "insider threats and outsider threats are no different. Protecting data solves both equally." Controls are split into non-technical policies, procedures, and guidelines, and technical solutions. It is easy to over-concentrate on one approach and dismiss alternative solutions; when in reality, the best protection against insider threat is a basic level of layered security-by-design endpoint protection paired with a combination of solutions that secure data according to its value, according to the principle of least privilege, and according to role-based access controls, as well as other technical controls, and that monitor personnel using bleeding-edge artificial intelligence, big data analytics, and solutions that automate cyber-hygiene and ensure verifiable accountability trails.

Non-Technical and Technical Controls

Recommendations

Utilize the Information Security Team

An information security team is vital to combating the insider threat epidemic. Josh Salmanson affirms, "Taking care of security from a comprehensive, multidisciplinary perspective is the best way to mitigate unintentional insider threats. Technologies like email sandboxing, SSL decryption solutions, ongoing packet capture solutions that allow for active hunting of events that preceded sensor discovery and persistent parallel NSM solutions provide a capable, but very expensive technical safety net. Technologies that assess behaviors and baseline user activities over time can be effective as well. Controls that assist mitigation have been well documented for some time. However, it's the willingness to do what is difficult and truly apply controls consistently across the respective enterprise. Today it is often easier or more likely affordable to apply controls seriously only to the most 'important systems.' The low-priority systems are often on the same network but because of age, criticality to operations/mission, availability/stability issues, they get waivers and limited compensatory controls. With this approach, the organization will feel good about its efforts but the low-priority systems end up/remain the easiest vector to compromise the 'important systems' and ultimately, the enterprise. You can't feel secure putting a steel door on a tent in bear country." The work of the information security team begins with a comprehensive risk analysis that identifies critical data assets, system vulnerabilities, risks according to the current threat landscape, and deficiencies in the organizational cybersecurity, cyber-hygiene training, or incident response plan. Without a risk assessment, the organization cannot make informed cybersecurity decisions.

It is important that the C-suite and senior management consult the information security team on cybersecurity decisions because the executives may not grasp the realistic view of the organization's cyber-posture in relation to the modern threat landscape. For instance, though a risk assessment might conclude that the impact of an insider threat is only moderate, trends in the threat landscape might indicate that the likelihood of repeated insider events is significant. This information could influence decisions about whether or not to invest in cybersecurity solutions and what solutions to implement. Further, the risk assessment should quantify cybersecurity risks such that the decision of whether or not to invest in prevention or mitigation solutions is directly correlated with the predicted likelihood or potential impact on organizational stakeholders.

Heed the Information Security Team

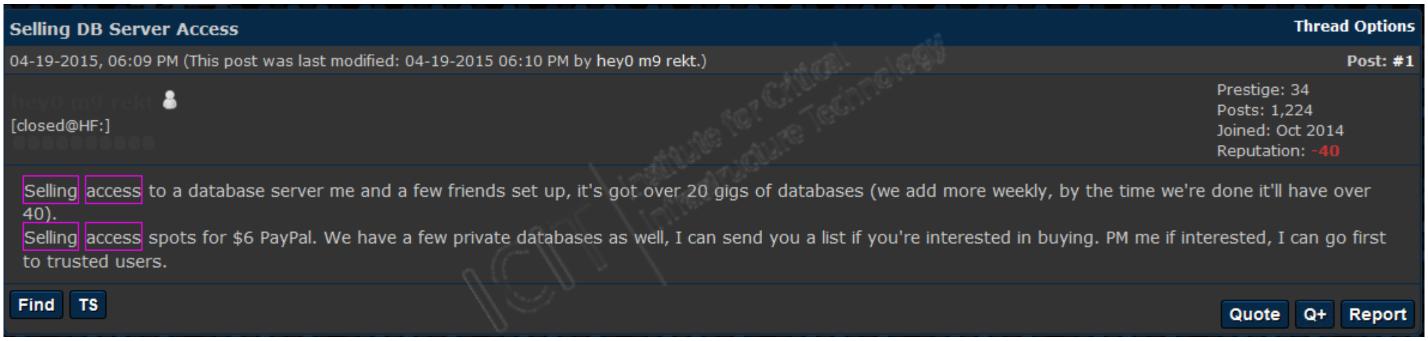
For many organizations, the most important step in deterring insider threats is to admit that insider threats exist in the first place. To combat insiders, the organization must recognize the threat and be willing to work with the information security team to mitigate the risk. Protenus' Robert Lord explains, "Leaders of organizations have a hard time accepting that their workforce might have internal bad actors while it's much easier for them to accept that bad actors exist outside of their institution. However, once an organization comes to terms with the reality of the situation - that bad actors exist both within and outside of the organization - it can implement the proper measures for keeping sensitive data safe." All too often, the policies, procedures, guidelines, and controls implemented by the information security team are only paid lip-service or are broadly interpreted. Admonitions urging employees to create complex passwords, recommendations to study policy documents, restrictions on BYOD devices, and other conveyed information are often neglected by staff and upper management alike. As a result, robust credentials are written down on easy to observe slips of paper within reach of sensitive systems, personal information is stored on employee devices, sensitive systems are connected to social media, valuable data are publically disclosed, or unknown individuals are granted access to restricted areas [6]. In most incidents, the non-technical and technical controls implemented by the information security team as a result of a comprehensive risk assessment would have precluded the compromise of critical systems or the exfiltration of sensitive data if personnel had only acted in accordance with the implemented controls.

Hire Trusted Personnel

The past behavior, activities, and actions of prospective personnel should be evaluated during the hiring process. Specific focus should be dedicated to the financial and emotional stability of the individual, any potential conflicts of interest, whether or not they were a responsible data steward in the past, and whether they can be trusted to manage information and sensitive systems. Applicants should not be naively categorized as "good" or "bad"; rather, they should be assessed based on their trustworthiness, decision-making capabilities, and their capacity to willfully misuse the privileges and access afforded to the position. Individuals who are prone to feeling mistreated, disrespected, or abused in the workplace could easily develop into insider threats [6].

Humanity's base motivators have not changed, despite the recent rise in technology and periodic changes in societal values. The same motivators used to blackmail and polarize critical infrastructure personnel during the Cold War (greed, sex, ideology, etc.) are just as powerful today, and the exploitable information is easier to obtain. In July 2015, a hacktivist group known as Impact Team stole the billing data from the Ashley Madison extramarital affair site and threatened to expose 37 million users' names, home addresses, search history, and credit card transaction records, unless the site was immediately shut down. Consumers were later embarrassed and exploited via the dumped data. At the time of the breach, it was speculated that the data had been stolen by a former employee or contractor or by an external adversary using that contractor's credentials [23] [24]. Speculation of attribution of the incident later diverted. Nevertheless, it is worthwhile to consider how the cybersecurity lessons learned from the Ashley Madison breach could be applied across critical infrastructure. For one, the incident was allegedly in protest of the unnecessary retention of stores of consumer data. More importantly, the publicity of the incident narrowly introduced the dialogue about how vital personnel could be denigrated or blackmailed as a result of their personal activities.

Figure 9: HackForums Database Sale



Selling DB Server Access

04-19-2015, 06:09 PM (This post was last modified: 04-19-2015 06:10 PM by hey0 m9 rekt.)

Post: #1

hey0 m9 rekt

[closed@HF:]

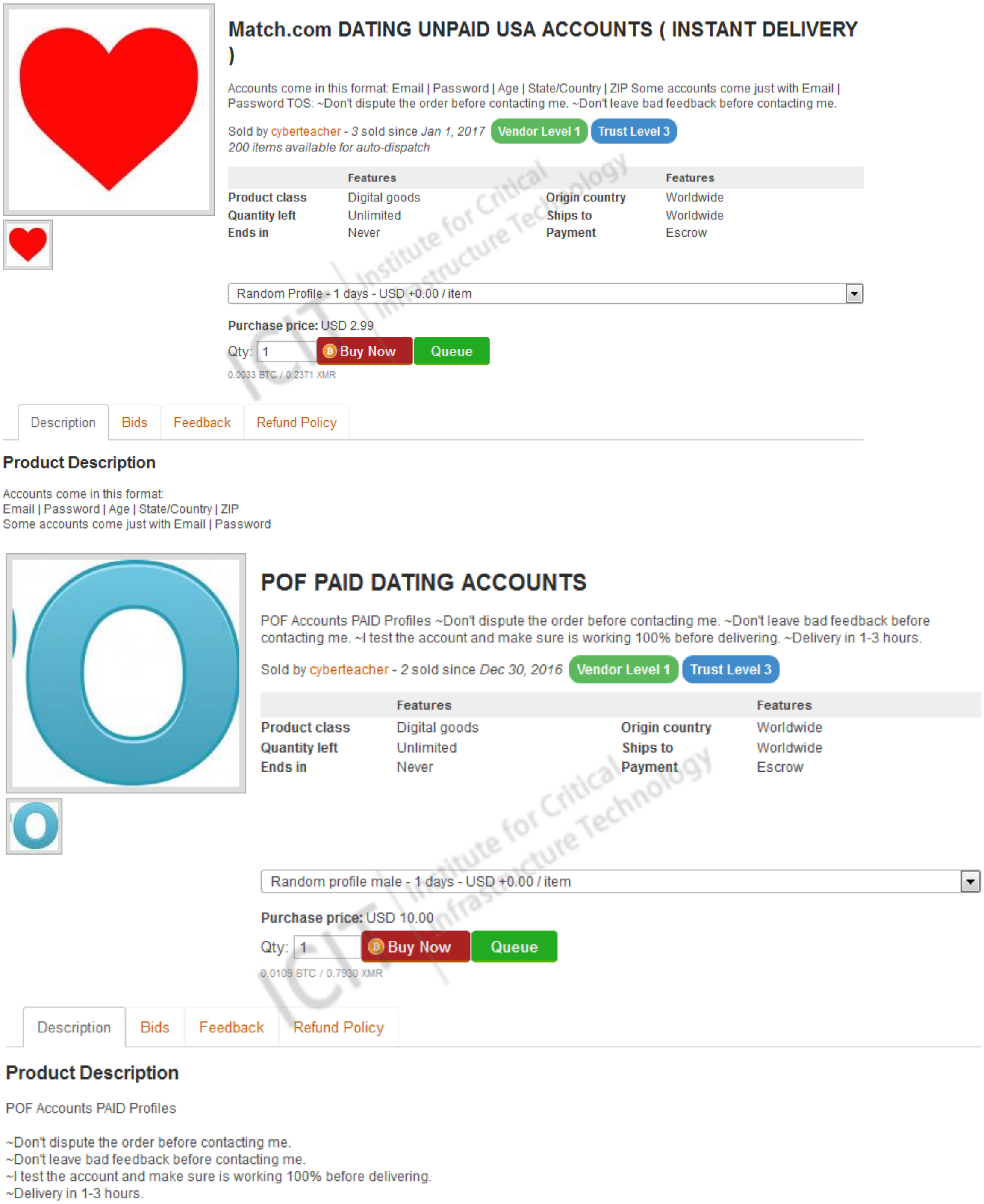
Prestige: 34
Posts: 1,224
Joined: Oct 2014
Reputation: -40

Selling access to a database server me and a few friends set up, it's got over 20 gigs of databases (we add more weekly, by the time we're done it'll have over 40).
Selling access spots for $6 PayPal. We have a few private databases as well, I can send you a list if you're interested in buying. PM me if interested, I can go first to trusted users.

Script kiddies on HackForums sell access to resources such as low-level databases

Ashley Madison is not the only service that has been breached. In 2015, AdultFriendFinder was breached by different adversaries. In both instances, consumers were targeted. In the former case, the Impact Team combed through the data for high profile names to threaten to expose prior to dumping the entire database. In the latter case, Andrew Auernheimer, a controversial computer hacker, publicly identify AdultFriendFinder customers, including a Washington police academy commander, an FAA employee, a California state tax worker and a naval intelligence officer, on Twitter, stating "I went straight for government employees because they seem the easiest to shame" [25]. How many of those exposed in either incident would have been willing to plug a malicious USB into a work computer rather than suffer the embarrassment and potential marital repercussions of exposure? How many would exfiltrate files to mitigate blackmail?

Figure 10: Deepweb Hacker for Hire



Match.com DATING UNPAID USA ACCOUNTS (INSTANT DELIVERY)

Accounts come in this format: Email | Password | Age | State/Country | ZIP Some accounts come just with Email | Password TOS: ~Don't dispute the order before contacting me. ~Don't leave bad feedback before contacting me.

Sold by cyberteacher - *3* sold since *Jan 1, 2017* Vendor Level 1 Trust Level 3
200 items available for auto-dispatch

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Random Profile - 1 days - USD +0.00 / item

Purchase price: USD 2.99

Qty: 1 Buy Now Queue
0.0033 BTC / 0.2371 XMR

Product Description

Accounts come in this format:
Email | Password | Age | State/Country | ZIP
Some accounts come just with Email | Password

POF PAID DATING ACCOUNTS

POF Accounts PAID Profiles ~Don't dispute the order before contacting me. ~Don't leave bad feedback before contacting me. ~I test the account and make sure is working 100% before delivering. ~Delivery in 1-3 hours.

Sold by cyberteacher - *2* sold since *Dec 30, 2016* Vendor Level 1 Trust Level 3

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Random profile male - 1 days - USD +0.00 / item

Purchase price: USD 10.00

Qty: 1 Buy Now Queue
0.0109 BTC / 0.7930 XMR

Product Description

POF Accounts PAID Profiles

~Don't dispute the order before contacting me.
~Don't leave bad feedback before contacting me.
~I test the account and make sure is working 100% before delivering.
~Delivery in 1-3 hours.

Figure 10 captures the sale of Match.com and Plenty of Fish dating website databases. Users of these services often fear exposure or repercussions and can consequently be exploited. Additionally, some user could be identified as critical infrastructure personnel and could be targeted.

According to stereotypes, technical personnel and especially those in critical infrastructure may not be the most extroverted individuals. Even if they have no qualms about interacting with people, they may not have much free time outside of work. As a result, many may use dating applications to form introductory relationships. While not as compromising as the aforementioned cases, consider that an external attacker could cross reference LinkedIn, Facebook, public records, or a custom-built database of government personnel with a database exfiltrated from a dating site in order to "catfish" or manipulate a critical infrastructure employee into acting as an insider threat. Obviously, organizations cannot regulate the personal lives of their staff, but critical infrastructure entities may benefit from considering possible insider polarization vectors when reviewing potential applications.

Cultivate a Culture of Trust

Ultimately, an organization is comprised of its personnel and systems, and its security is only as reliable as its most vulnerable liability. Without a culture of trust and employees' personal investment in the security of the organization, critical infrastructure organizations are breeding pools for insider threats. After personnel are screened, the onboarding process should equip new hires with the knowledge and skills necessary to perform their role. A culture of shared values, ethical behavior, and honesty should be ubiquitous throughout the organization. If the C-suite or senior management do not subscribe to the culture or adhere to policies and controls, then the lower level personnel are not likely to buy-in. Expectations of trustworthy behavior, cyber-hygiene, cybersecurity practices, organizational policies, and a definitive chain of command, should all be succinctly and clearly conveyed. Similarly, conditions and consequences of non-compliance should be made explicit from the outset. Personnel should be periodically reminded of these expectations and consequences. Mutual trust and clear communication should remain a priority within the workplace; though a healthy dose of skepticism and paranoia is necessary for personnel to remain vigilant to the threat posed by insiders. Employees should have clear and effortless mechanisms for anonymously reporting suspicious behavior in the workplace. Employees' trust and vigilance should be factored into their periodic performance reviews. Reports or allegations of insider activity should be thoroughly investigated before conclusive action is taken [6]. In order to mitigate negative culture, some solutions anonymize data until anomalous activity is detected; afterward, only a restricted set of individuals (usually the insider threat team and select members of management, HR, and legal) have access to the identity of the monitored threat [2].

Effectively Communicate

Without the clear and concise communication of cybersecurity and cyber-hygiene expectations and implemented policies, undertrained personnel will inevitably develop into malicious and non-malicious insider threat actors. Effective policies are actionable, are enforceable, and are regularly updated.

Users should be trained to detect suspicious insider activity and they should have access to a clear reporting mechanism and should know a clear chain-of-command. Additionally, in order to prevent insider radicalization due to perceived personal bias or chilling effects, personnel should be informed of exactly what privacy rights they retain in the workplace, and they should repeatedly be reminded (training, signs, login screens, etc.) of how their work activities are monitored. David McNeely of Centrify emphasizes, “Organizations should always explain their right to monitor security policies and user access to organizational data and computing systems, and users should not have an expectation of privacy when using these computer systems since it is not a personal device or computer. I do believe that users with a company owned laptop tend to use it for much of their own personal work and co-mingle the data. However that should not be allowed and users should be encouraged to acquire their own computers just like they have done with their mobile devices.” Informed employees who perceive corporate transparency will not be subject to a chilling effect that could otherwise impact their performance. This transparency empowers the organization to enlist employees in the defense of data assets and critical infrastructure systems [2].

While this information could enable a malicious insider to attempt to bypass controls, the goal of informing trusted personnel is to deter and prevent their radicalization into insider threats in the first place (keep good people good). Insider threat policies should be actionable enough to deter or hinder insider threats and technical controls should be sophisticated enough to detect malicious insiders despite their attempts to obfuscate their activities.

Appreciate Personnel

Save nation-state insiders, premeditated cybercriminals, and self-radicalized lone-wolf activists, critical infrastructure insider threats are developed over years of perceived mistreatment, frustration, and miscommunication. Public sector personnel do not make the same salaries as their private sector counterparts, and may consequently be more susceptible to temptations to act as an insider. Taking measures to ensure the fair treatment of personnel, to secure them fair and reasonable salaries and benefits (relative to the sector and economy), and the promotion of an amicable internal organizational culture are extremely cost-effective mechanisms for preventing, deterring, and detecting insider threats.

Train Personnel to Defend the Organization

Even the strongest layered cyber-defense cannot effectively protect critical infrastructure systems and data if it is perpetually undermined by non-malicious insider threats [26]. Igor Baikalov of Securonix remarks that, “Information security awareness training can go a long way towards preventing unintentional insider incidents. Reasonable (business-wise) and enforceable (security-wise) access control and data protection policies can further reduce risky behavior. Employee satisfaction and management awareness are the most underutilized non-technical controls in preventing Insider Threat." No matter how many pamphlets and lectures employees receive or how many meetings and seminars they endure, cyber-security awareness and training and fundamental cyber-hygiene does not seem to improve. If there is even one employee, out of tens or thousands, who does not pay attention and who later opens a malicious email, then the organization has failed to secure its data and systems. Many ignore security training because either the training lacks personal engagement or because a personal connection to the instructor forestalls absorption of the material. Consider the difficulty in conveying actionable information to massive groups of people or to individuals who share a working relationship. How many employees might be comfortable dictating policies and regulations to their boss? In order for targets to retain any amount of training, upper management must also receive the training and more importantly, they must lead by example and be subject to the same policies, procedures, and technical controls as lower level personnel. Ivory-tower management, which ignores controls or that demands asymmetric compliance, breeds resentment within the organization. Worse, they signal to others that subjection to technical and non-technical controls is relative or voluntary. A dedicated information security team, which is trained to teach personnel, or external instructors may be worthwhile investments to increase policy compliance rates and to decrease insider threat. At random periodic intervals after instruction, retention tests should be administered to staff to ensure that the staff remains vigilant and aware of their security responsibilities within the organization. Those who fail should be subject to repeat instruction or eventually more stringent consequences. If everyone except insider threats adhere to compliance regulations, policies, and procedures, then technical solutions will have a significantly greater chance of detecting or preventing insider threats before damage is realized.

Security rules are often perceived as cumbersome and excessive barriers that waste time or elevate frustrations. Lack of incentives to attend security training or to retain knowledge leads to depreciating cyber-hygiene and increasing malicious and non-malicious insider threat rates. Don MacLean from DLT contends, "Many technologies are available for this purpose, but in many cases are seen as perimeter defenses rather than safeguards against insider threats. Many security professionals tout the value of user training, but training is rarely effective. Users take it too infrequently, and the training itself is often trivial, even silly. It is undoubtedly helpful to train users to identify phishing and spam e-mails, but far more preferable to block such messages before they arrive at an in-box. Since phishing attacks change constantly, safeguards against them must follow suit. Machine learning systems can adapt quickly and automatically, so mail gateways that use machine learning are important ways to block such attacks. “Delivering effective, behavior-changing training can be difficult because staff has difficulty conceptualizing cybersecurity situations and internalizing training. Conventional cybersecurity training provides knowledge, but it does not teach the actual skills necessary to defend the organization [27]. Experience-based training, such as gamification, simulates realistic high-stakes, offensive and defensive cybersecurity situations that encourage active engagement and the long-term retention of cybersecurity training and awareness. Gamification incorporates gaming and entertainment mechanics to illicit user engagement while addressing non-gaming situations [28]. Gaming concepts are employed to break complex cybersecurity concepts and tasks into digestible lessons and to motivate personnel to collectively, collaboratively, and creatively approach realistic and dynamic challenges based on the modern hyper-evolving threat landscape [29].

Gamification can help participants become more cognizant of adversarial tools, tactics, and procedures as well as imparting proper incident response. It transforms the learning experience into a rewarding and engaging process. Gamification can be used to make cybersecurity seem interesting; it can even be used to draw in fresh talent to fill the estimated 1.5 million vacancies by 2020. Insider threat games incentivize cyber-hygienic behavior and militarize the workforce to identify and report non-conformist behaviors. Users may accumulate points by adhering to security practices or by mitigating threats. Competition between participants increases engagement. If nothing else, gamification teaches staff to care about the consequences of a cybersecurity incident, to recognize an insider threat, and to discover vulnerabilities, in a low-risk, high-reward environment [29].

Policies Procedures and Guidelines

Travis Farral from Anomali contends that “There are a few key things that any organization can do that would really help limit the impact of insider threats: Restrict administrative access as much as possible, limit access to crucial internal data and log access to it, and ensure that users only have access to the data they need and in the way they need. If users only need to view certain data, then restrict them to read-only access to it. These efforts may not prevent employees from developing into insider threats, but they will limit what harm insiders have the ability to do to the organization.” Ultimately, controlling the reach of potential insiders amounts to restricting privilege and access to the least necessary for the individual’s role in the organization.

Principle of Least Privilege

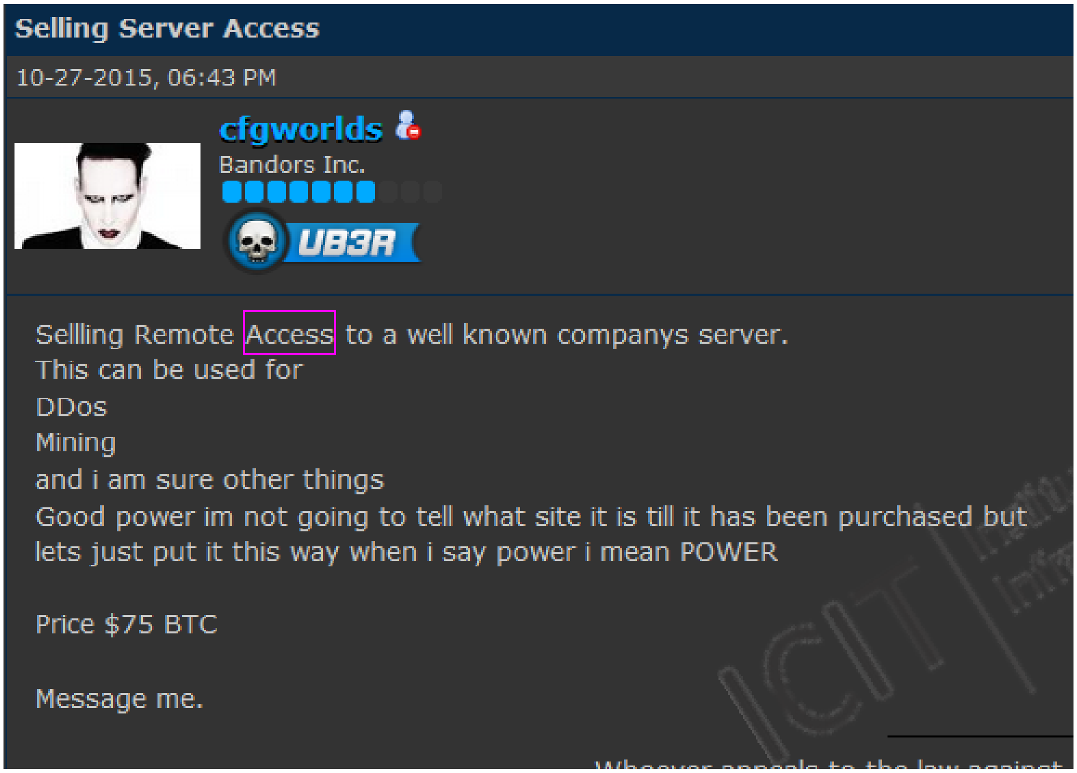
Critical assets may be servers containing personally identifiable information (PII), electronic health records (EHR), financial records, intellectual property, etc. or they could be vital services such as email, payroll, networked device control panels, etc. Personnel should only be assigned the least privileges necessary to fulfill their role in the organization. Privileges are often misallocated when network administrators create group or role-based accounts that automatically assign permissions, without evaluating whether the individual's role necessitates those privileges. These privileges should be periodically reassessed to ensure that roles and needs have not changed and to ensure that privileges are revoked from users who no longer perform the specified roles in the organization. 48 percent of US respondents to SailPoint's 2016 Market Pulse Survey indicated that they retained access to corporate accounts after termination [30]. Periodic audits of the access rights and privileges of random batches of users can help to ensure that no rogue accounts exist, to verify that an insider has not escalated their rights, and to decrease the likelihood that an external adversary establishes a persistent network presence via an artificial account.

Limit Access According to Duties

Critical assets can be best protected by minimizing the number of people with access to personnel who require access in order to fulfill their role in the organization. Even if a position requires access to a critical asset, it may not require access to all the data contained within that asset. For instance, a human resources employee should not be able to access or alter their own file or those of a relation, nor should they have access to any files outside of their assigned caseload.

These is a growing trend in IT sectors to allow personnel to access critical systems and data assets from home on their personal computers. These BYOD solutions save the organization money be reducing operational costs, they are more convenient for personnel, and they are believed to decrease personnel's resentment of their jobs. Contrary to this trend, reducing the likelihood of insider threat necessitates limiting remote access to systems and data assets to only essential roles.

Figure 11: HackForums Sale of Remote Access



Selling Server Access

10-27-2015, 06:43 PM

cfgworlds

Bandors Inc.

Sellling Remote Access to a well known companys server.
This can be used for
DDos
Mining
and i am sure other things
Good power im not going to tell what site it is till it has been purchased but
lets just put it this way when i say power i mean POWER

Price $75 BTC

Message me.

Whoever appeals to the law against

Insider threats can sell or exploit remote access . As a result, only trusted personnel should be granted the privilege according to necessity.

The compromise between these two corporate strategies is to award personnel who have proven their trust over an extended period of time with the option to work from home via a secure remote access application. However, organizations choosing this strategy should remember that any remote access can be exploited by cyber-adversaries and take the appropriate steps mitigate this risk.

Segregate Administrative Duties Based on Role

Administrative duties should be separated so that one individual does not have control over an entire process. For example, an employee should not be able to request, authorize, process, and receive payment for a product or service. Control over the entire business chain can tempt a typical employee into becoming an insider threat out of convenience, greed, or privilege. In terms of cybersecurity, not every system administrator needs to have the highest level of permissions nor should they have wholesale access to any data or system on the network. Segmenting administrative duties limits the potential lateral movement of insider threats. For example, a system administrator with access and permissions pertaining to an employee payroll database may not have permission to manipulate, or exfiltrate data, or they may lack the ability to access the performance records associated with the employees in the payroll database.

Address Cybersecurity in Service Level Agreements (SLAs)

Conventional cyber-hygiene, technical, and non-technical controls no longer guarantee the prevention, detection, or deterrence of insider threats prior to compromise. Consider that the NSA relies on some of the most evolved technologies and strict policies to protect national security; yet, even they have repeatedly suffered from insider threats over the past few years. One recent instance of a mismanaged third-party insider threat was Harold Martin, the 51 year-old Booz Allen Hamilton employee who was caught stealing classified documents from the NSA in 2016. Martin claims to have taken the data so that he could work at home in the evenings. There was no indication that Martin intended to exchange any of the information that he obtained; yet, the loss of data while in his stewardship could have compromised national security [31]. Service level agreements, clear communication, and a definitive chain of command can inform third parties and thereby prevent them from unintentionally acting as insider threats within the organization.

In 2015, one in three organizations were not cognizant of the current third-party access policies or contracts and 77% of information security professionals did not update third-party agreements or address third-party cyber-hygiene and system access in response to the hyper evolving cyber-threat landscape [32]. As a result, there were limited controls requiring third-parties to secure data and systems to the same degree as the organization. Travis Farral of Anomali adds, “Restricting access to only what is required for third-party organizations to deliver their service is an important step to take to help mitigate harm from insider threats. Logging and monitoring all activity by these providers is another important step to take. Limiting the data that is shared with or that third-parties have access to is also important. Lastly, ensuring that as part of contract negotiations, third-parties must have their own comprehensive internal threat programs in place is a further measure that could be taken.” Addressing cybersecurity in the service level agreement can ensure that critical infrastructure organizations are not victimized by internal or external threat actors at third-party organizations and that third-party contractors adhere to organizational cybersecurity non-technical and technical controls.

Purchase Consumer-Off-the-Shelf (COTS) Solutions from Reputable Vendors

Proprietary systems developed by critical infrastructure organizations are all-too-often rushed, inefficient, and costly systems that sacrifice security in favor of convenience. Government certified consumer-off-the-shelf (COTS) products from reputable vendors can be implemented in accordance with the financial and talent constraints experienced by critical infrastructure organizations. Layering COTS solutions that adhere to NSA’s Commercial Solutions for Classified (CSfC) program can be especially effective at securing critical infrastructure while bypassing the endless stream of silver-bullet vendor solutions [33].

Technical Controls

Up until the mid 2000s, cybersecurity-focused only on protecting the network perimeter using firewalls, signature-based antivirus, and similar antiquated solutions. The rise of advanced persistent threats necessitated the protection of internal systems, through signature based and network anomaly based defenses such as host antivirus, application log analysis, IPS/IDS, etc. Now, big data analytics (baseline, demographic, and psychographic), behavioral analysis, continuous monitoring, and other controls are necessary to defend enterprise networks from a variety of internal and external threats.

Data Encryption

Data should be protected according to its value and the potential harm that would result if it were stolen. Encryption does not prevent adversaries or insiders from exfiltrating data; however, it does deter or prevent the attacker from exploiting the stolen data unless they spend significant additional resources breaking the encryption or stealing the decryption keys. There are numerous encryption algorithms, methodologies, and applications. Field-level encryption (FLE) and format-preserving encryption (FPE) can mitigate the potential impact of data exfiltration by internal or external adversaries. Field-level encryption, the ability to encrypt data in specific fields, is often applied to PII, PHI, and other sensitive data [34]. The impact of the OPM breach may have been mitigated if field-level encryption had been implemented on the Frankensteined legacy systems. Format-preserving encryption can be used to encrypt data such that the format or structure of the data remains unaltered. The format of the ciphertext is the same as that of the plaintext. Consequently, FPE can be applied to legacy application frameworks that were previously thought to be unable to support encryption. FPE can also be applied to virtually any data type. FPE also preserves referential integrity and ensures consistency across applications [35].

Network and Security Segmentation

Network segmentation is the practice of dividing a network into smaller partitions, called subnets, in order to isolate critical assets from one another and to control access to sensitive data. Networks can be logically segmented via private Virtual Local Area Networks (VLANs), which restrict communication between hosts on different subnets, in addition to being physically segregated via air-gaps. Logical segmentation involves the institution of conditional rules to determine which devices are allowed to communicate with each other. Various tools and systems are deployed to guard the gateway of each subnet, specifically to coordinate traffic flow, to filter content, to control access, and to manage connections.

Just because information can be passed between two entities does not mean that it should pass between those entities. Layered security segmentation focuses on whether applications, systems, and users should be allowed to communicate. The approach minimizes unauthorized communication and minimizes the possible harm an attacker can inflict by creating least access compartments around application tiers, apps, environments, etc. Security segmentation occurs in the data center or cloud via layers of segmentation access-control rules. The strategy should consider whether or not the organization is the primary or sole custodian of the critical data, and upon whose networks its operations or data processes run. There are four basic segmentation layer categories. User-segmentation divides according to users, groups, and entitlements. Course segmentation determines access according to environment, geo-location, zone, etc. Micro-segmentation occurs at the application layer and can be used to control communication of applications, virtual systems, and physical systems. Finally, nano-segmentation regulates information flow according to port or protocol, process, and data container [47].

Predictive Artificial Intelligence

Detecting insider threat hinges on detecting anomalous behavior and preventing the compromise of critical systems or data containers. Even with massive information collection and big data analysis, this process can be time-consuming and can lead to too many false positives for conclusive action [36]. Outdated insider threat protection paradigms are centered around the protection of endpoints. This model is no longer realistic of the modern threat landscape because insider threats are often used to introduce new malware variants onto critical infrastructure networks. Without heuristics or signatures, most endpoint security fails to detect the malware and prevent the compromise. Michael Seguinot from Exabeam explains, “Machine-learning algorithms can process the flood of activity data dramatically faster than any human analyst. As a result, algorithms can amplify the abilities of human analysts, notifying them of developing threats and providing the context needed to respond effectively.” Predictive artificial intelligence based malware protection that leverages machine learning can protect endpoints from malware introduced directly by malicious insiders or inadvertently by non-malicious insiders. AI endpoint security can prevent systems compromise, and it can frustrate adversarial efforts long enough to allow the information security team to trace the event and apprehend the insider threat [36]. It can also prevent insiders from escalating privileges, planting logic bombs, exploiting 0-days, or executing unwanted programs [37]. By securing the endpoint from malware despite the lack of a signature, the organization can prevent insider threats from implementing the digital mechanism to collect or exfiltrate data. In the meantime, the adversary will be detected and the information security team can investigate the event, collect attribution indicators, and remove the threat actor.

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) solutions condense the event data from potentially thousands of devices and applications down to a small number of actionable alerts that signal vulnerabilities, risks, and anomalous behavior that could be attributed to insider threats [38]. SIEM solutions provide a layered centric or heterogeneous holistic view into infrastructures, workflows, and compliance and log management in the form of dashboards or "views" [39]. Dashboard tools significantly reduce event response time and allow organizations to better detect, prevent, and minimize the damage caused by an insider [2]. SIEM systems store, analyze, and correlate application security information and event data (authentication, anti-virus, audit, intrusion, etc.) [38]. These dashboards provide a streamlined and accelerated detection process by aggregating, prioritizing, and visualizing high-risk insider and cyber threat indicators from across all users, accounts, hosts, and enterprise endpoints [2]. Anomalous activities are detected by rules that alert the information security team of suspicious behaviors or that fully-automate responses based on predetermined conditions. SIEMs can be used to collect and centralize the event and log data across enterprise applications. SIEM systems aggregate logs from user devices, network switches, servers, firewalls, anti-virus software, intrusion detection/prevention systems, and from SNMP traps, or Syslogs [38]. SIEM provides automated verification of continuous monitoring, trends, and auditing in order to show value to executives. SIEM normalizes data as a two-part function, that includes translating jargon to readable data to be displayed and visualized to user or vendor defined classifications and characterizations (field mapping). Data are given context and form relationships based on rules, architecture, and alerts, in order to provide historical or real-time correlations [39]. SIEM alerts are pre-configured with default/ prepackaged rules or are custom tailored to reflect the security policies and a profile of the system under normal event conditions [38]. Finally, SIEMs are adaptable and scalable regardless of data source, application vendor, format, type, changes, or compliance requirements [39]. An insider threat SIEM signature can be used to detect the identity of potential insider threats based on suspicious activity, remote connection protocols, time of activity (i.e. whether it is during work hours), and other context-based rules [40]. SIEM solutions are not fool-proof for detecting insider threats, but they are a good starting point for insider threat detection and mitigation programs. Michael Crouse from Forcepoint warns "Least invasive tools including log analysis technologies like SIEM's, do not attribute information to a specific user; information to a machine, IP Address, etc.; This checks the box but does not provide the context required to truly identify the risk."

User and Entity Behavioral Analytics (UEBA)

According to Igor Baikalov from Securonix, "User and Entity Behavior Analytics (UEBA) is the most effective technology to deal with Insider Threat. It analyzes data from traditional protective controls such as Identity and Access Management (IAM), High-Privilege Account (HPA) monitoring, and Data Loss Prevention (DLP); security events like VPN logins, Windows Events, and Web proxies; as well as meta-data from HR and enterprise inventory systems to identify meaningful deviations from normal business activities. It can detect malicious activities of both insiders and also outsiders with hijacked credentials who masquerade as insiders."

User and entity behavioral analytics (UEBA) solutions audit and analyze the file and application access of an individual in order to detect and connect disparate data points that could indicate suspicious user or application behavior. The information security team establishes a baseline of user activity (file access, logins, network activity, etc.) over a predetermined period of time and then uses that baseline to rapidly detect any time the user deviates from that norm and to alert the information security team. UEBA solutions collect data from files, emails, IT resources, and other data streams without constraints on volume variety, or velocity of data. In many cases, the solution is able to assess the data and generate alerts in near real-time [38]. Some UEBA solutions pair the baseline with sector trend data and industry specific concerns in order to assign each data subject a dynamic "trust credit score". This variant of UEBA is proactive and predictive in addition to being protective. If the user's behavior ever deviates from the baseline, then the score indicates whether or not the system adds them to a watch list. The system institutes multiple levels of approval whenever a person on the list attempts to access new systems or data [2]. The user activity can be monitored cross-departmentally, with relevant investigators from the information security, legal, and human resources departments. Additionally, legal advisors can work with the information security team to ensure that UEBA does not infringe on the expectations of privacy set by the organization while also tailoring it to detect corporate adherence to policies [2].

In this manner, UEBA can detect when a trusted employee has developed into a malicious insider threat by detecting subtle changes in activity and behavior. Additionally, it can also be used to detect when an external attacker has stolen legitimate credentials by tricking an employee into acting as a non-malicious insider. UEBA excels at spotting variances in user activity and at handling unknown instances. For example, UEBA can be used to automatically detect if a user deletes thousands of files in a short amount of time if a user starts visiting unusual directories if they start accessing applications that are not specific to their role, etc. [38].

Virtual Infrastructure

Virtual Desktop Infrastructure (VDI) environments circumvent some of the risks of insider threats through a distributed data environment in which the user interacts via a local application on their PC, but all data is stored on remote servers. As such, potential insider threats do not have the ability to download and exfiltrate data. System administrators can focus on securing and managing a few servers and users can be responsible for their own PCs. VDI solutions are not without costs or risks. User PCs can still be lost or stolen. VDI solutions are often out of the reach of small and medium businesses because server software licenses cause VDI environments to cost twice as much as PC environments [41].

Though less secure, file server solutions are cost effective alternatives to VDIs. In this solution, all corporate data is stored on a centralized file server that is secured and managed by the system administrator, who controls access, monitors activity logs, and implements encryption. Users are restricted from transferring files outside the file server, and all activities are executed on the server. Digital rights management (DRM) features such as watermarks, or print prohibition controls can be used to detect, prevent, or trace data leaks. Backup servers are used to mitigate the risk of data loss due to an insider or an external adversary. Ransomware and similar attacks are mitigated through the use of whitelisted corporate applications [41].

Psychographics for Cloud Services

Cloud services vastly expand the scope and potential of insider threats by facilitating data leakage and exfiltration by remote users. Data leakage can occur as employees complete typical daily actions, such as downloading data. Meanwhile, immature auditing and governance controls relative to the estimated 9000 on-premise cloud applications have led to a broad range of internal and external attack vectors. The threat landscape is expanded because many organizations rely on cloud providers to protect critical infrastructure data from all external threats and insider threats within both the owner organization and within the cloud provider [4].

Organizations can leverage psychographic big data analytics of cloud traffic in order to detect and deter insider threats. Unlike general big data analytics, the psychographic machine learning and big data analysis of cloud traffic does not require data correlation across multiple sources. The process therefore requires fewer resources, less time, and less data source integration [4].

Identity and Access Management (IAM)

The security of an organization is dependent on the security of the identities of its personnel. The Verizon 2016 Data Breach Investigations Report found that 63% of data breaches involved weak, default, or stolen credentials [42]. Further, without a centralized solution that manages user identities across systems and applications, insider threats may shirk some legal liability by claiming that their credentials were stolen by an external adversary and that they are therefore not responsible for any suspicious activity detected by the information security team. Identity and access management (IAM) solutions centrally manage the provisioning and de-provisioning of identities, access, and privileges, and they manage the authentication and authorization of individual users within or across system and enterprise boundaries. IAM solutions greatly reduce the frustration and burden on individuals by automating cyber-hygiene. Without IAM, many users are inundated by the surplus of software-as-a-service credentials and privileged accounts credentials that they must remember daily. As a result, many users write down sensitive credentials or reuse credentials. This information can easily be stolen and abused by insider threats.

Effective cyber-hygiene hinges on each employee responsibly responding to every threat emerging from the hyper-evolving threat landscape. Personnel often find cyber-hygiene is daunting, exhausting, and distracting; meanwhile, cybersecurity awareness and training is often limited and the demanding responsibilities of personnel preclude their interest or ability to shore up their cyber-hygiene and their awareness of cybersecurity best practices [43].

Michael Seguinot from Exabeam notes, "Insider threats occur because organizations are not able to detect them. This is due to a combination of product problems (legacy security products are terrible at detecting threats that use credentials) and people problems (staffing shortages result in junior analysts that are unable to make sense of the attacks as they develop). Behavioral Analytics Automation is the best solution to augment both products and people in this scenario." Cyber-fatigue can be reduced through IAM components such as secure single sign-on (SSO), which manages credentials across multiple applications, and removes the tedious and repetitive aspects of cybersecurity. IAM can also be used to automate the implementation of certain policies such as the application of the principles of least-privilege and least-access across the network [44]. In 2015, privilege misuse (malicious insider activity) accounted for as much as 16% of observed incidents, while the unauthorized disclosure of information (non-malicious insider activity) accounted for 18% of all incidents [42]. Privileged Identity Management (PIM) solutions are a component of IAM through which user privileges and access rights are initiated at minimal values and are readjusted on a necessity-basis according to the current role of the user within the organization. PIM solutions enable the information security team to tailor access and privileges for internal personnel, outsourced/ third-party users, and for shared accounts across hybrid infrastructure.

Identity and Access Management solutions are critical to the protection of the Identity perimeter across mobile and cloud infrastructures. Multi-factor authentication (MFA) can be used to validate user identities through a combination of user knowledge (such as a username, password, PIN, security question response, etc.); a user possession (such as a smartphone, smart card, token, one-time passcode, etc.); and information characteristic of the user (biometrics, retina scans, voice recognition, gait analysis, etc.) [43]. IAM components such as

Multi-Factor Authentication (MFA), establish an accountability chain and prevent an insider threat from denying culpability if detected.

Data Loss Prevention (DLP)

Data loss prevention is the employment of reliable vendor tools to secure data when it is in transit, when it is at rest, and when it resides at endpoints. DLP often includes keyboard filtering, USB port access control, network transfer monitoring, field level encryption, and other mechanisms to deter internal and external threat actors [45] [41].

User Activity Monitoring (UAM)

Data loss prevention alone and other conventional tools that regulate the exchange of network data are insufficient to stymie the rising tide of insider threats because the tools were not designed for that purpose. The bottom line is that if an insider knows how DLP is implemented, they can likely discover a mechanism to bypass it. When layered, DLP tools form an effective security barrier, but dedicated insiders will still find a way to circumvent the controls because the amalgamated solution is operating outside the purpose and scope of the DLP controls. For example, when an organization relies solely on DLP to restrict document sharing, critical information may be leaked in even riskier ways. Worse, the forced implementation of misappropriated controls may entirely obstruct mission-critical operations. User activity monitoring (UAM) enables organizations to mitigate insider threats while maintaining business continuity, by recognizing the needs of the user, the security of the organization, and the crux of the insider threat problem.

UAM is user-centric rather than data-centric. UAM does not limit or reject any action; instead, user behavior is monitored and suspicious trends are extracted for case-by-case analysis. UAM is not a log aggregation platform, and it is not a data loss and spillage prevention tool. According to the Committee on National Security Systems Directive (CNSSD) 504, it is “The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing US Government information in order to detect insider threats and to support authorized investigations.” Minimal capabilities include keystroke monitoring, screen captures, full application content capture (email, chat, data ingress/egress, etc.), file shadowing, specific user activity attribution, an analysis system, and support for investigative requests, collection based triggers identified through psychographic data analytics or determined by policy, and the long-term retention of data (5 years). UAM can be integrated into existing architectures, its output can be fed into 3rd party enterprise tools such as ePO and various SIEMs, and it can integrate records such as facility access data, communication data, personnel and security records, financial, travel, community shared data, and other external sources to better detect insider threats. UAM security controls are hardened against sophisticated or privileged insider threats and captures immutable audit records of every action taken by operators and administrators so that analysts can be audited as well as data subjects, in order to establish a clear chain of custody. UAM balances security, privacy, and legal compliance through "Do Not Collect" policies that enable organizations to specify that certain communications should be handled differently. Role-based controls protect personal privacies, and built-in rules can exclude specific PII such as bank account information, social security numbers, credit card data, etc. UAM allows operators to specify what should be in the audit record through simple if/then statements. Typical audits record timestamps, usernames, workstation, devices accessed, files accessed, correspondence exchanged, etc. and typically audited activities include accessing sensitive data, writing files to removable media, etc. Overall, UAM erases insider threat attribution ambiguity and reduces the complexity of cyber-forensic investigations by capturing user activities in real-time, across all channels governed by policies, and on all endpoints (including those offline, via an encrypted, hidden partition).

Conclusion

Insider threats begin with trusted employees whose frustration, resentment, apathy, lack of cybersecurity training and awareness, or external motivations radicalize them to unintentionally or willfully inflict harm on the organization by compromising systems, assisting external cyber-threat actors in multi-vector information warfare, or exfiltrating treasure troves of valuable PII, PHI, and other sensitive data. Perimeter-based defenses cannot stop the threats who are already inside the network. Bleeding-edge defense-grade insider threat solutions, such as User Behavioral Analytics (UEBA), Identity and Access Management (IAM), Virtualization, and User Activity Monitoring (UAM), are necessary to detect, deter, and mitigate the mounting insider threat epidemic against critical infrastructure.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Sources:

[1] "IBM 2015 Cyber security intelligence index," 2015. [Online]. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03278USEN&attachment=SEJ03278USEN.PDF&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US. Accessed: Jan. 30, 2017.

[2] R. Rose, "The future of insider threats," in *Forbes*, Forbes, 2016. [Online]. Available: http://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#6f5e96cc6726. Accessed: Jan. 30, 2017.

[3] "Managing the insider threat: Improving Trustworthiness -ISF briefing paper - information security forum," in *Information Security Forum*, Information Security Forum, 2015. [Online]. Available: https://www.securityforum.org/research/managing-the-insf-briefing-paper/. Accessed: Jan. 23, 2017.

[4] K. Narayan, "5 devious instances of insider threat in the cloud | Skyhigh," Skyhigh, 2015. [Online]. Available: https://www.skyhighnetworks.com/cloud-security-blog/5-devious-instances-insider-threat-cloud/. Accessed: Jan. 20, 2017.

[5] P. Reidy, "Combating the Insider Threat at the FBI: Real World Lessons Learned," in *BlackHat*, 2013. [Online]. Available: https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf. Accessed: Jan. 20, 2017.

[6] S. Durbin, "Insiders are today's biggest security threat," Recode, 2016. [Online]. Available: http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin. Accessed: Jan. 22, 2017.

[7] "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," in U.S. Department of Health & Human Services. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed: Jan. 25, 2017.

[8] SentinelOne, "Insider threats in Cyber Security—More than just human error," in *CSO*, CSO Online, 2016. [Online]. Available: http://www.csoonline.com/article/3149754/security/insider-threats-in-cyber-security-more-than-just-human-error.html. Accessed: Jan. 24, 2017.

[9] Verizon, "Verizon's 2016 Data Breach Investigations Report," Verizon Enterprise Solutions, Apr. 27, 2016. [Online]. Available: http://www.verizonenterprise.com/verizon-insights-

[10] "Uroburos - highly complex espionage software with Russian roots," 2016. [Online]. Available: https://blog.gdatasoftware.com/2014/02/23968-uroburos-highly-complex-espionage-software-with-russian-roots. Accessed: Jan. 30, 2017.

[11] "Darkhotel's attacks in 2015," in GReAT, 2015. [Online]. Available: https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/. Accessed: Jan. 30, 2017.

lab/dbir/2016/. Accessed: Jan. 24, 2017.

[12] J. Grim, "Data Breach Digest Update: Data Ransomware – the Catch 22," in Verizon, Verizon, 2016. [Online]. Available: https://securityblog.verizonenterprise.com/#more-2659. Accessed: Jan. 24, 2017.

[13] J. Scott and D. Spaniel, *China's espionage dynasty: Economic death by a Thousand cuts* in *Amazon.com: Books*. CreateSpace Independent Publishing Platform, 2016. [Online]. Available: https://www.amazon.com/Chinas-Espionage-Dynasty-Economic-Thousand/dp/153532743X/ref=asap_bc?ie=UTF8. Accessed: Jan. 24, 2017.

[14] B.Krebs, "Target hackers broke in via HVAC company," 2017. [Online]. Available: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. Accessed: Jan. 30, 2017.

[15] T. Seals, "Target breach costs could total $1Bn," Infosecurity Magazine, 2015. [Online]. Available: https://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn/. Accessed: Jan. 30, 2017.

[16] S. Morgan, "Zero-percent cybersecurity unemployment, 1 million jobs unfilled," CSO Online, 2016. [Online]. Available: http://www.csoonline.com/article/3120998/techology-business/zero-percent-cybersecurity-unemployment-1-million-jobs-unfilled.html. Accessed: Jan. 22, 2017.

[17] D. Vinik, "What trump's hiring freeze means (and doesn't)," in *Politico*, The Agenda, 2017. [Online]. Available: http://www.politico.com/agenda/story/2017/01/what-trump-hiring-freeze-means-000287. Accessed: Jan. 24, 2017.

[18] "Health Warning: Cyberattacks are Targeting the Healthcare Industry," in *McAfee*. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-health-warning.pdf. Accessed: Jan. 25, 2017.

[19] "The greatest heist of the century: hackers stole $1 bln," in Kaspersky, 2015. [Online]. Available: https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/. Accessed: Jan. 30, 2017.

[20] "The Great Bank Robbery: the Carbanak APT," in *SecureList*. [Online]. Available: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/. Accessed: Jan. 30, 2017.

[21] D. Kravets, "San Francisco Admin Charged With Hijacking City’s Network," in *Wired*, WIRED, 2008. [Online]. Available: https://www.wired.com/2008/07/sf-city-charged/. Accessed: Jan. 23, 2017.

[22] B. Vielmetti, "Chinese engineer accused of stealing trade secrets from GE," 2014. [Online]. Available: http://archive.jsonline.com/news/crime/chinese-engineer-accused-of-stealing-trade-secrets-from-ge-unit-b99344912z1-274122821.html. Accessed: Jan. 30, 2017.

[23] D. Bisson, "The Ashley Madison Hack -- A Timeline," in *Cyber Security*, The State of Security, 2015. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/. Accessed: Jan. 30, 2017.

[24] B. Krebs, "Online cheating site AshleyMadison hacked," in *Krebs on Security*, 2015. [Online]. Available: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/. Accessed: Jan. 30, 2017.

[25] D. Goldman and J. Pagliery, "Adult dating site hack exposes sexual secrets," in CNN, CNN, 2015. [Online]. Available: http://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/. Accessed: Jan. 30, 2017.

[26] "Corporate Cybersecurity: A Serious Game,". [Online]. Available: http://www.tatainteractive.com/pdf/Cybersecurity_v4.pdf. Accessed: Jan. 30, 2017.

[27] M. Adams and M. Makramalla, "Comments," *Technology Innovation Management Review*, vol. 5, no. 1, 2015. [Online]. Available: https://timreview.ca/article/861. Accessed: Jan. 30, 2017.

[28] J. Amorim, "Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment," in *NATO*. [Online]. Available: https://www.sto.nato.int/publications/.../STO-MP-MSG-111/MP-MSG-111-18.pdf. Accessed: Jan. 30, 2017.

[29] B. Dickson, "4 ways gamification is advancing cybersecurity," The Next Web, 2016. [Online]. Available: https://thenextweb.com/insider/2016/06/24/4-ways-gamification-advancing-cybersecurity/. Accessed: Jan. 30, 2017.

[30] "2016 MARKET PULSE SURVEY," in *SailPoint*. [Online]. Available: http://img03.en25.com/Web/SailPointTechnologies/%7B9a1ba317-f96c-46c5-9c14-0d4c00422135%7D_sailpoint-market-pulse-2016.pdf?utm_campaign=16-Q1-SPS-WW-Website-Market-Pulse-Survey-2016-Report-SP-Form-Submitter-Email&utm_medium=email&utm_source=Eloqua&elqTrackId=C1942578F36D3F4D48A21DC. Accessed: Jan. 24, 2017.

[31] M. Mali, "Arrested NSA contractor is no Snowden, officials say," in *The Hill*, The Hill, 2016. [Online]. Available: http://thehill.com/policy/national-security/299925-arrested-nsa-contractor-is-no-snowden-officials-say. Accessed: Jan. 24, 2017.

[32] "Bridging the Data Security Chasm: Assessing the Results of Protiviti's 2014 IT Security and Privacy Survey," Protiviti, 2015. [Online]. Available: http://resources.idgenterprise.com/original/AST-0135695_2014-IT-Security-Privacy-Survey-Protiviti.pdf. Accessed: Jan. 22, 2016.

[33] J. Scott and D. Spaniel, "ICIT report: Utilizing the NSA's CSfC process- protecting national security systems with commercial layered solutions," in *ICIT*, 2016. [Online]. Available: http://icitech.org/icit-report-utilizing-the-nsas-csfc-process-protecting-national-security-systems-with-commercial-layered-solutions/. Accessed: Jan. 23, 2017.

[34] "Field-level data encryption," in *Microsoft*, 2016. [Online]. Available: https://msdn.microsoft.com/en-us/library/dn481562.aspx. Accessed: Jan. 30, 2017.

[35] "Format-preserving Encryption (FPE), data masking, Datatype Agnostic, Referential integrity | HPE security - data security," HPE Security - Data Security. [Online]. Available: https://www.voltage.com/technology/data-encryption/hpe-format-preserving-encryption/. Accessed: Jan. 30, 2017.

[36] B. Dickson, "How artificial intelligence and Analytics deal with insider threats," in *Huffington Post*, The Huffington Post, 2016. [Online]. Available: http://www.huffingtonpost.co.uk/ben-dickson/how-artificial-intelligen_b_13045254.html. Accessed: Jan. 30, 2017.

[37] C. Sherman, "The Forrester Wave™: Endpoint security suites, Q4 2016," 2016. [Online]. Available: https://www.forrester.com/report/The+Forrester+Wave+Endpoint+Security+Suites+Q4+2016/-/E-RES113145. Accessed: Jan. 30, 2017.

[38] K. Lonergan, "The critical difference between SIEM and UBA - and why you need both to combat insider threats," in *Security*, Information Age, 2015. [Online]. Available: http://www.information-age.com/critical-difference-between-siem-and-uba-and-why-you-need-both-combat-insider-threats-123460054/. Accessed: Jan. 25, 2017.

[39] "What is a SIEM?," in Tripwire, Tripwire, 2016. [Online]. Available: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/. Accessed: Jan. 22, 2017.

[40] "Insider threat control: Using a SIEM signature to detect potential precursors to IT sabotage," in *CERT Insider Threat Blog*, 2012. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2012/01/insider-threat-control-using-a-siem-signature-to-detect-potential-precursors-to-it-sabotage.html. Accessed: Jan. 26, 2017.

[41] Simon, "Insider threat prevention using a file server in an SMB (small & medium business)," in *Secudrive*, 2016. [Online]. Available: http://www.secudrives.com/2016/11/22/insider-threat-prevention-using-a-file-server/. Accessed: Jan. 25, 2017.

[42] "2016 Data Breach Investigations Report," Verizon, 2016. [Online]. Available: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/. Accessed: Jan. 22, 2016.

[43] http://icitech.org/icit-analysis-identity-and-access-management-solutions-automating-cybersecurity-while-embedding-pervasive-and-ubiquitous-cyber-hygiene-by-design/

[44] T. Kemp, "Identity is the new perimeter," 2015. [Online]. Available: http://blog.centrify.com/identity-is-the-new-perimeter-2/. Accessed: Jan. 21, 2016.

[45] P. Kanagasingham, "Data Loss Prevention," in *Sans Institute*, 2008. [Online]. Available: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883. Accessed: Jan. 26, 2017.

[46] B. Vielmetti, "Medical college researcher accused of espionage," 2013. [Online]. Available: http://archive.jsonline.com/news/crime/medical-college-researcher-charged-with-stealing-anticancer-compound-ls9cnn4-200958961.html. Accessed: Jan. 30, 2017.

[47] A. Cohen, "Why segmentation-in-depth is Foundational Cyber security," in Security Week, 2017. [Online]. Available: http://www.securityweek.com/why-segmentation-depth-foundational-cyber-security. Accessed: Jan. 31, 2017.