OCCAMSEC E-BRIEF // NOVEMBER 5th 2018

TABLE OF CONTENTS

Examining Cyber Pearl Harbor Warnings

The notion that the United States is vulnerable to a strategic surprise attack intended to destroy, degrade or disrupt the computer networks (and our national critical infrastructure) is often characterized by military commanders, scholars and the media as a "Cyber Pearl Harbor". In 2010 the CIA Director Leon Panetta testified before the House Permanent Select Committee: "The potential for the next Pearl Harbor could very well be a cyber-attack". Mr. Panetta certainly isn't the only intelligence official to raise the alarm about cyberthreats. Retired General Michael Hayden, and former Director of National Intelligence James Clapper have stated their concerns about the US preparedness for a "Cyber Pearl Harbor".

However, we believe the reality may be different. For various projects we have worked with organizations to determine the potential to slowly degrade their capabilities over time, ultimately leading to their business being unsustainable. This approach utilizes lower key attacks rather than a" full frontal assault" and in testing had the potential to fly under the radar.

We have been reminded of this approach in recent months due our continuing monitoring of ransomware and other malicious events. What if there will be no cyber Pearl Harbor but instead a large scale "death by a thousand cuts" as attacks continue to cause outages, leading to increased expenditure on security, a loss of faith by consumers, and at some point, creating an untenable position for many organizations.

The Intelligence Context

Warning intelligence refers to activities intended to detect and report on developments which may forewarn of hostile actions against a country or organization. Warning intelligence is unique in that it is the only discipline where old information is considered high value data. In traditional military conflicts historical information is studied (for indicators, indications, deception, and political strategy). Due to the asymmetrical nature of cyber-attacks and the actors behind them, there is a lack of historical information that helps to clearly define indicators that will warn of a surprise cyber-attack.

The consensus currently gravitates around the idea of a large scale cyber-attack having a massive impact, we are continuing our research to determine if in fact this focus is wrong and we are instead involved in a long game with our adversaries.

A Different Way of Viewing Cyber Pearl Harbor?

The consensus currently gravitates around the idea of a large scale cyber-attack having a massive impact (such as an attack on the power grid), we are continuing our research to determine if in fact this focus is wrong and we are instead involved in a long game with our adversaries.

But what if the intention of our adversaries is to create a situation where we find ourselves operating in a degraded or damaged state without the single catastrophic event? Many of the targets often cited in worst case scenarios are in reality not so easily attacked. True, the notion of a large scale cyber-attack may help to raise awareness and drive the adoption of security technologies and processes, but what if it is misplaced? What if we are in a long game with the objective of creating an environment where effective cyber security becomes impossible?

Pushing this further, we face the possibility of the cost of a security team becoming similar to that of maintaining a professional sports team, is this part of the long game? To create a situation where only the largest, wealthiest organizations can afford the expertise? Security is currently one of the hot employment sectors, but is this having the adverse effect of it becoming overpopulated with "experts" who are nothing of the sort?

Right now we do not know the answer to many of these questions, in the last month alone there were 9 ransomware events that came our way, and many more that we saw in the press. Much of this is no doubt the work of opportunists, but further up the chain malware needs to be created, exploits discovered, and tools released. The possibility of a large scale "death by a thousand cuts" cannot be ruled out, and given the results we have had with clients in playing out those scenarios we will continue our research into this area.

Source: OccamSec

GAO Finds Nearly All Weapon Systems Vulnerable to Cyberattack

In an October 2018 the United States Government Accountability Office (GAO) issued a report titled "Weapon Systems Cybersecurity - DoD Just Beginning to Grapple with Scale of Vulnerabilities" This was the first report in context to weapon systems and to present the information in an unclassified format details regarding specific vulnerabilities were not disclosed - a classified briefing will be provided to congress outlining their detailed findings. It should be noted this report primarily focused on new weapon systems being developed.

Test Teams Easily Took Control

Defense test teams were able to defeat weapon systems cybersecurity controls with relative ease. In one case it took a two-person test team one hour to gain initial access to a weapon system and one day to gain full control of the system they were testing.

Some programs were better protected than others, the report provides examples of test teams being unable to compromise systems remotely but this wasn't the case for insiders and near-insiders.

Test teams were able to bypass weapon systems cybersecurity controls using standard open source tools. In some cases simply scanning these systems resulted in parts of the systems to be shut down.

Key Takeaways

Organizations traditionally associated with cybersecurity such as the NSA and Cyber Command support some aspects of weapons cybersecurity. However, they are not responsible for reviewing the designs of most weapon systems to identify potential vulnerabilities. NSA officials stated they would provide advice to acquisition of weapon if asked to do so.

Cybersecurity has traditionally not been "baked-in" to the system development lifecycle. The GAO notes the highly complex systems of systems comprising modern weapon systems. The report provides information regarding various DoD initiatives addressing weapon systems cybersecurity but indicates a central authority or common standards across the organization is required.

The DoD faces the problem of finding and retaining individuals with the necessary skills to help identify potential vulnerabilities of modern weapon systems. The GAO recognizes the unique skillsets needed and the talent required being employed by the private sector where the salaries easily exceed over $250,000, an amount not even possible within the military or GS pay ranges. The report also goes on to state even when positions are filled general cybersecurity expertise is not the same as weapon systems expertise. “For example, officials said that professional IT certifications are not the same as systems security expertise which is essential to designing cyber-cyber-resilient systems”

Barriers to information sharing were cited by many officials according to GAO. Most officials interviewed by GAO acknowledged the difficulty in finding a correct balance between protecting information to prevent potential adversaries from access and sharing it. DoD officials explained there is no DoD wide cybersecurity classification guidance.

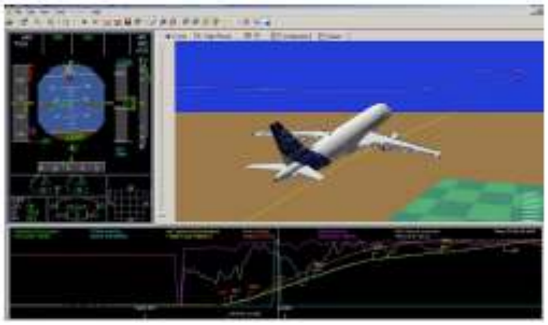
Source: OccamSec

Lack of Information Security Professionals a Key Risk to National Security

The unprecedented demand for well-trained cybersecurity workers continues to grow. Some experts predict that there will be a global shortage of two million cybersecurity professionals by next year. Enlisting the next generation of skilled cybersecurity workers and training existing employees will help build stronger defenses and restore confidence among digital citizens. Job seekers with nontraditional backgrounds may bring new experience and perspectives to the position, and a variety of industries – ranging from education, financial institutions, and banks to fashion, design, and retail – are hiring. The bottom line is that the profession is dedicated to helping make our borderless online world safer and more secure for everyone. Although they are often behind the scenes, these experts are truly on the front lines and have a measurable impact in our digital lives. The bottom line is that the profession is dedicated to helping make our borderless online world safer and more secure for everyone. A workforce with diverse expertise and backgrounds has a greater chance of defending our assets.

Source: Help Net Security

Aircraft Analysis Tool Facing the Internet Exposes Airlines to Risks



Security researchers discovered that more than two dozen systems used by airlines to analyze data from airplane sensors were available online and could be used to pivot into datacenter systems and servers vulnerable to legacy security issues. Security researcher HackerPom initially found up to 38 systems connected to the public internet running AirFASE software, a post flight data analysis tool developed by Teledyne Controls and Airbus. AirFASE stands for Aircraft Flight Analysis and Safety Explore and its purpose is to interpret information from various sensors aboard an aircraft to help determine operational issues, identify possible risks, and take corrective actions. The final number of exposed systems was 35, and most of them appeared to connect to data centers handled by Teledyne. This would make sense since the company also provides its customers with the infrastructure to collect data from the aircraft and deliver it to the back-office for analysis using AirFASE.

Analyzing the AirFASE web panel, the researchers noticed multiple security issues that could give an attacker sufficient details to mount an attack and breach the system running the utility. Apart from accepting sensitive traffic over HTTP, which would allow anyone sniffing the network to intercept credentials when operators log in, the portal itself is fundamentally insecure, from the way it handles incorrect logins to parsing login information. The messages returned by the software when submitting invalid credentials revealed database names that paint a good picture of the data available. Although none of the researchers tested this theory, HackerPom said that this could mean that SQL injection attacks were possible. Login attempts did not seem to be limited in any way, which would clear the way for brute-forcing the login.

Some of the devices exposed through the AirFASE utility had unsecured MySQL databases that store the info retrieved directly from the aircraft. The service was hosted via Apache Tomcat, which is exploitable in an automated way, via a Metasploit module. According to information from Teledyne, though, the data from the aircraft is first compressed and then sent in an encrypted form to the data centers. Another security issue discovered on Teledyne systems was JavaRMI, a Java remote invocation method that creates procedure calls and is vulnerable since 2011. One machine allowed anonymous connection to the FTP service, which exposed directories containing flight data.

Searching for the organizations that had the AirFASE systems exposed online and disclosing the issues in a responsible way was no easy task for the researchers. They were able to identify about 20 airlines, airports, and organizations; only three of which responded. They turned to A-ISAC, the Information Sharing and Analysis Center in the avionics industry, who informed the affected parties of the security risks. This move yielded some results, as it caused systems to be taken offline. Considering the sensitive information it makes available, it is unusual that AirFASE systems would be facing the Internet directly. There is also no apparent reason to have them online, since the purpose of the software is to analyze the data points from a landed aircraft and help operators determine if and when technical inspections and maintenance work is necessary; this task should not be done remotely.

Source: Bleeping Computer

Future Terror Groups will Seek to Copy ISIS, Turn Social Media into a Weapon

The Islamic State's 2014 invasion of Iraq, military futurist Peter Singer writes, "was launched with a hashtag." #AllEyesOnISIS became a viral propaganda machine that inspired followers, generated bots, and is credited in part with driving enough fear to lead thousands of US-trained and equipped Iraqi forces to abandon their posts. The organization fed that fear and gained followers by broadcasting terrifying orange suit-black hood beheadings, terror attacks, or the obscene cruelties awaiting anyone in their path.

Four years later, the coalition of nations that rose up against ISIS in Iraq and Syria sees conventional operations coming to a close, and ISIS' ability to manipulate social media has also been largely dismantled, said Chairman of the Joint Chiefs Marine Corps General Joseph Dunford. He spoke to reporters as he hosted defense chiefs from more than 80 nations at Andrews Air Force Base, Maryland, to discuss what needs to be done to keep other terror groups around the world from making a similar rise. Dunford said the group's ability to produce videos, web posts, and other outreach has been cut by more than 80 percent over the last two years, and that the group's once-flagship monthly propaganda magazine has not been published in more than a year.

ISIS' mastery of social media in its initial swath of victories in 2014 has created a dangerous model that is likely to be mimicked by future groups, said Singer, who wrote about the prominent role online campaigns will have in future conflicts in his new book, "Like War: The Weaponization of Social Media."

"I don't know exactly what 'ISIS 2.0' is, but I know we will learn about them on social media," Dunford said. The group was the first example of a terror network turning social media power into real global power. ISIS "didn't have the numbers [of fighters] or a weapons advantage, yet it defeated a defending force backed by the most powerful force in the world and caused Americans to become more fearful of terrorism than in the wake of 9-11." In the years since US forces first responded to ISIS's invasion in the summer of 2014, the military has been able to better counter social media warfare and other online weapons, such as gaining organizational or planning capabilities.

Source: Military Times

Russian Trolls get Digital Message from US Cyber Command

The US Cyber Command (USCYBERCOM) is engaging in a campaign to deter further disinformation operations by Russian operatives—individuals like those employed through Russian companies as part of the "Project Lakhta" program described in last week's Justice Department indictment of Elena Alekseevna Khusyaynova—by letting them know that they are being watched. According to a report from the New York Times' Julian E. Barnes, USCYBERCOM has directed operations to identify, track, and directly message individuals involved in disinformation campaigns associated with the upcoming midterm elections. The Cyber Command operation, described by unnamed senior military officials, is limited in scope and does not involve directly threatening Russian operatives. The measured steps are meant to avoid an escalation of operations by Russia to more serious computer-based attacks on US information systems and infrastructure. The operation reflects a more aggressive stance outlined in President Trump's recent executive order on national cyber strategy, which called for building a stronger deterrent. The new policy was accompanied by a loosening of Obama administration limits on use of offensive "cyber weapons" and a more "offenseforward" posture in information and network operations.

USCYBERCOM, which is led by Gen. Paul M. Nakasone (also director of the National Security Agency), has had a growing role in taking on foreign adversaries on the Internet. During operations against the Islamic State, CYBERCOM launched attacks intended to prevent Islamic State propagandists from accessing social media platforms. But the latest campaign targeting Russians working for private companies not directly funded by the Russian government is relatively new territory for the military command. Defense officials did not share the means by which warning messages were being delivered to the Russian disinformation operatives identified by USCYBERCOM. While not carrying a direct threat, the warnings being imparted could be interpreted by the recipients as a threat of public exposure, indictment, and sanctions from the US government.

Source: Ars Technica

Telegram Leaked IP Addresses of its Desktop App Users

Telegram reportedly contained a bug that can leak the IP addresses of its users. Known for providing end-to-end encryption, Telegram's desktop app has been discovered to be leaking not just public but private IP addresses of its users by-default during voice calls and users cannot turn off the feature. This means anyone and everyone attempting to make a voice call will be vulnerable to cyber-attacks. Telegram has, however, fixed the bug in one of the latest updates, and the security researcher who identified the bug has been awarded EUR 2,000 by the company.

The desktop version of the Telegram app was leaking IP addresses during voice calls made via a peer-to-peer framework. Smartphone users can turn off P2P calls by modifying the settings: Settings > Privacy and security > Calls > Peer-To-Peer but desktop users of Telegram are not offered this option. Telegram uses P2P framework to establish a direct connection between the two users when a voice call is to be initiated, and due to the bug, the IP addresses of both the participants were being exposed.

Telegram offers two unique features - namely Secret Chat and Nobody. Through Secret Chat, users can enable end-to-end encrypted calls/chats, while with the Nobody option users can prevent their IP addresses from being exposed during voice calls. When one enables the Nobody option, the voice calls are routed through Telegram's servers. The
Nobody option is not available for desktop users, which means the location of every desktop app user will be vulnerable to exposure and all an attacker needs to do to obtain someone's IP address is to make a call. As soon as the call is picked, the IP address is revealed.

When reported to the company, the issue was patched immediately in 1.3.17 beta and 1.4.0 versions of Telegram for Desktop. With this patch, the desktop version of the Telegram app now offers the Nobody feature as well. This can be enabled by clicking on this option: "P2P to Nobody/My Contacts via Settings → Private and Security → Voice Calls → Peer-To-Peer to Never or Nobody.

Source: HackRead

Analyst Comment: Telegram is a popular communication platform utilized by foreign terrorist organization sympathizers. Similarly, a recent article indicates that another popular anonymous communication platform for sympathizers, Whatsapp, can be compromised during a video call. At this time, it is unknown whether these recent breaches of anonymity will influence sympathizers to transition to new anonymous platforms.

Hackers Swipe Card Numbers from Local Government Payment Portals

A previously unknown hacker group is behind a mounting number of breaches that have been reported by local governments across the US. US cyber-security vendor FireEye has revealed that this yet-to-be-identified hacker group has been breaking into Click2Gov servers and planting malware that stole payment card details. Click2Gov is a popular self-hosted payments solution, a product of US software supplier Superion. It is sold primarily to US local governments and can be found installed anywhere from small towns to large metropolitan areas, where it is used to handle payments for utility bills, permits, fines, and more. FireEye says this new hacker group has been attacking Click2Gov portals for almost a year. The company's investigators believe hackers are using one or more vulnerabilities in one of
Click2Gov's components - the Oracle WebLogic Java EE application server- to gain a foothold and install a web shell named SJavaWebManage on hacked portals.

Forensic evidence suggests the hackers are using this web shell to turn on Click2Gov's debug mode, which, in turn, starts logging payment transactions, card details included. Hackers then use the same shell to upload two never-before-seen malware strains, FIREALARM and SPOTLIGHT, on the same server. The former can parse Click2Gov logs for payment card data, while the latter can detect and extract payment details from HTTP network traffic.

Superion itself released a statement in October 2017 about suspicious activity on a number of customer portals, claiming it was investigating the incidents. In June, Risk Based Security, another cyber-security firm, published a report about breaches at nine US cities, which they say, they tracked to Click2Gov portals. FireEye didn't release an official list of Click2Gov portals where the company identified the hackers' malware, but according to Risk Based Security, town municipalities appear to be doing their duty and notifying affected users.

Source: ZD Net

DHS Warns of Cybersecurity Threats to Agriculture Industry

A new report from the US Department of Homeland Security titled "Threats to Precision Agriculture" warns against the cybersecurity risks faced by the emerging technologies being adopted by the agricultural industry. Known as "precision agriculture," the technologies include internet of things (IoT) devices such as remote sensors and global position systems (GPS) and the communications networks that support them. These devices generate large amounts of data which is then analyzed by machine learning systems to improve crop yield and monitor the health of livestock.

The report stated that, "threats against precision agriculture systems can threaten any one of these. The danger is not just cyber-attacks per se, but any danger which could negatively affect

Confidentiality, Integrity, and Ability (CIA), such as natural disasters, terrorist attacks, equipment breakdown, or insider threats. Based on the diverse nature of the crop and livestock sectors, different aspects of the CIA model were identified as assuming greater importance at different points in the agriculture production chain."

The report warns that common cyber threats, such as spear phishing, malware, and improper use of USB thumb drives, could compromise these automated systems that the agricultural industry is coming to rely on. A successful cyber-attack could lead to theft of confidential data, destruction of equipment, loss of resources, and reputational damage. Agricultural cyber-attacks pose a threat not only to farmers, livestock producers, and workers, but also industries that provide supplies to them, such as fertilizer producers and seed companies.

Source: Bleeping Computer

Hackers Target Port Facilities in Ransomware Attacks

As September drew to a close, international shipping ports in Barcelona, Spain, and San Diego, California fell victim to ransomware attacks. These follow a successful attack on the China Ocean Shipping Company terminal at the Port of Long Beach this past July. This cluster of attacks should serve as a warning to the industry as a whole that there could be a hacker or hacker team targeting shipping companies and the facilities they rely on. While the details on both attacks are slim, the Port of San Diego did confirm to ZDNet that it was, in fact, a ransomware attack, though they did not get any more specific than that.

Like most industries, maritime shipping is becoming more reliant on technology. Too often, that technology was not developed with security as a core concept, as shown in the increasing number of reports centered around the critical vulnerabilities in the industrial internet of things (IIOT). The shipping industry has turned to software and hardware solutions to outright handle, or at least assist with, tasks such as loading cargo and navigation while at sea. These types of high-tech hacks could have crippling effects on the shipping companies, individuals aboard the ships, and even national economies.

Recent attempts align more with standard ransomware attacks: hackers likely gained access through poorly patched networks with external facing vulnerabilities. The other likely vector is social engineering, where a successful phishing attack targeted a known network or software vulnerability. Ransomware attacks can be absolutely devastating—look at the fallout of the Atlanta attack—and the massive amount of capital involved in literally moving the economy around the globe, the effects are amplified.

Source: Total Security Daily Advisor

Malware Hits Medical Devices at 18 Percent In Last Year

Nearly one in five provider organizations (18 percent) polled for a new joint report from CHIME and KLAS have seen malware or ransomware infect or impact medical devices in the past year and a half. While few of those incidents ultimately resulted in compromised health information or an audit by the Office for Civil Rights, according to almost 150 chief information officers, chief information security officers, chief technology officers, and other IT and information security leaders polled for the report, those device vulnerabilities were a big concern to most of them. Fewer than 40 percent of respondents said they are "very confident or confident" that their health systems' existing strategies were adequate to safeguard those devices, protecting patient safety and preventing interruptions in clinical workflow, according to the survey.

The Medical Device Security 2018 report suggests progress is being made as hospitals and health systems try to protect their IT systems and connected devices from malicious remote access and corruption from malware. More than one in four of respondents said their security programs were substantial and fully functional, and almost half said they were developed during this calendar year, reflecting a readiness and responsiveness to persistent and fast-evolving threats. Still, "progress has been slow," according to CHIME and KLAS, which found the CIOs and CISOs they polled citing internal factors – more than 75 percent cited insufficient resources – as major challenges to devices.

Poor asset and inventory processes were some other hurdles respondents cited, as well as ambiguous org charts that created murky security ownership and responsibilities. There were also big complaints about medical device vendors and the regulatory agency that oversees them. A huge majority of those polled - 96 percent - said security vulnerabilities stemmed from manufacturer-related factors. Just as many said they face challenges managing outmoded operating systems and patching devices. Nearly two-thirds of survey respondents said manufacturers shift blame to FDA regulations they claimed hinder them from improving device security. Another third, meanwhile, said lack of clarity with FDA policies gave manufacturers an excuse to duck responsibility for device flaws.

"Safeguarding medical devices requires a joint effort from both provider organizations and device manufacturers," added KLAS President Adam Gale. "Many providers have the basic building blocks for a general security program in place and are making progress, although it is difficult and time-consuming, toward developing a mature program. We also are seeing some manufacturers being more proactive and accountable." "Unsecured and poorly secured medical devices put patients at risk of great harm if those devices are hacked," said CHIME CEO Russ Branzell in a statement. "In recent years, that risk has increased exponentially as devices in hospitals and health organizations have become more and more interconnected. Our members are looking for ways to safeguard these devices, but they need resources and support to be effective."

Source: Healthcare IT News

ATM Wiretapping is on the Rise, Secret Service Warns

The US Secret Service warns of a recent surge in incidents of ATM wiretapping. According to a copy of the notice, the alert states that multiple reports have been received relating to the ATM hacking tactic. ATM wiretapping or eavesdropping is more complicated than many other attacks. In order to be successful, a criminal must drill a large hole in a cash machine and use a combination of magnets and devices to attach a skimmer directly to the ATM card reader. This skimmer then harvests credit card information. The hole is concealed with metal or a decal, and cameras are also embedded to capture PIN number input. They are often installed directly above a PIN card and disguised with a false fascia. An endoscope, a thin, long tube with a camera at its end most commonly used in medical applications, is often part of the criminal's kit, as it allows users to check inside a compromised ATM's innards to see if the skimmer is in place. Though, this has not stopped criminals adopting the card skimming technique in larger numbers than before. Sources speaking to the cybersecurity expert said that how-to documents which describe the possible ways to conduct these attacks are being shared widely. This may give threat actors the knowledge required to further ramp up ATM wiretapping attack rates in the future. The attack setup can demand days of tampering, which makes it not only risky, but difficult, and there is a delay between installing skimmers and cameras in order to make sure anti-tampering alarms stay dormant. Originating in Russia, Europe, and Asia, jackpotting is another issue which has recently reached American shores. IBM has experienced a 300 percent increase in ATM testing requests since 2017.

Source: ZD Net - Author: Charlie Osborne

Suspicious Network Activity on a US City Government Network

The city clerk for a US city government on 13 August 2018 notified the city government's information technology (IT) staff that repeated lockouts had occurred against the clerk's user login profile, according to a DHS report derived from a state law enforcement official with firsthand knowledge of the information contained in network activity logs. The lockouts occurred on the day prior to the 14 August 2018 primary election for the 06 November 2018 general election, according to the same report. The city IT director discovered unknown cyber actors made hundreds of failed attempts to log in to two computers belonging to the city clerk. Network settings caused the city clerk's account to lock each time there were four failed login attempts, according to the same report. Unknown cyber actors on 14 August 2018 made hundreds of similar failed login attempts against the user login profile for a city IT employee, subsequently locking the employee's user login profile, according to the same report.

All unauthorized login attempts resolved to the city's terminal server, according to the same report. Elections in this state are administered at the municipal level, which is where the described activity took place, according to the same report. No successful login sessions by unauthorized actors were detected, and no data was exfiltrated during these events.

All ports on the city's terminal server were open to the Internet, according to the same report. Geo-Internet Protocol (IP) filtering, which can deny access to specific country IP addresses, was not employed at the time of these incidents. All users within the city were able to log into the remote desktop protocol (RDP) for the terminal server, and two-factor authentication was not employed, according to the same report. During the response to these incidents, cybersecurity personnel enabled logging, and the city turned on a commercial product to enable free auditing. Cybersecurity personnel recommended the city employ Geo-IP filtering and two factor authentication and reduce the list of people with access to RDP, according to the same report.

Support to Computer Network Defense

Cybersecurity personnel analyzed hypertext transfer protocol secure (HTTPS) traffic to the city's terminal server from 10-14 August 2018 and identified 451 suspicious access attempts originating from 89 IP addresses in the United States and 14 other countries, according to the same report. The chart below lists the suspicious IP addresses with country of origin and number of access attempts against each IP address. There were no city personnel traveling anywhere outside the United States at the time of the incident, according to the same report.

Reporting Computer Security Incidents

To report a computer security incident, either contact NCCIC at 888-282-0870, or go to https://forms.uscert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

Prepared by the Office of Intelligence and Analysis (I&A), Cyber Mission Center (CYMC). Coordinated with the National Cybersecurity and Communications Integration Center (NCCIC).

Source: DHS I&A, CYMC, and NCCIC

National Cyber Strategy Released

Under the newly-released National Cyber Strategy, the Pentagon, United States Cyber Command, and other federal departments will take lead fighting malicious cyberattacks, going more on the offensive to deter future attacks.

Cyberattacks are a constant threat to state and local governments. In March, a ransomware attack took Atlanta's network servers, affecting 30 percent of the city's online applications and potentially costing the city millions. Baltimore's 9-1- 1 system was breached by hackers the same month, forcing dispatchers to take emergency calls manually.

A more robust federal cybersecurity strategy may address some issues, but state, local, tribal, and territorial (SLTT) governments can see the writing on the wall and should be working to secure their networks now.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) offers SLTT governments state-of-the-art tools and resources for cybersecurity prevention, protection, response, and recovery. They can assist with malware analysis, log analysis, forensic analysis, and vulnerability assessments.

Through a free membership, SLTT governments also have access to up-to-date cyber threat and vulnerability information, training resources, educational opportunities, members-only webcasts, and more.

Most importantly, the MS-ISAC can help SLTT governments with cyber incidents whether they are members or not. Their highly trained staff can assist your agency or department if you experience disruption or defacement of websites, compromised passwords, all kinds of malware, and unauthorized use of system data.

October is National Cyber Security Awareness Month, an optimal time for taking the steps to secure your systems. Visit the MS-ISAC website for more information on joining and how they can assist with your cybersecurity concerns.

Source: MS-ISAC

Corporate Insiders Willing to Share Secret Info With Cyber Criminals

- Amazon said this week it's investigating whether company insiders have been selling proprietary information to buyers in Asia in order to give them a selling advantage.
- Many companies, especially in big technology, banking and telecom, face heavy incentives overseas for employees to sell internal information or access.
- The problem is so common that in some jurisdictions, criminal enterprises post "job ads" looking for specific insiders to aid in targeted schemes.

In Russia, one organization is looking for "long-term, quality employees" from telecommunications providers with the promise of "fair, on-time" pay. Another group promises experienced bankers around $2,000 per month for "one hour of work per day." In Mexico, another ad promises employees from well-known banks high pay with little risk, on the condition of "absolute discretion.”

This is today's competitive job market for criminal corporate insiders.
This week, Amazon said it is investigating claims that company insiders across Asia were making money by selling retail secrets. In their case, corporate insiders may have been trading in proprietary information to help Amazon marketplace sellers based in the region get an unfair sales advantage.

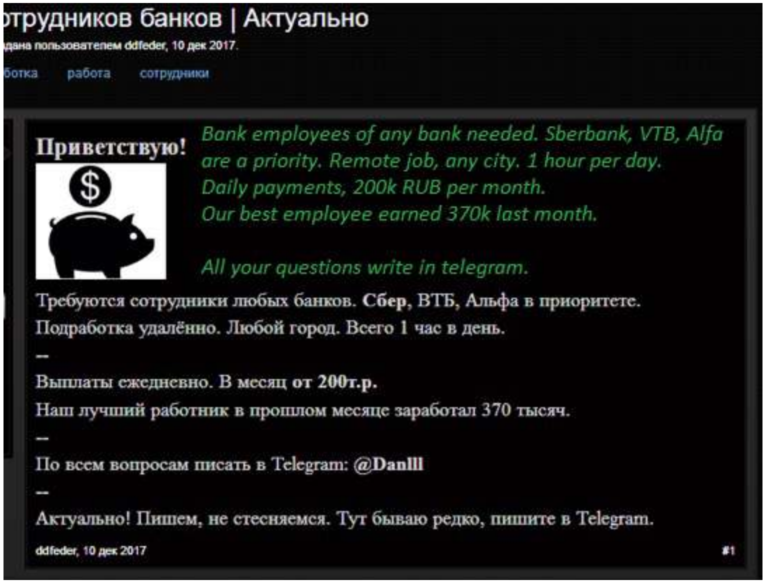
But Amazon is far from the only company facing pervasive insider threats, especially in locations in Eastern Europe, Russia, Asia and North Africa. There, employees can sometimes quadruple their salaries or more by working with a criminal enterprise to sabotage their own employer.

'Employees of any bank needed'

According to Ziv Mador, vice president of research for cybersecurity and compliance management company Trustwave, global corporations are facing this problem more requently, as even trusted employees may find themselves on the receiving end of unwanted solicitations to take part in simple, but illegal, "side work."

In monitoring the dark web — parts of the internet accessible only with specific search engines, software or configurations — Mador has observed numerous postings seeking very specific types of employees at big-name employers.

Examples shown here come from Russia and Mexico.



отрудников банков | Актуально

дана пользователем ddfeder, 10 дек 2017.

ботка работа сотрудники

Приветствую!

Bank employees of any bank needed. Sberbank, VTB, Alfa are a priority. Remote job, any city. 1 hour per day.
Daily payments, 200k RUB per month.
Our best employee earned 370k last month.

All your questions write in telegram.

Требуются сотрудники любых банков. **Сбер**, ВТБ, Альфа в приоритете.
Подработка удалённо. Любой город. Всего 1 час в день.
—
Выплаты ежедневно. В месяц **от 200т.р.**
Наш лучший работник в прошлом месяце заработал 370 тысяч.
—
По всем вопросам писать в Telegram: **@Danlll**
—
Актуально! Пишем, не стесняемся. Тут бываю редко, пишите в Telegram.

ddfeder, 10 дек 2017 #1

"The salaries listed are quite high, sometimes 10 times what the average salary for an average job at a bank would be," he said. Insider threats proliferate, he said, in areas where salaries may below and law enforcement is lax in looking for employees who might be participating in insider crimes.

"[Criminal recruiters] are looking for many different tasks: increasing withdrawal limits on bank accounts, getting more information about people who they want to target. They are looking for people who work in tax offices, or in other cases, they look for people who can tell them how to log in and how to connect to certain accounts," Mador said.

Mador also said he's observed recent cases of corporate employees posting on these same types of forums, offering their services as corporate insiders.

The continued trend is just one part of the greater intellectual property and privacy concerns of big companies doing business overseas. Tech giants like Apple, Amazon and IBM have been concerned that new competition rules in China -- ostensibly meant to elevate China-based competitors -- give the state and competing Chinese firms too much access to their proprietary secrets and code.

In July, Xiaolang Zhang, a Chinese Apple employee, was arrested at the San Jose airport after telling his colleagues he was moving back to China to be close to his ill mother. The U.S. Department of Justicesaid that Zhang was carrying "a confidential 25-page document containing detailed schematic drawings of a circuit board designed to be used in the critical infrastructure of a portion of an [Apple] autonomous vehicle." Zhang has pleaded not guilty in the case.

In another case, in 2017, an insider at Dupont was alleged to have stolen valuable trade secrets related to the company's Chemours chemical division. Employee Jerry Jingdong Xu was said to have taken hundreds of millions in chemical trade secrets in order to sell them to Chinese investors, according to the company, along with a co-conspirator. He also has pleaded not guilty.

Source: CNBC

Attackers Use Voicemail Hack To Steal WhatsApp Account

Another online account hijacking attack has emerged, this time targeting WhatsApp. The Israeli agency responsible for cybersecurity has warned its citizens about the attack, which can often be conducted without any knowledge or interaction on their part. All the attacker needs is the victim's phone number.

First documented by security researchers last year, the security flaw has now hit the mainstream. Last week, ZDNet reported that the Israeli National Cybersecurity Authority issued an alert warning that WhatsApp users could lose control of their accounts.

The hack capitalizes on users' tendency not to change default access credentials on cellphone voicemail numbers. The attacker makes a request to register the victim's telephone number to the WhatsApp application on their own phone. By default, WhatsApp sends a six-digit verification code in an SMS text message to the victim's phone number, to verify that the person making the request owns it.

Ideally, the victim would see the message, alerting them that something was up. The attacker avoids that by launching the attack at a time when the victim would not answer their phone, such as in the middle of the night, or while they are on a flight. Many users may even have their phones set to 'do not disturb' during this time.

The attacker doesn't have access to the victim's phone, and so cannot see the code to enter it. WhatsApp then offers to call the victim's number with an automated phone message reading out the code. Because the victim is not accepting calls, the automated message is left as a voicemail.
The attacker then exploits a security flaw on many carrier networks, which provide generic telephone numbers that users can call to access voicemail. The only credential required to hear the voicemail is a four-digit PIN, and many carriers set this by default to something simple like 0000 or 1234. These default passwords are easily discovered online.
When the attacker uses the default PIN to access the victim's voicemail, they can hear the code and then enter it into their own device, completing the transfer of the victim's phone number to their own WhatsApp account.

To seal the deal, the attacker can then enable two-step verification, which is an optional feature that WhatsApp has been offering since 2017. This requires the user to set a custom PIN, which they must then re-enter if they wish to reverify their phone number. Turning on this feature prevents the victim from regaining control over their own phone number.

Security researcher Martin Vigo explored and expanded on automated phone message attacks in a talk at DEF CON this August titled “Compromising online accounts by cracking voicemail systems”. He went beyond simple default voicemail PINs, using a Python script that brute-forced voicemail accounts using the cloud-based telephony API Twilio.

During the talk, he called out several online services that he said were vulnerable to attacks like this. PayPal, Netflix, Instagram and LinkedIn supported password reset by automated phone call, he said, adding that Apple, Google, Microsoft and Yahoo support the use of automated voicemails for two-factor authentication (2FA).

In a blog post describing the talk, he lamented the fact that we’re still using 30 year-old technologies to secure sensitive systems.

How can you protect your WhatsApp and other accounts from hijackers?

Using application-based 2FA (such as Sophos Authenticator, which is also included in our free Sophos Mobile Security for Android and iOS) mitigates a lot of the risk, because these mobile authentication apps don’t rely on communications tied to phone numbers.

If you must use a service that relies on automated voice messages, then set a strong PIN for your voicemail inbox.

Finally, enable two-step verification on your WhatsApp account, by opening WhatsApp and going to Settings > Account > Two-step verification > Enable.

Source: Naked Security

Airport Mislays World's Most Expensive USB Stick

Like so many stories of data disaster, this one started innocently enough.
In October 2017, a member of the public noticed a USB flash drive lying in the street in a London suburb.

After plugging the drive into a computer at their local public library, they discovered it contained 1,000 files held in 76 folders and a trove of data on security systems and procedures at one of the world’s largest airports, Heathrow.

Because we’re writing about this in the first place, you can already guess that none of the data was encrypted or password-protected.

The member of the public decided to tell The Sunday Mirror newspaper about the find, which days later published a story claiming the loss could potentially have compromised airport security, including putting Queen Elizabeth II, politicians and VIPs at risk.

Yesterday, the company with the job of looking after the data, Heathrow Airport Ltd (HAL), was fined £120,000 ($160,000) by the UK Information Commissioner's Office (ICO) for allowing this to happen.

What was on the drive?

Heathrow Airport claimed that only 1% of the data on the memory stick was personal data, which would have been a good argument if that hadn't included a training video exposing names, dates of birth, vehicle registrations, passport details, and mobile numbers for 10 people involved in important security procedures at the airport.

It also contained information on between 12 and 50 personnel involved in security, including their names and job titles. This, it turned out, was visible in the video, printed on some ring-binder pages that someone carelessly filmed.

The newspaper said the stick contained other security data including patrol timetables, routes taken through the airport by British Cabinet ministers and foreign dignitaries, and security measures to protect the Queen.

What went wrong

Many staff were using USB sticks, including their own, despite Heathrow having no "adequate technical controls" to stop them saving unencrypted data to them. Barely any had received training about the security risks of using USB sticks.

Heathrow Airport seems to have been in denial that anyone might save data to drives or, if they did, would fail to secure them properly. It was as if USB sticks with gigabytes of capacity had never been invented.
The only reason Heathrow Airport has had to acknowledge problems at all is because an employee dropped one on his or her way to work, which was picked up by a member of the public and sent to a newspaper. Arguably, then, the incident was a stroke of luck given the possibility that data might eventually fall into the wrong hands through carelessness.

The airport has admitted it has no idea what other data might have been copied on to USB sticks in the past.

Perhaps now they will take steps to make USB disks less of a data breach risk, for example by limiting the range of USB hardware drives that are allowed; vetting what gets copied onto them; and encrypting any sensitive data that genuinely needs to be backed up onto removable devices.

Source: Naked Security

Pentagon Data Breach Puts Personal Details of 30,000 Staff At Risk

The Pentagon has admitted that up to 30,000 military workers and civilian personnel have had their personal information and credit card data exposed following a security breach.

The security breach occurred at a third-party vendor which provides travel management services to the Department of Defense.

The vendor, which has not as yet been publicly identified due to security concerns and ongoing contracts, was not however responsible for informing the Pentagon of the breach. Instead it appears that the DoD's own computer security team which discovered a breach had occurred.

According to an *Associated Press* report, it it possible that the breach happened "some months ago," and that further investigations may uncover that even more staffers were exposed.

The Department of Defense says that it has started notifying individuals affected by the security breach, and that those impacted will be offered prepaid identity theft monitoring services.

Pentagon spokesperson Lt. Col. Joseph Buccino issued a statement confirming the breach does not affect all staff who have used travel management services:

"The Department is continuing to gather additional information about the incident, which involves the potential compromise of personally identifiable information (PII) of DoD personnel maintained by a single commercial vendor that provided travel management services to the Department. This vendor was performing a small percentage of the overall travel management services of DoD."

The one piece of good news is that it appears no classified material is likely to have been put at risk through the breach.
News of the breach does, however, come at an awkward time for the US Department of Defense which is currently smarting from a report issued last week by the US Government Accountability Office (GAO).

That report concluded that poor security has made next-generation weapons systems easy to hack.

In one case, it was reported that it was possible for unauthorized users to gain access to a weapons system within just one hour, and that the Pentagon was not following basic security practices such as changing default passwords.

"One test report indicated that the test team was able to guess an administrator password in nine seconds. Multiple weapon systems used commercial or open source software, but did not change the default password when the software was installed."

There have, of course, been US government data breaches that have affected a far larger number of individuals than the 30,000 estimated to be impacted in this latest incident.

But that doesn't make it any less important for organizations like the Department of Defense to consider not only how they best protect their systems, but also how well their third-party service suppliers are securing sensitive DoD data.

Source: Hot For Security

Hacker Discloses New Windows Zero-Day Exploit On Twitter

A security researcher with Twitter alias SandboxEscaper—who two months ago publicly dropped a zero-day exploit for Microsoft Windows Task Scheduler—has yesterday released another proof-of-concept exploit for a new Windows zero-day vulnerability.

SandboxEscaper posted a link to a Github page hosting a proof-of-concept (PoC) exploit for the vulnerability that appears to be a privilege escalation flaw residing in Microsoft Data Sharing (dssvc.dll).

The Data Sharing Service is a local service that runs as LocalSystem account with extensive privileges and provides data brokering between applications.

The flaw could allow a low-privileged attacker to elevate their privileges on a target system, though the PoC exploit code (deletebug.exe) released by the researcher only allows a low privileged user to delete critical system files—that otherwise would only be possible via admin level privileges.

"Not the same bug I posted a while back, this doesn't write garbage to files but actually deletes them.. meaning you can delete application dll's and hope they go look for them in user write-able locations. Or delete stuff used by system services c:\windows\temp and hijack them," the researcher wrote.
Since the Microsoft Data Sharing service was introduced in Windows 10 and recent versions of Windows server editions, the vulnerability does not affect older versions of Windows operating systems including 7 or 8.1.

The PoC exploit has successfully been tested against "fully-patched Windows 10 system" with the latest October 2018 security updates, Server 2016 and Server 2019, but we do not recommend you to run the PoC, as it could crash your operating system.

This is the second time in less than two months SandboxEscaper has leaked a Windows zero-day vulnerability.

In late August, the researcher exposed details and PoC exploit for a local privilege escalation vulnerability in Microsoft Windows Task Scheduler occurred due to errors in the handling of the Advanced Local Procedure Call (ALPC) service.

Shortly after the PoC released for the previous Windows zero-day flaw, the exploit was found actively being exploited in the wild, before Microsoft addressed the issue in the September 2018 Security Patch Tuesday Updates.

SandboxEscaper's irresponsible disclosure once again has left all Windows users vulnerable to the hackers until the next month's security Patch Tuesday, which is scheduled for November 13, 2018.

Source: The Hacker News

NATO Cybersecurity Command Center To Be Fully Staffed in 2023

A NATO command center capable of launching cyberattacks with the help of U.S., British and Estonian cyber capabilities will be fully operational and staffed in 2023, a senior general said Tuesday, Reuters' Robin Emmott reports.

Why it matters: NATO computer networks and communications are the targets of hundreds of hacking attempts per month — but there's still a long way to go for NATO to come into its own as a cyber actor. NATO determined cyberspace is a war fighting domain only two years ago, and it still must determine what exactly in cyberspace will trigger the alliance's collective defense.

Source: AXIOS

GreyEnergy: New Malware Targeting Energy Sector with Espionage

In its recent research, ESET, an IT security company, has revealed details of a new group of cybercriminals dubbed as GreyEnergy, which seems to be the replacement of BlackEnergy APT group. The BlackEnergy group's last activity was observed in December 2015, when nearly 230,000 people had to deal with a prolonged blackout due to a cyber attack on Ukrainian power grids.

Since 2016, ESET researchers have noticed GreyEnergy has been attacking energy firms and other valuable targets in Poland and Ukraine since 2016. It appears the targets are critical infrastructure in Ukraine. Researchers also believe the group is closely linked to the BlackEnergy group, and attackers may be looking to launch cyber espionage attacks in the near future.

Furthermore, ESET researchers have evidence that GreyEnergy is linked to the group behind the highly destructive malware NotPetya, Telebots. Telebots is believed to have the backing of the GRU, Russian military intelligence service. Previously, researchers linked Telebots to another malware campaign Industroyer, which caused another blackout in Ukraine in 2016.

It is worth noting that ESET has not really associated GreyEnergy to any specific state of the group, but has only suspected it to have links with different attacks on Ukrainian power grids in the past. They have declared GreyEnergy as one of the most "dangerous APT groups" that's been attacking Ukraine for the last three years.

It is identified that GreyEnergy's primary focus is on targeted attacks and stealth campaigns while the attackers utilize all possible sources to evade detection. Evidently, the key targets are the energy companies specifically those where industrial control system workstations run on SCADA software.

ESET researchers believe that GreyEnergy is tied to BlackEnergy because both are modular, and employ a mini backdoor prior to obtaining admin rights after which a full backdoor is rolled out. Another similarity is that both the groups' malware use remote command and control servers through active Tor relays. It is an operational security technique that the group uses to operate covertly.

Moreover, both the campaigns target the energy and critical infrastructure in Ukraine. One of the victims of BlackEnergy has also been targeted by GreyEnergy. BlackEnergy has remained inactive from the same time since GreyEnergy has been active, which further substantiates the fact that both groups are linked.

There are also signs GreyEnergy is an evolved form of BlackEnergy, considering its ultra-modern toolkit that focuses more on stealth and the AES-256 encrypted fileless modules are pushed only when it is most necessary. These modules run in the memory to hinder the analysis and detection process.

GreyEnergy attacks through spear-phishing emails where users are lured into activating infected macros, and another method is by compromising public web servers. Vulnerable servers are used to obtain entry into networks and then gradually move across the network to attack targeted systems. Moreover, the group uses publicly available tools such as WinExe, Nmap, Mimikatz, and PsExec to carry out its malicious activities while remaining under the radar at the same time.

ESET warns that the group is active, and quite possibly it is preparing another wave of attacks or maybe another APT group is being established to carry out more advanced operations. For an organization to avoid getting attacked by GreyEnergy, here’s what ESET researcher Robert Lipovskэ recommends.

“Use multi-layered security solutions, including Endpoint Detection and Response, 2FA, backups, updated and patched software, and educate employees to not to fall prey to spear-phishing attacks.”

Source: HackRead

Analyst Comment: While there is no indication that there is any impact for the US, organizations should still implement strict zone models, multi-factor authentication, aggressive patching and updates, and good detective controls.

Ancestry Sites Could Soon Expose Nearly Anyone's Identity

Genetic testing has helped plenty of people gain insight into their ancestry, and some services even help users find their long-lost relatives. But a new study published this week in Science suggests that the information uploaded to these services can be used to figure out your identity, regardless of whether you volunteered your DNA in the first place.

The researchers behind the study were inspired by the recent case of the alleged Golden State Killer.

Earlier this year, Sacramento police arrested 72-year-old Joseph James DeAngelo for a wave of rapes and murders allegedly committed by DeAngelo in the 1970s and 1980s. And they claimed to have identified DeAngelo with the help of genealogy databases.

Traditional forensic investigation relies on matching certain snippets of DNA, called short tandem repeats, to a potential suspect. But these snippets only allow police to identify a person or their close relatives in a heavily regulated database. Thanks to new technology, the investigators in the Golden State Killer case isolated the genetic material that's now collected by consumer genetic testing companies from the suspected killer's DNA left behind at a crime scene. Then they searched for DNA matches within these public databases.

This information, coupled with other historical records, such as newspaper obituaries, helped investigators create a family tree of the suspect's ancestors and other relatives. After zeroing in on potential suspects, including DeAngelo, the investigators collected a fresh DNA sample from DeAngelo—one that matched the crime scene DNA perfectly.

But while the detective work used to uncover DeAngelo's alleged crimes was certainly clever, some experts in genetic privacy have been worried about the grander implications of this method. That includes Yaniv Erlich, a computer engineer at Columbia University and chief science officer at MyHeritage, an Israel-based ancestry and consumer genetic testing service.

Erlich and his team wanted to see how easy it would be in general to use the method to find someone's identity by relying on the DNA of distant and possibly unknown family members. So they looked at more than 1.2 million anonymous people who had gotten testing from MyHeritage, and specifically excluded anyone who had immediate family members also in the database. The idea was to figure out whether a stranger's DNA could indeed be used to crack your identity.

They found that more than half of these people had distant relatives—meaning third cousins or further—who could be spotted in their searches. For people of European descent, who made up 75 percent of the sample, the hit rate was closer to 60 percent. And for about 15 percent of the total sample, the authors were also able to find a second cousin.

Much like the Golden State investigators, the team found they could trace back someone's identity in the database with relative ease by using these distant relatives and other demographic but not overly specific information, such as the target's age or possible state residence.

In one specific case, they were able to cross-reference a woman's anonymous genetic profile from another research project with the same service used by Golden State Killer investigators—a website called GEDmatch—and find her identity. The woman had been identified in an earlier study conducted by Erlich, using a different method that relied on figuring out the genetic profile of her husband, but the search was even easier and required less upfront information than their previous method.

For Erlich, the findings are both reassuring and frightening.

"Of course, there's some good news. If someone did something wrong out there, then [law enforcement] is going to be able to catch them," he told Gizmodo. "But down the road, as things continue to evolve, there could be people who use this for illegitimate reasons."

That could include scientists who try to identify research subjects from other projects, as well as companies and individuals that might try to leverage and sellyour information elsewhere. Another concern is genetic discrimination.

Erlich said there are ways to stop the potential misuse of these databases. Agencies such as the U.S. Department of Health and Human Services have regulations for federally funded research that involves human subjects. Known as the common rule, a revision of these guidelines was set to be implemented in 2017, but won't come in full effect until 2019. The revised common rule doesn't currently consider our genomes to be identifiable information, but Erlich noted that the HHS is allowed to change that status as technology advances. That might stop unscrupulous scientists, who would stand to lose federal funding if they were caught trying to pilfer people's identities.

Genetic testing services could also take their own steps to protect their consumers. They could encrypt the raw genetic data they send out with cryptographic signatures, a technique touted by other scientists concerned about genetic privacy. Genealogy services would then only run searches through their database if a query was confirmed to be coming from a customer (as a supplement to the paper, the researchers have uploaded their demo source code for such a signature on GitHub).

In an ideal world, law enforcement agencies could also still access these services, but only obtaining after explicit permission, such as through a warrant. As of right now, MyHeritage does not allow researchers or law enforcement officials to use their genealogy service without permission, and according to the company, no one has been granted permission as of yet.

"We need to think about oversight, about checks and balances, now, before these concrete concerns show up" said Erlich.

Though the details are still being worked out, it's almost certain that all of us will need our genetic information to be safeguarded, even if you do decide to turn down a well-meaning gift of a free DNA test. According to the researchers, it will take only about 2 percent of an adult population having their DNA profiled in a database before it becomes theoretically possible to trace any person's distant relatives from a sample of unknown DNA—and therefore, to uncover their identity. And we're getting ever closer to that tipping point.

"Once we reach 2 percent, nearly everyone will have a third cousin match, and a substantial amount will have a second cousin match," Erlich explained. "My prediction is that for people of European descent, we'll reach that threshold within two or three years."

For those concerned about their criminal misdeeds coming back to bite them, there's already plenty to be worried about. The authors note that more law enforcement officials in the U.S. are starting to adopt this technique. Since April, at least 13 criminal cases have seemingly been solved with the help of genealogy searches. And while most of these involved cold cases, it's also been used to find the suspect of a crime committed just this April. Private forensic testing companies have also recently announced their own sweeps of cold cases using a similar technique.

What this means for you: If you want to protect your genetic privacy, the best thing you can do is lobby for stronger legal protections and regulations. Because whether or not you've ever submitted your DNA for testing, someone, somewhere, is likely to be able to pick up your genetic trail.

Source: Gizmodo