Issue 52, 2013

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE-CT First Responders

CYBER NEWS

www.cbrne-terrorism-newsletter.com

Cyber-terrorism Shut Down Israel's Carmel Tunnel

Source: http://www.infosecurity-magazine.com/view/35289/cyberterrorism-shut-down-israels-carmel-tunnel/

When the Carmel Tunnel, a six-mile road tunnel through the Carmel mountain directly under the city of Haifa, was closed in September, officials initially blamed a malfunction with traffic control. Now it appears to be the work of hackers.

The Carmel Tunnel, actually a series of tunnels through the Carmel mountains beneath Haifa, is more than 6 km in total length. It is designed to reduce traffic congestion in the city, and can reduce travel time across the city from 30-50 minutes down to just 6 minutes.

On September 8 it was closed for 20 minutes. On September 9, it was closed for 8 hours causing major traffic congestion and disruption. The Jerusalem Post reported simply, "The Northbound and Southbound Carmel tunnel was temporarily closed on Monday due to a malfunction with traffic control. Police are asking local residents to use alternative routes."

But now it appears that the problem was a sophisticated – but not that sophisticated – cyber attack. Earlier this month the Israel Defense Forces (IDF) chief, Lt. Gen. Benny Gantz spoke at a conference at the Begin-Sadat Center for Strategic Studies, and warned that a future war could begin with a missile strike or a cyber attack on Israel's traffic light system.

He probably had the Carmel Tunnel incident in mind. According to a new Associated Press report, "One expert, speaking on condition of anonymity because the breach of security was a classified matter, said

a Trojan horse attack targeted the security

Israel is, of course, accustomed to being both

camera apparatus in the Carmel Tunnels toll road on September 8."

Few details are available, but investigators believe the attack was likely to be the work of Anonymous-style activists – it was sophisticated, but "not sophisticated enough to be the work of an enemy government like Iran." Gantz's comments linking such an attack to the start of a war clearly demonstrates, however, that he believes Israel must prepare for all-out cyberwar in conjunction with any possible land war.

on the receiving end of pro-Arab hacktivism and launching its own cyber attacks. Anonymous has an ongoing #OpIsrael campaign ostensibly in support of Gaza, but the official Twitter page makes no mention of nor claim on the Carmel Tunnel incident. The two most recent claims, both dated 5 August, were for attacks against Israeli companies Bable Engineering and Aganim.

Israel itself was famously – or infamously – involved in the Stuxnet attack against Iran's nuclear program.

CyberPro Newsletter

Source: http://www.nsci-va.org/CyberProNewsletter.htm

The CyberPro newsletter is published once every two weeks and distributed via email. It is intended to increase cyberspace awareness and contains **a summary of numerous open-source cyber-related news articles, with links to the complete articles**. In addition, we periodically publish question and answer interviews with key senior leaders and original articles from our subscribers.

EDITOR'S COMMENT: A very useful source of cyber-information! Check the archives for latest newsletter available.

The Dangers of Using Unprotected Wi-Fi Hotspots

Source: http://i-hls.com/2013/10/the-dangers-of-using-unprotected-wi-fi-hotspots/?utm_source=activetrail&utm_medium=email&utm_campaign=English%20Newsletter%2030/10/2013

It's almost second nature now, whiling away a few moments online using a Wi-Fi hot spot. But hooking up to the network can carry hidden risks. Despite this, more than a third of users take no additional precautions when logging on to public Wi-Fi, according to the Kaspersky Consumer Security Risks survey conducted by B2B International and Kaspersky Lab in 2013.

Nowadays it's easy to get online – in addition to cellular networks and broadband cable communication networks, there is often have at least one hotspot which can connect computers and mobile devices to the Internet.

However, many of these hotspots skimp on protection for users – and many users are unaware or unconcerned about the potential problems this can cause. In our survey, 34% of users said they took no special measures to protect online activity using a hotspot, while 14% were happy to bank or shop online using any network that came to hand. Just 13% take the time to check the encryption standard of any given access point. Does extra caution make sense when using public Wi-Fi, or is it all a worry too far?

The answer is YES. You never know what "that guy with the laptop at the next table" might be doing. Maybe, like you, he's checking his email or chatting with friends. But maybe he's monitoring the Internet traffic of everyone around him – including yours. A Man-in-the-Middle attack makes this possible. Any Wi-Fi access point is a window to the Internet for all the devices attached to it. Every request from a device goes via an access point, and only then reaches the sites that users want to visit. Without any encryption of communications between users and the access point it's a simple task for a CYBERcriminal to intercept all the data a user enters. That might include data sent to a bank, or an online store. Moreover, attacks like this are possible even if the hotspot is password protected and a secure https-connection between the required site and the user's browser is established.

What data are CYBERcriminals interested in? Anything they can use to make a profit – especially account logins and passwords for e-mail, e-banking, e-payment and social networks. It's obvious that we need to secure Wi-Fi connections – but how? First of all, Kaspersky Lab recommends only using secure connections to access points. This alone will greatly reduce the risk of the traffic being intercepted by CYBERcriminals. However, when users are planning to use sites which demand personal information such as usernames and passwords, this basic precaution must be joined with additional protective tools.

New Subjects Added to Cyber's Most Wanted List

11/05/13

Source: http://www.fbi.gov/news/stories/2013/november/new-subjects-added-to-cybers-most-wanted-list/new-subjects-added-to-cybers-most-wanted-list?utm_campaign=email-Immediate&utm_medium=email&utm_source=fbi-top-stories&utm_content=272149

Five individuals have been added to the FBI's Cyber Most Wanted list for their roles in domestic and international hacking and fraud crimes collectively involving hundreds of thousands of victims and tens of millions of dollars in losses.

In announcing the addition of the new subjects—along with rewards of up to $100,000 for information leading to their arrests—Executive Assistant Director of our Criminal, Cyber, Response, and Services Branch Richard McFeely said, "Throughout its history, the FBI has depended on the public's help and support to bring criminals to justice. That was true in the

gangster era, and it's just as true in the cyber era. We need the public's help to catch these individuals who have made it their mission to spy on and steal from our nation and our citizens."

The new fugitives on our Cyber's Most Wanted list are:

- Pakistani nationals **Farhan Arshad** and **Noor Aziz Uddin**, wanted for their alleged involvement in an international telecommunications hacking scheme. Between 2008 and 2012, the pair gained unauthorized access to business telephone systems, resulting in losses exceeding $50 million. Arshad and Uddin are part of an international criminal ring that the FBI believes extends into Pakistan, the Philippines, Saudi Arabia, Switzerland, Spain, Singapore, Italy, Malaysia and elsewhere.
- **Carlos Perez-Melara**, wanted for a variety of cyber crimes—including running a fraudulent website in 2003 that offered customers a way to "catch a cheating lover." Those who took the bait downloaded spyware that secretly installed a program on their computers that allowed scammers to steal the victims' identities and personal information.
- Syrian national **Andrey Nabilevich Taame**, wanted for his alleged role in Operation Ghost Click, a malware scheme that compromised more than four million computers in more than 100 countries between 2007 and October 2011; there were at least 500,000 victims in the United States alone.
- Russian national **Alexsey Belan**, wanted for allegedly remotely accessing the computer networks of three U.S.-based companies in 2012 and 2013 and stealing sensitive data as well as employees' identities.

Rewards are being offered for each of the five fugitives, all of whom are believed to be living outside the U.S. See the accompanying "Wanted By the FBI" posters for more information.

The FBI's Most Wanted program is best known for its Ten Most Wanted Fugitives list. The Top Ten list was established more than six decades ago and has become a symbol of the Bureau's crime-fighting ability around the world. But the Bureau highlights other wanted fugitives as well—terrorists, white-collar criminals, and increasingly, those who commit cyber crimes.

The FBI leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. The expansion of the Cyber's Most Wanted list is a reflection of the FBI's increased efforts in this area, McFeely said. "The cyber fugitives we seek have caused significant losses to individuals and to our economy," he explained. "And cyber crime continues to pose a significant threat to our national security."

► **We need your help.** If you have information about any of the five individuals mentioned above, or the other fugitives on our Cyber's Most Wanted list, please submit a tip on our website or contact your local FBI office or the nearest U.S. Embassy or Consulate.

☞ **Visit the source URL for more details on persons mentioned herein.**

2013 Cyber Security Report: One Serious Incident Could Cost $649k

Source: http://i-hls.com/2013/11/2013-cyber-security-report-one-serious-incident-could-cost-649k/

$649,000 is the average cost incurred by large companies in the wake of a CYBER-attack, according to the 2013 Global Corporate IT Security Risks survey conducted by B2B International, in conjunction with Kaspersky Lab.

Any CYBER-attack can cause damages for a company, but how can those damages be quantified in financial terms? In 2013, experts calculated the damages stemming from CYBER-attacks based on the results of a survey of companies around the world.

In order to get the most accurate picture of costs, the researchers included only incidents that had occurred in the previous 12 months; the assessment was based on information about losses sustained as a direct result of security incidents. This comprised two main components:

- Damage resulting from the incident itself – i.e. losses stemming from critical data leakage, business continuity,and the costs associated with engaging incident remediation specialists;

- Unplanned 'response' costs required to prevent future, similar attacks, including hiring/training staff and hardware, software and other infrastructural updates.

Researchers did not incorporate data about some losses and expenses incurred by a comparatively small number of surveyed companies, such as costs stemming from the need to release a public statement about the incident.

Cost structure

After crunching the numbers, it appears that the lion's share of losses are caused by the incident itself — lost opportunities and profits, as well as payments to third-party remediation specialists, average out at $566,000. "Response" expenses for hiring and training staff, as well as updating the hardware and software infrastructure adds an additional average payment of $83,000. Incidentally, damages may vary depending on the region in which the targeted company operates. **For example, the largest damages were associated with incidents that involved companies operating in North America — an average of $818,000. The number was only slightly lower in South America at $813,000. Western Europe saw a lower, but still substantial average amount of losses from CYBER-attacks, coming in at $627,000.**

SME costs

The costs of a CYBER-attack against small and mid-sized enterprises are lower than for large corporations. Nonetheless, considering the smaller size of these companies, the amounts still deal a significant blow. The average loss resulting from IT security incidents for mid-sized companies came in at roughly $50,000, of which approximately $36,000 is accounted for by the incident itself, while the remaining $14,000 comes from other associated expenditures. The largest average losses from CYBER-attacks among small and mid-sized businesses were recorded at $96,000 for companies in Asia-Pacific. Second place went to companies in North America, with average losses of $82,000. The lowest losses from CYBER-attacks were seen in Russia, at $21,000 on average.

The survey also revealed that in some cases the financial losses incurred by small companies are accompanied by other losses amounting to approximately 5% of annual revenues. In one case, a company lost all of its business in a region where it had been successful prior to the incident.

Proper protection

A key lesson to be drawn from this study is that even the most destructive and expensive attacks could have been prevented. Attacks exploited holes in company security that could have been patched up if only the targeted corporations had used quality IT security solutions and managed IT infrastructure appropriately.

Typically, companies that have fallen prey to CYBER-attacks only come to understand the importance and value of these solutions after an incident occurs – meaning additional, preventable costs. A simple comparison of the scale of expenses against the costs and damages caused by a CYBER-attack shows that, in the overwhelming majority of cases, investment in quality, effective IT security would have been considerably less than the costs incurred following a breach.

9900: The Israeli Satellite Intelligence Unit

Source: http://i-hls.com/2013/11/9900-the-israeli-satellite-intelligence-unit/

The famous British philosopher and strategist Sir Basil Henry Liddell Hart, who coined the term "indirect approach strategy", used to say that "the deepest truth about war is that the outcome of battles is decided by the minds of opposing commanders, not by the bodies of soldiers," and that "to succeed in combat one must always keep one's intentions unclear, and strike the enemy when it least expects and where it is the most vulnerable." Based on that it can be determined with almost total certainty that "modern battles are decided by the minds of inventors and developers of advanced technologies, allowing for the implementation of new combat techniques that were considered science fiction only a few decades ago." The existence of the covert intelligence IDF unit 9900 supports this theory. The unit is referred to as "nine nine-hundred", or officially as

"the satellite unit" within the "visual intelligence formation", part of the Intelligence Division.

Precision, real time visual intelligence – that's the capability that is the most pivotal to winning battles, more than ever before. This unique intelligence is presented by 9900 not only to the analysts of the Intelligence Division, it is also given to field commanders so that they

can find out exactly what the enemy is doing anywhere in the battlefield, including areas beyond hilltops and in various dead zones. This information is gathered by 9900 using satellites orbiting the Earth, high above the combat arena. In addition to satellites, 9900 uses manned and unmanned aircraft, manned and unmanned surveillance, and advanced sensors capable of distinguishing between real and fake.

In the summer of 2010 the Ofek-9 intelligence satellite was successfully launched, joining the other defense establishment satellites in orbit: Ofek-5, Ofek-7, Eros A, Eros B, and one of the most advanced satellites in the world – TecSAR. Ofek-9 has unique targeting capabilities – it can track multiple targets simultaneously and in 3D, gather visual information through heavy cloud cover, receive and transmit visuals at night and during harsh weather conditions, display high-resolution images and cover wide areas. It has another unique capability – operators in Israel can aim its cameras at different targets no matter where it is in orbit. The satellite can receive commands from ground stations anywhere, not just directly below it. The connectivity between the Ofek-9, the TecSAR, and other defense satellites operating continuously, allows for surveillance of arenas and targets thousands of kilometers away from Israel, including Iran.

The satellite unit operators work in underground bunkers and control most of the long range intelligence arena, while the IDF uses unmanned aerial vehicles (UAVs) to gather intelligence in the short range. An example of 9900's abilities was presented in 2009 by then-commander of the IDF's visual array, Colonel Eli Polack, at a Fischer Institute and Science Ministry space exploration convention. During the convention a 3D model of the uranium enrichment facility in Netanz was displayed, including underground structures. "Without satellites Israel probably couldn't have operated at these ranges", said Polack.

It's no secret that Israel is a "satellite superpower". Israeli researchers explain that "seven countries today operate in space using their own knowledge and capabilities." Israel is right behind the U.S. in satellite quality and technologies, and it is one of the only states that manufactures both advanced satellites and their launchers. One of Israel's unique advantages is the development of lightweight satellites, almost the size of home refrigerators. An example of the Israeli expertise: France asked Israel to share its advanced technologies. According to the French offer Israel is supposed to build the satellite itself while France will manufacture the payload. In order to develop the payload France issued an international tender, and surprisingly the winner was El-Op, owned by the Israeli Elbit.

Using 9900's capabilities the IDF transmits 3D images of the targets to forces in the field. Using this information the soldiers know exactly where they're going: ground cover in the area, suspicious buildings, likely ambush spots and more. In addition, the unit supplies forces with detailed maps, not simple satellite photos but detailed 3D maps, which include all the important routes and targets.

9900 supplies real time information to all levels of the establishment: The political leadership, top military decision makers, battalion commanders and even smaller units. Since 9900 can monitor distant countries most of the demand for its information comes from the defense establishment. The unit's commander explains: "Information is sent out immediately after the request is received. We instantly aim a satellite camera at the requested zone. Since Israel has 10 satellites, each one orbiting the earth every hour and a half or so, we effectively have worldwide coverage. An Elbit system, for example, synchronizes surveillance activities in a certain order, and that's how we receive real time information."

Unit 9900 deals with more than just simple information gathering, it also assists complex operations undertaken by the IDF special forces and Air Force. "Today we know how to build an accurate, miniaturized model of the target, or run a 3D simulation, thus allowing fighters to understand how things actually look," adds the commander. "We assist all levels, from high command to soldiers in the field, while in the past we could only assist the high command."

The commander also adds that "Field units grew very familiar with our capabilities over the last few years, and their demands for our pre-operation assistance grew. Today we know how to send fighters in the field aerial photos under very short timetables. The images received by commanders reflects the reality. We update the information so that ground forces know everything down to the contents of every house and even room, what's happening in the area they're in and what they can expect along the way. Our specialty is not only information gathering, it's also streaming that information to where it's needed in real time."

9900 has received new information processing systems that allow it to fully utilize the gathered intelligence. The unit can receive requests from various IDF and intelligence community sources at any time, and assists in monitoring and documenting. In the past the unit had to process photos taken a few days before the operation, but now it can transmit images in real time even if the operation takes places thousands of kilometers away.

Emerging cyber threats report 2014

Source: http://www.gtsecuritysummit.com/2014Report.pdf#!

Losing Control of Cloud Data

As companies move data to the cloud, trade-offs between security and usability hamper business

Highlights:

• Business data is regularly stored in the cloud without any security beyond that provided by the cloud storage firm

• While private-key encryption is an option, encrypting data in the cloud robs businesses of much of the cloud's utility

• Searchable encryption continues to have trade-offs between security, functionality, and efficiency

Insecure But Connected Devices

The "Internet of Things" continues to expand, but security remains untested

Highlights:

• Detecting compromised and counterfeit devices continues to be resource intensive, though research on fingerprinting devices has advanced

• Companies need to evaluate the security of their suppliers as well as their own security

• Critical infrastructure companies must find better ways to secure their devices and prevent possible outages

• The Internet of Things will have an unprecedented view into people's lives, but will be difficult to secure after the fact,

Attackers Adapt to Mobile Ecosystems

While mobile platforms have largely been safe for consumers and businesses, researchers and attackers are finding ways around the ecosystems' security

Highlights:

• As sensors—and not just computing platforms—mobile devices bring a new set of threats, including allowing malicious software an unparalleled look into victims' lives

• Employee-owned devices make platform-specific security difficult, suggesting that focusing on protecting data may be more effective

• Researchers and attackers have found ways to bypass the inherent security of the "gated community" of app stores
• The implications to society of tracking ubiquitous mobile devices is not well understood, and U.S. courts have not yet come to a consensus on government access to the data

Costs of Defending Against Cyber Attacks Remain High

Mitigating the risk of cyber attacks continues to be uncertain and costly, but gaining better visibility into threats and mitigating specific risks can help

Highlights:

• Chasing technology and creating multiple layers of static defenses has driven up security costs
• Companies need to focus on gaining visibility into their networks and the external threats targeting their business
• Shifting focus from devices to data can simplify defensive concepts and better cope with the bring-your own-device (BYOD) trend, but usability continues to be a problem
• While the market for cyber insurance is growing, fundamental problems continue to prevent broad acquisition of policies to mitigate risk

Information Manipulation Advances

Online recommendation and reputation systems increase in importance while threats to them mature

Highlights:

• As companies and governments rely more on data and intelligence to operate efficiently, information manipulation will become an increasingly important attack
• With reputation increasingly being used to make security decisions, attackers will continue attempts to poison or whitewash reputation
• Using cross-site request forgery, unscrupulous website owners can inject higher-value content to poison the profile of visitors and profit by fooling advertising networks
• Techniques for using information pollution and manipulation could be used to hide or camouflage attacks.

► **Read the full report at source's URL**

Cyberattack Trends in Latin America

By Holly Gilbert

Source: http://www.securitymanagement.com/print/12859

Latin America is experiencing tremendous growth—unfortunately the growth in question relates to cyberattacks. "If you look at Peru, you see 28 times as much malware in 2012 as in 2011; Mexico about 16 times; Brazil about 12 times; Chile about 10; and Argentina about seven times," said Andrew Lee, CEO of ESET. These tremendous growth rates are expected to continue in the coming years, Lee noted.

Lee was talking specifically about mobile malware, especially on Android operating systems. The landscape for these types of attacks is broadening at a rapid pace, with more than 1.3 million new Android activations worldwide each day. "If we look at the evolution of Android malware, it's kind of mirrored the evolution of the mobile platform; it's gone from being clunky and fairly low in function to very sophisticated and a very high-end function," he said.

That's just one aspect of the cyber threatscape analyzed by Lee and other panelists during a panel discussion titled "Emerging Threats and Trends: The Latin American Landscape." The panel was part of the SegurInfo conference in Washington, D.C. The conference was hosted by the Organization of American States (OAS), which was originally established in 1948 to promote peace and justice in the Americas.

Another panelist was Tom Kellermann, vice president of cybersecurity at Trend Micro, a network security solutions company. He discussed a report that Trend Micro released jointly with OAS called Latin

American and Caribbean Cybersecurity Trends and Government Responses.

Kellermann noted that while organized crime groups, such as narco-traffickers, have embraced cybercrime, the governments of Latin American countries haven't been able to keep up in terms of defending against this type of crime. "Only two out of five countries have an effective cybercrime law, let alone effective law enforcement to hunt [cyberattackers]," he said.

Another finding was that Latin America is experiencing tremendous growth in the area of Web-based attacks, as well as custom attacks against the financial sector and industrial control systems, the latter of which are used in utilities and critical infrastructure. These are being heavily targeted now with hundreds of attacks daily, according to Kellermann.

Also highlighted in the report is the emergence of underground markets for dealing in cybercrime tools and expertise in Latin America. Hackers are "distributing weapons in this community through various blogs and many social networking and social media sites," according to Kellermann.

"Now there are wholesale arms bazaars that are widely available specific to Latin America that allow you to leverage the latest attack capabilities. For example, for less than $600, you can leverage attacks that can bypass most of the perimeter defenses that are established by most organizations under ISO standards," Kellermann explains.

Another issue is the lack of sophisticated defenses in place, leaving systems vulnerable to older malware that might not be effective in other countries and regions. "We've found, surprisingly, that Configure, an old polymorphic worm, is still very prevalent in the region," Kellermann said. "This can be due to a lot of reasons, but I think the largest part is going to be the lack of vulnerability management by users, partners, and ecosystems in the region."

In discussing the mobile threat, Lee cited SMS Trojans as one of the most common cyberattack vectors in Latin America. He specifically noted the existence of Boxer, a variant that has been detected in the region. With this particular SMS Trojan, users unwittingly download malware to their mobile devices by opening a text message that appears to be coming from a known sender. "Then that [mobile device] will start sending SMS on your behalf to a premium malware vendor," sccording to Lee. "Ultimately this is a very simple attack. It's become very prevalent because it works—it works very well—and the attacker makes a lot of money from it."

Lee explained that Latin America has seen an increase in tailored malware attacks. The hallmark of these types of attacks is that the hackers slightly modify the malicious software over time in order to increase the likelihood of a successful attack. Each version of the malware that the hackers produce is adjusted to provide a more effective attack or to evade detection. "[T]here's been a lot of work put into the development of those pieces of malware," Lee attests.

Also on the panel was Kevin Haley, director of product management at Symantec Security Response. He spoke in general about the threat that arises when hackers leverage smaller businesses to get to the intellectual property of larger organizations. This is a trend that is explained in Symantec's latest annual Internet Security Threat Report.

"If you look by industry at who's being attacked, the most growth we saw in 2012 was actually manufacturers, and that growth was mainly due to small manufacturers being attacked," noted Haley. "The bad guys are going after the small manufacturers to learn the secrets that their larger partners are sharing with them."

As far back as 2004, OAS did establish guidelines for fighting cybercrime in the Latin American region when it adopted the Inter-American Cyber Security Strategy that founded a multidisciplinary approach to cybersecurity. However, as the Trend Micro report on the region pointed out, the guidelines have not made the desired headway. The paper recommends further action. For example, the report urges governments to raise awareness among critical infrastructure operations and government agencies, offer more cyber education, and further institutionalize cybersecurity practices and regulations.

Haley added that any multipronged cybersecurity strategy should include law enforcement and diplomacy.

FBI: Cyber-attacks surpassing terrorism as major domestic threat

Source: http://rt.com/usa/fbi-cyber-attack-threat-739/

FBI Director James Comey testifies before the Senate Homeland Security Committee hearing on "Threats to the Homeland", on Capitol Hill in Washington November 14, 2013. (Reuters / Yuri Gripas)

Cyber-attacks are increasingly becoming the primary threat against the United States, according to the head of the FBI.

During his first testimony as the new FBI director, James Comey told Congress on Thursday that while the threat of traditional terrorist strikes inside the United States is now lower than it was before 2001, the potential threat from cyber-attacks continues to rise.

"That's where the bad guys will go," Comey said, as quoted by the Guardian. *"There are no safe neighborhoods. All of us are neighbors [online]."*

Comey's comments were echoed by Rand Beers, the acting secretary for the Department of Homeland Security, and Matt Olsen, the director of the National Counterterrorism Center, both of whom also testified before the Senate Homeland Security and Government Affairs Committee.

The three officials agreed that while the potential for an attack on the scale of 9/11 is more likely to occur overseas, Congress should be wary of rolling back surveillance programs like the one employed by the National Security Agency. **Over the next decade, cyber-attacks are likely to become the primary domestic threat, they said.**

The officials added that any changes to the US surveillance program should be on the *"margins,"* and not directly affect the agencies' *"core capabilities."*

In fact, Beers and Comey both pushed Congress to expand the government's power to gain access to data held by privately owned companies, with Beers suggesting that new legislation grant corporations liability protection for sharing sensitive information with federal agencies.

According to the Guardian, at least one senator, Tom Coburn (R-Okla.), expressed concern over the suggestion, saying that companies should have the chance to willingly cooperate with the government before being told to hand over data.

In 2008, the US passed legislation protecting telecommunications companies and internet providers helping the government conduct warrantless surveillance from privacy lawsuits.

USA Today reported that the officials noted how difficult it is to detect self-radicalized terrorists, and that Americans are urged to report something suspicious when they see it.

"The challenge of the home-grown violent extremist is that [the person] really doesn't hit all the trip wires," Olsen said.

► Read also the comments at the end of the article at source's URL. **Interesting!**

Hacktivists have been stealing information from U.S. computers for a year

Source: http://www.homelandsecuritynewswire.com/dr20131122-hacktivists-have-been-stealing-information-from-u-s-computers-for-a-year

The Federal Bureau of Investigation (FBI) reports that activist hackers linked to the group Anonymous have been accessing the computers of numerous government agenciesfor almost a year, and stealing sensitive information. The hackers took advantage of a flaw in Adobe Systems Inc's ColdFusion software to launch a series of intrusions which began December 2012, and then left "back doors" to return to the computers

multiple times, as recent as last month.

ColdFusion is an Adobe software used by several companies to build Web sites. Adobe spokeswoman Heather Edell, said the majority of attacks involving ColdFusion have exploited systems which were not updated with the latest security patches.

CRN reports that according to an FBI memo, the FBI described the attacks as "a widespread problem that should be addressed." The security breach is said to have affected the U.S. Army, Department of Energy (DOE), Department of Health and Human Services (HHS), and perhaps several other agencies.

The FBI continues to gather information to understand the scope of the case, and the agency has issued a notice to system administrators providing methods to determine whether a system has been compromised.

Reuters reports that an internal e-mail from Kevin Knobloch, chief of staff for Energy Secretary Ernest Moniz, notes that the stolen data included personal information on at least 104,000 employees and individuals associated with DOE, along with information in almost 2,000 bank accounts.

Previous intrusions by Anonymous include the attack on Sony which disrupted its PlayStation network for weeks; the assault on PayPal after PayPal stopped processing donations to anti-government privacy site, Wikileaks; and an attack on security firm HBGary in which thousands of sensitive emails were leaked to the public.

CRN notes that members of Anonymous have claimed that their recent attacks were in retaliation for the prosecution of hackers, including Jeremy Hammond, who was sentenced last week to ten years in prison for his role in the attacks on the private security intelligence firm Stratfor. Stratfor acknowledged that its systems were breached and hackers used stolen credit card data to charge $700,000 worth of fraudulent donations to nonprofit groups.

"The majority of the intrusions have not yet been made publicly known," according to the FBI. "It is unknown exactly how many systems have been compromised, but it is a widespread problem that should be addressed."

Stuxnet's Secret Twin

By Ralph Langner

Source:http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack?page=0,2&goback=.gde_1528217_member_580942631673427558 6

Three years after it was discovered, Stuxnet, the first publicly disclosed cyberweapon, continues to baffle military strategists, computer security experts, political decision-makers, and the general public. A comfortable narrative has formed around the weapon: how it attacked the Iranian nuclear facility at Natanz, how it was designed to be undiscoverable, how it escaped from Natanz against its creators' wishes. Major elements of that story are either incorrect or incomplete.

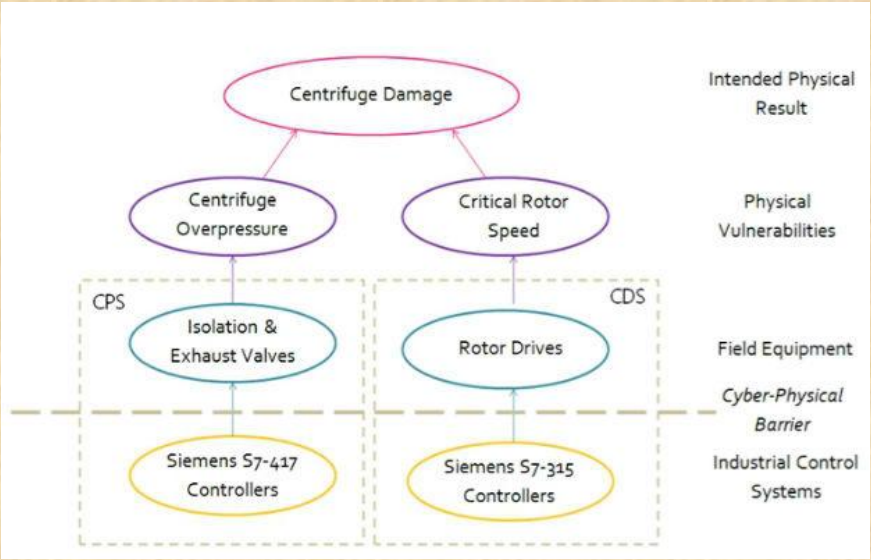
That's because Stuxnet is not really one weapon, but two. The vast majority of the attention has been paid to Stuxnet's smaller and simpler attack routine -- the one that changes the speeds of the rotors in a centrifuge, which is used to enrich uranium. But the second and "forgotten" routine is about an order of magnitude more complex and stealthy. It qualifies as a nightmare for those who understand industrial control system security. And strangely, this more sophisticated attack came *first*. The simpler, more familiar routine followed only years later -- and was discovered in comparatively short order.

With Iran's nuclear program back at the center of world debate, it's helpful to understand with more clarity the attempts to digitally sabotage that program. Stuxnet's actual impact on the Iranian nuclear program is unclear, if only for the fact that no information is available on how many controllers were actually infected. Nevertheless, forensic analysis can tell us what the attackers *intended* to achieve, and how. I've spent the last three years conducting that analysis -- not just of the computer code, but of the physical characteristics of the plant environment that was attacked and of the process that this nuclear plant operates. What I've found is that the full picture, which includes the first and lesser-known Stuxnet variant, invites a re-evaluation of the attack. It turns out that it was far more dangerous than the cyberweapon that is now lodged in the public's imagination.

***

In 2007, an unidentified person submitted a sample of code to the computer security site VirusTotal. It later turned out to be the first variant of Stuxnet -- at least, the first one that we're aware of. But that was only realized five years later, with the knowledge of the second Stuxnet variant. Without that later and much simpler version, the original Stuxnet might still today sleep in the archives of anti-virus researchers, unidentified as one of the most aggressive cyberweapons in history. Today we now know that the code contained a payload for severely interfering with the system designed to protect the centrifuges at the Natanz uranium-enrichment plant.

Stuxnet's later, and better-known, attack tried to cause centrifuge rotors to spin too fast and at speeds that would cause them to break. The "original" payload used a different tactic. It attempted to overpressurize Natanz's centrifuges by sabotaging the system meant to keep the cascades of centrifuges safe. "Protection systems" are used anywhere where abnormal process conditions can result in equipment damage or threaten the health of operators and the environment. At Natanz, we see a unique protection system in place to enable sustained uranium enrichment using obsolete and unreliable equipment: the IR-1 centrifuge. This protection system is a critical component of the Iranian nuclear program; without it, the IR-1s would be pretty much useless.



The IR-1 centrifuge is the backbone of Iran's uranium-enrichment effort. It goes back to a European design from the late 1960s and early 1970s that was stolen and slightly improved by Pakistani nuclear trafficker A.Q. Khan. The IR-1 is an all-metal design that *can* work reliably. That is, if parts are manufactured with precision and critical components such as high-quality frequency converters and constant torque drives are available. But the Iranians never managed to get a high degree of reliability from the obsolete design. So they had to lower the operating pressure of the centrifuges at Natanz. Lower operating pressure means less mechanical stress on the delicate centrifuge rotors, thereby reducing the numbers of centrifuges that have to be put offline because of rotor damage. But less pressure means less throughput -- and thus less efficiency. At best, the IR-1 was half as efficient as its ultimate predecessor.

As unreliable and inefficient as the IR-1 is, it offered a significant benefit: Iran managed to produce the antiquated design at industrial scale. Iran compensated reliability and efficiency with volume, accepting a constant breakup of centrifuges during operation because they could be manufactured faster than they crashed. But to make it all work, the Iranians needed a bit of a hack. Ordinarily, the operation of fragile centrifuges is a sensitive industrial process that doesn't tolerate even minor equipment hiccups. Iran built a cascade protection system that

allows the enrichment process to keep going, even when centrifuges are breaking left and right.
At the centrifuge level, the cascade protection system uses sets of three shut-off valves, installed for every centrifuge. By closing the valves, centrifuges that run into trouble -- indicated by vibration -- can be isolated from the rest of the system. Isolated centrifuges are then run down and can be replaced by maintenance engineers while the process keeps running.

Then-President Mahmoud Ahmadinejad looks at SCADA screens in the control room at Natanz in 2008. The screen facing the photographer shows that two centrifuges are isolated, indicating a defect, but that doesn't prevent the respective cascade from continuing operation (red highlighting added).

But the isolation valves can turn into as much of a problem as a solution. When operating basically unreliable centrifuges, one will see shut-offs frequently, and maintenance workers may not have a chance to replace damaged centrifuges before the next one in the same enrichment stage gets isolated. Once multiple centrifuges are shut off within the same stage, operating pressure -- the most sensitive parameter in uranium enrichment using centrifuges -- will increase, which can and will lead to all kinds of problems.
The Iranians found a creative solution for this problem -- basically another workaround on top of the first workaround. For every enrichment stage, an exhaust valve is installed that allows pressure to be relieved if too many centrifuges within that stage get isolated, causing pressure to increase. For every enrichment stage, pressure is monitored by a sensor. If the pressure exceeds a certain threshold, the exhaust valve is opened, and overpressure is released.
The system might have keep Natanz's centrifuges spinning, but it also opened them up to a cyberattack that is so far-out, it leads one to wonder whether its creators might have been on drugs.
Natanz's cascade protection system relies on Siemens S7-417 industrial controllers to operate the valves and pressure sensors of up to six cascades, or groups of 164 centrifuges each. A controller can be thought of as a small embedded computer system that is directly connected to physical equipment, such as valves. Stuxnet was designed to infect these controllers and take complete control of them in a way that previous users had never imagined -- and that had never even been discussed at industrial control system conferences.
A controller infected with the first Stuxnet variant actually becomes decoupled from physical reality. Legitimate control logic only "sees" what Stuxnet wants it to see. Before the attack sequence executes (which is approximately once per month), the malicious code is kind enough to show operators in the control room the physical reality of the plant floor. But that changes during attack execution.
One of the first things this Stuxnet variant does is take steps to hide its tracks, using a trick straight out of Hollywood. Stuxnet records the cascade protection system's sensor values for a period of 21 seconds. Then it replays those 21 seconds in a constant loop during the execution of the attack. In the control room, all appears to be normal, both to human operators and any software-implemented alarm routines.
Then Stuxnet begins its malicious work. It closes the isolation valves for the first two and last two enrichment stages. That blocks the outflow of gas from each affected cascade and, in turn, raises the pressure on the rest of the centrifuges. Gas centrifuges for uranium enrichment are extremely sensitive to increases of pressure above near vacuum. An increase in pressure will result in more uranium hexafluoride getting into the centrifuge, putting higher mechanical stress on the rotor. Rotor wall pressure is a function of velocity (rotor speed) and operating pressure; more gas being pressed against the rotor wall means more mechanical force against the thin tube. Ultimately, pressure may cause the gaseous uranium hexafluoride to solidify, thereby fatally damaging centrifuges.

The attack continues until the attackers decide that enough is enough, based on monitoring centrifuge status. Most likely, they would use vibration sensors, which let them abort a mission before the matter hits the fan. If catastrophic destruction is intended, one simply has to sit and wait. But in the Natanz case, causing a solidification of process gas would have resulted in simultaneous destruction of hundreds of centrifuges per infected controller. While at first glance this might sound like a goal worthwhile achieving, it would also have blown the attackers' cover; the cause of the destruction would have been detected fairly easily by Iranian engineers in postmortem analysis. The implementation of the attack with its extremely close monitoring of pressures and centrifuge status suggests that the attackers instead took great care to *avoid* catastrophic damage. The intent of the overpressure attack was more likely to increase rotor stress, thereby causing rotors to break early -- but not necessarily during the attack run.

Nevertheless, the attackers faced the risk that the attack would not work at all because the attack code is so overengineered that even the slightest oversight or any configuration change would have resulted in zero impact or, worse, in a program crash that would have been detected by Iranian engineers quickly.

The results of the overpressure attack are unknown. Whatever they were, the attackers decided to try something different in 2009.

This new Stuxnet variant was almost entirely different from the old one. For one thing, it was much simpler and much less stealthy than its predecessor. It also attacked a completely different component of the Natanz facility: the centrifuge drive system that controls rotor speeds.

This new Stuxnet spread differently too. The malware's earlier version had to be physically installed on a victim machine, most likely a portable engineering system, or it had to be passed on a USB drive carrying an infected configuration file for Siemens controllers. In other words, it needed to be disseminated deliberately by an agent of the attackers.

The new version self-replicated, spreading within trusted networks and via USB drive to all sorts of computers, not just to those that had the Siemens configuration software for controllers installed. This suggests that the attackers had lost the capability to transport the malware to its destination by directly infecting the systems of authorized personnel, or that the centrifuge drive system was installed and configured by other parties to which direct access was not possible.

What's more, Stuxnet suddenly became equipped with an array of previously undiscovered weaknesses in Microsoft Windows software -- so-called "zero day" flaws that can fetch hundreds of thousands of dollars on the open market. The new Stuxnet also came equipped with stolen digital certificates, which allowed the malicious software to pose as legitimate driver software and thus not be rejected by newer versions of the Windows operating system.

All this indicates that a new organization began shaping Stuxnet -- one with a stash of valuable zero days and stolen certificates. In contrast, the development of the overpressure attack can be viewed as the work of an in-group of top-notch industrial control system security experts and coders who lived in an exotic ecosystem quite remote from standard IT security. The overspeed attacks point to the circle widening and acquiring a new center of gravity. If Stuxnet is American-built -- and, according to published reports, it most certainly is -- then there is only one logical location for this center of gravity: Fort Meade, Maryland, the home of the National Security Agency.

But the use of the multiple zero days came with a price. The new Stuxnet variant was much easier to identify as malicious software than its predecessor was, because it suddenly displayed very strange and very sophisticated behavior. In comparison, the initial version looked pretty much like a legitimate software project for Siemens industrial controllers used at Natanz; the only strange thing was that a copyright notice and license terms were missing. The newer version, equipped with a wealth of exploits that hackers can only dream about, signaled to even the least vigilant anti-virus researcher that this was something big, warranting a closer look.

Just like its predecessor, the new attack operated periodically, about once per month, but the trigger condition was much simpler. While in the overpressure attack various process parameters were monitored to check for conditions that might occur only once in a blue moon, the new attack was much more straightforward.

The new attack worked by changing rotor speeds. With rotor wall pressure being a function of process pressure and rotor speed, the easy road to trouble is to overspeed the rotors, thereby increasing rotor wall pressure. And this is what Stuxnet did. The normal operating speed of the

IR-1 centrifuge is 63,000 revolutions per minute (rpm). Stuxnet increased that speed by a good one-third to 84,600 rpm for 15 minutes. The next consecutive run brought all centrifuges in the cascade basically to a stop (120 rpm), only to speed them up again, taking a total of 50 minutes. The IR-1 is a supercritical design, meaning that the rotor has to pass through so-called critical speeds before reaching normal operating speed. Every time a rotor passes through these critical speeds, also called harmonics, it can break.

If a single rotor did crack during an attack sequence, the cascade protection system would kick in to isolate and run down the respective centrifuge. But if multiple rotors were to crash -- a likely possible outcome -- Iranian operators would be left with the question of why all of a sudden so many centrifuges broke at once. Not that they didn't have enough new ones in stock for replacement, but unexplained problems like this are among any control system engineer's most frustrating experiences, usually referred to as *chasing a demon* in the machine.

At some point the attacks should have been recognizable by plant floor staff just by the old eardrum. Bringing 164 centrifuges or multiples thereof from 63,000 rpm to 120 rpm and getting them up to speed again would have been noticeable -- if experienced staff had been cautious enough to remove protective headsets in the cascade hall. It's another sign that the makers of this second Stuxnet variant had decided to accept the risk that the attack would be detected by operators.

***

Much has been written about the failure of Stuxnet to destroy a substantial number of centrifuges or to significantly reduce Iran's enriched-uranium production. While that is undisputable, it doesn't appear that either was the attackers' intention. If catastrophic damage had been caused by Stuxnet, that would have been by accident rather than on purpose. The attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention of reducing the lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding.

Reasons for such tactics are not difficult to identify. When Stuxnet was first deployed, Iran had already mastered the production of IR-1 centrifuges at industrial scale. During the summer of 2010, when the Stuxnet attack was in full swing, Iran operated about 4,000 centrifuges, but kept another 5,000 in stock, ready to be commissioned. A one-time destruction of the Iranians' operational equipment would not have jeopardized that strategy, just like the catastrophic destruction of 4,000 centrifuges by an earthquake back in 1981 did not stop Pakistan on its way to getting the bomb. By my estimates, Stuxnet set back the Iranian nuclear program by two years; a simultaneous catastrophic destruction of all operating centrifuges wouldn't have caused nearly as big a delay.

Centrifuge inventory at Natanz between 2008 and 2010. Iran constantly kept a stockpile of at least 50 percent spare centrifuges, invalidating the idea that a simultaneous catastrophic destruction of all operating centrifuges would have meant the end of its nuclear ambitions.

The low-yield approach also offered added value. It drove Iranian engineers crazy, up to the point where they might have ultimately ended up in total frustration about their capabilities to get a stolen plant design from the 1970s running and to get value from their overkill digital protection system.

When comparing the Pakistani and Iranian uranium-enrichment programs, one cannot fail to notice a major performance difference. Pakistan basically managed to go from zero to successful low-enriched uranium production within just two years during shaky economic

times, without the latest in digital control technology. The same effort took Iran over 10 years, despite the jump-start from Pakistan's A.Q. Khan network and abundant money from sales of crude oil. If Iran's engineers didn't look incompetent before, they certainly did during the time when Stuxnet was infiltrating their systems.

Legend has it that in the summer of 2010, while inflicting its damage on Natanz, Stuxnet "escaped" from the nuclear facility due to a software bug that came with a version update. While that is a good story, it cannot be true. Stuxnet propagated only between computers that were attached to the same local network or that exchanged files though USB drives. In other words, Stuxnet must have spread largely by human hands. But in these days of remote access by modem or via Internet virtual private networks, human hands can extend across continents.

Contractors serving at Natanz worked for other clients as well. And those contractors most likely carried their Stuxnet-infected laptop computers to their secondary clients and connected their laptops to the clients' "local" networks. Let's say they spread it to a cement plant. That cement plant then had other contractors, who in turn connected their mobile computers to the infected "local" network. Those computers carried the malware farther -- to another cement plant, maybe in another country. At some link in the chain, infected contractors or employees remotely accessed their machines, allowing the virus to travel over continents. All of a sudden, Stuxnet has made its way around the globe -- not because of the fact that billions of systems are connected to the Internet, but because of the trusted network connections that tunnel through the Internet these days. For example, remote maintenance access often includes the capability to access shared folders online, giving Stuxnet a chance to traverse through a secure digital tunnel. My colleagues and I saw exactly that when we helped Stuxnet-infected clients in industries completely unrelated to the nuclear field back in 2010.

Given that Stuxnet reported Internet protocol addresses and hostnames of infected systems back to its command-and-control servers, it appears that the attackers were clearly anticipating (and accepting) a spread to noncombatant systems and were quite eager to monitor that spread closely. This monitoring would eventually deliver information on contractors working at Natanz, their other clients, and maybe even clandestine nuclear facilities in Iran.

Stuxnet also provided a useful blueprint to future attackers by highlighting the royal road to infiltration of hard targets. Rather than trying to infiltrate directly by crawling through 15 firewalls, three data diodes, and an intrusion detection system, the attackers acted indirectly by infecting soft targets with legitimate access to ground zero: contractors. However seriously these contractors took their cybersecurity, it certainly was not on par with the protections at the Natanz fuel-enrichment facility. Getting the malware on the contractors' mobile devices and USB sticks proved good enough, as sooner or later they physically carried those on-site and connected them to Natanz's most critical systems, unchallenged by any guards.

Any follow-up attacker will explore this infiltration method when thinking about hitting hard targets. The sober reality is that at a global scale, pretty much every single industrial or military facility that uses industrial control systems at some scale is dependent on its network of contractors, many of which are very good at narrowly defined engineering tasks, but lousy at cybersecurity. While experts in industrial control system security had discussed the insider threat for many years, insiders who unwittingly helped deploy a cyberweapon had been completely off the radar. Until Stuxnet.

And while Stuxnet was clearly the work of a nation-state -- requiring vast resources and considerable intelligence -- future attacks on industrial control and other so-called "cyber-physical" systems may not be. Stuxnet was particularly costly because of the attackers' self-imposed constraints. Damage was to be disguised as reliability problems. I estimate that well over 50 percent of Stuxnet's development cost went into efforts to hide the attack, with the bulk of that cost dedicated to the overpressure attack which represents the ultimate in disguise - at the cost of having to build a fully-functional mockup IR-1 centrifuge cascade operating with real uranium hexafluoride. Stuxnet-inspired attackers will not necessarily place the same emphasis on disguise; they may *want* victims to know that they are under cyberattack and perhaps even want to publicly claim credit for it.

And unlike the Stuxnet attackers, these adversaries are also much more likely to go after civilian critical infrastructure. Not only are these systems more accessible, but they're standardized. Each system for running a power plant or a chemical factory is largely configured like the next. In fact, all modern plants operate with standard industrial control system architectures and products from just a handful of vendors per industry, using similar or even identical

configurations. In other words, if you get control of one industrial control system, you can infiltrate dozens or even hundreds of the same breed more.

***

Looking at the two major versions of Stuxnet in context leaves a final clue -- a suggestion that during the operation, something big was going on behind the scenes. Operation Olympic Games -- the multiyear online espionage and sabotage campaign against the Iranian nuclear program -- obviously involved much more than developing and deploying a piece of malware, however sophisticated that malware was. It was a campaign rather than an attack, and it appears that the priorities of that campaign shifted significantly during its execution.

When my colleagues and I first analyzed both attacks in 2010, we first assumed that they were executed simultaneously, maybe with the idea to disable the cascade protection system during the rotor-speed attack. That turned out to be wrong; no coordination between the two attacks can be found in the code. Then we assumed that the attack against the centrifuge drive system was the simple and basic predecessor after which the big one was launched, the attack against the cascade protection system. The cascade protection system attack is a display of absolute cyberpower. It appeared logical to assume a development from simple to complex. Several years later, it turned out that the opposite was the case. Why would the attackers go back to basics?

The dramatic differences between both versions point to changing priorities that most likely were accompanied by a change in stakeholders. Technical analysis shows that the risk of discovery no longer was the attackers' primary concern when starting to experiment with new ways to mess up operations at Natanz. The shift of attention may have been fueled by a simple insight: Nuclear proliferators come and go, but cyberwarfare is here to stay. Operation Olympic Games started as an experiment with an unpredictable outcome. Along the road, one result became clear: *Digital weapons work*. And different from their analog counterparts, they don't put military forces in harm's way, they produce less collateral damage, they can be deployed stealthily, and they are dirt cheap. The contents of this Pandora's box have implications much beyond Iran; they have made analog warfare look low-tech, brutal, and *so 20th century*.

In other words, blowing the cover of this online sabotage campaign came with benefits. Uncovering Stuxnet was the end of the operation, but not necessarily the end of its utility. Unlike traditional Pentagon hardware, one cannot display USB drives at a military parade. The Stuxnet revelation showed the world what cyberweapons could do in the hands of a superpower. It also saved America from embarrassment. If another country -- maybe even an adversary -- had been first in demonstrating proficiency in the digital domain, it would have been nothing short of another Sputnik moment in U.S. history. So there were plenty of good reasons not to sacrifice mission success for fear of detection.

We're not sure whether Stuxnet was disclosed intentionally. As with so many human endeavors, it may simply have been an unintended side effect that turned out to be critical. One thing we do know: It changed global military strategy in the 21st century.

Ralph Langner began his research on Stuxnet in 2010. He is a principal with the Langner Group, a cyberdefense consultancy, and a non-resident fellow with the Brookings Institution.

Inside the Clever Hack That Fooled the AP and Caused the DOW to Drop 150 Points

Source: http://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused-the-dow-to-drop-150-points-2013-11?goback=.gde_4709642_member_5809990367986085888#!

Back in April, agents of the Syrian Electronic Army took control of the Associated Press official Twitter account and punched out a single tweet.

"Breaking: Two Explosions in the White House and Barack Obama was injured"

The AP Corporate Communications account quickly tried to mitigate the damage, tweeting, "That is a bogus @AP tweet."

The initial tweet cost the DOW 150 points, which it later recovered when the news was rectified. Nonetheless, it was a huge PR victory for SEA.

Kevin Mandia, CEO of Mandiant — the company that outed China's super-secret military hacking unit — recently talked at a National Military Family Association event and explained exactly how the SEA breached the

Associated Press twitter account.

"I just wanted to share with you the details of the attack, to see the ingenuity behind these people," said Mandia, who got his start in Air Force signals intelligence.

"[First] they sent a spearfishing email to approximately ten people at a media company," said Mandia, referring to the Associated Press. "Spearfishing is a fake email, you're purporting to be someone you're not and the content is a ruse to getting someone to do something, click on a link or open a document."

The email looked like a newsbreak from the United Nations, telling the reporters to check out an article from the Washington Post. Mandia notes that the hackers "did their homework," and even used a name from a real person in the U.N.

Inside the email was a hyperlink that ostensibly led to the WaPo article. Instead, the url led to a site mirroring the login for Outlook, the email platform AP reporters use.

"To the unwitting victim, [they think] 'oh I got an email from the United Nations about something, let me click on this link,' and what they got was a new login back into their email, and their conclusion was, 'hey I just got kicked out of my email,' so they typed in their user ID and password and 'logged back in' to the email, but what they were really doing was giving the Syrian Electronic Army access to their email."

"It took them less than ten minutes to get the information," Mandia said.

The journalists that fell for it quickly filled out the field's like normal and clicked "login in," which then sent the info to the hackers.

That's how the SEA got the access codes to the official Twitter, but, as Mandia points out, they could have done much worse.

"The real problem with this isn't that they tweeted something, it's that they now know the contact list of all the Syrian rebels who are emailing western reporters," said Mandia.

Mandia contends that the SEA is much more advanced than people think.

"Is that a non-fancy attack? Well ... it worked, and it worked in less than ten minutes," said Mandia. As for the SEA's M-O being media attacks, he thinks they're capable of worse.

"Now imagine if we had attacked Syria, I think they're rules of engagement would change," said Mandia.

NATO holds largest-ever cyber security exercises

Source: http://www.presstv.ir/detail/2013/11/27/336878/nato-holds-cyber-defense-exercises/

File photo shows soldiers sitting in front of computers at the NATO airbase in the German town of Geilenkirchen.
Wed Nov 27, 2013 2:15AM GMT

The North Atlantic Treaty Organization (NATO) has started its largest-ever cyber security exercises to practice thwarting large and simultaneous attacks on member states and their partners.

The defense exercises, which started on Tuesday and are scheduled to continue until November 28, are based at the alliance's cyber defense center in Estonia, Russia Today reported.

Codenamed Cyber Coalition 2013, the exercises involve participants from more than 30 countries across Europe, including five non-NATO nations: Austria, Finland, Ireland, Sweden, and Switzerland. New Zealand and the European Union have observer status.

According to NATO, around 300 cyber defense experts will take part in the operation from their home countries and partner nations while an additional 80 experts will work from the military training facility in the Estonian city of Tartu.

The exercises are aimed at training technical personnel and their leadership as well as testing the capability of NATO and its partners to coordinate their efforts in foiling multiple simulated cyber attacks.

"Cyber attacks are a daily reality and they are growing in sophistication and complexity. NATO has to keep pace with this evolving threat and Cyber Coalition 2013 will allow us to fully test our systems and procedures to effectively defend our networks - today and in the future," said Jamie Shea, the deputy assistant secretary general for emerging security challenges at NATO.

Reports say that the exercises' scenario includes simulated multiple, simultaneous attempts to infiltrate information networks with diverse cyber warfare techniques.

NATO has not decided yet if a cyber attack against one member would require a collective response as outlined under Article 5 of the Washington Treaty. Currently, cyber security is regarded as a national responsibility. Estonia has hosted the NATO Cooperative Cyber Defense Center of Excellence since 2008, after a series of cyber attacks on the country in April 2007, which targeted the websites of the Estonian parliament, banks, ministries, newspapers and broadcasters.

Earlier in November, NATO held the Steadfast Jazz military drill, which involved 6,000 soldiers from the Western military alliance as well as non-members Sweden, Finland and Ukraine.

Western officials said the drills would examine the capability of NATO's rapid reaction force to respond to a difficult crisis on its northern borders.

The military exercise came after Russia held massive maneuvers with Belarus in September.

Cyber Weapons and International Stability: New Destabilization Threats Require New Security Doctrines

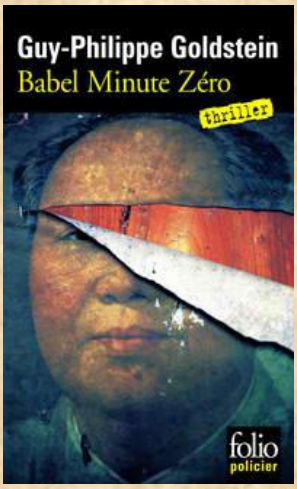
By Guy-Philippe Goldstein

Source: http://i-hls.com/2013/11/cyber-weapons-and-international-stability-new-destabilization-threats-require-new-security-doctrines/

Though cyberspace is a domain of strategic importance, cyber weapons have not yet been associated with publicly well-enunciated doctrines of use comparable to that of the nuclear age. Taking two very different approaches from the strategic literature—Jervis' security dilemma and Zagare & Kilgoure's perfect deterrence model—cyber weapons are demonstrated in both cases to induce a higher level of international instability. In particular, instability is favored by the attribution issue and the lack of clear thresholds. The outline of a cyber-defense doctrine, focusing on the two mentioned informational issues, is then suggested.

In 2013 cyberspace is a domain of strategic importance. The threat of cyber-attacks has been placed at the top of the list of national security risks in the "Intelligence Community

Worldwide Threat Assessment of 2013," and computer network warfare is one of the only military areas in both the US and in NATO countries that is expected to grow.3 Beginning in 2009, the United States Cyber Command, for example, was established as a unified command under the United States Strategic Command. As was stated qUASi-officially by the *Wall Street Journal* in June 2011, computer sabotage that is generated in another country is sometimes considered by the Pentagon as an act of war. In that sense, since the effects of cyber weaponry could be substantially vast, key decisions require direct approval from the US President, as they "should be unleashed only on the direct orders of the commander in chief."



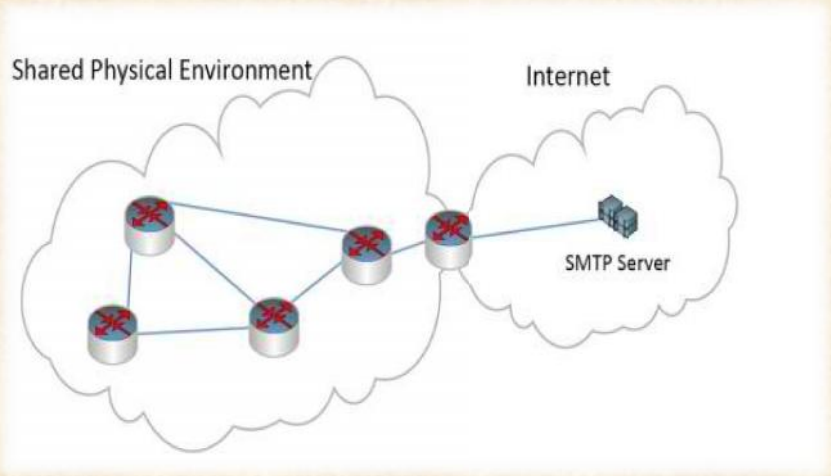
There is, however, no doctrine of use that is as clearly communicated as the doctrine of nuclear deterrence. First, many rules remain secretive and strictly in the realm of the highest echelon of the executive powers. Second, the domain itself is not clearly defined: it may be a in the war fighting domain, or not. Is cyberspace critical only because it is conducive to military assurance? Or is it critical in its own right due to the increasing value of the data stored and protected in cyberspace? Finally, the development of a doctrine takes time and historical precedents. Though concepts of nuclear deterrence began emerging in 1946 following the works of Brodie,8 Mutually Assured Destruction (MAD) did not come to the forefront before the late 1950s. In the USSR, the nuclear strategy's "learning curve" was even less advanced. Certainly, the field of cyber studies is still relatively young, and cyber weaponry in itself is constantly evolving in scale and scope.

Guy-Philippe Goldstein *MBA, HEC (France), is the author of Babel Minute Zero, a bestseller about international cyber warfare.*

Scientist-developed malware covertly jumps air gaps using inaudible sound

Source: http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/

Computer scientists have developed a malware prototype that uses inaudible audio signals to communicate, a capability that allows the malware to covertly transmit keystrokes and other sensitive data even when infected machines have no network connection.



The proof-of-concept software—or malicious trojans that adopt the same high-frequency communication methods—could prove especially adept in penetrating highly sensitive environments that routinely place an "air gap" between computers and the outside world. Using nothing more than the built-in microphones and speakers of standard computers, the researchers were able to transmit passwords and other small amounts of data from distances of almost 65 feet. The software can transfer data at much greater distances by employing an acoustical mesh network made up of attacker-controlled devices that repeat the audio signals.

The researchers, from Germany's Fraunhofer Institute for Communication, Information Processing, and Ergonomics, recently disclosed their findings in a paper published in the Journal of Communications. It came a few weeks after a security researcher said his computers were infected with a mysterious piece of malware that used high-frequency transmissions to jump air gaps. The new research neither confirms nor disproves Dragos Ruiu's claims of the so-called badBIOS infections, but it does show that high-frequency networking is easily within the grasp of today's malware.

"In our article, we describe how the complete concept of air gaps can be considered obsolete as commonly available laptops can communicate over their internal speakers and microphones and even form a covert acoustical mesh network," one of the authors, Michael Hanspach, wrote in an e-mail. "Over this covert network, information can travel over multiple hops of infected nodes, connecting completely isolated computing systems and networks (e.g. the internet) to each other. We also propose some countermeasures against participation in a covert network."

The researchers developed several ways to use inaudible sounds to transmit data between two Lenovo T400 laptops using only their built-in microphones and speakers. The most effective technique relied on software originally developed to acoustically transmit data under water. Created by the Research Department for Underwater Acoustics and Geophysics in Germany, the so-called adaptive communication system (ACS) modem was able to transmit data between laptops as much as 19.7 meters (64.6 feet) apart. By chaining additional devices that pick up the signal and repeat it to other nearby devices, the mesh network can overcome much greater distances.

The ACS modem provided better reliability than other techniques that were also able to use only the laptops' speakers and microphones to communicate. Still, it came with one significant drawback—a transmission rate of about 20 bits per second, a tiny fraction of standard network connections. The paltry bandwidth forecloses the ability of transmitting video or any other kinds of data with large file sizes. The researchers said attackers could overcome that shortcoming by equipping the trojan with functions that transmit only certain types of data, such as login credentials captured from a keylogger or a memory dumper.

"This small bandwidth might actually be enough to transfer critical information (such as keystrokes)," Hanspach wrote. "You don't even have to think about all keystrokes. If you have a keylogger that is able to recognize authentication materials, it may only occasionally forward these detected passwords over the network, leading to a very stealthy state of the network. And you could forward any small-sized information such as private encryption keys or maybe malicious commands to an infected piece of construction."

Remember Flame?

The hurdles of implementing covert acoustical networking are high enough that few malware developers are likely to add it to their offerings anytime soon. Still, the requirements are modest when measured against the capabilities of Stuxnet, Flame, and other state-sponsored malware discovered in the past 18 months. And that means that engineers in military organizations, nuclear power plants, and other truly high-security environments should no longer assume that computers isolated from an Ethernet or Wi-Fi connection are off limits.

The research paper suggests several countermeasures that potential targets can adopt. One approach is simply switching off audio input and output devices, although few hardware designs available today make this most obvious countermeasure easy. A second approach is to employ audio filtering that blocks high-frequency ranges used to covertly transmit data. Devices running Linux can do this by using the advanced Linux Sound Architecture in combination with the Linux Audio Developer's Simple Plugin API. Similar approaches are probably available for Windows and Mac OS X computers as well.

The researchers also proposed the use of an audio intrusion detection guard, a device that would "forward audio input and output signals to their destination and simultaneously store them inside the guard's internal state, where they are subject to further analyses."

Flying hacker contraption hunts other drones, turns them into zombies

Source: http://arstechnica.com/security/2013/12/flying-hacker-contraption-hunts-other-drones-turns-them-into-zombies/

Serial hacker Samy Kamkar has released all the hardware and software specifications that hobbyists need to build an aerial drone that

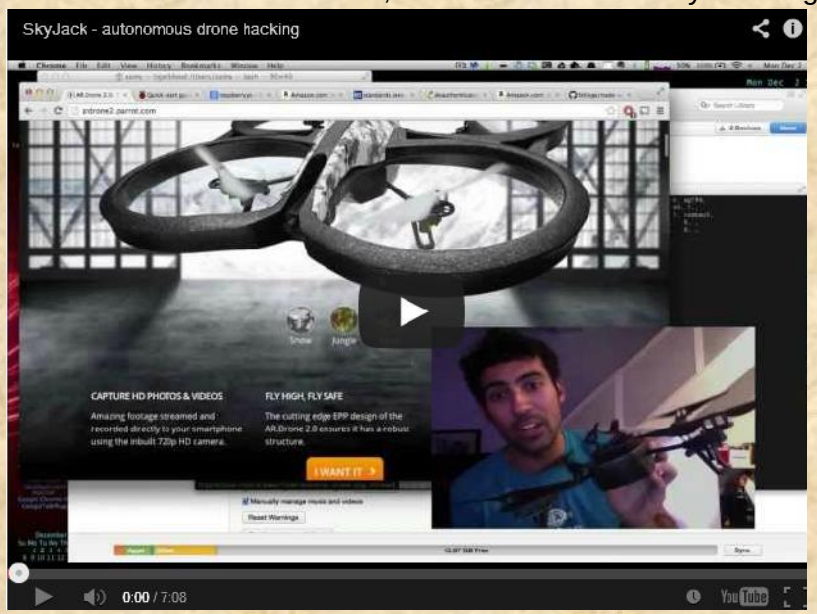
seeks out other drones in the air, hacks them, and turns them into a conscripted army of unmanned vehicles under the attacker's control.

Dubbed SkyJack, the contraption uses a radio-controlled Parrot AR.Drone quadcopter carrying a Raspberry Pi circuit board, a small battery, and two wireless transmitters. The devices run a combination of custom software and off-the-shelf applications that seek out wireless signals of nearby Parrot drones, hijack the wireless connections used to control them, and commandeer the victims' flight-control and camera systems. SkyJack will also run on land-based Linux devices and hack drones within radio range. At least 500,000 Parrot drones have been sold since the model was introduced in 2010.

Kamkar is the creator of the infamous Samy worm, a complex piece of JavaScript that knocked MySpace out of commission in 2005 when the exploit added more than one million MySpace friends to Kamkar's account. Kamkar was later convicted for the stunt. He has since devoted his skills to legal hacks, including development of the "evercookie," a highly persistent browser cookie with troubling privacy implications. He has also researched location data stored by Android devices.

SkyJack made its debut the same week that Amazon unveiled plans to use drones to deliver packages to customers' homes or businesses.

"How fun would it be to take over drones, carrying Amazon packages... or take over any other drones and make them my little zombie drones," Kamkar asked rhetorically in a blog



post published Monday. "Awesome."

SkyJack works by monitoring the media access control (MAC) addresses of all Wi-Fi devices within radio range. When it finds a MAC address belonging to a block of addresses used by Parrot AR.Drone vehicles, SkyJack uses the open-source Aircrack-ng app for Wi-Fi hacking to issue a command that disconnects

the vehicle from the iOS or Android device currently being used to control and monitor it. Operators of the flying hacker drone are then able to use their own smart device to control the altitude, speed, and direction of the hijacked drone and to view its live video feeds.

At the moment, SkyJack is engineered to target a small range of drones. That's because it's programmed to take over drones only if their MACs fall inside an address block reserved by Parrot AR.Drone vehicles. If the MAC falls outside that range, SkyJack takes no action at all. But the software is built in a way to easily target other types of drones that have communication systems that are similar to Parrot. That means a much broader range of devices may be susceptible to radio-controlled hijacking if they fail to adequately secure their connections.