CIA stops spying on friendly nations in W. Europe

WASHINGTON (AP) — Stung by the backlash over a German caught selling secrets to the U.S. and the revelations of surveillance by the National Security Agency, the CIA has stopped spying on friendly governments in Western Europe, according to current and former U.S. officials.

The pause in decades of espionage was designed to give CIA officers time to examine whether they were being careful enough and to evaluate whether spying on allies is worth running the risk of discovery, said a U.S. official who has been briefed on the situation.

Under the stand-down order, case officers in Europe largely have been forbidden from undertaking "unilateral operations" such as meeting with sources they have recruited within allied governments. Such clandestine meetings are the bedrock of spying.

CIA officers are still allowed to meet with their counterparts in the host country's intelligence service and conduct joint operations with host country services. Recently, unilateral operations targeting third country nationals — Russians in France, for example — were restarted. But meetings with independent sources in the host country remain on hold, as do new recruitments.

The CIA declined to comment.

James Clapper, the director of national intelligence, said during a public event Thursday that the U.S. is assuming more risk because it has stopped spying on "specific targets," though he didn't spell out details.

Spying stand-downs are common after an operation is

compromised, but “never this long or this deep,” said a former CIA official, who, like others interviewed for this article, spoke on condition of anonymity because it’s illegal to discuss classified material or activities. The pause, which has been in effect for about two months, was ordered by senior CIA officials through secret cables.

The pullback comes at an inopportune time, with the U.S. worried about monitoring European extremists who have fought in Syria, Europe’s response to Russian aggression and European hostility to American technology companies following revelations the companies turned over data to the NSA. While the U.S. cooperates closely with Europe against terrorism, spying can help American officials understand what their allies are planning and thinking, whether about counterterrorism or trade talks.

The current stand-down was part of the fallout from the July 2 arrest of a 31-year-old employee of the German intelligence service. Suspected of spying for Russia, he told authorities he passed 218 German intelligence documents to the CIA.

In a second case, authorities searched the home and office of a German defense official suspected of spying for the U.S., but he denied doing so, and no charges have been filed against him.

A few days later, Germany asked the CIA station chief in Berlin to leave the country, an unprecedented demand from a U.S. ally. The move demonstrated how seriously the Germans were taking the situation, having already been stung by revelations made by Edward Snowden, a former NSA systems administrator, that the agency had tapped German Chancellor Angela Merkel’s mobile phone.

The NSA disclosure infuriated Merkel, who demanded explanations from President Barack Obama. It embarrassed both world leaders and has left many Germans skeptical about

cooperating with the U.S.

CIA managers were worried that the incident could lead European security services to begin closely watching CIA personnel. Many agency officers in Europe, operating out of U.S. embassies, have declared their status as intelligence operatives to the host country.

The “EUR” division, as it is known within the CIA, covers Canada, Western Europe and Turkey. While spying on Western European allies is not a top priority, Turkey is considered a high-priority target – an Islamic country that talks to U.S. adversaries such as Iran, while sharing a border with Syria and Iraq. It was not known to what extent the stand-down affected operations in Turkey.

European countries also are used as safe venues to conduct meetings between CIA officers and their sources from the Middle East and other high-priority areas. Those meetings have been rerouted to other locales while the pause is in place.

The European Division staff has long been considered among the most risk-averse in the agency, several former case officers said, speaking on condition of anonymity because they weren’t authorized to discuss secret intelligence matters by name.

A former CIA officer who worked under nonofficial cover wrote a 2008 book in which he described a number of operational “stand-downs” in Europe, including one in France in 1998 because of the World Cup soccer championship, and another in a European country in 2005, in response to unspecified security threats.

The former officer, whose real name has not be disclosed, wrote “The Human Factor: Inside the CIA’s Dysfunctional Intelligence Culture,” under a pseudonym, Ishmael Jones. He is a former Marine who served 15 years in the agency before resigning in 2006. The CIA acknowledged his status as a case officer when it successfully sued him for publishing the book

without first submitting it for pre-publication censorship, as required under his secrecy agreement.

The CIA last faced that sort of blowback from a European ally in 1996, when several of its officers were ordered to leave France. An operation to uncover French positions on world trade talks was unraveled by French authorities because of poor CIA tactics, according to a secret CIA inspector general report, details of which were leaked to reporters.

The Paris flap left the EUR division much less willing to mount risky espionage operations, many former case officers have said.

http://hosted.ap.org/dynamic/stories/U/US_CIA_EUROPE_SPYING_PAUSE?SITE=CAOAK&SECTION=HOME&TEMPLATE=DEFAULT

Governments spy on journalists with weaponized malware – WikiLeaks

Journalists and dissidents are under the microscope of intelligence agencies, Wikileaks revealed in its fourth SpyFiles series. A German software company that produces computer intrusion systems has supplied many secret agencies worldwide.

The weaponized surveillance malware, popular among intelligence agencies for spying on *"journalists, activists and political dissidents,"* is produced by FinFisher, a German company. Until late 2013, FinFisher used to be part of the UK-based Gamma Group International, revealed WikiLeaks in the

latest published batch of secret documents.

FinFisher's spyware exploits and monitors systems remotely. It's capable of intercepting communications and data from OS X, Windows and Linux computers, as well as Android, iOS, BlackBerry, Symbian and Windows Mobile portable devices. Three back-end programs are required for the spy program to operate. FinFisher Relay and FinSpy Proxy programs are FinFisher suite components that route and manage intercepted traffic, redirecting it to the FinSpy Master collection program. The spyware can steal keystrokes, Skype conversations, and even connect to your webcam and watch you in real time.

The whistleblower has a list of FinFisher surveillance software buyers. Among the German malware developer's clients are intelligence agencies and police forces from Australia, Bosnia, Estonia, Hungary, Italy, Mongolia, the Netherlands, Pakistan and Qatar.

According to WikiLeaks' estimates, FinFisher has already earned about 50 million euros in sales.

"FinFisher continues to operate brazenly from Germany selling weaponized surveillance malware to some of the most abusive regimes in the world," the founder and editor-in-chief of Wikileaks, Julian Assange, said.

Earlier this year, the tapping of Chancellor Angela Merkel's mobile phone by the American National Security Agency (NSA) created a scandal that rocked the German political establishment: a revelation made thanks to documents exposed by the former NSA contractor and whistleblower Edward Snowden.

Yet, despite all this, FinFisher continues its activities in Germany unhindered.

"The Merkel government pretends to be concerned about privacy, but its actions speak otherwise. Why does the Merkel government continue to protect FinFisher?" Assange asked.

Assange is calling for an 'antidote' to the German-made FinFisher FinSpy PC spyware, saying a tool is needed to repel such activities and expose those who do the surveillance by tracking down spying command and control centers.

WikiLeaks has made newly indexed FinFisher breach material public via torrents, *"including new brochures and a database of the customer support website, that provide updated details on their product line and a unique insight into the company's customer-base."*

"In order to make the data more easily accessible and consumable, all the new brochures, videos and manuals are now available organized under the related FinFisher product name. The database is represented in full, from which WikiLeaks compiled a list of customers, their eventual attribution, all the associated support tickets and acquired licenses, along with the estimated costs calculated from FinFisher's price list," the WikiLeaks memo said.

After the scandal that followed revelations of mass NSA spying worldwide, Germany and France came up with an idea to build a trustworthy data protection network in Europe to avoid data passing through the US.

The US slammed such plans to construct an EU-centric communication system, designed to prevent emails and phone calls from being swept up by the NSA, warning that such a move is a violation of trade laws.

http://rt.com/news/188052-german-spyware-wikileaks-journalists/

China wants explanation on allegations of US spying

China has demanded a clear explanation from the United States following reports that it infiltrated the servers of the Chinese telecoms giant, Huawei.

The company said it would condemn the invasion of its networks if the reports in the New York Times were true.

The newspaper quoted documents, allegedly from the US National Security Agency (NSA), released by the former contractor, Edward Snowden.

They said the NSA had spied on Huawei and had information on its customers.

The NSA has made no mention of the reports but said it focused only on what it called valid foreign intelligence targets.

It said it did not use intelligence to steal the secrets of foreign companies to help US businesses.

Chinese foreign ministry spokesman, Hong Lei, said China was extremely concerned about the allegations.

“China has already lodged many complaints with the United States about reports of its espionage activities,” he said demanding that Washington cease its activities and explain itself.

The New York Times said one of the goals of the US operation was to find out whether Huawei had connections with the People’s Liberation Army.

It said the operation, codenamed “Shotgiant”, also sought to conduct espionage through the systems and telephone networks that Huawei sold to other countries.

The newspaper said that the NSA had gained access to Huawei headquarters in the southern Chinese city of Shenzhen and found information on the internal workings of its switches and routers.

The German magazine, Der Spiegel, also citing what it said were NSA documents from Edward Snowden, said the US was positioned to launch cyber offensive operations against the Chinese leadership through its access to Huawei networks.

Washington has long seen Huawei as a potential security threat and has blocked some business deals in the US for fear that it would open the door to Chinese military hackers.

Edward Snowden fled to Hong Kong last year and has since been granted asylum in Russia.

He continues to release information that claims to reveal the global activities of the NSA.

http://www.bbc.com/news/world-asia-26712564

Busted! – U.S. Tech Giants Knew Of NSA Spying Says Agency's Senior Lawyer

GIH: As it turns out, tech giants were in fact working with the NSA to collect user data electronically. They have vehemently denied this. It seemed to make more sense, that NSA had worked with them, compared to NSA being able to hack on multiple levels their systems. Although the NSA has developed many technologies for advanced electronic surveillance, in many cases, they still rely on old world spy

tricks, such as tapping into data lines at the point of transmission. But now we can't trust the NSA, and we can't trust tech giants, who is left?

Submitted by Michael Krieger of Liberty Blitzkrieg blog,

This is why I've been so confused and frustrated by the repeated reports of the behavior of the US government. When our engineers work tirelessly to improve security, we imagine we're protecting you against criminals, not our own government.

The US government should be the champion for the internet, not a threat. They need to be much more transparent about what they're doing, or otherwise people will believe the worst.

I've called President Obama to express my frustration over the damage the government is creating for all of our future. Unfortunately, it seems like it will take a very long time for true full reform.

So it's up to us – all of us – to build the internet we want. Together, we can build a space that is greater and a more important part of the world than anything we have today, but is also safe and secure. I'm committed to seeing this happen, and you can count on Facebook to do our part.

– Facebook CEO, Mark Zuckerberg in a post last week

Last week, Mark Zuckerberg made headlines by posting about how he called President Barack Obama to express outrage and shock about the government's spying activities. Of course, anyone familiar with **Facebook** and what is going on generally between private tech behemoths and U.S. intelligence agencies knew right away that his statement was one gigantic heap of stinking bullshit. Well now we have the proof.

Earlier today, the senior lawyer for the NSA made it

completely clear that U.S. tech companies were fully aware of all the spying going on, including the PRISM program (on that note read my recent post: **The Most Evil and Disturbing NSA Spy Practices To-Date Have Just Been Revealed**).

So stop the acting all of you Silicon Valley CEOs. We know you are fully on board with extraordinary violations of your fellow citizens' civil liberties. We know full well that you have been too cowardly to stand up for the values this country was founded on. We know you and your companies are compromised. Stop pretending, stop bullshitting. You've done enough harm.

From *The Guardian*:

The senior lawyer for the National Security Agency stated unequivocally on Wednesday that US technology companies were fully aware of the surveillance agency's widespread collection of data, contradicting month of angry denials from the firms.

Rajesh De, the NSA general counsel, said all communications content and associated metadata harvested by the NSA under a 2008 surveillance law occurred with the knowledge of the companies – both for the internet collection program known as Prism and for the so-called "upstream" collection of communications moving across the internet.

Asked during at a Wednesday hearing of the US government's institutional privacy watchdog if ***collection under the law****, known as Section 702 or the Fisa Amendments Act,* ***occurred with the "full knowledge and assistance of any company from which information is obtained," De replied: "Yes."***

When the Guardian and the Washington Post broke the Prism story in June, thanks to documents leaked by whistleblower Edward Snowden, nearly all the companies listed as participating in the program – Yahoo, Apple, Google, Microsoft, Facebook and AOL –claimed they did not know about a surveillance practice described as giving NSA vast access to

their customers' data. Some, like Apple, said they had "never heard" the term Prism.

The disclosure of Prism resulted in a cataclysm in technology circles, with tech giants launching extensive PR campaigns to reassure their customers of data security and successfully pressing the Obama administration to allow them greater leeway to disclose the volume and type of data requests served to them by the government.

The NSA's Wednesday comments contradicting the tech companies about the firms' knowledge of Prism risk entrenching tensions with the firms NSA relies on for an effort that Robert Litt, general counsel for the director of national intelligence, told the board was "one of the most valuable collection tools that we have."

Move along serfs, move along.

Full article here.

Why HTTPS and SSL are not as secure as you think

GIH: We are led to believe that by installing a certificate, or by other common security practices, we are safe. The following shows that this may not be the case, especially considering the vulnerabilities of HTTPS protocol, the commonly accepted 'safe' way to browse:

In this day and age of well-known NSA spying, everyone keeps saying that the only way to be safe is to use SSL/TLS,

commonly known as “browsing with https://”.

The sad reality is that HTTPS does virtually nothing to protect you from the prying eyes of alphabet soup agencies – or anybody else with enough knowledge about how these supposedly “secure” connections actually work.

It’s true that connecting to web sites with SSL will certainly prevent “script kiddies” and other more winky opponents from eavesdropping on your surfing or otherwise interfering in your affairs. But as for the Real Bad Guys, forget it…

We shall begin by taking a brief dive down the rabbit hole of SSL, hopefully in a way that will make sense to even the least technically inclined among us.

This issue is, after all, so extremely important that I think everyone needs to understand what is really going on, and how web security actually works, without needing a PhD in cryptography, computer science, or engineering!

Our story begins with a little e-mail I received the other day. The basic message can be found here:

Microsoft Security Advisory (2880823)

Of course, the idea that Microsoft of all companies is warning me about security is kind of laughable, so I didn’t pay much attention. Nevertheless, there was this little voice in the back of my mind that kept pestering me, so I decided to dig in and see what all the hoopla was about… or indeed if any hoopla was even warranted.

Boy, is it ever warranted!

From the above link, we read:

> *Microsoft is announcing a policy change to the Microsoft Root Certificate Program. The new policy will no longer allow root certificate authorities to issue X.509 certificates using the*

> *SHA-1 hashing algorithm for the purposes of SSL and code signing after January 1, 2016. Using the SHA-1 hashing algorithm in digital certificates could allow an attacker to spoof content, perform phishing attacks,* ***or perform man-in-the-middle attacks****.*
>
> *Microsoft recommends that certificate authorities no longer sign newly generated certificates using the SHA-1 hashing algorithm and begin migrating to SHA-2. Microsoft also recommends that customers replace their SHA-1 certificates with SHA-2 certificates at the earliest opportunity. Please see the Suggested Actions section of this advisory for more information.*

Okay, so that's probably like trying to read a foreign language to most people. Even I didn't understand exactly how these hashing algorithms were used with SSL. So, I started digging. What I found nearly floored me:

MD5 considered harmful today: Creating a rogue CA certificate

Now, if you thought the M$ advisory was confusing, take a peek at the above link.

WOW! That's wild.

In summary, way back in 2008, some smart people figured out a way to make themselves a Fake SSL Certificate Authority, and they accomplished this feat by using a weakness in the MD5 hashing algorithm.

"Eureka! This must be the key to our mystery," I thought.

So, I began to read… and re-read… and think… and re-read. And then it clicked. To paraphrase Inspector Finch:

> *I suddenly had this feeling that everything was connected. It's like I could see the whole thing, one long chain of events that stretched all the way back before the MD5 hash*

> *advisory in 2008. I felt like I could see everything that happened, and everything that is going to happen. It was like a perfect pattern, laid out in front of me. And I realised we're all part of it, and all trapped by it.*

"Well, that's stunningly dramatic," you think, "But just… What is going on?!"

First, let's define some terms – hopefully in Plain English:

SSL Web Site Certificate

This is a digital certificate, with a digital signature, that verifies that a website is who they say they are. When you connect to a web site using SSL (HTTPS), your browser says, "Papers, please!" The remote site then sends the SSL Web Site Certificate to your browser. Your browser then verifies the authenticity of this "passport". Once verified, encrypted communications ensue. The point of the SSL Web Site Certificate is that under no circumstances should anyone else be able to create a valid, signed certificate for a web site that they do not own and operate. In order to obtain an SSL Web Site Cert, you must verify by varied means that you are the owner and operator of the web site involved. So, using HTTPS is not only for encryption of communications, but also a way to verify that the site you are communicating with is the Real Thing, and not an imposter. And of course you must pay for the certificate!

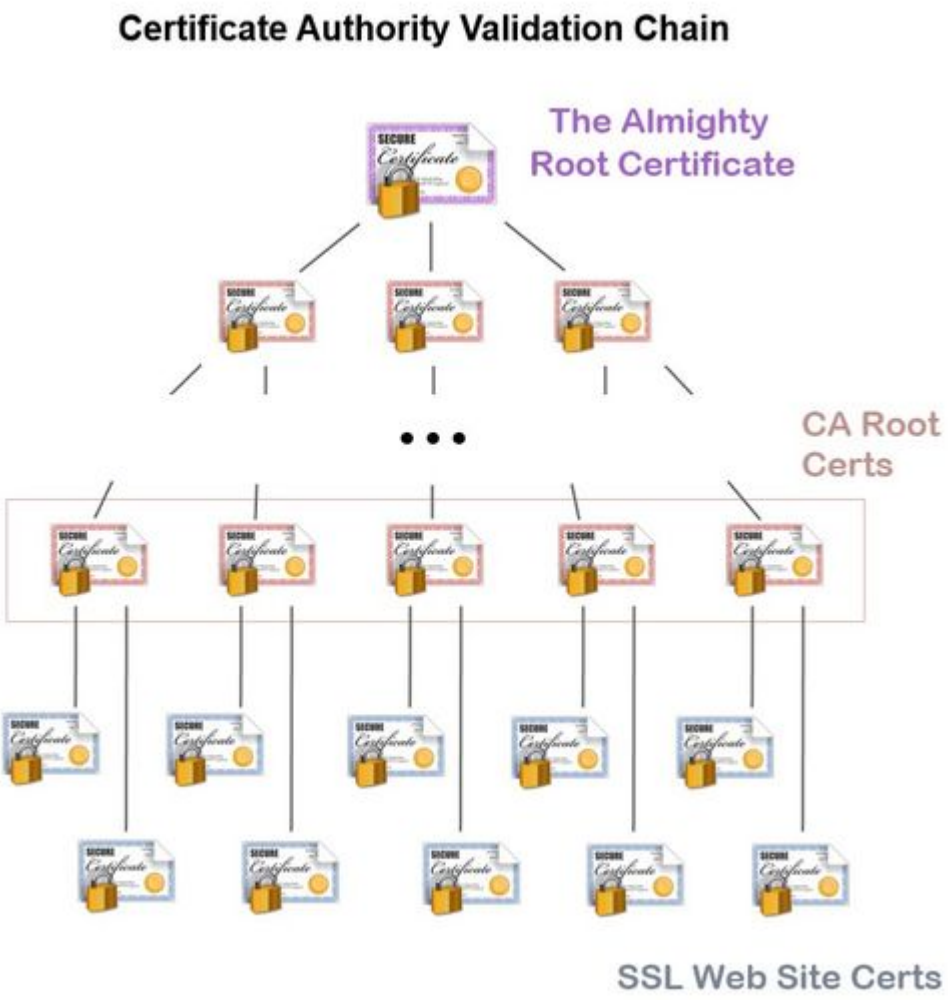
Certificate Authority (CA) Root Certificate

This is also a digital certificate, with a digital signature… But in this case, this certificate can be used to create and digitally sign normal SSL Web Site Certificates. This is the kind of certificate that a CA (Certificate Authority) has. These certificates also get passed to browser makers, and are then included in your web browser. This is so that when your browser receives an SSL Web Site cert, it can use the CA Root Certificate to verify that the Web Site Cert is in fact valid.

Certificate Authority (CA)

A CA is the kind of web site from which you would buy a valid, secure SSL Web Site Certificate to use for HTTPS on your site. For example: Verisign.com, RapidSSL.com, Geotrust.com, etc. are Certificate Authorities. They have CA Root Certificates for generating and signing valid SSL Web Site Certificates.

It’s helpful to understand that with all these certificates, there is a “chain of command”. SSL Web Site Certificates are validated and authenticated using CA Root Certificates. CA Root Certificates are validated with yet higher-authority certificates, all the way up the pyramid to The One Great Root Certificate, which is like the God of Certificates. Thus, each lower-ranking certificate is verified up the chain of command. This all happens behind the scenes, and you have no idea it’s occurring.



Each lower level certificate is validated using a certificate from the level above it.
Piece of cake, right?

Now, where do these hash algorithms like MD5, SHA-1, and SHA-2 come into play?

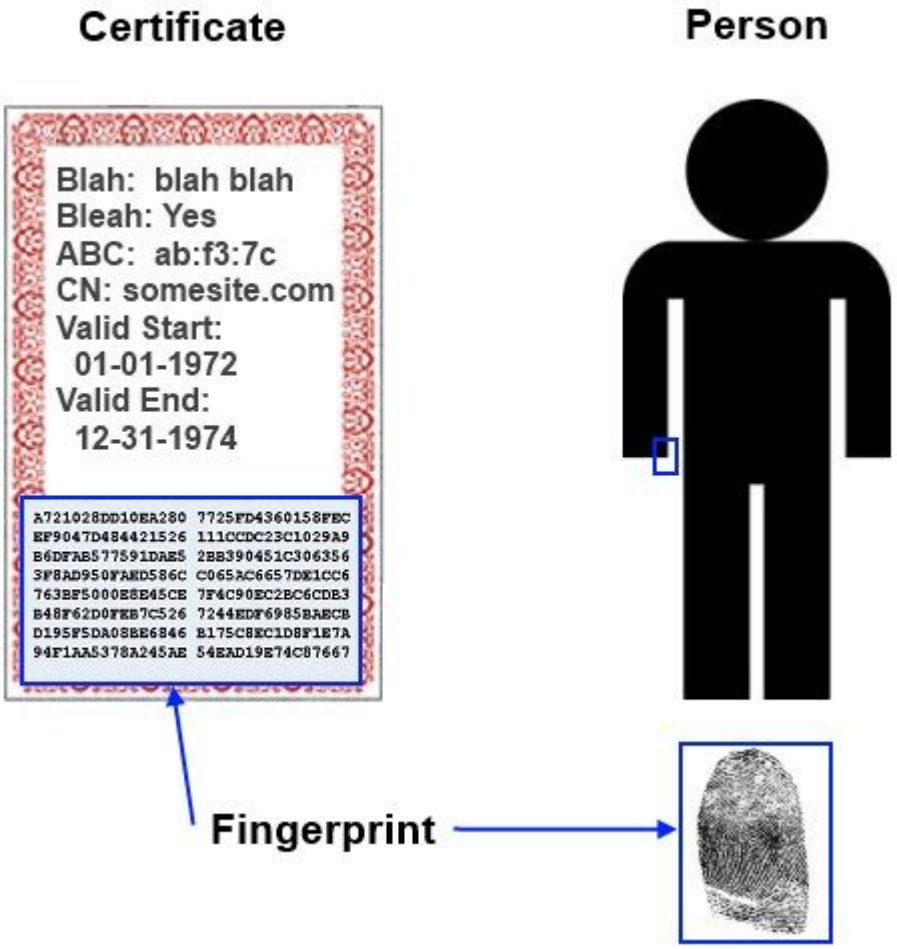
All certificates contain information, like:

- Web site domain (www.mysite.com)
- Site location (country, state, etc.)
- Site owner info (company name)
- Period of validity

This information is verified before a certificate is issued. Once verified, a hash of the data is generated. This hash acts as the digital signature for the certificate. The only thing you really need to understand about hash algorithms is that

what is supposed to happen is this:

1. Data of any length (30 characters, 3000 characters, 40MB, whatever) is passed into the hash algorithm
2. The hash algorithm chops up the data and mathematically processes it, thereby spitting out a signature – or digital fingerprint – of the data
3. The hash of no two chunks of data should ever be the same – just as the fingerprints of no two people should ever be the same
4. The hash output is always the same size, regardless of the size of the input data (just like a fingerprint – no matter the size of the person)



Right. There is such a thing as a “hash collision”. This is when you have 2 hashes that are identical, but they were generated from different data. That’s like if you and your neighbor suddenly had the same thumbprint. **OOPS!**

Now, think about that for a minute… If the police were using these hashes, or thumbprints, to verify your identity, they might mistake you for your neighbor, or your neighbor for you, if you "had the same thumbprint". If they did no other checking, and just relied on that thumbprint, they might very well "authenticate" your identities completely incorrectly. **BIG OOPS!**

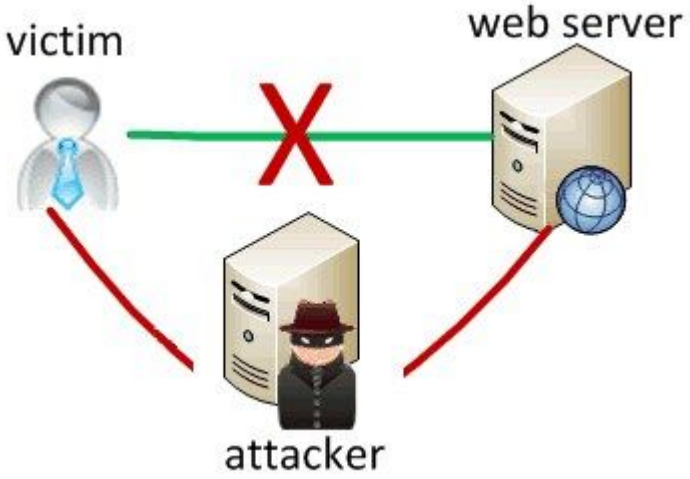
This is exactly what happened with the MD5 SSL attack outlined at the above link.

These smarty-pants people were able to carefully buy a valid SSL Web Site Certificate from RapidSSL in 2008. Before they did that, they created their own CA Root Certificate in such a way that the hash (fingerprint) of their valid, just-purchased Web Site Cert was identical to the hash of the FAKE CA Root Certificate that they created out of thin air.

Since RapidSSL had just said, "Dudes, this Web Site Certificate fingerprint is valid!", and since this was the same fingerprint on the fake CA Root Cert, the forged CA Root Certificate becomes valid.

Now, recall that a CA Root Certificate – as long as it has a valid hash/fingerpint that will validate up the "chain of authority" – **can be used to generate a valid SSL Web Site Certificate for any web site in the world… And neither you, nor RapidSSL, nor your browser will ever know that anything is amiss.**

Why is this a problem? For starters, consider a man-in-the-middle attack.



© x-services.nl
You want to go to https://www.gmail.com. But some “hackers” have used another type of hack to insert their server between you and Gmail. Normally, this would not be possible, because you’re using HTTPS! You’re SAFE!

WRONG!

As far as anyone knows, you are connected to gmail.com over HTTPS. But in reality, what’s happening is this:

1. You try to connect to https://www.gmail.com
2. The attacker diverts your request (perhaps using DNS cache poisoning or some other such attack) to a fake server
3. Since Attacker’s Server contains a falsely generated, perfectly valid SSL Web Site Certificate using the tricks outlined above, your browser doesn’t know any better. Everything appears to be legit.
4. You begin doing e-mail, but all your data is actually going encrypted to Attacker’s Server, being decrypted and recorded/modified, and then Attacker’s Server then passes the data on to the real https://www.gmail.com (using Gmail’s actual, valid SSL cert).
5. You have absolutely no clue that your “secure” communications are not secure in the least!

In other words, SSL / HTTPS means that the connection between your browser and the destination server at the URL you're visiting is supposed to be encrypted. But due to the fact the certain types of SSL certificates (which help handle the encryption) can be forged, an attacker could set up their fake server that pretends to the be the real destination server, and thus insert themselves in the middle of the connection. When that is done, the attacker has control over the connection and the data, and can thus decrypt your data, manipulate it, and/or pass it on to the real intended destination server.

Now, isn't that a daisy?

"But wait!" you say. "Isn't it therefore *good* for Microsoft to recommend changing the hash function to SHA-256 if SHA-1 has the same potential problem as MD5 did back in 2008?"

An excellent question! Unfortunately, yes and no. Even if you, as a web site owner, change your SSL Web Site Certificate from one that is signed using SHA-1 to a new cert that is signed using SHA-2, you are still unsafe.

Why?

Because all it takes is for ONE Certificate Authority to use a "weak" hash algorithm, and someone who is up to no good can generate a forged CA Root Certificate. Once they have that, they can generate as many SSL Web Site Certs as they want – using any hashing algorithm they please – **including a fake-yet-valid cert that they can use to impersonate your "secure" site!**

In other words, the weakness in the hashing algorithm is just the tip of the iceberg. Due to the hierarchical "chain of authority" in the whole certificate system, if anyone manages to create a false CA Root Cert, they are more or less god in terms of creating false SSL Web Site Certs.

Thus, in order for Microsoft's words to have an effect, there must not be ANY Certificate Authority (Web Site Cert issuer) in the whole world that still uses SHA-1. In order for the "security" to actually be more secure, everyone must upgrade right now. But this isn't going to happen.

Now, if that isn't bad enough, think about all the NSA spying. Think about how many people said, "Naw, man, I just surf using HTTPS, and I'm totally safe!"

You think so?

I don't. You know why? Well, you should, by now… But there's more!

Guess who??!
Guess who invented the SHA-1 hash algorithm in 1995?

The NSA.

Guess who invented SHA-2 in 2001?

The NSA.

So, why should all the Certificate Authorities switch from the NSA's SHA-1 to the NSA's SHA-2? Why, because the NSA created it the way they did for a reason!

SHA-1 already has been theoretically breached, and there are a few indications that SHA-2 isn't quite as super-duper-safe as everyone thinks.

Imagine you are the NSA. You want to spy on everyone, everyone's grandmother, the grandmothers' cats, and the mice that are currently being digested inside the cats. SSL is kind of a problem… It can use pretty annoying encryption. Well, hell! No problem. Just compromise the "certificate authority chain" by forging one little CA Root Certificate, and blammo! You can eavesdrop and man-in-the-middle anybody you darn well please, SSL or not!

Web sites over SSL? **No problem.**

E-mail over SSL? **No problem.**

I have said it before, and I'll say it again: There never was security or privacy on the internet, there is no security or privacy on the internet now, and most likely there never will be. Not unless some very big changes are made…

And do you know why all this (and much, much more) is possible?

Because just like you, I had no knowledge of the gaping holes in SSL. Awareness of this and many other issues – technological, political, psychological, social, etc. – is absolutely essential.

Otherwise, frankly, we're screwed.

Scott Ogrin

Scott Ogrin is an electrical and computer engineer with a BSEE and MSEE. After working in the automotive and telecom industries in hardware and testing, he ended up as a software engineer.

He joined SOTT in 2003 as an editor, and is currently the webmaster and Chief Techie for Sott.net. He is also part-owner of French publishing company Les Editions Pilule Rouge, and a member of the board of directors and engineering consultant for Quantum Future Group, Inc.

Although born in the USA, he became a Slovenian citizen and currently lives in France. He speaks English, French, Slovenian, and Spanish.

In his spare time, he works on his popular blog at ScottiesTech.Info.

'What does ISP mean?'

GIH: Shocking information has come forth that government officials responsible for cybersecurity initiatives do not have basic knowledge about the internet, such as what an "ISP" is. How can those who know nothing about a topic regulate or execute it?

One of the world's leading cyberwarfare experts has warned of the damaging lack of government literacy in cybersecurity issues, pointing out that some senior officials don't know how to use email, and that one US representative about to negotiate cybersecurity with China asked him what an "ISP"

was.

Speaking at the SXSW festival, Dr Peter W Singer, director of the Center for 21st Century Security & Intelligence, cited a 2014 poll by the Pew research institute that found Americans are more afraid of cyberattack than attack by Iran or North Korea, climate change, the rise of China or authoritarian Russia.

Sketching out the scale of technology in our lives, Singer said that 40 trillion emails are sent a year, that 30 trillion websites now exist and that 9 new pieces of malware are discovered every second. He claimed that 97% of Fortune 500 companies have admitted they've been hacked – the other 3% just aren't ready to admit it yet.

The consequent rise in cybercrime and state-sponsored attacks has not gone unnoticed. 100 nations now have cyber command, and the Pentagon's own briefings, which contained the word 'cyber' 12 times during 2012, have already mentioned it 147 times so far this year.

Yet former head of US homeland security Janet Napolitano once told Singer. "Don't laugh, but I just don't use email at all," Singer recalled. "It wasn't a fear of privacy or security – it's because she just didn't think it was useful. A supreme court justice also told me 'I haven't got round to email yet' – and this is someone who will get to vote on everything from net neutrality to the NSA negotiations."

Obama himself, Singer said, had expressed concern that the complexity of the issue was overwhelming policy makers.

Singer added that another US official about to negotiate cybersecurity with China asked him to explain what "ISP" meant. "That's like going to negotiate with the Soviets and not knowing what 'ICBM' means. And I've had similar experiences with officials from the UK, China and Abu Dhabi.

At the G20 conference diplomats were spearfished by an email with a link to nude photos of former French first lady Carla Bruni-Sarkozy, and many clicked – downloading spyware onto their computers.

“Cybersecurity is crucial, and as intimate to your life as your bank account. It’s treated as an area only for IT folk, and the technical community that understands the hardware and software but not the wetware – the human side. Without proper tools we cannot understand both what is possible and what is proper. Past myth and future hype weave together to obscure to what actually happen with where we will be in the future.”

Cybersecurity should be treated like public health

Singer also said many cybersecurity threats and solutions are misrepresented or overblown. Power lines are taken down far more often by squirrels, for example. The government response is often too reactionary – akin to the treatment of pirates and privateers in the age of sail – whereas investment in a public cyberhealth campaign would be far more effective.

“Ben Franklin said an ounce of prevention is worth a pound of cure. The Centre for Disease Control and Prevention says that is true of public health but it is also true of cybersecurity… very basic cyber hygiene would go an very long way. The top control measures would stop 90% of all cyber attacks.”

The most significant penetration of US secure networks happened when an infected USB stick was dropped in the car park after a ‘candy drop’; an employee picked it up and plugged it into his computer on their secure network. “That’s not cyber hygiene, that’s basic hygiene – the five second rule.”

Another problem is that different parts of government operate

in contradiction to each other. “Tor was originally paid for by Navy money, and pushed by state departments as a way of dissidents and state departments to protect themselves simultaneously, but if you use it you get swept up by the NSA who assumes you are up to no good. We have to figure out these balances.”

Snowden – traitor or hero?

The argument over NSA surveillance has been reduced to bumper sticker values, Singer argued.

Three different kinds of activity have been exposed. The first is that the NSA carries out espionage against American enemies – smart, strategic espionage. The second is legally and politically questionable, and related to mass collection of American citizens’ information collected either directly by the agency or by its allies.

“The third is what you could kindly call unstrategic – or stupid – directly targeting close American allies and leaders and undermining American technology companies. People want to say Snowden was a traitor or a whistleblower and we pull from the bucket we care the most about, but that’s a bumper sticker way of talking about it because people can simultaneously do both good and bad actions.”

• **Julian Assange tells SXSW audience: ‘NSA has grown to be a rogue agency’**

How the NSA Plans to Infect

‘Millions’ of Computers with Malware

GIH: As more information comes out about various spy agencies and their cyber divisions, it seems that those such as the NSA pose a larger threat to internet security than the hackers they are supposedly protecting us from. The following information should make any user of the internet, be it a business or individual or government, reconsider use, policies, protocols, and security.

 One presentation outlines how the NSA performs “industrial-scale exploitation” of computer networks across the world.

Top-secret documents reveal that the National Security Agency is dramatically expanding its ability to covertly hack into computers on a mass scale by using automated systems that reduce the level of human oversight in the process.

The classified files – provided previously by NSA whistleblower Edward Snowden – contain new details about groundbreaking surveillance technology the agency has developed to infect potentially millions of computers worldwide with malware “implants.” The clandestine initiative enables the NSA to break into targeted computers and to siphon out data from foreign Internet and phone networks.

The covert infrastructure that supports the hacking efforts operates from the agency’s headquarters in Fort Meade, Maryland, and from eavesdropping bases in the United Kingdom and Japan. GCHQ, the British intelligence agency, appears to have played an integral role in helping to develop the implants tactic.

In some cases the NSA has masqueraded as a fake Facebook

server, using the social media site as a launching pad to infect a target's computer and exfiltrate files from a hard drive. In others, it has sent out spam emails laced with the malware, which can be tailored to covertly record audio from a computer's microphone and take snapshots with its webcam. The hacking systems have also enabled the NSA to launch cyberattacks by corrupting and disrupting file downloads or denying access to websites.

The implants being deployed were once reserved for a few hundred hard-to-reach targets, whose communications could not be monitored through traditional wiretaps. But the documents analyzed by *The Intercept* show how the NSA has aggressively accelerated its hacking initiatives in the past decade by computerizing some processes previously handled by humans. The automated system — codenamed TURBINE — is designed to "allow the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually."

In a top-secret presentation, dated August 2009, the NSA describes a pre-programmed part of the covert infrastructure called the "Expert System," which is designed to operate "like the brain." The system manages the applications and functions of the implants and "decides" what tools they need to best extract data from infected machines.

Mikko Hypponen, an expert in malware who serves as chief research officer at the Finnish security firm F-Secure, calls the revelations "disturbing." The NSA's surveillance techniques, he warns, could inadvertently be undermining the security of the Internet.

"When they deploy malware on systems," Hypponen says, "they potentially create new vulnerabilities in these systems, making them more vulnerable for attacks by third parties."

Hypponen believes that governments could arguably justify

using malware in a small number of targeted cases against adversaries. But millions of malware implants being deployed by the NSA as part of an automated process, he says, would be "out of control."

"That would definitely not be proportionate," Hypponen says. "It couldn't possibly be targeted and named. It sounds like wholesale infection and wholesale surveillance."

The NSA declined to answer questions about its deployment of implants, pointing to a new presidential policy directive announced by President Obama. "As the president made clear on 17 January," the agency said in a statement, "signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes."

"Owning the Net"

The NSA began rapidly escalating its hacking efforts a decade ago. In 2004, according to secretinternal records, the agency was managing a small network of only 100 to 150 implants. But over the next six to eight years, as an elite unit called Tailored Access Operations (TAO) recruited new hackers and developed new malware tools, the number of implants soared to tens of thousands.

To penetrate foreign computer networks and monitor communications that it did not have access to through other means, the NSA wanted to go beyond the limits of traditional signals intelligence, or SIGINT, the agency's term for the interception of electronic communications. Instead, it sought to broaden "active" surveillance methods – tactics designed to directly infiltrate a target's computers or network devices.

In the documents, the agency describes such techniques as "a

more aggressive approach to SIGINT" and says that the TAO unit's mission is to "aggressively scale" these operations.

But the NSA recognized that managing a massive network of implants is too big a job for humans alone.

"One of the greatest challenges for active SIGINT/attack is scale," explains the top-secret presentation from 2009. "Human 'drivers' limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)."

The agency's solution was TURBINE. Developed as part of TAO unit, it is described in the leaked documents as an "intelligent command and control capability" that enables "industrial-scale exploitation."

TURBINE was designed to make deploying malware much easier for the NSA's hackers by reducing their role in overseeing its functions. The system would "relieve the user from needing to know/care about the details," the NSA's Technology Directorate notes in one secret document from 2009. "For example, a user should be able to ask for 'all details about application X' and not need to know how and where the application keeps files, registry entries, user application data, etc."

In practice, this meant that TURBINE would automate crucial processes that previously had to be performed manually – including the configuration of the implants as well as surveillance collection, or "tasking," of data from infected systems. But automating these processes was about much more than a simple technicality. The move represented a major tactical shift within the NSA that was expected to have a profound impact – allowing the agency to push forward into a

new frontier of surveillance operations.

The ramifications are starkly illustrated in one undated top-secret NSA document, which describes how the agency planned for TURBINE to "increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants." (CNE mines intelligence from computers and networks; CNA seeks to disrupt, damage or destroy them.)

Eventually, the secret files indicate, the NSA's plans for TURBINE came to fruition. The system has been operational in some capacity since at least July 2010, and its role has become increasingly central to NSA hacking operations.

Earlier reports based on the Snowden files indicate that the NSA has already deployed between 85,000 and 100,000 of its implants against computers and networks across the world, with plans to keep on scaling up those numbers.

The intelligence community's top-secret "Black Budget" for 2013, obtained by Snowden, lists TURBINE as part of a broader NSA surveillance initiative named "Owning the Net."

The agency sought $67.6 million in taxpayer funding for its Owning the Net program last year. Some of the money was earmarked for TURBINE, expanding the system to encompass "a wider variety" of networks and "enabling greater automation of computer network exploitation."

Circumventing Encryption

The NSA has a diverse arsenal of malware tools, each highly

sophisticated and customizable for different purposes.

One implant, codenamed UNITEDRAKE, can be used with a variety of “plug-ins” that enable the agency to gain total control of an infected computer.

An implant plug-in named CAPTIVATEDAUDIENCE, for example, is used to take over a targeted computer’s microphone and record conversations taking place near the device. Another, GUMFISH, can covertly take over a computer’s webcam and snap photographs. FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts. GROK is used to log keystrokes. And SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer.

The implants can enable the NSA to circumvent privacy-enhancing encryption tools that are used to browse the Internet anonymously or scramble the contents of emails as they are being sent across networks. That’s because the NSA’s malware gives the agency unfettered access to a target’s computer before the user protects their communications with encryption.

It is unclear how many of the implants are being deployed on an annual basis or which variants of them are currently active in computer systems across the world.

Previous reports have alleged that the NSA worked with Israel to develop the Stuxnet malware, which was used to sabotage Iranian nuclear facilities. The agency also reportedly worked with Israel to deploy malware called Flame to infiltrate computers and spy on communications in countries across the Middle East.

According to the Snowden files, the technology has been used to seek out terror suspects as well as individuals regarded by the NSA as “extremist.” But the mandate of the NSA’s hackers is not limited to invading the systems of those who pose a

threat to national security.

In one secret post on an internal message board, an operative from the NSA's Signals Intelligence Directorate describes using malware attacks against systems administrators who work at foreign phone and Internet service providers. By hacking an administrator's computer, the agency can gain covert access to communications that are processed by his company. "Sys admins are a means to an end," the NSA operative writes.

The internal post – titled "I hunt sys admins" – makes clear that terrorists aren't the only targets of such NSA attacks. Compromising a systems administrator, the operative notes, makes it easier to get to other targets of interest, including any "government official that happens to be using the network some admin takes care of."

Similar tactics have been adopted by Government Communications Headquarters, the NSA's British counterpart. As the German newspaper *Der Spiegel* reported in September, GCHQ hacked computers belonging to network engineers at Belgacom, the Belgian telecommunications provider.

The mission, codenamed "Operation Socialist," was designed to enable GCHQ to monitor mobile phones connected to Belgacom's network. The secret files deem the mission a "success," and indicate that the agency had the ability to covertly access Belgacom's systems since at least 2010.

Infiltrating cellphone networks, however, is not all that the malware can be used to accomplish. The NSA has specifically tailored some of its implants to infect large-scale network routers used by Internet service providers in foreign countries. By compromising routers – the devices that connect computer networks and transport data packets across the Internet – the agency can gain covert access to monitor Internet traffic, record the browsing sessions of users, and intercept communications.

Two implants the NSA injects into network routers, HAMMERCHANT and HAMMERSTEIN, help the agency to intercept and perform "exploitation attacks" against data that is sent through aVirtual Private Network, a tool that uses encrypted "tunnels" to enhance the security and privacy of an Internet session.

The implants also track phone calls sent across the network via Skype and other Voice Over IP software, revealing the username of the person making the call. If the audio of the VOIP conversation is sent over the Internet using unencrypted "Real-time Transport Protocol" packets, the implants can covertly record the audio data and then return it to the NSA for analysis.

But not all of the NSA's implants are used to gather intelligence, the secret files show. Sometimes, the agency's aim is disruption rather than surveillance. QUANTUMSKY, a piece of NSA malware developed in 2004, is used to block targets from accessing certain websites. QUANTUMCOPPER, first tested in 2008, corrupts a target's file downloads. These two "attack" techniques are revealed on a classified list that features nine NSA hacking tools, six of which are used for intelligence gathering. Just one is used for "defensive" purposes – to protect U.S. government networks against intrusions.

"Mass exploitation potential"

Before it can extract data from an implant or use it to attack a system, the NSA must first install the malware on a targeted computer or network.

According to one top-secret document from 2012, the agency can deploy malware by sending out spam emails that trick targets into clicking a malicious link. Once activated, a "back-door

implant" infects their computers within eight seconds.

There's only one problem with this tactic, codenamed WILLOWVIXEN: According to the documents, the spam method has become less successful in recent years, as Internet users have become wary of unsolicited emails and less likely to click on anything that looks suspicious.

Consequently, the NSA has turned to new and more advanced hacking techniques. These include performing so-called "man-in-the-middle" and "man-on-the-side" attacks, which covertly force a user's internet browser to route to NSA computer servers that try to infect them with an implant.

To perform a man-on-the-side attack, the NSA observes a target's Internet traffic using its global network of covert "accesses" to data as it flows over fiber optic cables or satellites. When the target visits a website that the NSA is able to exploit, the agency's surveillance sensors alert the TURBINE system, which then "shoots" data packets at the targeted computer's IP address within a fraction of a second.

In one man-on-the-side technique, codenamed QUANTUMHAND, the agency disguises itself as a fake Facebook server. When a target attempts to log in to the social media site, the NSA transmits malicious data packets that trick the target's computer into thinking they are being sent from the real Facebook. By concealing its malware within what looks like an ordinary Facebook page, the NSA is able to hack into the targeted computer and covertly siphon out data from its hard drive. A top-secret animation demonstrates the tactic in action.

The documents show that QUANTUMHAND became operational in October 2010, after being successfully tested by the NSA against about a dozen targets.

According to Matt Blaze, a surveillance and cryptography

expert at the University of Pennsylvania, it appears that the QUANTUMHAND technique is aimed at targeting specific individuals. But he expresses concerns about how it has been covertly integrated within Internet networks as part of the NSA's automated TURBINE system.

"As soon as you put this capability in the backbone infrastructure, the software and security engineer in me says that's terrifying," Blaze says.

"Forget about how the NSA is intending to use it. How do we know it is working correctly and only targeting who the NSA wants? And even if it does work correctly, which is itself a really dubious assumption, how is it controlled?"

In an email statement to *The Intercept*, Facebook spokesman Jay Nancarrow said the company had "no evidence of this alleged activity." He added that Facebook implemented HTTPS encryption for users last year, making browsing sessions less vulnerable to malware attacks.

Nancarrow also pointed out that other services besides Facebook could have been compromised by the NSA. "If government agencies indeed have privileged access to network service providers," he said, "any site running only [unencrypted] HTTP could conceivably have its traffic misdirected."

A man-in-the-middle attack is a similar but slightly more aggressive method that can be used by the NSA to deploy its malware. It refers to a hacking technique in which the agency covertly places itself between computers as they are communicating with each other.

This allows the NSA not only to observe and redirect browsing sessions, but to modify the content of data packets that are passing between computers.

The man-in-the-middle tactic can be used, for instance, to

covertly change the content of a message as it is being sent between two people, without either knowing that any change has been made by a third party. The same technique is sometimes used by criminal hackers to defraud people.

A top-secret NSA presentation from 2012 reveals that the agency developed a man-in-the-middle capability called SECONDDATE to "influence real-time communications between client and server" and to "quietly redirect web-browsers" to NSA malware servers called FOXACID. In October, details about the FOXACID system were reported by the *Guardian*, which revealed its links to attacks against users of the Internet anonymity service Tor.

But SECONDDATE is tailored not only for "surgical" surveillance attacks on individual suspects. It can also be used to launch bulk malware attacks against computers.

According to the 2012 presentation, the tactic has "mass exploitation potential for clients passing through network choke points."

Blaze, the University of Pennsylvania surveillance expert, says the potential use of man-in-the-middle attacks on such a scale "seems very disturbing." Such an approach would involve indiscriminately monitoring entire networks as opposed to targeting individual suspects.

"The thing that raises a red flag for me is the reference to 'network choke points,'" he says. "That's the last place that we should be allowing intelligence agencies to compromise the infrastructure — because that is by definition a mass surveillance technique."

To deploy some of its malware implants, the NSA exploits security vulnerabilities in commonly used Internet browsers such as Mozilla Firefox and Internet Explorer.

The agency's hackers also exploit security weaknesses in network routers and in popular software plugins such as Flash and Java to deliver malicious code onto targeted machines.

The implants can circumvent anti-virus programs, and the NSA has gone to extreme lengths to ensure that its clandestine technology is extremely difficult to detect. An implant named VALIDATOR, used by the NSA to upload and download data to and from an infected machine, can be set to self-destruct – deleting itself from an infected computer after a set time expires.

In many cases, firewalls and other security measures do not appear to pose much of an obstacle to the NSA. Indeed, the agency's hackers appear confident in their ability to circumvent any security mechanism that stands between them and compromising a computer or network. "If we can get the target to visit us in some sort of web browser, we can probably own them," an agency hacker boasts in one secret document. "The only limitation is the 'how.'"

Covert Infrastructure

The TURBINE implants system does not operate in isolation.

It is linked to, and relies upon, a large network of clandestine surveillance "sensors" that the agency has installed at locations across the world.

The NSA's headquarters in Maryland are part of this network, as are eavesdropping bases used by the agency in Misawa, Japan and Menwith Hill, England.

The sensors, codenamed TURMOIL, operate as a sort of high-tech surveillance dragnet, monitoring packets of data as they are sent across the Internet.

When TURBINE implants exfiltrate data from infected computer systems, the TURMOIL sensors automatically identify the data and return it to the NSA for analysis. And when targets are communicating, the TURMOIL system can be used to send alerts or "tips" to TURBINE, enabling the initiation of a malware attack.

The NSA identifies surveillance targets based on a series of data "selectors" as they flow across Internet cables. These selectors, according to internal documents, can include email addresses, IP addresses, or the unique "cookies" containing a username or other identifying information that are sent to a user's computer by websites such as Google, Facebook, Hotmail, Yahoo, and Twitter.

Other selectors the NSA uses can be gleaned from unique Google advertising cookies that track browsing habits, unique encryption key fingerprints that can be traced to a specific user, and computer IDs that are sent across the Internet when a Windows computer crashes or updates.

What's more, the TURBINE system operates with the knowledge and support of other governments, some of which have participated in the malware attacks.

Classification markings on the Snowden documents indicate that NSA has shared many of its files on the use of implants with its counterparts in the so-called Five Eyes surveillance alliance – the United Kingdom, Canada, New Zealand, and Australia.

GCHQ, the British agency, has taken on a particularly important role in helping to develop the malware tactics. The Menwith Hill satellite eavesdropping base that is part of the TURMOIL network, located in a rural part of Northern England, is operated by the NSA in close cooperation with GCHQ.

Top-secret documents show that the British base – referred to

by the NSA as "MHS" for Menwith Hill Station – is an integral component of the TURBINE malware infrastructure and has been used to experiment with implant "exploitation" attacks against users of Yahoo and Hotmail.

In one document dated 2010, at least five variants of the QUANTUM hacking method were listed as being "operational" at Menwith Hill. The same document also reveals that GCHQ helped integrate three of the QUANTUM malware capabilities – and test two others – as part of a surveillance system it operates codenamed INSENSER.

GCHQ cooperated with the hacking attacks despite having reservations about their legality. One of the Snowden files, previously disclosed by Swedish broadcaster SVT, revealed that as recently as April 2013, GCHQ was apparently reluctant to get involved in deploying the QUANTUM malware due to "legal/policy restrictions." A representative from a unit of the British surveillance agency, meeting with an obscure telecommunications standards committee in 2010, separately voiced concerns that performing "active" hacking attacks for surveillance "may be illegal" under British law.

In response to questions from *The Intercept*, GCHQ refused to comment on its involvement in the covert hacking operations. Citing its boilerplate response to inquiries, the agency said in a statement that "all of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate, and that there is rigorous oversight."

Whatever the legalities of the United Kingdom and United States infiltrating computer networks, the Snowden files bring into sharp focus the broader implications. Under cover of secrecy and without public debate, there has been an unprecedented proliferation of aggressive surveillance techniques. One of the NSA's primary concerns, in fact, appears to be that its clandestine tactics are now being

adopted by foreign rivals, too.

“Hacking routers has been good business for us and our 5-eyes partners for some time,” notes one NSA analyst in a top-secret document dated December 2012. “But it is becoming more apparent that other nation states are honing their skillz [sic] and joining the scene.”

___

Documents published with this article:

- Menwith Hill Station Leverages XKeyscore for Quantum Against Yahoo and Hotmail
- Five Eyes Hacking Large Routers
- NSA Technology Directorate Analysis of Converged Data
- Selector Types
- There Is More Than One Way to Quantum
- NSA Phishing Tactics and Man in the Middle Attacks
- Quantum Insert Diagrams
- The NSA and GCHQ’s QUANTUMTHEORY Hacking Tactics
- TURBINE and TURMOIL
- VPN and VOIP Exploitation With HAMMERCHANT and HAMMERSTEIN
- Industrial-Scale Exploitation
- Thousands of Implants

ALERT: Point of Sale RAM scraper malware

Advances in technology have led to more sophisticated crimes by exploiting security vulnerabilities of new technologies. This is exacerbated by the fact that understanding of these

technologies and their use is only by a few, while the majority of end-users are unaware. Generally speaking, following standard security practices will thwart 95% of electronic crimes such as phishing, hacking, etc. This includes using complex passwords (Sf9$fpq%f82bsS), using network firewalls, encrypted emails, etc. But the new POS RAM scraper is dangerous because the vendors are not the victims of their bad security, and you may never know where your credit card or other information was scraped from.

A look at Point of Sale RAM scraper malware and how it works

From Sophos:

A special kind of malware has been hitting the headlines recently – that which attacks the RAM of Point of Sale (PoS) systems.

Although it's been getting quite a bit of publicity recently, we actually first identified it as a threat back in December 2009 and wrote about it in an article on Naked Security entitled Will RAM scraping loosen the sky and make it fall?.

Answering that question today, it just might!

Actually, the situation isn't that bad – yet – but this malware family has definitely become more complex and far-reaching. In this article, we take a step back from the technical details and look at the evolution of PoS RAM scrapers.

What do PoS RAM scrapers do?

In a nutshell, PoS RAM scrapers steal payment data – such as credit card track one and track two data – from the RAM of PoS systems.

The payment card industry has a set of data security standards known asPCI-DSS. These standards require end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to rogue callhome servers.

Why do we care about PoS RAM scrapers? How does it hurt me?

I believe this malware family has a higher probability of burning a hole in your pocket compared to other prevalent malware families.

In today's plastic money economy people are carrying cash a lot less than before. Aside from a handful of stores, the majority of retailers accept debit or credit cards. Payment cards are convenient, quick, supposedly-secure, and you don't have change jingling around in your pockets.

PoS RAM scrapers target the systems which process debit and credit card transactions and steal the sensitive payment information. Your home computer might be super secure, but there is no guarantee the PoS system at your neighborhood grocery store has the same level of security. You might end up losing your credit card data buying a candy bar!

How have PoS RAM scrapers evolved?

Sophos detects PoS RAM scraper malware under the family name *Trackr*(e.g. Troj/Trackr-Gen, Troj/Trackr-A) Other AV

vendors detect this malware family with a variety of names, the most common name being *Alina*.

Some of the earliest variants of Trackr had simple functionality that worked like this:

1. Install as a service
2. Use a legitimate-looking name
3. Scan RAM for credit card track one and track two data
4. Dump the results into a text file. This text file was then probably accessed remotely or manually.

Over the years Trackr has become more industrialized, with some cosmetic changes and added bot and network functionality.

Our friends at Trustwave SpiderLabs have written two excellent articles,Alina: Casting a Shadow on PoS and Alina: Following The Shadow, about the inner workings of the Trackr family.

Till now we have observed the following types of Trackr:

- Basic version (not packed, scrapes RAM for credit card information)
- Complex version (added socially-engineered filenames, bot and network functionality)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping)
- Versions one and two packed with a commercially-available packer
- Versions one and two packed with a custom packer

Most recently, SophosLabs discovered the highly-prevalent Citadel crimeware targeting PoS systems.

The Citadel malware uses screen captures and keylogging instead of the RAM-scraping technique used by Trackr. Citadel's focus on PoS systems demonstrates that this avenue is fast becoming a point of serious concern.

Who do PoS RAM scrapers target?

One of the earliest serious PoS RAM scraper attacks that we observed was back in November 2011 when we found that a university and several hotels had their PoS systems compromised. Later we saw varied targets including an auto dealership in Australia infected with Trackr.

To better understand the threat we gathered statistics about the various industries targeted by Trackr during the past 6 months (as observed using Sophos Live Protection):

It doesn't come as a surprise that the biggest targeted industries are:

- Retail
- Service
- Healthcare
- Food services
- Education
- Hotel and tourism

In these industries there's a high volume of credit and debit card transactions taking place, meaning they have goldmines of payment data that can be harvested.

Compromising a single PoS system (e.g. in a fast food outlet) may yield thousands of credit cards per week, cheaply – much easier to gather 10,000 credit card details from one PoS system then attempt to infect 10,000 PCs, hoping to grab the data from there.

If not protected properly, PoS systems become easy targets – a single point of failure that can affect thousands of people.

In addition to the breakdown of industries targeted, we also looked at the countries where we saw Trackr infections over the same time period:

Again, no surprises that the developed countries top this chart with the US, where credit cards are abundant, taking the #1 spot.

In fact, the Trackr infection numbers match up closely with the credit card country usage statistics published by Visa.

So how does Trackr get on a PoS system?

We have used the term PoS quite generally throughout this article. PoS is the place where a retail transaction is completed. So a PoS could be some custom hardware/software solution, a regular PC running PoS software, a credit card transaction server, or something similar.

Big box retailers and chain stores have security-hardened PoS systems, and we have not seen any major evidence of these large organizations getting compromised with Trackr.

The victims tend to be mostly small to medium sized organizations who will typically have less investment in defensive counter-measures.

Based on our analysis there were two main methods of infection:

Insider job

Someone with active knowledge of the payment processing setup installs a RAM scraper to gather data. The early Trackr samples dropped their harvested data in a plain text file which we suspect was manually retrieved or remotely accessed.

The malware had no network functionality and we found no evidence of a top-level dropper/installer.

Phishing/Social Engineering

These are the common infection vectors with the more complex versions of Trackr. The socially engineered filenames we have

observed
includeTaskmgr.exe, windowsfirewall.exe, sms.exe, java.exe, win-firewall.exe, andadobeflash.exe. This suggests that the files were delivered as part of a phishing campaign, or social engineering tricks were used to infect the system.

Importantly however, Trackr is not seen regularly in the mass-spammed malware campaigns that we observe daily. Rather it is highly targeted towards a group of relevant businesses.

To conclude, it is not always a safe solution to pay for everything with cards.

Everyone should follow computer security best practices and consumers should proactively sign-up for credit monitoring services so they don't becomes victims of credit or identity theft.

Businesses big and small need to make investments to protect their critical PoS infrastructure. Just like they wouldn't keep their cash registers unlocked for someone to grab money out of them, PoS systems need proper protection.

FBI moves from policy of Law Enforcement to National Security

The FBI's creeping advance into the world of counterterrorism is nothing new. But quietly and without notice, the agency has

finally decided to make it official in one of its organizational fact sheets. Instead of declaring "law enforcement" as its "primary function," as it has for years, the FBI fact sheet now lists "national security" as its chief mission. The changes largely reflect the FBI reforms put in place after September 11, 2001, which some have criticized for de-prioritizing law enforcement activities. Regardless, with the 9/11 attacks more than a decade in the past, the timing of the edits is baffling some FBI-watchers.

"What happened in the last year that changed?" asked Kel McClanahan, a Washington-based national security lawyer.

McClanahan noticed the change last month while reviewing a Freedom of Information Act (FOIA) request from the agency. The FBI fact sheet accompanies every FOIA response and highlights a variety of facts about the agency. After noticing the change, McClanahan reviewed his records and saw that the revised fact sheets began going out this summer. "I think they're trying to rebrand," he said. "So many good things happen to your agency when you tie it to national security."

Although a spokesman with the agency declined to weigh in on the timing of the change, he said the agency is just keeping up with the times. "When our mission changed after 9/11, our fact sheet changed to reflect that," FBI spokesman Paul Bresson told Foreign Policy. He noted that the FBI's website has long-emphasized the agency's national security focus. "We rank our top 10 priorities and CT [counterterrorism] is first, counterintel is second, cyber is third," he said. "So it is certainly accurate to say our primary function is national security." On numerous occasions, former FBI Director Robert Mueller also emphasized the FBI's national security focus in speeches and statements.

FBI historian and Marquette University professor Athan Theoharis agreed that the changes reflect what's really happening at the agency, but said the timing isn't clear. "I

can't explain why FBI officials decided to change the fact sheet… unless in the current political climate that change benefits the FBI politically and undercuts criticisms," he said. He mentioned the negative attention surrounding the FBI's failure in April to foil the bomb plot at the Boston Marathon by Dzhokhar and Tamerlan Tsarnaev.

Whatever the reason, the agency's increased focus on national security over the last decade has not occurred without consequence. Between 2001 and 2009, the FBI doubled the amount of agents dedicated to counterterrorism, according to a 2010 Inspector's General report. That period coincided with a steady decline in the overall number of criminal cases investigated nationally and a steep decline in the number of white-collar crime investigations.

"Violent crime, property crime and white-collar crime: All those things had reductions in the number of people available to investigate them," former FBI agent Brad Garrett told *Foreign Policy*. "Are there cases they missed? Probably."

Last month, Robert Holley, the special agent in charge in Chicago, said the agency's focus on terrorism and other crimes continued to affect the level of resources available to combat the violent crime plaguing the city. "If I put more resources on violent crime, I'd have to take away from other things," he told *The Chicago Tribune.*

According to a 2007 *Seattle Post-Intelligencer* investigation, the Justice Department did not replace 2,400 agents assigned to focus on counterterrorism in the years following 9/11. The reductions in white-collar crime investigations became obvious. Back in 2000, the FBI sent prosecutors 10,000 cases. That fell to a paltry 3,500 cases by 2005. "Had the FBI continued investigating financial crimes at the same rate as it had before the terror attacks, about 2,000 more white-collar criminals would be behind bars," the report concluded. As a result, the agency fielded criticism for failing to crack

down on financial crimes ahead of the Great Recession and losing sight of real-estate fraud ahead of the 2008 subprime mortgage crisis.

In many ways, the agency had no choice but to de-emphasize white-collar crime. Following the 9/11 attacks, the FBI picked up scores of new responsibilities related to terrorism and counterintelligence while maintaining a finite amount of resources. What's not in question is that government agencies tend to benefit in numerous ways when considered critical to national security as opposed to law enforcement. "If you tie yourself to national security, you get funding and you get exemptions on disclosure cases," said McClanahan. "You get all the wonderful arguments about how if you don't get your way, buildings will blow up and the country will be less safe."

– See more at: http://thecable.foreignpolicy.com/posts/2014/01/02/us_customs_not_sorry_for_destroying_11_rare_flutes_of_renowned_musician#sthash.dTe9DVfT.L8CLoAYR.dpuf

---

Inside TAO: Documents Reveal Top NSA Hacking Unit

More leaked documents reveal a secret NSA hacking operation, with techniques ranging from physical implants of malware (sometimes hardware) to infiltrating Telecom networks, and even exploiting Microsoft updates to infect the target machine. TAO has existed since 1997, but recently interest in the program is exploding, as seen by the drastic increase in the number of TAO operation facilities, and the number of employees.

> *The NSA's TAO hacking unit is considered to be the intelligence agency's top secret weapon. It maintains its own covert network, infiltrates computers around the world and even intercepts shipping deliveries to plant back doors in electronics ordered by those it is targeting… One example of the sheer creativity with which the TAO spies approach their work can be seen in a hacking method they use that exploits the error-proneness of Microsoft's Windows. Every user of the operating system is familiar with the annoying window that occasionally pops up on screen when an internal problem is detected, an automatic message that prompts the user to report the bug to the manufacturer and to restart the program. These crash reports offer TAO specialists a welcome opportunity to spy on computers. The technique can literally be a race between servers, one that is described in internal intelligence agency jargon with phrases like: "Wait for client to initiate new connection," "Shoot!" and "Hope to beat server-to-client response." Like any competition, at times the covert network's surveillance tools are "too slow to win"..*

Read the full article here – Inside TAOs_ Documents Reveal Top NSA Hacking Unit – SPIEGEL ONLINE Considering TAO is an NSA sponsored hacking program, it wouldn't be a stretch to see Spiegel soon hacked, so we are keeping this article here on Global Intel Hub.