SPIEGEL ONLINE
12/29/2013 09:18 AM

Inside TAO

Documents Reveal Top NSA Hacking Unit

By SPIEGEL Staff

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.

In January 2010, numerous homeowners in San Antonio, Texas, stood baffled in front of their closed garage doors. They wanted to drive to work or head off to do their grocery shopping, but their garage door openers had gone dead, leaving them stranded. No matter how many times they pressed the buttons, the doors didn't budge. The problem primarily affected residents in the western part of the city, around Military Drive and the interstate highway known as Loop 410.

In the United States, a country of cars and commuters, the mysterious garage door problem quickly became an issue for local politicians. Ultimately, the municipal government solved the riddle. Fault for the error lay with the United States' foreign intelligence service, the National Security Agency, which has offices in San Antonio. Officials at the agency were forced to admit that one of the NSA's radio antennas was broadcasting at the same frequency as the garage door openers. Embarrassed officials at the intelligence agency promised to resolve the issue as quickly as possible, and soon the doors began opening again.

It was thanks to the garage door opener episode that Texans learned just how far the NSA's work had encroached upon their daily lives. For quite some time now, the intelligence agency has maintained a branch with around 2,000 employees at Lackland Air Force Base, also in San Antonio. In 2005, the agency took over a former Sony computer chip plant in the western part of the city. A brisk pace of construction commenced inside this enormous compound. The acquisition of the former chip factory at Sony Place was part of a massive expansion the agency began after the events of Sept. 11, 2001.

On-Call Digital Plumbers

One of the two main buildings at the former plant has since housed a sophisticated NSA unit, one that has benefited the most from this expansion and has grown the fastest in recent years -- the Office of Tailored Access Operations, or TAO. This is the NSA's top operative unit -- something like a squad of plumbers that can be called in when normal access to a target is blocked.

According to internal NSA documents viewed by SPIEGEL, these on-call digital plumbers are involved in many sensitive operations conducted by American intelligence agencies. TAO's area of operations ranges from counterterrorism to cyber attacks to traditional espionage. The documents reveal just how diversified the tools at TAO's disposal have become -- and also how it exploits the technical weaknesses of the IT industry, from Microsoft to Cisco and Huawei, to carry out its discreet and efficient attacks.

The unit is "akin to the wunderkind of the US intelligence community," says Matthew Aid, a historian who specializes in the history of the NSA. "Getting the ungettable" is the NSA's own description of its duties. "It is not about the quantity produced but the quality of intelligence that is important," one former TAO chief wrote, describing her work in a document. The paper seen by SPIEGEL quotes the former unit head stating that TAO has contributed "some of the most significant intelligence our country has ever seen." The unit, it goes on, has "access to our very hardest targets."

A Unit Born of the Internet

Defining the future of her unit at the time, she wrote that TAO "needs to continue to grow and must lay the foundation for integrated Computer Network Operations," and that it must "support Computer Network Attacks as an integrated part of military operations." To succeed in this, she wrote, TAO would have to acquire "pervasive, persistent access on the global network." An internal description of TAO's responsibilities makes clear that aggressive attacks are an explicit part of the unit's tasks. In other words, the NSA's hackers have been given a government mandate for their work. During the middle part of the last decade, the special unit succeeded in gaining access to 258 targets in 89 countries -- nearly everywhere in the world. In 2010, it conducted 279 operations worldwide.

Indeed, TAO specialists have directly accessed the protected networks of democratically elected leaders of countries. They infiltrated networks of European telecommunications companies and gained access to and read mails sent over Blackberry's BES email servers, which until then were believed to be securely encrypted. Achieving this last goal required a "sustained TAO operation," one document states.

This TAO unit is born of the Internet -- created in 1997, a time when not even 2 percent of the world's population had Internet access and no one had yet thought of Facebook, YouTube or Twitter. From the time the first TAO employees moved into offices at NSA headquarters in Fort Meade, Maryland, the unit was housed in a separate wing, set apart from the rest of the agency. Their task was clear from the beginning -- to work around the clock to find ways to hack into global communications traffic.

Recruiting the Geeks

To do this, the NSA needed a new kind of employee. The TAO workers authorized to access the special, secure floor on which the unit is located are for the most part considerably younger than the average NSA staff. Their job is breaking into, manipulating and exploiting computer networks, making them hackers and civil servants in one. Many resemble geeks -- and act the part too.

Indeed, it is from these very circles that the NSA recruits new hires for its Tailored Access Operations unit. In recent years, NSA Director Keith Alexander has made several appearances at major hacker conferences in the United States. Sometimes, Alexander wears his military uniform, but at others, he even dons jeans and a t-shirt in his effort to court trust and a new generation of employees.

The recruitment strategy seems to have borne fruit. Certainly, few if any other divisions within the agency are growing as quickly as TAO. There are now TAO units in Wahiawa, Hawaii; Fort Gordon, Georgia; at the NSA's outpost at Buckley Air Force Base, near Denver, Colorado; at its headquarters in Fort Meade; and, of course, in San Antonio.

One trail also leads to Germany. According to a document dating from 2010 that lists the "Lead TAO Liaisons" domestically and abroad as well as names, email addresses and the number for their "Secure Phone," a liaison office is located near Frankfurt -- the European Security Operations Center (ESOC) at the so-called "Dagger Complex" at a US military compound in the Griesheim suburb of Darmstadt.

But it is the growth of the unit's Texas branch that has been uniquely impressive, the top secret documents reviewed by SPIEGEL show. These documents reveal that in 2008, the Texas Cryptologic Center employed fewer than 60 TAO specialists. By 2015, the number is projected to grow to 270 employees. In addition, there are another 85 specialists in the "Requirements & Targeting" division (up from 13 specialists in 2008). The number of software developers is expected to increase from the 2008 level of three to 38 in 2015. The San Antonio office handles attacks against targets in the Middle East, Cuba, Venezuela and Colombia, not to mention Mexico, just 200 kilometers (124 miles) away, where the government has fallen into the NSA's crosshairs.

Targeting Mexico

Mexico's Secretariat of Public Security, which was folded into the new National Security Commission at the beginning of 2013, was responsible at the time for the country's police, counterterrorism, prison system and border police. Most of the agency's nearly 20,000 employees worked at its headquarters on Avenida Constituyentes, an important traffic artery in Mexico City. A large share of the Mexican security authorities under the auspices of the Secretariat are supervised from the offices there, making Avenida Constituyentes a one-stop shop for anyone seeking to learn more about the country's security apparatus.

Operation WHITETAMALE

That considered, assigning the TAO unit responsible for tailored operations to target the Secretariat makes a lot of sense. After all, one document states, the US Department of Homeland Security and the United States' intelligence agencies have a need to know everything about the drug trade, human trafficking and security along the US-Mexico border. The Secretariat presents a potential "goldmine" for the NSA's spies, a document states. The TAO workers selected systems administrators and telecommunications engineers at the Mexican agency as their targets, thus marking the start of what the unit dubbed Operation WHITETAMALE.

Workers at NSA's target selection office, which also had Angela Merkel in its sights in 2002 before she became chancellor, sent TAO a list of officials within the Mexican Secretariat they thought might make interesting targets. As a first step, TAO penetrated the target officials' email accounts, a relatively simple job. Next, they infiltrated the entire network and began capturing data.

Soon the NSA spies had knowledge of the agency's servers, including IP addresses, computers used for email traffic and individual addresses of diverse employees. They also obtained diagrams of the security agencies' structures, including video surveillance. It appears the operation continued for years until SPIEGEL first reported on it in October.

The technical term for this type of activity is "Computer Network Exploitation" (CNE). The goal here is to "subvert endpoint devices," according to an internal NSA presentation that SPIEGEL has viewed. The presentation goes on to list nearly all the types of devices that run our digital lives -- "servers, workstations, firewalls, routers, handsets, phone switches, SCADA systems, etc." SCADAs are industrial control systems used in factories, as well as in power plants. Anyone who can bring these systems under their control has the potential to knock out parts of a country's critical infrastructure.

The most well-known and notorious use of this type of attack was the development of Stuxnet, the computer worm whose existence was discovered in June 2010. The virus was developed jointly by American and Israeli intelligence agencies to sabotage Iran's nuclear program, and successfully so. The country's nuclear program was set back by years after Stuxnet manipulated the SCADA control technology used at Iran's uranium enrichment facilities in Natanz, rendering up to 1,000 centrifuges unusable.

The special NSA unit has its own development department in which new technologies are developed and tested. This division is where the real tinkerers can be found, and their inventiveness when it comes to finding ways to infiltrate other networks, computers and smartphones evokes a modern take on Q, the legendary gadget inventor in James Bond movies.

Having Fun at Microsoft's Expense

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.

When TAO selects a computer somewhere in the world as a target and enters its unique identifiers (an IP address, for example) into the corresponding database, intelligence agents are then automatically notified any time the operating system of that computer crashes and its user receives the prompt to report the problem to Microsoft. An internal presentation suggests it is NSA's powerful XKeyscore spying tool that is used to fish these crash reports out of the massive sea of Internet traffic.

The automated crash reports are a "neat way" to gain "passive access" to a machine, the presentation continues. Passive access means that, initially, only data the computer sends out into the Internet is captured and saved, but the computer itself is not yet manipulated. Still, even this passive access to error messages provides valuable insights into problems with a targeted person's computer and, thus, information on security holes that might be exploitable for planting malware or spyware on the unwitting victim's computer.

Although the method appears to have little importance in practical terms, the NSA's agents still seem to enjoy it because it allows them to have a bit of a laugh at the expense of the Seattle-based software giant. In one internal graphic, they replaced the text of Microsoft's original error message with one of their own reading, "This information may be intercepted by a foreign sigint system to gather detailed information and better exploit your machine." ("Sigint" stands for "signals intelligence.")

One of the hackers' key tasks is the offensive infiltration of target computers with so-called implants or with large numbers of Trojans. They've bestowed their spying tools with illustrious monikers like "ANGRY NEIGHBOR," "HOWLERMONKEY" or "WATERWITCH." These names may sound cute, but the tools they describe are both aggressive and effective.

According to details in Washington's current budget plan for the US intelligence services, around 85,000 computers worldwide are projected to be infiltrated by the NSA specialists by the end of this year. By far the majority of these "implants" are conducted by TAO teams via the Internet.

Increasing Sophistication

Until just a few years ago, NSA agents relied on the same methods employed by cyber criminals to conduct these implants on computers. They sent targeted attack emails disguised as spam containing links directing users to virus-infected websites. With sufficient knowledge of an Internet browser's security holes -- Microsoft's Internet Explorer, for example, is especially popular with the NSA hackers -- all that is needed to plant NSA malware on a person's computer is for that individual to open a website that has been specially crafted to compromise the user's computer. Spamming has one key drawback though: It doesn't work very often.

Nevertheless, TAO has dramatically improved the tools at its disposal. It maintains a sophisticated toolbox known internally by the name "QUANTUMTHEORY." "Certain QUANTUM missions have a success rate of as high as 80%, where spam is less than 1%," one internal NSA presentation states.

A comprehensive internal presentation titled "QUANTUM CAPABILITIES," which SPIEGEL has viewed, lists virtually every popular Internet service provider as a target, including Facebook, Yahoo, Twitter and YouTube. "NSA QUANTUM has the greatest success against Yahoo, Facebook and static IP addresses," it states. The presentation also notes that the NSA has been unable to employ this method to target users of Google services. Apparently, that can only be done by Britain's GCHQ intelligence service, which has acquired QUANTUM tools from the NSA.

A favored tool of intelligence service hackers is "QUANTUMINSERT." GCHQ workers used this method to attack the computers of employees at partly government-held Belgian telecommunications company Belgacom, in order to use their computers to penetrate even further into the company's networks. The NSA, meanwhile, used the same technology to target high-ranking members of the Organization of the Petroleum Exporting Countries (OPEC) at the organization's Vienna headquarters. In both cases, the trans-Atlantic spying consortium gained unhindered access to valuable economic data using these tools.

The NSA's Shadow Network

The insert method and other variants of QUANTUM are closely linked to a shadow network operated by the NSA alongside the Internet, with its own, well-hidden infrastructure comprised of "covert" routers and servers. It appears the NSA also incorporates routers and servers from non-NSA networks into its covert network by infecting these networks with "implants" that then allow the government hackers to control the computers remotely. (Click here to read a related article on the NSA's "implants".)

In this way, the intelligence service seeks to identify and track its targets based on their digital footprints. These identifiers could include certain email addresses or website cookies set on a person's computer. Of course, a cookie doesn't automatically identify a person, but it can if it includes additional information like an email address. In that case, a cookie becomes something like the web equivalent of a fingerprint.

A Race Between Servers

Once TAO teams have gathered sufficient data on their targets' habits, they can shift into attack mode, programming the QUANTUM systems to perform this work in a largely automated way. If a data packet featuring the email address or cookie of a target passes through a cable or router monitored by the NSA, the system sounds the alarm. It determines what website the target person is trying to access and then activates one of the intelligence service's covert servers, known by the codename FOXACID.

This NSA server coerces the user into connecting to NSA covert systems rather than the intended sites. In the case of Belgacom engineers, instead of reaching the LinkedIn page they were actually trying to visit, they were also directed to FOXACID servers housed on NSA networks. Undetected by the user, the manipulated page transferred malware already custom tailored to match security holes on the target person's computer.

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 the race." Often enough, though, they are effective. Implants with QUANTUMINSERT, especially when used in conjunction with LinkedIn, now have a success rate of over 50 percent, according to one internal document.

Tapping Undersea Cables

At the same time, it is in no way true to say that the NSA has its sights set exclusively on select individuals. Of even greater interest are entire networks and network providers, such as the fiber optic cables that direct a large share of global Internet traffic along the world's ocean floors.

One document labeled "top secret" and "not for foreigners" describes the NSA's success in spying on the "SEA-ME-WE-4" cable system. This massive underwater cable bundle connects Europe with North Africa and the Gulf states and then continues on through Pakistan and India, all the way to Malaysia and Thailand. The cable system originates in southern France, near Marseille. Among the companies that hold ownership stakes in it are France Telecom, now known as Orange and still partly government-owned, and Telecom Italia Sparkle.

The document proudly announces that, on Feb. 13, 2013, TAO "successfully collected network management information for the SEA-Me-We Undersea Cable Systems (SMW-4)." With the help of a "website masquerade operation," the agency was able to "gain access to the consortium's management website and collected Layer 2 network information that shows the circuit mapping for significant portions of the network."

It appears the government hackers succeeded here once again using the QUANTUMINSERT method.

The document states that the TAO team hacked an internal website of the operator consortium and copied documents stored there pertaining to technical infrastructure. But that was only the first step. "More operations are planned in the future to collect more information about this and other cable systems," it continues.

But numerous internal announcements of successful attacks like the one against the undersea cable operator aren't the exclusive factors that make TAO stand out at the NSA. In contrast to most NSA operations, TAO's ventures often require physical access to their targets. After all, you might have to directly access a mobile network transmission station before you can begin tapping the digital information it provides.

Spying Traditions Live On

To conduct those types of operations, the NSA works together with other intelligence agencies such as the CIA and FBI, which in turn maintain informants on location who are available to help with sensitive missions. This enables TAO to attack even isolated networks that aren't connected to the Internet. If necessary, the FBI can even make an agency-owned jet available to ferry the high-tech plumbers to their target. This gets them to their destination at the right time and can help them to disappear again undetected after even as little as a half hour's work.

Responding to a query from SPIEGEL, NSA officials issued a statement saying, "Tailored Access Operations is a unique national asset that is on the front lines of enabling NSA to defend the nation and its allies." The statement added that TAO's "work is centered on computer network exploitation in support of foreign intelligence collection." The officials said they would not discuss specific allegations regarding TAO's mission.

Sometimes it appears that the world's most modern spies are just as reliant on conventional methods of reconnaissance as their predecessors.

Take, for example, when they intercept shipping deliveries. If a target person, agency or company orders a new computer or related accessories, for example, TAO can divert the shipping delivery to its own secret workshops. The NSA calls this method interdiction. At these so-called "load stations," agents carefully open the package in order to load malware onto the electronics, or even install hardware components that can provide backdoor access for the intelligence agencies. All subsequent steps can then be conducted from the comfort of a remote computer.

These minor disruptions in the parcel shipping business rank among the "most productive operations" conducted by the NSA hackers, one top secret document relates in enthusiastic terms. This method, the presentation continues, allows TAO to obtain access to networks "around the world."

Even in the Internet Age, some traditional spying methods continue to live on.

REPORTED BY JACOB APPELBAUM, LAURA POITRAS, MARCEL ROSENBACH, CHRISTIAN STÖCKER, JÖRG SCHINDLER AND HOLGER STARK

URL:

http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Related SPIEGEL ONLINE links:

Shopping for Spy Gear Catalog Advertises NSA Toolbox (12/29/2013)
http://www.spiegel.de/international/world/0,1518,940994,00.html
Friendly Fire How GCHQ Monitors Germany, Israel and the EU (12/20/2013)
http://www.spiegel.de/international/world/0,1518,940135,00.html
Oil Espionage How the NSA and GCHQ Spied on OPEC (11/11/2013)
http://www.spiegel.de/international/world/0,1518,932777,00.html
Fresh Leak on US Spying NSA Accessed Mexican President's Email (10/20/2013)
http://www.spiegel.de/international/world/0,1518,928817,00.html
Quantum Spying GCHQ Used Fake LinkedIn Pages to Target Engineers (11/11/2013)
http://www.spiegel.de/international/world/0,1518,932821,00.html
Ally and Target US Intelligence Watches Germany Closely (08/12/2013)
http://www.spiegel.de/international/world/0,1518,916029,00.html

Related internet links

"Washington Post": Bericht über Cyber-Attacken 2011
http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html
SPIEGEL ONLINE is not liable for the content of external web pages.