



Are We Really Under Cyber Attack?

By Ira Wilsker

Russian Hackers Have Been in White House System for Months, Officials Say

Apr 7, 2015, 6:39 PM ET

By BRIAN ROSS, LEE FERRAN and ALI WEINBERG

f Like

7.6k

f share

300

t Tweet

701

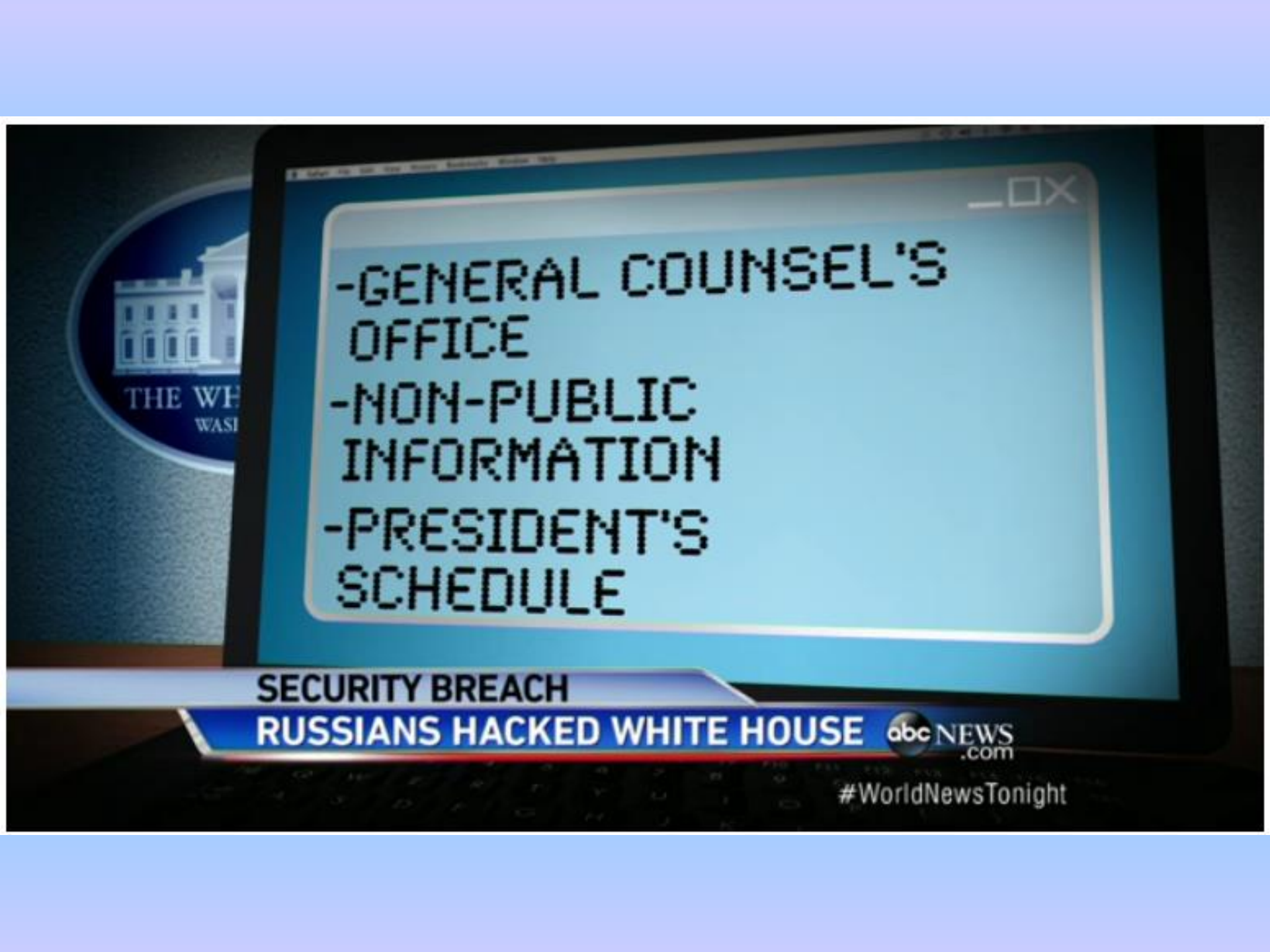
g+1

53



223 Comments



- 
- GENERAL COUNSEL'S OFFICE
 - NON-PUBLIC INFORMATION
 - PRESIDENT'S SCHEDULE

SECURITY BREACH

RUSSIANS HACKED WHITE HOUSE

abc NEWS
.com

#WorldNewsTonight

Exclusive: FBI warns retailers to expect more credit card breaches

Thu, Jan 23 2014

By [Jim Finkle](#) and [Mark Hosenball](#)

WASHINGTON (Reuters) - The FBI has warned U.S. retailers to prepare for more cyber attacks after discovering about 20 hacking cases in the past year that involved the same kind of malicious software used against Target Corp in the holiday shopping season.

The U.S. Federal Bureau of Investigation distributed a confidential, three-page report to retail companies last week describing the risks posed by "memory-parsing" malware that infects point-of-sale (POS) systems, which include cash registers and credit-card swiping machines found in store checkout aisles.

"We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it," said the FBI report, seen by Reuters.

"The accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cyber crime attractive to a wide range of actors," the FBI said.

The report was dated January 17 and entitled "Recent Cyber Intrusion Events Directed Toward Retail Firms." A spokeswoman for the FBI confirmed the agency had issued the report as part of efforts to share information about threats with the private sector.

Retail, credit card and bank industry executives have become increasingly concerned about the security of payment card networks after Target, the No. 3 U.S. retailer, last month disclosed one of the biggest retail cyber attacks in history.

The attack ran undetected for 19 days during the busy holiday shopping season and resulted in the theft of about 40 million credit and debit card records. The personal information of 70 million customers was also compromised.

Luxury retail chain Neiman Marcus has said it too was the victim of a cyber attack, and sources have told Reuters that other retail chains have also been breached. Neiman Marcus said about 1.1 million customer cards were exposed by a data breach from July 16 to October 30 last year.

In all these attacks, cyber criminals used memory-parsing software, also known as a "RAM scraper." When a customer swipes a credit or debit card, the POS terminal grabs the transaction data from the magnetic stripe and transfers it to the retailer's payment processing provider. While the data is encrypted during the process, RAM scrapers extract the information while it is in the computer's live memory, where it very briefly appears in plain text.

RAM scraping technology has been around for a long time, but its use has increased in recent years. Developers of the malware have also enhanced its features to make it more difficult to be detected by anti-virus software deployed on POS systems running Windows software.

MALWARE ON SALE UNDERGROUND



FBI WARNING TO RETAIL BUSINESSES

UNCLASSIFIED



FBI *Cyber Division*



Private Industry Notification

DATE: 17 January 2014

PIN #: 140117 - 001

(U) Recent Cyber Intrusion Events Directed Toward Retail Firms

(U) Executive Summary

(U) Law enforcement officials and private security researchers have identified a rise in intrusions into point-of-sale (POS) systems. These attacks are perpetrated with the intent to obtain credit and debit card data as well as personally identifiable information. The Department of Homeland Security (DHS), in conjunction with iSIGHT Partners and the Secret Service, has released a TLP-Green report outlining the details surrounding the recent incidents affecting major US retailers. The United States Secret Service has the lead on those investigations. This report will outline high-level analytics involving POS-related malware to include incidents investigated by the FBI within the last year.

(U) Malware Targeting Point of Sale Systems

(U) There are several variations of malware that have been designed to exploit POS systems. This family of malware has also been identified by the names “Ram scraping” or “Memory Parsing.” While POS malware varies in type, it is primarily designed to locate and extract specific financial transaction data. In a typical POS intrusion, there are two tracks of data targeted for exfiltration. Track 1 contains cardholder data (including names and account numbers) and Track 2 contains card data (including credit card numbers and expiration dates). This data is extracted from volatile memory by the malware and exfiltrated back to the individual committing the intrusion. Each time a customer’s card is swiped at a POS terminal, Track 1 and Track 2 data is retrieved from the magnetic stripe and transferred electronically to the company’s payment processing provider. It is during this process that the data is extracted from the system’s RAM by the malware installed on the machine. This technique is designed to circumvent any encryption utilized during the electronic transfer of data to the payment processing provider, as the data remains in plaintext while in memory on the POS terminal. It is important to note, however, that POS malware is rarely designed to be an all inclusive and automated malware package. Malicious actors are usually required to conduct reconnaissance to ascertain where the POS systems reside within a corporate architecture and then design several pieces of malware to conduct further reconnaissance to locate the appropriate systems, extract the information, and then surreptitiously exfiltrate it back to the actor. The networks that need to be accessed by the actor are typically not flat and may require bypassing several networks with various levels of administrative access. Point-of-Sale systems are connected via a LAN, but are not internet addressable. POS malware samples are typically stand alone tools that are dropped by other types of malware. Many of the POS systems that large retailers deploy utilize lightweight, embedded operating systems distributed via a centralized server. The actors

FBI WARNING TO RETAIL BUSINESSES (CONTINUED)

- (U) **Dexter** is a Windows-based malware with several variants. Security researchers noted that in one instance of infection, the low number of victim machines suggested the actors may have been testing the software between mid-October and mid-November 2013.
- (U) **Trojan.POSRAM** monitors information in payment application programs. When the malware determines unencrypted track data is in RAM, the information is stolen.
- (U) **VSkimmer**, which may be a successor to Dexter, also targets Windows machines. Researchers have determined that if a VSkimmer-infected machine is not connected to the internet, the program will wait until a USB drive with the volume name KARTOXA007 is inserted into the computer, and download stolen information to the USB drive.

(U) In addition to the above, malware known as “Alina” malware illustrates the evolving nature of POS malware in that the author(s) introduced an option to update the malware remotely. This highlights the persistent nature of the malware in commercial or retail settings.


(U) Initial Infection Vectors

(U) The POS malware is typically introduced into a system after the system has already been compromised. In other words, the POS malware serves as the payload as a result of the initial intrusion. The attack can take various forms, such as phishing e-mails, compromised Web sites, and other common infection vectors.

(U) Analytical Findings

(U) At least one version of POS malware has been observed for sale for up to \$6,000 in a well-known criminal forum. Of the current ongoing FBI cases of POS related malware intrusions, most were primarily infections of small-to-medium sized local or regional businesses. The estimated losses to affected



A close-up photograph of a person's face, focusing on the eye and nose area. A large, semi-transparent red shape is overlaid on the image, partially obscuring the eye and nose. The background is dark and out of focus.

companies related to these intrusions range from in the tens of thousands to millions of dollars. Open source information reported from CTO Daniel Ingevaldson of Easy Solutions cited a recent massive flow of stolen credit card data in December, as well as a second round of stolen credit card numbers discovered on Jan 4th. The second group of cards contained an inordinate amount of premier, high-limit credit accounts. The dollar value of these types of intrusions can have a significant impact on both individuals and corporations. Variations of cyber POS attacks can be exceedingly sophisticated. The high dollar value gained from some of these compromises can encourage intruders to develop high sophistication methodologies, as well as incorporate mechanisms for the actors to remain undetected.

(U) As the NCCIC report suggests, the growing popularity of this type of malware, the accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially-motivated cyber crime attractive to a wide range of actors. We believe POS malware crime will continue to grow over the near term despite law enforcement and security firms' actions to mitigate it.

(U) Administrative Notes

No portion of this report should be released to the media, the general public, or over non-secure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.

COUNTERFEIT CREDIT CARDS

Krebs on Security

In-depth security news and investigation



24 Feds Infiltrate, Bust Counterfeit Card Shop

JAN 14



Federal authorities in New Jersey announced a series of arrests and indictments of 14 individuals thought to be connected to an online one-stop shop selling embossed, counterfeit credit cards and holographic overlays.

According to documents released by prosecutors in New Jersey and North Carolina, the men ran or otherwise profited from the Web site **fakeplastic[dot]net**, which specializes in selling high-quality, custom-made counterfeit credit and debit cards, as well as holographic overlays used to create fake driver's licenses.

THERE ARE SEVERAL FACTORS THAT DETERMINED THE PRICE OF THE STOLEN TARGET CREDIT AND DEBIT CARDS: THE CREDIT LIMIT ON THE CARD, EXPIRATION DATE, LOCATION OF ISSUING BANK, TYPE OF CARD, ETC.

Load [Mozilla Firefox](#) [Google Chrome](#) [Opera](#)

Country	Dump type	Dump mark	Debit/Credit
<input type="text"/>	All <input type="text"/>	All <input type="text"/>	All <input type="text"/>
Bins	Bank & State & City	Base and other	Additional
2, 376282	All <input type="text"/> <input type="text"/>	All <input type="text"/>	<input type="checkbox"/> Expired 12/13 <input type="checkbox"/> Track1 Exp. date (1312) Last 4 Digits Select code <input type="text"/>

Find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [REDACTED] [500k of fresh dumps](#)

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price	Cart
551686	MASTERCARD	DEBIT	STANDARD	11/14	Yes	101	United States, MI, GRAND RAPIDS, 49512	CHEMICAL BANK	Tortuga-6	26.6\$	<input type="button" value="+"/> <input type="button" value="-"/>
414709	VISA	CREDIT	SIGNATURE	02/16	Yes	101	United States, PA, HARRISBURG, 17111	CAPITAL ONE BANK (USA) N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	39.2\$	<input type="button" value="+"/> <input type="button" value="-"/>
512107	MASTERCARD	CREDIT	GOLD	02/16	Yes	101	United States, AZ, MESA, 85206	CITIBANK N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	44.8\$	<input type="button" value="+"/> <input type="button" value="-"/>

Card shopping options at mn0g0.su

Included in the mn0g0.su database are more than **81,000 sets of credit and debit card numbers**, along with their associated **expiration dates and card security code**.

Each listing also includes the owner's name, address and phone number and/or email address.

The Social Security number, mother's maiden name and date of birth are available for some cardholders.

The site **does not accept credit card payments**; shopper accounts are funded by deposits from "virtual currencies," such as **WebMoney** and **LibertyReserve (and now, BitCoins)**.

COUNTERFEIT CREDIT CARDS FOR SALE

Product categories

- All
- Blank plastic
- Canada
- Philippines
- UK
- Embossed Plastics
- Holograms
- ID Overlays
- Misc

Now Accepting ...



ORDER HISTORY

[Back](#)

[Pay For Order with BTC](#)

Product information:

Product	Price	Quantity	Product Data
Embossed plastics	\$15.00	1	408540 ,sabrina 419
	\$12.00	1	Capital One No Hassle
	\$12.00	1	Capital One Dolphin
			



Product categories

- All
- Blank plastic
- Canada
- Philippines
- UK
- Embossed Plastics
- Holograms
- ID Overlays
- Misc

SAMPLES - Blank plastic

Amex Citi Aadvantage



in stock: 35 12.00 USD

[add to cart](#)

Amex Green



in stock: 18 12.00 USD

[add to cart](#)

Amex Optima



in stock: 41 12.00 USD

[add to cart](#)

Barclays Black



in stock: 15 12.00 USD

[add to cart](#)

Barclay Card



in stock: 95 12.00 USD

[add to cart](#)

BOA Alaska Airlines



in stock: 12 12.00 USD

[add to cart](#)

Now Accepting ...



TARGET CREDIT CARD FRAUD SUSPECTS ARRESTED AT TEXAS BORDER

McALLEN, Texas - Police in South Texas say account information stolen during [the Target security breach](#) is now being divided up and sold off regionally as evidenced by the arrest of two Mexican citizens in [connection to 96 fraudulent credit cards](#).

McAllen Police Chief Victor Rodriguez said Monday that 27-year-old Mary Carmen Garcia and 28-year-old Daniel Guardiola Dominguez, both of Monterrey, Mexico, used cards containing the [account information of South Texas residents](#). The chief says they were used to [buy tens of thousands of dollars' worth of merchandise at national retailers in the area](#).

The two were arrested on Sunday morning trying to re-enter the U.S. at the border.

According to [CBS affiliate KGBT](#), Garcia and Dominguez were arrested after authorities found the 96 cloned or counterfeit credit cards under their clothes.

Police Chief Rodriguez said the credit cards were made using data stolen from Rio Grande Valley residents during the Target data breach.

McAllen police are reportedly working with federal officials to investigate how the two ended up with the cards, who made them and who provided them with the data.

The Target security breach is believed to have involved [40 million credit and debit card accounts and the personal information of 70 million customers](#).

CBP Seizes 400+ Counterfeit Credit Cards at Santa Teresa Port

(Wednesday, May 09, 2012)

Santa Teresa, N.M. – U.S. Customs and Border Protection (CBP) officers working at the Santa Teresa port of entry seized 422 counterfeit credit cards and gift cards Tuesday night. Two people from Chihuahua City, Chihuahua, Mexico were arrested in in the case.



"Homeland security is our primary mission however the anti-terrorism operations we perform do routinely and frequently uncover other violations," said CBP Santa Teresa Port Director Joanne Thale-Lembo. "Every violation we stop at the border is important to the overall security of our nation."

The seizure was made just before 8 p.m. Tuesday night when a 2011 Ford Focus entered the port from Mexico. CBP officers initiated a search of the vehicle and occupants. CBP officers found that one person was carrying 411 fraudulent cards and 11 additional counterfeit cards being carried by another person. CBP officers contacted U.S. Secret Service agents who responded to the port of entry and took custody of the pair. Federal prosecution was accepted. The two are slated to make their initial appearance in federal court in Las Cruces Thursday.

CBP officers found that one person was carrying 411 fraudulent cards and 11 additional counterfeit cards being carried by another person.



CBP.gov

Securing America's Borders

About CBP

New

Chinese hackers suspected in attack on The Post's computers



Alex Wong/GETTY IMAGES - The Washington Post building in downtown Washington, DC.

The Washington Post

The Times and The Post used the same Alexandria-based security company, Mandiant, to secure their systems. Grady Summers, a vice president at Mandiant, declined to comment on the intrusion at The Post but said that in general, Chinese government hackers “want to know who the sources are, who in China is talking to the media. . . . They want to understand how the media is portraying them — what they’re planning and what’s coming.”

Wall Street Journal says also hit by Chinese hackers

AFP

By Rob Lever | AFP – Fri, Feb 1, 2013



AFP/Stan Honda -

The Wall Street Journal says its computers have been hit by Chinese hackers. It is the latest US media organization citing an effort to spy on its journalists covering China.

Wall Street Journal says also hit by Chinese hackers



By Rob Lever | AFP – Fri, Feb 1, 2013

The Wall Street Journal has become the second major US media organization to accuse Chinese hackers of targeting its computers in an apparent effort to spy on journalists covering China.

The announcement on Thursday came a day after The New York Times said hackers, possibly connected to China's military, had infiltrated its computers in response to its expose of the vast wealth amassed by a top leader's family.

The Journal reported that the attacks were "for the apparent purpose of monitoring the newspaper's China coverage" and suggested that Chinese spying on US media has become a "widespread phenomenon."

N.Y. Times hacked: How large is China's campaign to control, intimidate?

The list of media outlets infiltrated by Chinese cyberspies doesn't end with The New York Times or Wall St. Journal, cybersecurity experts say. Anyone reporting on China is a potential target.

By Mark Clayton | [Christian Science Monitor](#) – Fri, Feb 1, 2013

Cyberspies who breached computer networks of [The New York Times](#) and [Wall Street Journal](#) are part of a far larger global campaign of intrusions targeting news organizations worldwide that report on [China](#), according to cybersecurity experts and China policy analysts.

Early Thursday, the Times reported that cyberintruders last fall infiltrated its networks via Internet domains and addresses based in China, attempting to remove notes files and other information related to its reporting on the fortunes amassed by relatives of China's premier, [Xi Jinping](#). Later in the day, the Journal reported that its networks, too, had been hacked by intruders from China.

Intelligence Report: China Targets U.S. with Cyber-Espionage

By Barry Levine February 11, 2013

The National Intelligence Estimate noted that hacking for economic intelligence has been conducted by Russia, Israel and France, but said their efforts were minor compared with the attacks emanating from China. According to The Washington Post, the Obama administration is reviewing options, including formal diplomatic protests or expulsion of Chinese diplomats.

According to a report in Sunday's Washington Post, the National Intelligence Estimate pinpoints China as aggressively attempting to infiltrate the computers of American companies and governmental agencies, as a way to gain economic leverage.

There have also been cyber-attacks that reportedly came from China on the network security company RSA Security, the defense contractor Lockheed Martin, and The New York Times, The Wall Street Journal and The Washington Post.

Richard Clarke: China has hacked every major US company

By Emil Protalinski March 27, 2012, 1:04pm PDT

Summary: *Cybersecurity advisor Richard Clarke is warning the U.S. that its major companies are being regularly infiltrated by Chinese hackers employed by the Chinese government to steal R&D.*

Richard Clarke, a former cybersecurity and cyberterrorism advisor for the White House, was a U.S. government employee for 30 years: between 1973 and 2003. He worked during the times of Ronald Reagan, George H.W. Bush, Bill Clinton, and even George W. Bush. He may not be working under current U.S. president Barack Obama, but that doesn't mean he doesn't have something to warn about. He says state-sanctioned Chinese hackers are stealing R&D from U.S. companies, threatening the long-term competitiveness of America. We've heard this



before, but the way Clarke puts it makes the situation look even more dire.

Richard Clarke: China has hacked every major US company (CONTINUED)

By Emil Protalinski | March 27, 2012, 1:04pm PDT

"I'm about to say something that people think is an exaggeration, but I think the evidence is pretty strong," Clarke said during an interview with the [Smithsonian](#). "Every major company in the United States has already been penetrated by China. My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese. And we never really see the single event that makes us do something about it. That it's always just below our pain threshold. That company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars on R&D and that information goes free to China....After a while you can't compete."

Clarke notes that while the U.S. government is involved in espionage against other governments, it doesn't hack Chinese companies and then hand over intelligence to their American counterparts. He argues that the same cannot be said for the Chinese government.

Clarke's most famous warning came 10 weeks in advance of the events of 9/11: on July 5, 2001. The FAA, the Coast Guard, the FBI, the Secret Service, and the INS had gathered at the White House, where Clarke stated that "something really spectacular is going to happen here, and it's going to happen soon." For the sake of the U.S. economy, let's hope his warning about China doesn't eclipse the one from over 10 years ago.

Richard Clarke: China has hacked every major US company

By Emil Protalinski | March 27, 2012, 1:04pm PDT

"Every major company in the United States has already been penetrated by China. My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese."

TECHNOLOGY | April 21, 2009

Computer Spies Breach Fighter-Jet Project

By SIOBHAN GORMAN, AUGUST COLE and YOCHI DREAZEN

WASHINGTON -- Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

The latest intrusions provide new evidence that a battle is heating up between the U.S. and potential adversaries over the data networks that tie the world together. The revelations follow a recent Wall Street Journal report that computers used to control the U.S. electrical-distribution system, as well as other infrastructure, have also been infiltrated by spies abroad.

[U.S.](#) | [WORLD](#) | [CRIME](#) | [THE WEEK](#) | [NEWS PICS](#) | [BLOGS](#)

Chinese hackers stole F-35 fighter jet blueprints in Pentagon hack, Edward Snowden documents claim

The documents allege to show that the data was used in China's production of its own J-31 fighter jet, which has similarities to the F-35 stealth jet. Chinese officials denied the allegations.

BY SASHA GOLDSTEIN

[Follow](#)

/ NEW YORK DAILY NEWS

Tuesday, January 20, 2015, 9:22 AM

A A A

13

5

SHARE THIS URL



Share



Tweet



Reddit



+



+

nydn.us/1DY669v

COPY



BARTON GELLMAN/GETTY IMAGES

Former NSA contractor Edward Snowden released documents that claim to show Chinese hackers stole Pentagon information about its F-35 fighter jet program.

Chinese hackers stole “many terabytes” of data about the American F-35 stealth fighter jet, new documents provided by NSA whistle-blower Edward Snowden contend.

The stolen materials, taken from the Pentagon and contractor Lockheed Martin Corp., included radar designs and engine schematics used in the crown jewel of American military aircraft.

The Pentagon had previously admitted hackers were able to breach governmental networks, but never pointed to China and claimed that no classified information was taken.

China’s version of the stealth fighter, the newly released J-31, has similar design elements, defense experts told Reuters.

But Chinese authorities vehemently denied the hack claim, despite the document’s printed Sunday in German outlet, Der Spiegel.

New Snowden Documents Reveal Chinese Behind F-35 Hack

Experts have long argued that China has copied the F-35 design for its own fighter jets. Is this the proof?

By Franz-Stefan Gady
January 27, 2015



493 Shares
49 Comments

Last week, *Der Spiegel* published a new tranche of documents provided to the German weekly magazine by the former U.S. National Security Agency contractor, Edward Snowden. The documents are the first public confirmation that Chinese hackers have been able to extrapolate top secret data on the F-35 Lightning II joint strike fighter jet. According to sources, the data breach already took place in 2007 at the prime subcontractor Lockheed Martin. A U.S. government official recently claimed that as of now, "classified F-35 information is protected and remains secure."



Image Credit: U.S. Air Force

The Snowden files outline the scope of Chinese F-35 espionage efforts, which focused on acquiring the radar design (the number and types of modules), detailed engine schematics (methods for cooling gases, leading and trailing edge treatments, and aft deck heating contour maps) among other things. The document claims that many terabytes of data specific to the F-35 joint strike fighter program were stolen.

The *Byzantine Hades* hacks – the code name given to the attacks by U.S. investigators who traced the hacks back to a specific unit of the Chinese People’s Liberation Army first **revealed** by *Wikileaks* – have also targeted other programs and “cause serious damage to DoD interests,” **according** to a top secret power point presentation. The Chinese hackers were also successful in obtaining data on the B-2 stealth bomber, the F-22 jet, space-based lasers, missile navigation and tracking systems, as well as nuclear submarine/anti-air missile designs.

The power point furthermore lists at least 30,000 hacking incidents, more than 500 significant intrusions in DoD systems, at least 1600 DoD computers penetrated, and more than 600,000 user accounts compromised, in addition to over 300,000 user ID/passwords and 33,000 U.S. Air Force officer records compromised. The presentation makes the point of equating the amount of data extracted (50 terabytes) to be equal to five Libraries of Congress. Overall damage is estimated to be more than \$100 million.

As usual, the Chinese government has, denied any involvement in the attacks. “The allegations are totally groundless and unproven,” **emphasized** Chinese Foreign Ministry spokesman, Hong Lei, during a press conference last week. “We, on the other hand, do have documents that show a certain country has a dishonorable record on cyber security.”



F-35 LIGHTNING II

China's J-20 Stealth Jet Meant to Counter F-22, F-35, U.S. Analysis Says

By Tony Capaccio - Jan 6, 2011 5:43 PM CT

China's new stealth fighter likely was designed "to counter" the U.S. F-22 and F-35 jets, according to U.S. Navy intelligence analysts.



U.S. F-35 LIGHTNING II



What are the NATIONAL SECURITY implications of this “alleged” data theft?

Do they look similar?

CHINA allegedly stole TERABYTES

of technical and design data on the F-35



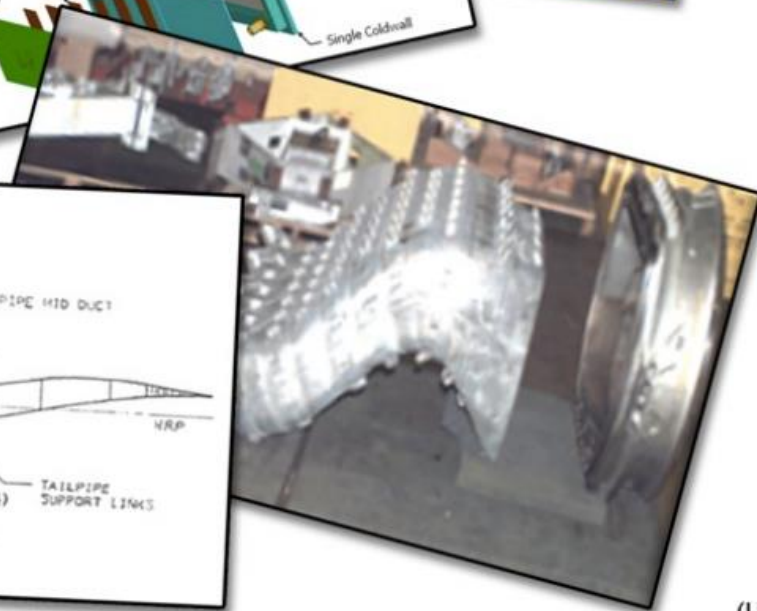
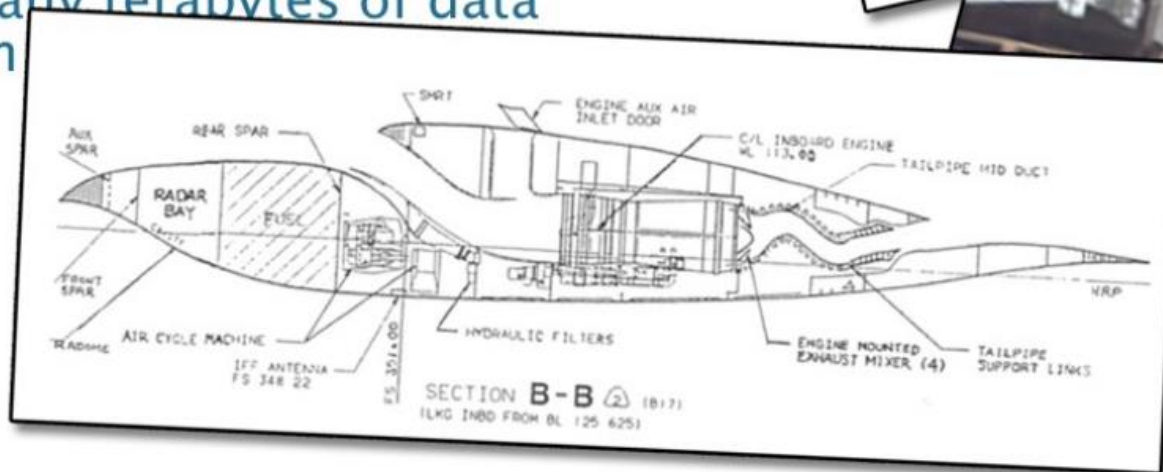
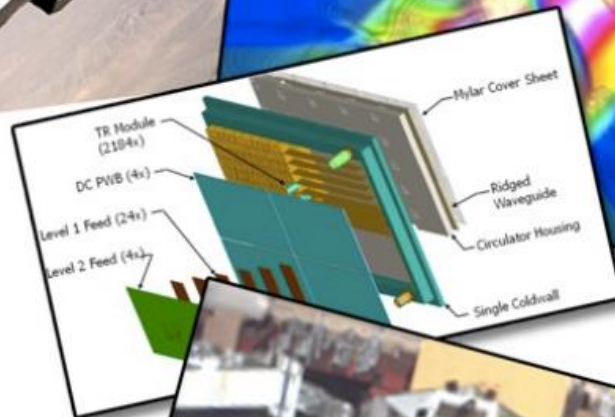
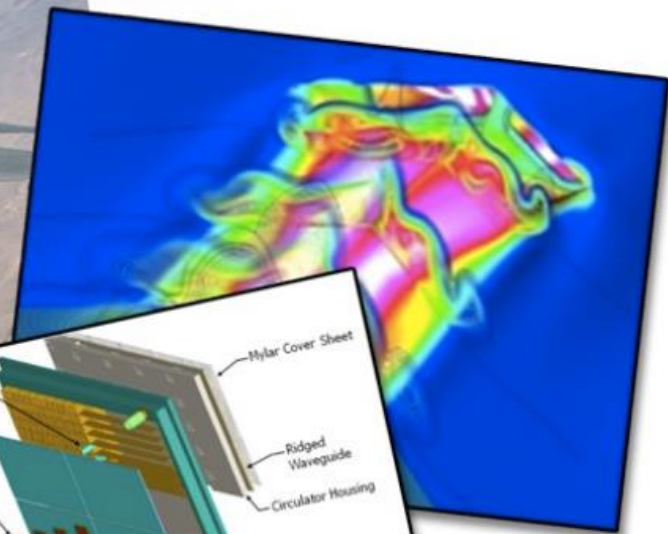
China's J-20 stealth fighter

(S//REL) Chinese Exfiltrate Sensitive Military Technology



- (U) Acquired radar design
 - (U) Numbers and types of modules
- (U) Detailed engine schematics
 - (U) Methods for cooling gases
 - (U) Leading and trailing edge treatments
 - (U) Aft deck heating contour maps
- (U) Many terabytes of data stolen

(U)



(U)



(S//REL) BYZANTINE HADES Causes Serious Damage to DoD Interests

(S//REL)

(S//REL) Resources Expended Towards

Response to Attacks

(S//REL) Personnel, Network, Logistics Data, Compromises

- At least +30,000 Incidents/+500 Significant Intrusions in DoD Systems
- At least +1600 Network Computers Penetrated
- At least 600,00 User Accounts Compromised
- +\$100 Million to Assess Damage, Rebuild Networks
- USPACOM: Air Refueling Schedules (CORONET)
- USTRANSCOM: Single Mobility System (SMS)
- U.S. Air Force: 33,000 General/Field Grade Officer Records
- Navy: Over 300,00 User ID/Passwords Compromised
- Navy: Missile Navigation and Tracking Systems
- Navy: Nuclear Submarine/Anti-Air Missile Designs

(S//REL) Science & Technology Export Controlled Data

- International Traffic and Arms Restrictions (ITAR) Data
- Contractor Research & Development
- Defense Industrial Espionage
 - B2, F-22, F-35, Space-Based Laser, Others

(S//REL)

(S//REL) Estimated Equivalent of Five Libraries of Congress (50 Terabytes)



TECHNOLOGY | April 8, 2009

Electricity Grid in U.S. Penetrated By Spies

By SIOBHAN GORMAN



Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

TECHNOLOGY | April 8, 2009

Electricity Grid in U.S. Penetrated By Spies

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."

TECHNOLOGY | April 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Intelligence officials worry about cyber attackers taking control of electrical facilities, a nuclear power plant or financial networks via the Internet.

Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, "If we go to war with them, they will try to turn them on." Officials said water, sewage and other infrastructure systems also were at risk.

"A number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure."

Last year, a senior Central Intelligence Agency official, Tom Donahue, told a meeting of utility company representatives in New Orleans that a cyberattack had taken out power equipment in multiple regions outside the U.S.

Russian and Chinese officials have denied any wrongdoing.

US POWER GRID ATTACKED BY HACKERS



Al Qaeda Encouraging Cyber Attacks on US



NEWS ROOM

BEWARE THE "ELECTRONIC JIHAD"
al Qaeda now encouraging "cyber attacks"

CNN

Haley to campaign with Walker in Wisconsin

NAS -31.56

Homeland Security Warns Cyber 9/11 Could Shut Down U.S.

NEWSFACTOR

By Jennifer LeClaire January 30, 2013

U.S. Secretary of Homeland Security Janet Napolitano said Friday she believes a "cyber 9/11" could happen "imminently." A coordinated terrorist cyberattack could effectively shut down the country, she says, and more needs to be done to prepare. "We shouldn't wait until there is a 9/11 in the cyber world," Napolitano told Reuters news service, referring to the massive terrorist attacks against the U.S. on September 11, 2001. "There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage."

"We are entering an era that will be marked by unprecedented attacks on our critical infrastructure"

The U.S. is ill-prepared to deal with mainstream malware outbreaks and unsophisticated network intrusions, let alone a highly coordinated attack.

DISCUSSION

Are We Really Under Cyber Attack?

CHINA? AL QAEDA?

RUSSIA? IRAN?

WHAT CAN THEY DO TO US?

WHAT CAN WE DO ABOUT IT?

HOW CAN WE PROTECT

OURSELVES?