National Aeronautics and Space Administration

NASA COUNTERINTELLIGENCE

Summer 2012

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

Message from Joseph S. Mahaley, NASA Assistant Administrator for Protective Services

It's a great pleasure and an honor for me to join NASA's incredibly talented team, including our counterintelligence/counterterrorism (CI/CT) professionals. In the short time that I've been here, I've already become well aware of the significant accomplishments and positive impact the counterintelligence effort has had on the protection of NASA's people, information, facilities, and operations every day.

Today, NASA, as well as other Federal agencies, continues to operate in a very challenging environment. The foreign intelligence and security service threats against NASA are real, multidimensional, and growing. We must address and confront these threats with our best efforts, every single day. That means not only working ongoing cases, but constantly doing our best to maximize our Agency workforce awareness of today's increasingly challenging CI/CT threats. It also means doing our best to understand our colleagues' work and how it interacts with and impacts our NASA-wide CI/CT program. This is crucial if we're going to maximize our CI/CT program's overall effectiveness.

Maximizing our CI/CT effectiveness is more important today than it's ever been. Each Center has an Office of Protective Services (OPS) CI/CT office, and I encourage all of you to get to know the agents assigned to your Center office. All CI/CT offices are prepared to provide you with current threat analysis and are also prepared to brief and prepare you for overseas travel threats.

The protection of NASA's workforce from foreign intelligence and terrorist activity is everyone's responsibility. The NASA CI/CT program is only a part of the total effort we all must make to ensure we keep NASA protected from the dangerous threats of espionage and terrorism.

Office of Protective Services

Assistant Administrator
Joseph S. Mahaley
202-358-3752

(b) (7)(E)

Counterintelligence/ Counterterrorism Division

Director
(b) (6), (b) (7)(C)

Operations
(b) (6), (b) (7)(C)

Arthur Payton
(b) (6), (b) (7)(C)

Administrative Assistant
(b) (6), (b) (7)(C)

Traveling Light in a Time of Digital Thievery

Adapted from an article published in the New York Times *on February 10, 2012, by Nicole Perlroth. The full article is available at* http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all.

When U.S. Government aerospace employee Bud Stemple travels to certain sensitive foreign destinations that are known to aggressively monitor visiting information technology (IT) devices, he follows a routine that seems straight from a spy film. He leaves his cell phone and laptop at home and instead brings "loaner" devices, which he erases before he leaves the U.S. and wipes clean the minute he returns. For instance, when he travels to China, he disables Bluetooth and wireless fidelity (WiFi), never lets his phone out of his sight, and, in meetings,

Continued on next page

Counterintelligence Quote

"Foreign attempts to collect U.S. technological and economic information by cyber espionage will continue at a high level in 2012 and will represent a growing and persistent threat to U.S. economic security."

—Antone Gonsalves, InformationWeek

the iBAHN broadband and entertainment service offered to guests of hotel chains such as Marriott International, Inc.

The practice of distributing malware through hotel chains' Internet connections is a domestic and international problem. A software engineer staying at a Marriott International hotel in the U.S. noticed that code was being injected into Web sites via the hotel WiFi connections for the purpose of pushing third-party advertisements to users. Marriott International released an official statement that this was done "unbeknownst to the hotel." In this situation, the advertisements were harmless; however, this cannot be reassuring to guests of the Marriott International—that the hotel chain did not know what was going on in their own network.

You don't have to leave the country or stay in a hotel to have your computer hacked by a foreign entity. Firms that have been compromised in this type of attack are believed to include Research in Motion Ltd. and Boston Scientific Corporation, as well as some of the largest corporations and niche innovators in sectors such as aerospace, semiconductors, pharmaceuticals, and biotechnology. By hacking into these companies hackers may have had access to millions of confidential e-mails, even encrypted ones, and company information.

NASA Counterintelligence Perspective

The best advice for NASA foreign travelers is to not perform any updates over a public, untrusted network. In fact, if you are traveling with any sensitive data or with a computer that later will be connected to a network with sensitive data, it makes sense to do as little as possible online. The idea is to take nothing along that you cannot afford to lose—including data.

NASA civil servants and contractors are encouraged to not initiate updates that pop up while using a hotel's WiFi connection. Avoid WiFi networks if you can. In some countries, wireless networks are controlled by security services and in all cases they are not secure. Spy software, which intercepts and transmits information without a user's knowledge, can be implanted in both wired and wireless Internet portals in cafes, hotels, transportation depots, and elsewhere. Once installed, malicious software can be used to further compromise computer systems and networks. Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Sanitize your laptops prior to travel and ensure no sensitive contact, research, or personal data is on them. Backup all information you take and leave that at home. If feasible, use a new e-mail account while traveling.

Clear your browser after each use by doing the following: delete history files, caches, cookies, and temporary Internet files. In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. If information might be valuable to another government, company, or group, you should assume that it will be intercepted and retained. Change all your passwords, including your voicemail's, and check your devices for malware when you return before communicating with home networks and especially before connecting to NASA networks.

2011 Congressional Report on Cyberspace Espionage

Foreign economic collection and industrial espionage against the U.S. represent significant and growing threats to the Nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now take place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect. Read more in "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace—October 2011 Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011" at *http://www.dni.gov/reports/20111103_report_fecie.pdf*.

NASA Center CI Offices

Ames Research Center
(b) (6), (b) (7)(C)

Dryden Flight Research Center
(b) (6), (b) (7)(C)

Glenn Research Center
(b) (6), (b) (7)(C)

Goddard Space Flight Center
(b) (6), (b) (7)(C)

Jet Propulsion Laboratory
(b) (6), (b) (7)(C)

Johnson Space Center
(b) (6), (b) (7)(C)

Kennedy Space Center
(b) (6), (b) (7)(C)

Langley Research Center
(b) (6), (b) (7)(C)

Marshall Space Flight Center
(b) (6), (b) (7)(C)

Stennis Space Center
(b) (6), (b) (7)(C)

CI homepage website
(b) (7)(E)

NASA COUNTERINTELLIGENCE

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

Summer 2012

"The Chinese are very good at covering their tracks," said (b) (6) a former FBI agent who specialized in counterintelligence and computer intrusion. "In most cases, companies don't realize they've been burned until years later when a foreign competitor puts out their very same product—only they're making it 30 percent cheaper."

"We've already lost our manufacturing base," he said. "Now we're losing our R&D [research and development] base. If we lose that, what do we fall back on?"

NASA Counterintelligence Perspective

NASA employees have legal obligations to protect U.S. sensitive information and technologies from being compromised. NASA employees are not immune to foreign intelligence cyberthreats while on travel. The targeting of NASA IT devices is low-cost and low-threat to perpetrators, and it's proven to yield high payoffs. Perpetrators are known to target both personal and professional IT devices that are in a NASA employee's possession for personally identifiable information, NASA intellectual property and trade secrets, and any information related to developing/game-changing NASA technologies to advance their own economies or aerospace industries and endanger U.S. technological advantages at a global level.

NASA civil servants and contractors who require the use of NASA-owned computer equipment while on foreign travel are required to adhere to the guidelines in NPD 2540.1G. The NASA Policy Directive (NPD) states it is the responsibility of the NASA civil servant or contractor to keep possession of NASA equipment at all times while on travel. When traveling by plane, it directs that all NASA IT equipment must remain with you as a carry on—never check your laptop with your luggage. Never let a laptop out of your sight in an airport. When traveling by vehicle, NASA IT equipment should not be left unattended or visible in the vehicle. These tips are for the safety and security of your equipment and will help guard against theft and from having malicious software downloaded onto your devices, which could extract information or install a virus, infecting the NASA network.

NPD 2540.1G

(1) Domestic Travel—When IT and/or computer equipment is taken out of the workplace (i.e., telework, offsite business meetings, and conferences), it is the responsibility of the employee to ensure that the equipment remains in their custody, is handled and maintained properly, and is returned in good condition. In the event that the equipment is lost, stolen, or damaged, the employee shall notify the NASA Enterprise Help Desk or NASA Security Operations Center as soon as possible after the occurrence of an incident.

(2) International Travel—The employee shall use only equipment officially approved for use outside of the U.S. for international business meetings, conferences, symposia, etc. The employee must ensure that the hardware remains in his or her possession while outside the U.S. Any loss, damage, or tampering shall be reported immediately/at the earliest opportunity to the Center CIO. Under no circumstances should Agency laptops or personal computers be used for official business on international trips unless written authorization is first obtained from the Center CIO.

NASA counterintelligence strongly recommends that NASA civil servants and contractors traveling abroad coordinate with their NASA IT Loaner Pool Program in advance to obtain loaner equipment such as laptops and smartphones for use while on travel.

Foreign Travel Alert: Beware of Malware Installed via Hotel Networks

The Federal Bureau of Investigation (FBI), through the Internet Crime Complaint Center (ISC3), has issued a warning that "malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms."

According to FBI findings, there has been an increase in instances of travelers' notebooks being infected with malicious software when connected to hotel Internet networks. It is thought that the method of infecting the notebooks occurs while users attempt to set up Internet connections in their rooms. Some users have been presented with a pop-up window that notifies users of an update from a widely used software product/company. When the users accept the update, malicious software is installed on their notebooks.

The FBI's Internet Crime Complaint Center has issued the following good advice for travelers:

- Carry out all software updates before traveling.
- Check the author or digital certificate of any prompted update to see if it corresponds to the software vendor.
- Download software updates directly from the vendor's Web site.

In addition to these helpful tips, it is recommended that all important information—including, but not limited to—e-mails, documents, instant messages (IMs), and Web logins should be sent over a secure Hypertext Transfer Protocol (HTTP) or a virtual private network (VPN). This FBI advisory follows a report from Bloomberg news which claims that Chinese hackers have stolen private data from as many as 760 firms by hacking into

Continued on next page

the iBAHN broadband and entertainment service offered to guests of hotel chains such as Marriott International, Inc.

The practice of distributing malware through hotel chains' Internet connections is a domestic and international problem. A software engineer staying at a Marriott International hotel in the U.S. noticed that code was being injected into Web sites via the hotel WiFi connections for the purpose of pushing third-party advertisements to users. Marriott International released an official statement that this was done "unbeknownst to the hotel." In this situation, the advertisements were harmless; however, this cannot be reassuring to guests of the Marriott International—that the hotel chain did not know what was going on in their own network.

You don't have to leave the country or stay in a hotel to have your computer hacked by a foreign entity. Firms that have been compromised in this type of attack are believed to include Research in Motion Ltd. and Boston Scientific Corporation, as well as some of the largest corporations and niche innovators in sectors such as aerospace, semiconductors, pharmaceuticals, and biotechnology. By hacking into these companies hackers may have had access to millions of confidential e-mails, even encrypted ones, and company information.

NASA Counterintelligence Perspective

The best advice for NASA foreign travelers is to not perform any updates over a public, untrusted network. In fact, if you are traveling with any sensitive data or with a computer that later will be connected to a network with sensitive data, it makes sense to do as little as possible online. The idea is to take nothing along that you cannot afford to lose—including data.

NASA civil servants and contractors are encouraged to not initiate updates that pop up while using a hotel's WiFi connection. Avoid WiFi networks if you can. In some countries, wireless networks are controlled by security services and in all cases they are not secure. Spy software, which intercepts and transmits information without a user's knowledge, can be implanted in both wired and wireless Internet portals in cafes, hotels, transportation depots, and elsewhere. Once installed, malicious software can be used to further compromise computer systems and networks. Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Sanitize your laptops prior to travel and ensure no sensitive contact, research, or personal data is on them. Backup all information you take and leave that at home. If feasible, use a new e-mail account while traveling.

Clear your browser after each use by doing the following: delete history files, caches, cookies, and temporary Internet files. In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. If information might be valuable to another government, company, or group, you should assume that it will be intercepted and retained. Change all your passwords, including your voicemail's, and check your devices for malware when you return before communicating with home networks and especially before connecting to NASA networks.

2011 Congressional Report on Cyberspace Espionage

Foreign economic collection and industrial espionage against the U.S. represent significant and growing threats to the Nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now take place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect. Read more in "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace—October 2011 Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011" at *http://www.dni.gov/reports/20111103_report_fecie.pdf*.

NASA Center CI Offices

Ames Research Center
(b) (6), (b) (7)(C)

Dryden Flight Research Center
(b) (6), (b) (7)(C)

Glenn Research Center
(b) (6), (b) (7)(C)

Goddard Space Flight Center
(b) (6), (b) (7)(C)

Jet Propulsion Laboratory
(b) (6), (b) (7)(C)

Johnson Space Center
(b) (6), (b) (7)(C)

Kennedy Space Center
(b) (6), (b) (7)(C)

Langley Research Center
(b) (6), (b) (7)(C)

Marshall Space Flight Center
(b) (6), (b) (7)(C)

Stennis Space Center
(b) (6), (b) (7)(C)

CI homepage website
(b) (7)(E)