OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

USGS IT SECURITY VULNERABILITIES

This is a revised version of the report prepared for public release.

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

OCT 17 2018

Memorandum

To: William H. Werkheiser
Acting Director, U.S. Geological Survey

From: Matthew T. Elliott
Assistant Inspector General for Investigations

Subject: Management Advisory – USGS IT Security Vulnerabilities

The Office of Inspector General (OIG) initiated an investigation into suspicious internet traffic discovered during an IT security audit of the computer network at the U.S. Geological Survey (USGS), Earth Resources Observation and Science (EROS) Center satellite imaging facility in Sioux Falls, SD. The audit found indications that USGS employee [redacted] computer was compromised and infected with malware. We sought to confirm how a compromise occurred.

We found that [redacted] knowingly used U.S. Government computer systems to access unauthorized internet web pages. We also found that those unauthorized pages hosted malware. The malware was downloaded to [redacted] Government laptop, which then exploited the USGS' network. Our digital forensic examination revealed that [redacted] had an extensive history of visiting adult pornography websites. Many of the 9,000 web pages [redacted] visited routed through websites that originated in Russia and contained malware. Our analysis confirmed that many of the pornographic images were subsequently saved to an unauthorized USB device and personal Android cell phone connected to [redacted] Government-issued computer. We found that [redacted] personal cell phone was also infected with malware.

During the investigation, we identified two vulnerabilities in the USGS' IT security posture: web-site access and open USB ports. Malware is rogue software that is intended to damage or disable computers and computer systems. In addition, a common goal of malware is to steal confidential information while spreading to other systems. Common methods to prevent malware incidents involve a combination of employee training (Rules of Behavior) and access controls (hardware and software technologies).

The U.S. Department of the Interior's (DOI's) IT Rules of Behavior prohibit employees from using DOI systems for illegal or inappropriate activities, explicitly including the viewing or distribution of pornography (Rule 6). The IT Rules of Behavior also direct employees to refrain from connecting personal devices, such as USB drives and cell phones, to Government-issued computers or networks (Rule 9). The USGS currently does not disable USB connections on Government-issued computers.

The DOI's annual IT security training requires employees to sign a statement indicating they understand the directives and agree to abide by them. [redacted] admitted he received the required IT security training annually, and we confirmed he agreed to the Rules of Behavior for several years prior to detection.

Recommendations

We recommend that the USGS enforce a strong blacklist policy of known rogue Uniform Resource Locators (more commonly known as a web addresses) or domains and regularly monitor employee web usage history. Since this incident, the EROS Center has deployed enhanced intrusion detection systems and firewall technology to assist in the prevention and detection of rogue websites trying to communicate with Government systems. An ongoing effort to detect and block known pornographic web sites, and web sites with suspicious origins, will likely enhance preventative countermeasures.

We further recommend that USGS employ an IT security policy that would prevent the use of unauthorized USB devices on all employee computers. Best practices for malware incident protection include restricting the use of removable media and personally owned mobile devices.[1]

Please provide a written response within 90 days of receipt of this management advisory indicating whether you intend to implement the suggested recommendations. We periodically send this information to Congress and the Department and use it for internal review purposes. You may either email your response to doioigreferrals@doioig.gov, or mail it to:

Office of Inspector General
U.S. Department of the Interior
381 Elden Street, Suite 3000
Herndon, VA 20170

In accordance with the IG Empowerment Act of 2016, we intend to publish this memorandum on our website, in redacted form, no later than 3 days from the date we issue it to you. Within the next 10 business days, a representative from our Office of Investigations will contact you, or your designee, to discuss the memo and the status of your response. If you have any questions or need further information concerning this matter, please contact me at 202-208-5745.

cc: [redacted], HR Specialist, Headquarters Personnel Office, U.S. Geological Survey
Judy Nowakowski, Chief of Staff, U.S. Geological Survey

[1] NIST Special Publication 800-83, Rev. 1, "*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*", at http://dx.doi.org/10.6028/NIST.SP.800-83r1, pages 7, 9.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doioig.gov

By Phone: 24-Hour Toll Free: 800-424-5081
Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240