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

INVESTIGATIVE REPORT OF IT SECURITY INCIDENT AT USGS FACILITY

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

Report Number: 17-0444 Web Posting Date: November 20, 2018

SYNOPSIS

The Office of Inspector General investigated 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 a USGS employee's computer was compromised and infected with malware. We sought to confirm how a compromise occurred.

We found that the employee knowingly used U.S. Government computer systems to access unauthorized internet web pages. We also found that those unauthorized pages hosted malware that downloaded to the employee's Government laptop. The malware then exploited USGS' system; it introduced additional malicious code, reduced the Department's ability to monitor exploits, introduced a covert channel program, and automatically connected to malicious websites in Russia. We did not find evidence that the employee intentionally introduced the malware, nor was there evidence of data exfiltration. We issued a separate Management Advisory related to this investigation discussing vulnerabilities in USGS' IT security posture.

The employee retired a day before his employment was to be terminated. We are providing this report to the Director of the USGS for any action deemed appropriate.

DETAILS OF INVESTIGATION

The Office of Inspector General investigated 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 discovered a U.S. Department of the Interior (DOI) Domain Name Server (DNS) requesting a .SU (Soviet Union) IP address. Our initial log reviews indicated that an EROS employee's laptop contained malware, some of which automatically connected to multiple servers for approximately 11 months, including sites hosting pornography and sites in the .RU (Russia) domain. Though the EROS Center houses classified information, we found no indication that classified material was released.

Malware, also known as malicious computer code, is a generic term that describes a covertly inserted program intended to destroy data; run destructive or intrusive programs; or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, operating system, or computer network.[1] Examples of malware include computer viruses, spyware, ransomware, Trojans, worms, and similar destructive programs. Malware can cause widespread damage and disruption and may require extensive recovery efforts after infection.

USGS Employee Knowingly Used Government Property for Unauthorized Purposes

Our investigation substantiated that the employee's unauthorized activity introduced malware onto the network. The employee confessed to routinely visiting adult pornography websites for many years, using his USGS-issued laptop. The employee admitted that he knew it was wrong to

[1] Adapted from 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, page 2.

view pornography on his Government computer.

Our digital forensic examination revealed the employee's extensive history of adult pornography surfing. We confirmed that between September 26, 2016 and March 13, 2017, the employee's user profile accessed more than 9,000 web pages containing adult pornography. Most of those web pages contained multiple pornographic images per page. Many of those web pages routed through websites that originated in Russia and contain 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 the employee's Government-issued computer.

The digital forensic examination results also confirmed the presence of malware, which was introduced to the USGS network via the employee's internet activity. The personal cell phone that the employee connected to his Government computer was also infected, though we could not determine whether that occurred through his downloading of unauthorized images from his work computer, or from another source, such as his home computer. Though the introduction of unauthorized devices was intentional, we found no evidence that the employee intended to infect Government systems with malware, or that he knew it was there, either through the website downloads or the connection of unauthorized USB devices.

The 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). USGS policy does not require that USB connections be disabled on Government-issued computers.

The DOI's annual IT security training for employees requires employees to sign a statement indicating they understand the directives and agree to abide by them. The employee admitted he received the required IT security training annually, and we confirmed that he completed Federal Information Systems Security Awareness + Privacy and Records Management training each year, from 2009 to 2016, and completed the DOI Rules of Behavior and Warning Banner training in 2017. All of these courses included Rules of Behavior training. In addition, our forensic analysis revealed that the acceptable use warning banner was installed on the employee's laptop, which prompts the user to acknowledge the warning at the time of each login for the system to fully boot and become functional.

SUBJECT

GS-12 employee (retired)
Earth Resources Observation and Science Center
U.S. Geological Survey
Sioux Falls, SD

DISPOSITION

The employee retired from USGS on November 25, 2017, the day before his employment was to be terminated. We are providing this report to the Director of the USGS for any action deemed appropriate.

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