

Government Credentials on the Open Web

Recorded Future identified the possible exposures of login credentials for 47 United States government agencies across 89 unique domains. As of early 2015, twelve of these agencies allowed some of their users access to computer networks without any form of two-factor authentication. Doing so heightens the risk of cyber espionage, crime, or attack for these agencies.

The data presented here was identified through open source intelligence (OSINT) collection and analysis of seventeen paste sites including Pastebin.com during a one year period ending in November 2014. Recorded Future shared this information with the majority of affected agencies in late 2014 and early 2015.

At the time of our analysis, the Department of Energy had the widest exposure, with email/password combinations for nine different domains identified on the open Web. The Department of Commerce was the second hardest hit, with seven domains suffering exposures.

The February 2015 [Office of Management and Budget \(OMB\) report to Congress](#) highlighted twelve agencies that do not require most privileged users to use any form of two-factor authentication to log in: General Services Administration; USAID; and the departments of State, Veterans Affairs, Agriculture, Housing and Urban Development, Transportation, Treasury, Health and Human Services, Energy, Interior and Homeland Security.

All of these agencies had domains paired with passwords listed on the open Web in late 2013 and 2014.

The presence of these credentials on the open Web leaves these agencies vulnerable to espionage, socially engineered attacks, and tailored spear-phishing attacks against their workforce. While some agencies employ VPNs, two-factor authentication, and other tokens to provide a safety net, many agencies lag behind as cited by the OMB report to Congress.

Recent Senate testimony suggested that these factors - and the lack of two-factor authentication - directly affected the recently identified [Office of Personnel Management \(OPM\) breach](#).

Of note, most of these exposures identified by Recorded Future occurred outside the government agencies' reach due to vulnerabilities in third-party websites and employee use of government email accounts to register for Web-based services.

Often, and in a large majority of the exposed credentials, passwords were "weak" and lacked complexity, making it trivial for cyber criminals to decode hashes using lookup tables and easily obtainable password cracking tools.

According to multiple studies of password habits, [approximately 50%](#) of Americans use the same username/password combination to access multiple sites—including their employers' networks. As a result, if a third-party website's username/password database is hacked and the employee used the same login credentials on that website as at work, those credentials could allow unauthorized access to the employer's network.

What is a paste site?

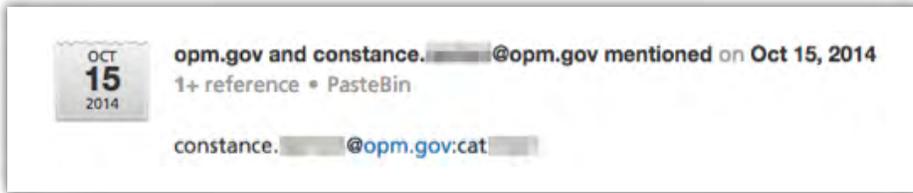
All of the credentials identified by Recorded Future were found in paste sites.

A "paste site" is a Web application that allows a user to store and share plain text. These sites are regularly used to share snippets of code. The largest site is Pastebin, although dozens of similar sites exist. In many cases, the paste was removed after a short period of time.

In practice, paste sites have become a dumping ground for stolen credentials, and [Facebook has begun mining them](#) to enhance user security.

OPM Focused Survey

Recorded Future analyzed a range of domains associated with the Office of Professional Management. OPM.gov was found paired with multiple clear text or hashed passwords in our open source analysis.



An OPM leaked credential from Recorded Future analysis.

What Constitutes Exposure?

An exposure consists of an email and password combination, with the two most common variants taking the following forms:

Email + plain text password

[redacted]@hhs.gov | [redacted]lawn8

Email + hashed password

[redacted]@dot.gov | [redacted]3486c32492326b78400

Supported by publicly available information on data.gov, this OSINT research analyzed Recorded Future's indexed paste sites for mentions of all [Federal Executive Agency domains](#) (e.g., [whitehouse.gov](#)) on seventeen paste sites including Pastebin.com from November 3, 2013 to November 3, 2014.



Example of a query and returned results.

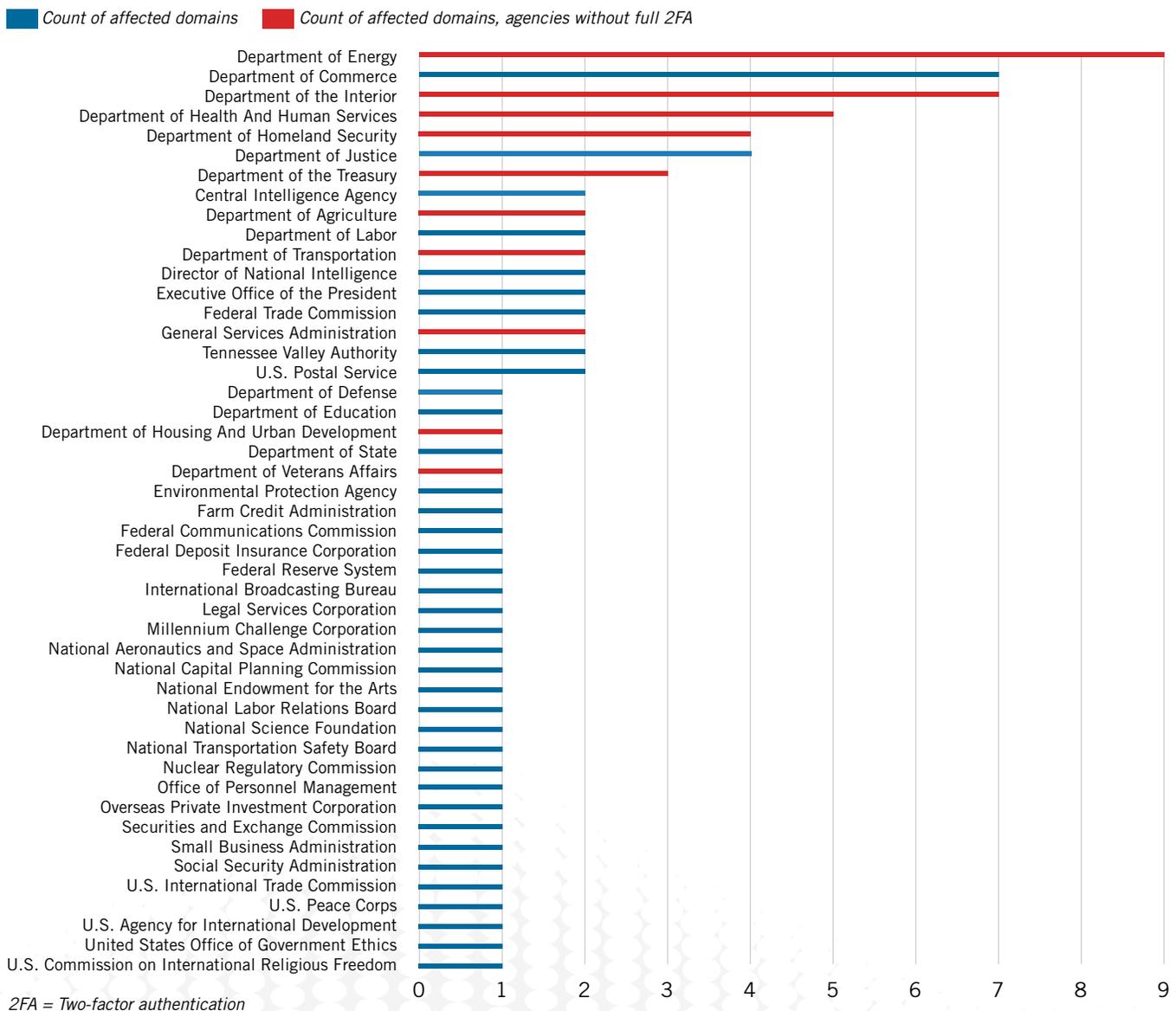
Gauging Exposure is Difficult

When results returned for the various domains, Recorded Future confirmed the presence of U.S. government email accounts paired with plain text or hashed passwords.

In many cases, our research identified the immediate removal of the credentials by sites such as pastebin.com. However, to Recorded Future’s knowledge, no efforts have been made to contact government agencies whose credentials may be posted on a paste site. Further, while the information may be removed from a paste site, it likely still circulates in private circles and is available to the original attackers. Due to the lack of context with most publicly announced data exfiltration, it’s unclear when specific attacks occurred or if the original attacker had attempted to leverage any stolen information.

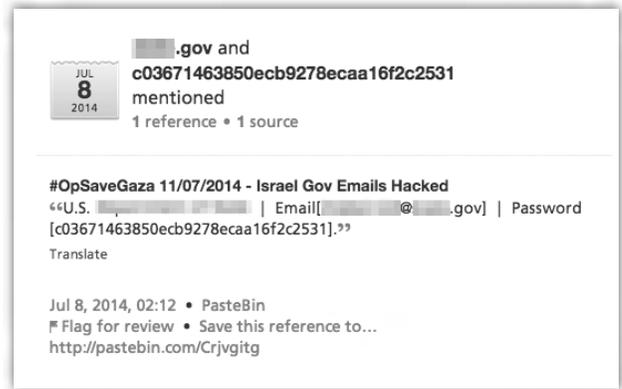
However, in multiple cases, government email addresses paired with a password remain easily identifiable online. Because approximately 50% of workers reuse a single password, many of these password combinations were likely valid at some point in time.

Count of Domains With Leaked Credentials, per Department or Agency



The leaked credentials originated from a range of vectors, targeted and untargeted. Government agencies have been specifically targeted by hacktivists with political motivations, such as individuals associated with #OpSaveGaza, and #OpLeak. Other leaks were perpetrated by actors claiming affiliation with LulzSec, SwaggSec, Wikileaks, and Anonymous.

However, many credentials are just included in email and password dumps from hacks that lacked targeting and exploited a window of opportunity on a vulnerable third-party site, service, or individual. Examples of this include the hacking of a natural history museum, a sports news site, and an individual USG employee. Often, these attacks leverage freely-traded exploits against unpatched sites and servers.



Many of these government entities maintain both classified and unclassified networks, storing privileged information on the classified networks. Much can be gleaned from examining unclassified systems readily accessible from the open Web, and login portals are easily found through simple search engine queries.

Recommended Actions

Exposure via Third-Parties



- › Enable multi-factor authentication and/or VPNs.
- › Require Government employees to use stronger passwords and change those passwords with greater regularity.
- › Gauge and define use of government email addresses on third-party sites.
- › Maintain awareness of third-party breaches and regularly assess exposure.
- › Ensure Robot Exclusion Standard (robots.txt) is set for government login pages to prevent listing of webmail/Web-services in search engines.

Where Are the Specific Domains and Logins?

As with our previous research on exposed credentials, Recorded Future made the editorial decision to not identify the list of specific exposed domains and associated credentials, since an email/password pairing from a third-party site does not guarantee a valid credential for that agency’s webmail or network. We do not aim to claim any specific breaches, only to highlight potential evidence in open source. Further, some agencies have VPNs, two-factor authentication, tokens, etc. that would remediate such a leak.

That said, many credentials with easily discoverable logins remain posted to social media, forums, and paste sites. While

Pastebin.com attempts to monitor its content, many similar paste sites do not, and we refrain from highlighting them in this document.

Scope and Methodology

Recorded Future analysts leveraged real-time indexes of over 660,000 open Web sources - focusing on a subset a data covering hard-to-navigate paste sites. The analysts queried Recorded Future with large lists of USG domains identified on data.gov. Searches leveraging technical entities and a mix of terms associated with credential exposures were used to identify references to USG credentials.

Recorded Future analyzed data from November 3, 2013 to November 3, 2014 and focused on a small subset of our open Web data, which suggests a much larger level of exposure than is currently identifiable.

Recorded Future regularly works with government organizations and private companies to identify emerging threats including cyber attacks. No privileged information was included in this analysis and our research was conducted with only openly available information on the Web. This analysis was not conducted on behalf of any Recorded Future client.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA | © Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners. | 2/15
Released: June 2015