Recorded Future

The Fortune 500's Unfortunate 221

Threat Intelligence Report

Released: October 29, 2014 • Reference ID: 2014-01

Recorded Future Special Intelligence Desk

The Fortune 500's Unfortunate 221

Recorded Future analysis identified employee credential exposures for at least 44% of Fortune 500 companies in 2014. These 221 companies account for 51% of top financial firms, 62% of technology firms, and 49% of public utilities in the Fortune 500. Thirty eight financial firms suffered exposures, opening the door for advanced persistent threats (APTs) and well-tailored spear-phishing attacks.

Of note, most of these exposures occurred outside the companies' reach due to vulnerabilities on third-party sites or employee use of work email accounts to register for Web-based services. "High-touch" industries were hit the hardest: 35 consumer services companies suffered exposures, second only to the financial industry.

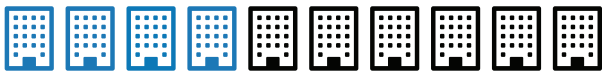
Efforts to leverage these stolen credentials against the companies are not fully known. The recent claimed attack against Dropbox followed this model, as "attackers … used these stolen credentials to try to login to sites across the internet, including Dropbox."

Open Source Intelligence Analysis

This analysis of open source intelligence (OSINT) focused on corporate email and password combinations posted to a variety of forums and paste sites from January 1, 2014 through October 8, 2014. Most of these posted exposures resulted from small-scale cyber attacks leveraging freely-traded exploit tools against unpatched sites and servers.

The identification of corporate email accounts paired with either fully or partially (hashed) exposed passwords was drawn from Recorded Future's coverage of over 600,000 open Web sources across seven languages.

The presence of these credentials on the open Web leaves these 221 companies vulnerable to corporate espionage, socially engineered cyber attacks, and tailored spear-phishing attacks. While some companies employ virtual private networks (VPNS), two-factor authentication, and other tokens to provide a safety net, many others don't.



44%

of Fortune 500 companies have employees with leaked credentials on the open Web.

Fortune 500 Exposures by Industry

Total	Industry
38	Finance
35	Retail / Consumer Services
26	Technology
19	Public Utilities
19	Capital Goods
17	Basic Industries
16	Healthcare
15	Energy
15	Consumer Non-Durables
11	Consumer Durables
10	Transportation
221	**Total Fortune 500 Exposures**

In particular, Recorded Future research highlighted multiple public utilities with webmail login pages easily discovered with Google searches.

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

Additionally, the exposure of company email addresses tied to trade associations, partner companies, etc. leaves the door open to spear-phishing campaigns similar to those used most recently by the Sandworm Team.

Nearly all of the exposed credentials were singular in nature due to their one-off use for registration on a third-party site. Some were due to poor employee operational security (OPSEC). Our analysis identified multiple instances of corporate email used for registration of personal accounts including commentary on blogs, hotel testimonials, and antique sites.

Recorded Future's identification of the 221 companies affected by recent credential exposures was drawn from the public domain and focused on paste sites and forums. Most often, exposed credentials were posted online by hacktivists in support of a variety of causes, or to just build community credibility. The presence of these exposed credentials may enable larger and more capable attacks by nation states and criminal enterprises.

Gauging Exposure is Difficult

In many cases, our research identified the immediate removal of the credentials which is likely a result of company complaints. Due to the lack of context with most publicly announced data exfiltration, it's unclear when the specific attacks occurred or if the attacker had attempted to leverage any of the stolen information.

However, in multiple cases, Fortune 500 company email addresses paired with a password remain easily identifiable online. As over half of American workers reuse a single password, these password combinations were more than likely valid at some point in time.

What is a Paste Site?

Most 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.

Exposure via Third-Parties

Where Are the Company Names?

Recorded Future made the editorial decision to not name the 221 exposed companies, as a leaked credential pairing from a third-party site does not guarantee a valid credential for that company's webmail or network. We do not aim to claim any specific breaches, only to highlight potential evidence in open source. Further, many companies have VPNs, two-factor authentication, tokens, etc. that would remediate such a leak.

However, many credentials for companies with easily discoverable logins remain posted to forums and paste sites. While Pastebin attempts to monitor its content, many similar paste sites do not, and we refrain from highlighting them in this document.

If you feel you may be one of the exposed companies then please have your information security department contact us at info@recordedfuture.com and we'll share the details in a confidential manner.

Scope Note

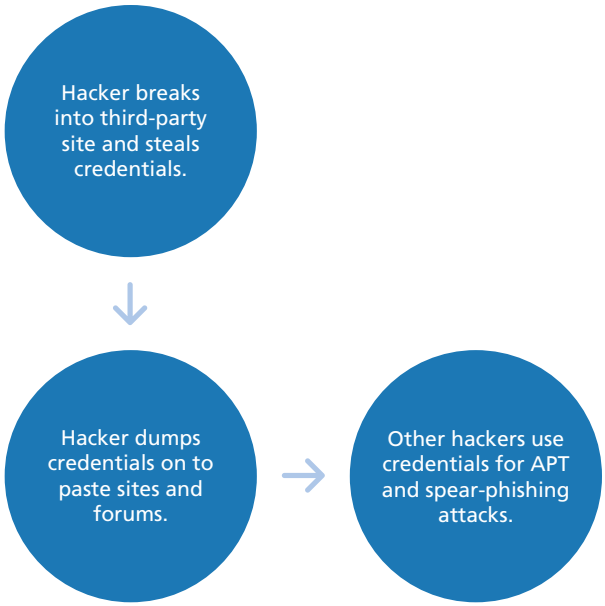
This analysis leveraged real-time indexing of more than 600,000 open Web sources. Recorded Future analysts applied large lists of domains associated with the Fortune 500 to the data. Searches leveraging technical entities and a mix of terms associated with credential exposures were used to identify references to company credentials.

Recorded Future's analysis did not include all subdomains of companies or divisions associated with the parent Fortune 500 company. This, combined with the focus on open source postings, suggests a much larger level of exposure than is currently discoverable.

Recorded Future frequently works with companies to identify emerging threats including cyber attacks. No privileged information was included in this analysis.

This report was not conducted on behalf of any Recorded Future customer.

Credential Exploitation Process



Recommended Actions

With this information your security team should:

- Develop clear policies on employee use of company credentials on external sites.
- Enable multi-factor authentication.
- Consider secure email certificates.
- Require employees to change passwords with greater regularity.
- Maintain awareness of third-party breaches and routinely assess exposure.
- Tag webmail login pages to prevent listing in search engines.

About Recorded Future

Real-Time Threat Intelligence

The open Web is both a platform to create attacks and a source of information to prevent attacks. To shift the balance of power in your favor, our revolutionary technology organizes the public Web for analysis to provide you future, present, and past insight for emerging cyber threats.

Our Web Intelligence Engine structures data around cyber security events, actors, locations, and time to give you forecasting power. Operating at a massive scale in real time, Recorded Future scans, collects, and analyzes hundreds of thousands of Web sources in seven languages, and processes 5 billion events to cast the widest open source intelligence net and deliver tailored, timely insights to you.

REQUEST DEMO

www.recordedfuture.com

Media Inquiries
media@recordedfuture.com