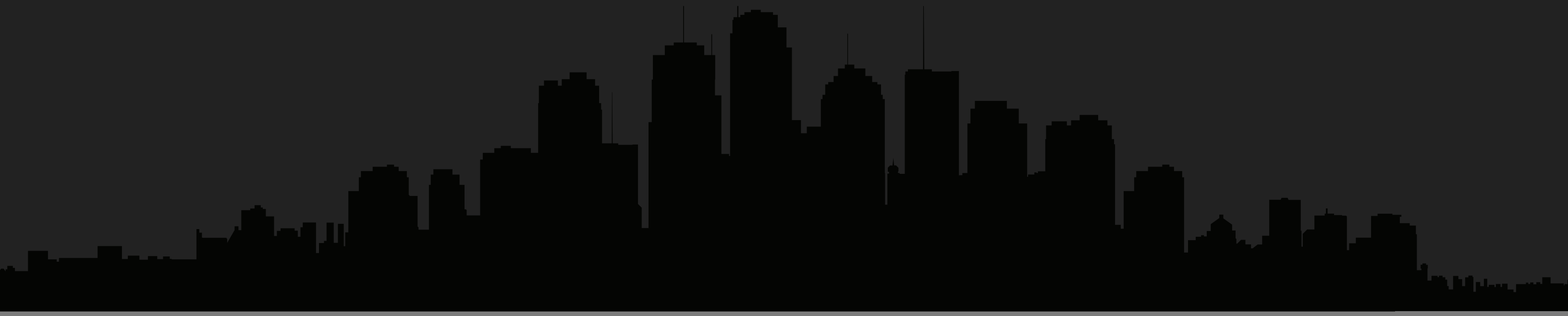
Recorded Future

Hackers Expose 49% of FT 500 Europe



Threat Intelligence Report

Released: June 2, 2015 • Reference ID: 2015-01

Recorded Future Special Intelligence Desk

Hackers Expose 49% of FT 500 Europe

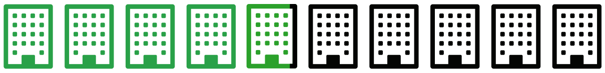
Recorded Future analysis identified recent employee credential exposures for at least 49% of the FT 500 Europe, a Financial Times listing of Europe's largest companies. These 244 companies account for 57% of top banks, 50% of oil and gas producers, and 64% of mobile telecommunications companies in the FT 500 Europe. Scores of companies supporting critical infrastructure were identified as having exposed network credentials on the open Web in just the last six months (Appendix A). This includes utility companies, healthcare providers, and defense contractors.

Of note, most of these exposures occurred outside the companies' reach due to vulnerabilities in third-party websites or employee use of work email accounts to register for a Web-based service. The hardest hit industries, as categorized by the Financial Times, include Industrial Engineering (81% of industry total), Electronics and Electrical Equipment (80%), and the Automotive (73%) industry. Of note, the Forestry and Paper industry saw all three companies exposed.

Mandiant research highlights stolen credentials as being present in 100% of attacks. The recent attack against Sony was perpetrated using this method, as explained in this quote by Gizmodo, "... whoever hacked Sony Pictures Entertainment did so by stealing credentials from a systems administrator." Efforts to leverage these stolen credentials against the exposed FT 500 Europe are not fully known. Figure 1 highlights how hackers can exploit exposed credentials.

Open Source Intelligence Analysis

This open source intelligence (OSINT) analysis focused on corporate email and password combinations posted to over two dozen paste sites during a six month period from November 5, 2014 through May 7, 2015. Most of these posted exposures resulted from small-scale cyber attacks leveraging freely-traded exploit tools against unpatched sites and servers.



49%

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

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.com, 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. Recorded Future analyzes text from 28 different paste sites.

The identification of corporate email accounts paired with either fully or partially (hashed) exposed passwords was drawn from Recorded Future's analysis of over 650,000 open Web sources across seven languages.

The presence of these credentials on the open Web leaves these FT Europe 500 companies vulnerable to corporate espionage, socially engineered cyber attacks, and tailored spear-phishing attacks against their workforce. While some companies employ VPNs, two-factor authentication, and other tokens to provide a safety net, many companies and industries lag behind.

In particular, Recorded Future research identified multiple utilities with webmail and extranet login pages easily discoverable with Google or Bing 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. Furthermore, multiple companies were identified to be using what appeared to be default passwords, even in the case of probable website administrative accounts.

Additionally, the exposure of company email addresses tied to trade associates, partner companies, etc., leaves the door open to spear-phishing campaigns similar to those used recently in the Woolen Goldfish campaign targeting European companies. Recorded Future research found 73 additional FT 500 Europe companies with corporate addresses traded and shared on paste sites.

In one case, an ISIS-associated hacking group posted a list of corporate email addresses, claiming to hold them responsible for the death of ISIS members. This particular paste (Appendix B) and the list of email addresses remained publicly available as of May 14, 2015.

Gauging Exposure is Difficult

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

Exposure via Third-Parties

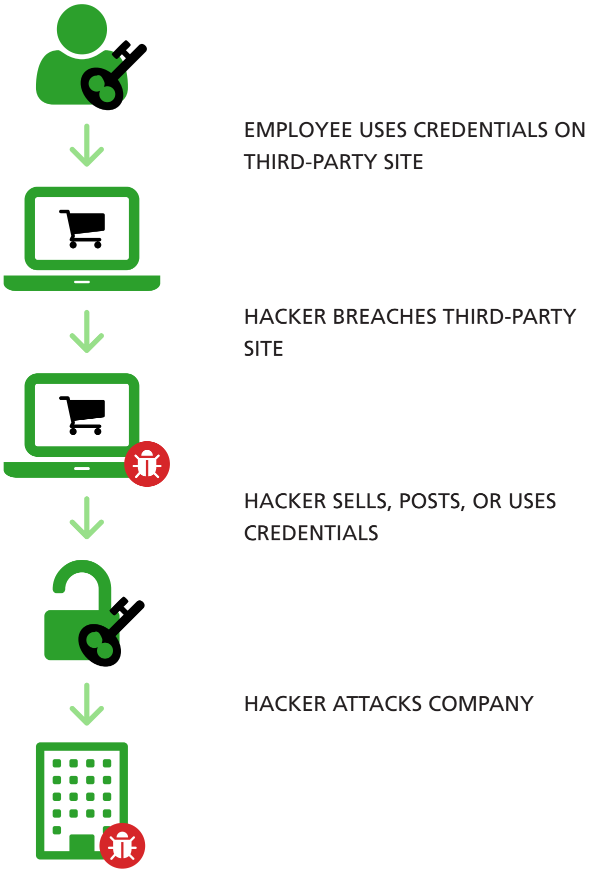

EMPLOYEE USES CREDENTIALS ON THIRD-PARTY SITE
HACKER BREACHES THIRD-PARTY SITE
HACKER SELLS, POSTS, OR USES CREDENTIALS
HACKER ATTACKS COMPANY

Figure 1: Process hackers use to exploit stolen credentials.

of corporate email personal usage for registration including travel sites, universities, commentary on blogs, and airline testimonials.

Recorded Future's identification of the 244 companies affected by recent credential exposures was drawn from the public domain and focused on paste sites. 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.

In many cases, our research identified the immediate removal of the credentials. However, to Recorded Future's knowledge, no efforts are made to contact companies 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, FT 500 Europe company email addresses paired with a password remain easily identifiable online. As over half of European workers reuse a single password, these password combinations were more than likely valid at some point in time.

Using Recorded Future's Web Intelligence Engine, we identified a consistent stream of leaked/stolen credentials (Appendix A) with no particular pattern. The only identified commonality was the significant number of third-party sites as sources of the spilled information.

Where Are the Company Names?

As with last year's report focusing on exposed credentials for major companies in the United States, Recorded Future made the editorial decision to not name the 244 exposed companies. 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, some companies have VPNs, two-

FT 500 Europe Exposures by Industry

Total	Industry
32	Banks
17	Chemicals
17	Industrial Engineering
12	Oil and Gas Producers
11	Automobiles and Parts
10	Nonlife Insurance
10	Support Services
9	Media
9	Pharmaceuticals and Biotechnology
7	Construction and Materials
7	Mobile Telecommunications
7	Personal Goods
7	Travel and Leisure
6	Fixed Line Telecommunications
6	Life Insurance
5	Aerospace and Defence
5	Electricity
5	Food Producers
5	General Industrials
5	Industrial Transportation
5	Software and Computer Services
5	Technology Hardware and Equipment
4	Beverages
4	Electronic and Electrical Equipment
4	Food and Drug Retailers
4	Gas, Water and Multiutilities
4	Household Goods and Home Construction
4	Oil Equipment and Services
3	Financial Services
3	Forestry and Paper
3	Health Care Equipment and Services
3	Mining
2	General Retailers
2	Industrial Metals and Mining
1	Real Estate Investment Trusts
1	Tobacco
0	Alternative Energy
0	Real Estate Investment and Services
244	**Total FT 500 Europe Exposures**

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

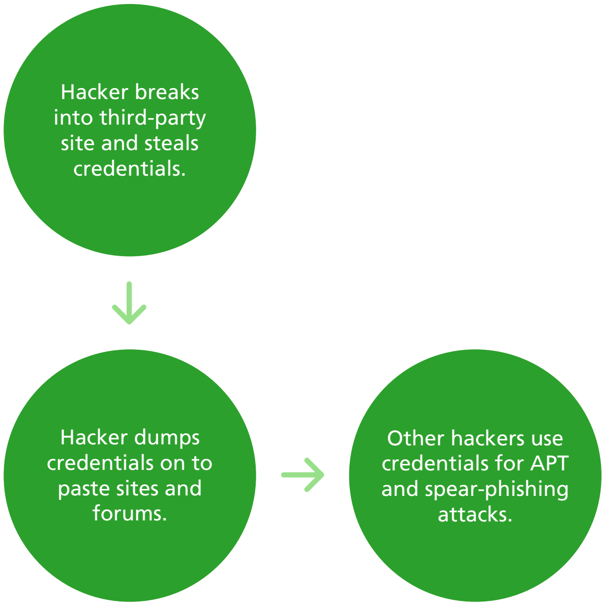
Recorded Future's analysis leveraged a real-time indexing of more than 650,000 open Web sources, including dozens of paste sites. Recorded Future analysts applied large lists of likely domains associated with the FT 500 Europe to the data. Searches leveraging technical entities and a mix of terms associated 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 FT 500 Europe company. This, combined with the focus on open Web postings, suggests a much larger level of exposure than is currently discoverable.

Recorded Future regularly 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


Hacker breaks into third-party site and steals credentials.

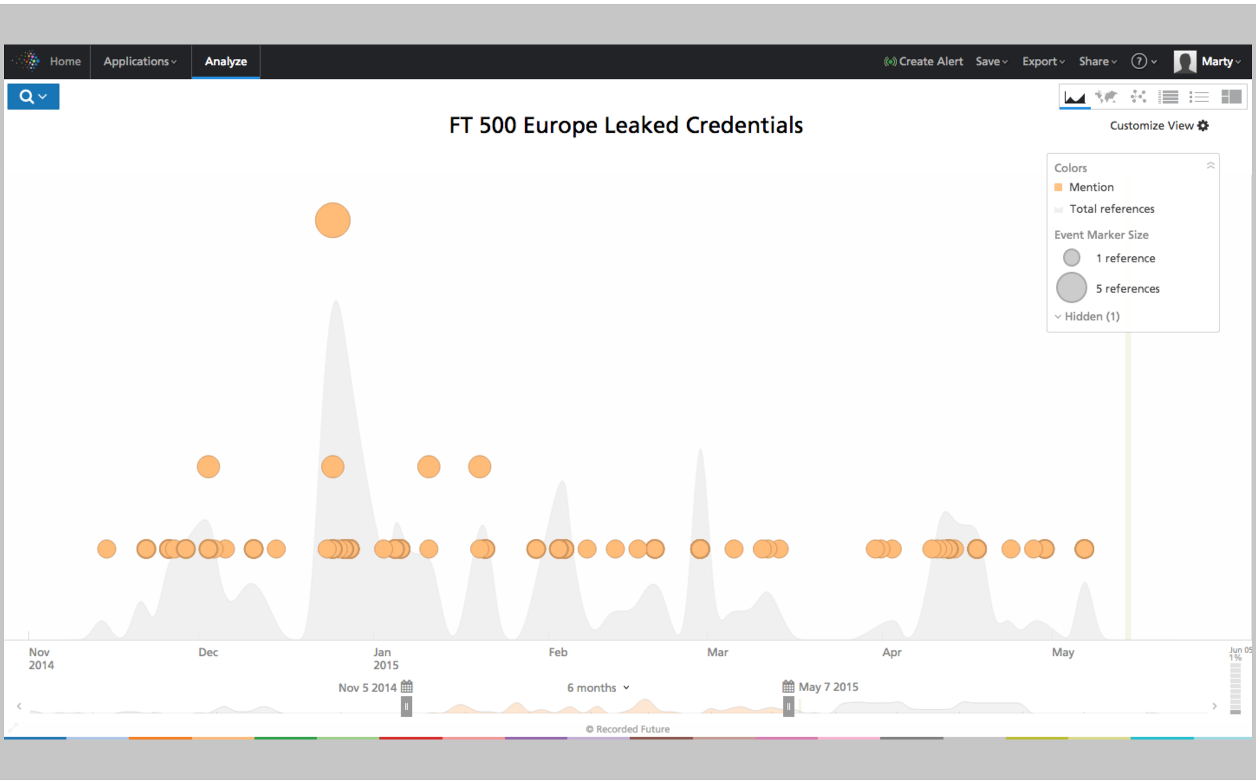
Hacker dumps credentials on to paste sites and forums.

Other hackers use credentials for APT and spear-phishing attacks.

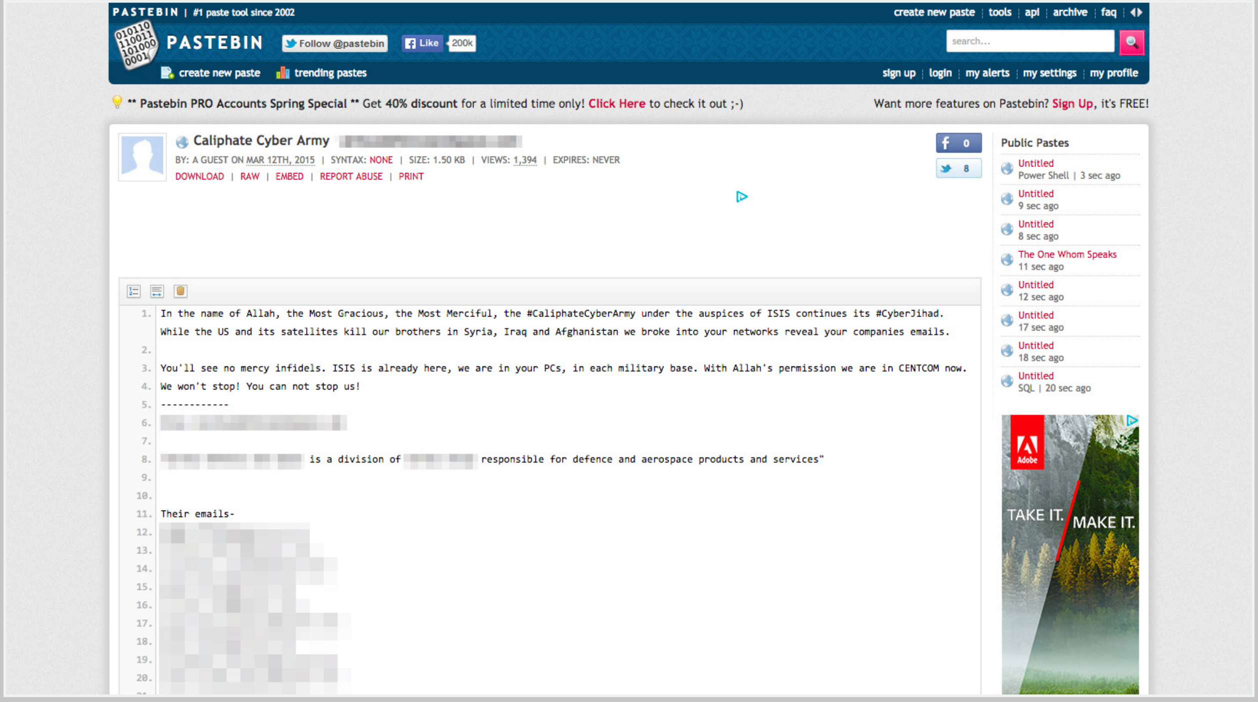
Recommended Actions

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.



Appendix A: Timeline showing consistent FT 500 Europe leaked credentials on the open Web over a six-month span.


PASTEBIN | #1 paste tool since 2002
create new paste | tools | api | archive | faq
PASTEBIN
Follow @pastebin
Like 200k
search...
create new paste
trending pastes
sign up | login | my alerts | my settings | my profile

** Pastebin PRO Accounts Spring Special ** Get 40% discount for a limited time only! Click Here to check it out ;-) Want more features on Pastebin? Sign Up, it's FREE!

Caliphate Cyber Army [redacted]

BY: A GUEST ON MAR 12TH, 2015 | SYNTAX: NONE | SIZE: 1.50 KB | VIEWS: 1,394 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
In the name of Allah, the Most Gracious, the Most Merciful, the #CaliphateCyberArmy under the auspices of ISIS continues its #CyberJihad.
While the US and its satellites kill our brothers in Syria, Iraq and Afghanistan we broke into your networks reveal your companies emails.

You'll see no mercy infidels. ISIS is already here, we are in your PCs, in each military base. With Allah's permission we are in CENTCOM now.
We won't stop! You can not stop us!
------------
[redacted]

[redacted] is a division of [redacted] responsible for defence and aerospace products and services"



Their emails-
[redacted]
```

Public Pastes

- Untitled
  Power Shell | 3 sec ago
- Untitled
  9 sec ago
- Untitled
  8 sec ago
- The One Whom Speaks
  11 sec ago
- Untitled
  12 sec ago
- Untitled
  17 sec ago
- Untitled
  18 sec ago
- Untitled
  SQL | 20 sec ago

Appendix B: Paste from Pastebin by Caliphate Cyber Army listing email addresses for an aerospace company in the FT 500 Europe.

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 Web for analysis to provide you future, present, and past insight into 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