

The image shows the Anomali logo in white, set against a dark blue background. The background is filled with a pattern of binary code (0s and 1s) and glowing blue lines, suggesting a digital or network environment. The logo itself is in a clean, sans-serif font with a trademark symbol.

ANOMALI™

**The FTSE 100:
Targeted Brand Attacks and Mass Credential Exposures**

Anomali Labs Report

Overview

A company's brand is a source of value and a target for cyber attackers. The brand represents the trust the company has invested in and developed with its customers. Exploiting trust or "hacking the human" is an essential part of the initial attacker activities. These involve getting the human to do something that might be against their best interests. These activities are represented as the initial steps in a chain of events known as the Cyber Kill Chain¹ (see Figure 1). The first phase of the Cyber Kill Chain, initial reconnaissance, is often problematic for organizations who don't know where to start to collect information about registrations of malicious domains and monitor company email address / plain text password combinations found in the dark web or places such as Pastebin.



Figure 1 -- Lockheed Martin Cyber Kill Chain courtesy of SANS

The attacker can often craft a domain name that is only slightly different from a company's domain name. This fake domain name can be leveraged as part of a social engineering-based attack with the aim of tricking users into clicking a URL and either entering credentials into a phishing website or exploiting the user's web browser and installing malware. Once malware gets into a targeted organization, it can act on behalf of a trusted employee or customer. Monitoring both suspicious domain registrations and compromised credentials can often amount to an early warning system for targeted attacks.

Anomali, as part of its threat intelligence platform service, uses machine learning algorithms to comb automatically new domain registrations looking for those that can be considered suspicious and represent a potential attack vector. Anomali also attempts to identify the registrant and country of origin for these suspicious domains.

Suspicious Domain Registrations

The focus of this report is to look at the Financial Times Stock Exchange 100 (FTSE 100 Index) to identify suspicious domain registrations and potentially compromised accounts that could be used as part of an attack. The purpose of the report is not to disclose specific company names but rather to examine trends and heighten awareness of this kind of data as a valuable tool for early warning of a possible attack. The following represents a snapshot of data on the FTSE 100 we've collected over the last three months and our observations of this growing problem.

¹The Cyber Kill Chain is a registered trademark of Lockheed Martin Corporation

Malicious Domains

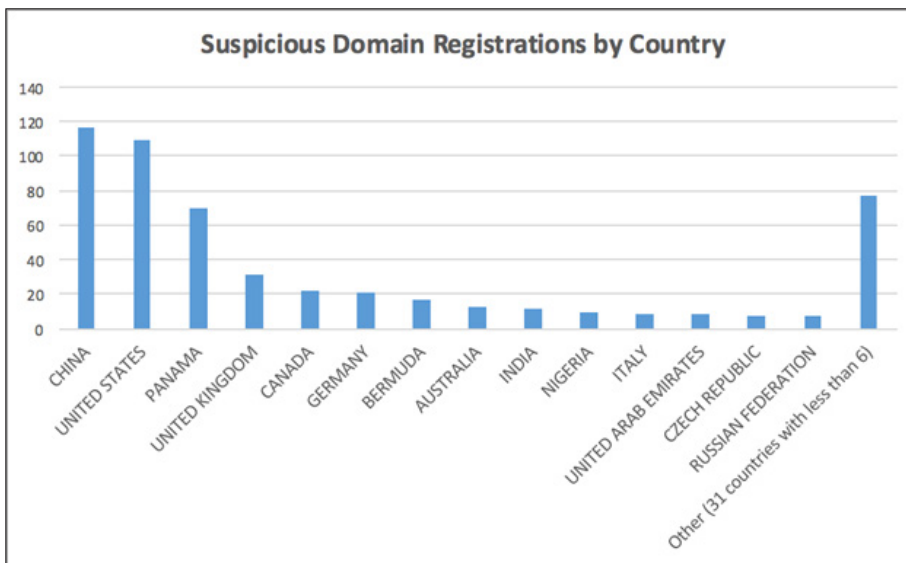


Figure 2 -- Suspicious Domain Registrations by Country

- Eighty-one companies in the FTSE 100 had potentially malicious domain registrations against them.
- The total number of detected malicious domain names registered is 527 or an average of 5 per company.
- Most of the suspicious domains were registered using a Chinese address. The second most were from the US and the third most were from Panama.
- The verticals hardest hit with suspicious domain registrations is Financial Services with 376 with Retail at 175 and Critical Infrastructure at 75

Mass Credential Exposures

Mass compromised credential exposures are becoming a major problem. This often occurs when websites are compromised and collected usernames and passwords are stolen and either published or sold. It is a problem because the vast majority of users reuse passwords across many sites, and many companies still do not have universal adoption of multi-factor authentication.

There are a lot of employees that use their work email and password on sites outside of their work. Many of the sites they go to off-hours were likely compromised in a way that allowed the credentials to end up on the dark web. Often large dumps of credentials are obtained by adversaries performing web application attacks such as SQL injection, command injection or by compromising a website and logging all user logins. In addition, they may be obtained by gaining access to an organization's internal network and then pivoting around until a large database or file share is discovered and compromised.

The oil and gas business vertical was the hardest hit for the period we reviewed. This can be troubling as the connection between business IT systems and 20 to 30-year-old industrial control systems grow more tightly interconnected. We hear so much about the banks and yet based on our data they don't seem to be as popular as many other industry verticals.

- 5,275 FTSE 100 compromised email and plain text password accounts were seen on the dark web, on paste sites, on hacking forums, or posted through accidental exposure.
- The list includes not only included companies with headquarters in the UK, but also any global subsidiary of those companies.
- The Oil and Gas vertical accounted for nearly 20% with 1,090 accounts.

The top ten verticals for exposed email and plain text passwords for the FTSE 100 are shown in the graphic below.

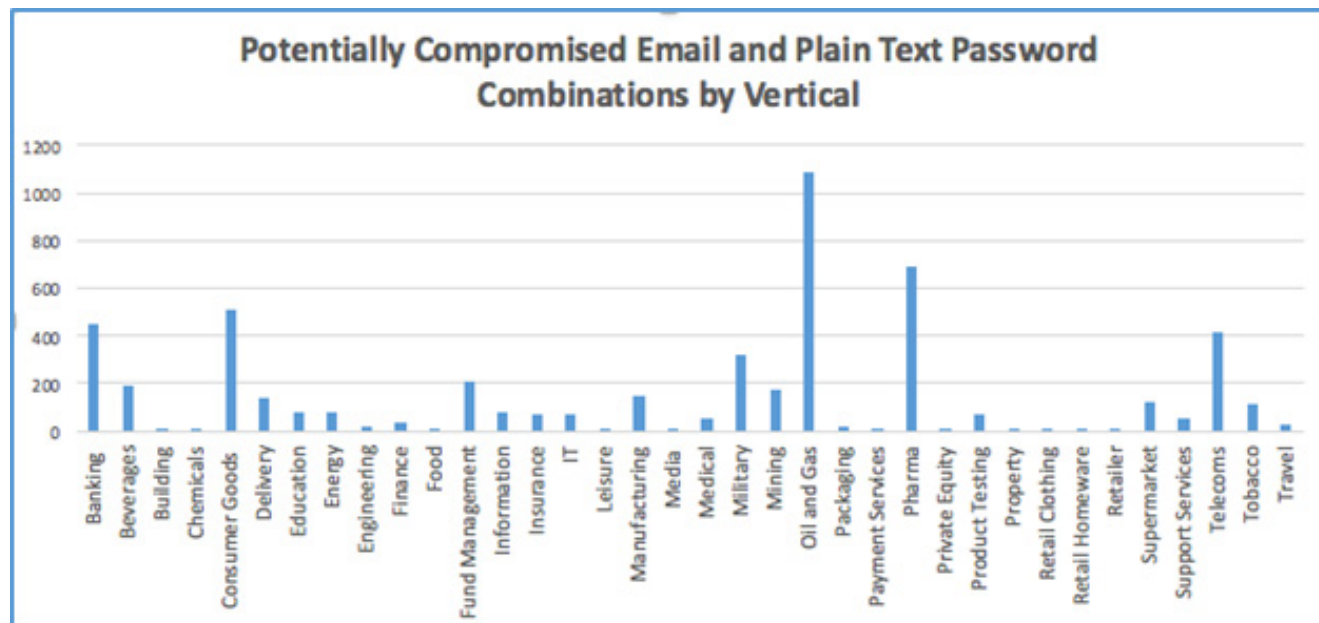


Figure 3 -- Anomali Labs - Potentially Compromised Email / Plain Text Password Combinations

Conclusions

On average, 50 employees for each FTSE 100 company have their credentials exposed when 3rd party sites they have accounts on are breached. For example, over 40 corporate credentials across 23 companies were compromised in April when a Major UK Based Football Website had its database dumped and exposed on the dark web. Employees need to be reminded of the dangers of surfing to these types of websites and logging in using corporate email addresses and passwords. Companies should monitor for compromised employee credentials so they can force reset accounts and gather metrics about how often employees are using their work email addresses for access to non-work related websites.

Understanding the importance of monitoring domain registrations can't be overstated. This is your window into how your business might be targeted and by whom. A good threat intelligence platform will help you find out what new domains related to your business might be suspicious. The registrant email address can be used to see what other domains the registrant might have created and all the IPs associated with each domain. The IPs and Domains can be fed to network security gateways to keep inbound and outbound communication to these domains from occurring.



Anomali Labs is the Research and Development arm of Anomali. Our mission is to conduct threat research and rapid prototyping for the purpose of enhancing and advancing customers' mission-critical security and threat hunting operations.

We proactively identify new and targeted threats and share this intelligence through our threat intelligence platforms, Anomali Enterprise and ThreatStream 6.0. We publish threat intelligence on actors, campaigns, incidents, TTPs, and signatures as well as being the leading producer of indicators of compromise (IoC) and indicators of warning (IoW) within the Anomali threat intelligence platform.

For more information about Anomali's products, please visit to www.anomali.com.