The FTSE 100: Targeted Brand Attacks and Mass Credential Exposures

Overview

A corporate brand represents the trust a company has developed between themselves and their customers. This makes it a source of great value and an ideal target for cyber attackers. In order to damage a corporate brand, threat actors will conduct a series of events illustrated by the Cyber Kill Chain (see Figure 1). The second phase of the Cyber Kill Chain, weaponization, 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.

Malicious third parties will register variations of legitimate domains with misspellings or seemingly legitimate variations. This sets up social engineering-based attacks with the intent of tricking users into clicking a URL and either entering credentials into a phishing website or exploiting the user's web browser to install malware. Once malware is present within an organization it can remain undetected for long periods of time and provide adversaries with access to critical information or a doorway for more destructive actions. Monitoring both suspicious domain registrations and compromised credentials can often act as an early warning system for targeted attacks.

Anomali, as part of its Threat Intelligence Platform service, uses machine learning algorithms to automatically search new domain registrations 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

This report was created to identify suspicious domain registrations and potentially compromised accounts that could be used as part of an attack against the Financial Times Stock Exchange 100 (FTSE 100). The purpose of this report is not to disclose specific company names, but rather to examine trends and emphasize the effectiveness of this kind of data in warning against possible attacks. The following represents an analysis of the FTSE 100 data that we have collected over the past three months and our observations of this growing problem.

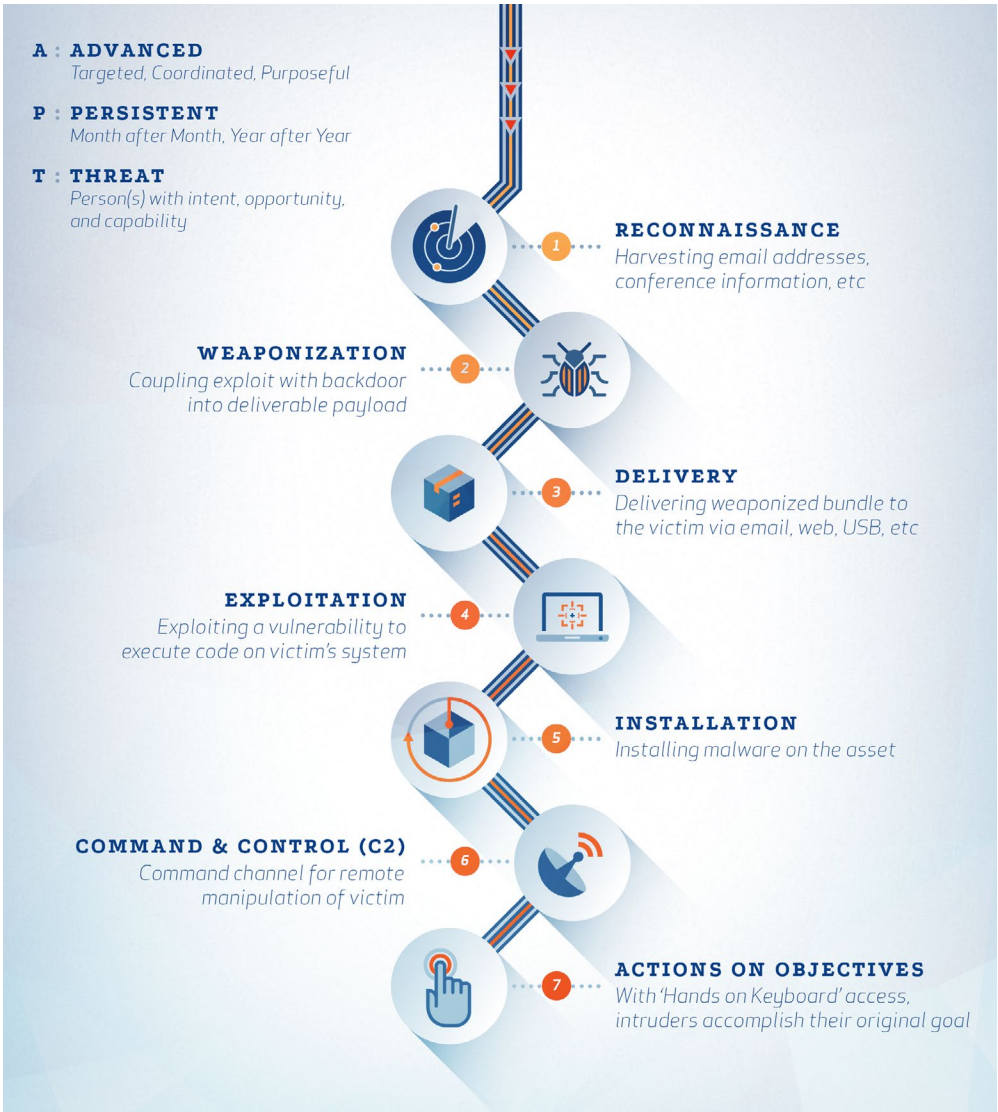

Figure 1. Lockheed Martin Cyber Kill Chain. Courtesy of SANS

Malicious Domains

- A total of 439 suspicious domains were identified across the FTSE 100, with an average of 4.39 potentially suspicious domain registrations per company.
- Eighty-two percent of FTSE 100 companies had at least one potentially suspicious domain registration and thirteen percent had 10 or more suspicious domains.
- The majority of suspicious domains were registered in the United States at thirty-eight percent, a jump from last year's eighteen percent. Last year China represented the majority of suspicious domains at nineteen percent. This year they represented the second most suspicious domains at twenty-three percent.
- Eighteen percent of companies had no suspicious domains registered against them. This is similar to last year, where nineteen percent of companies has no suspicious domains registered against them.
- The vertical hit hardest with suspicious domain registrations was Banking at 83 registrations, which was more than double of the next industry, Energy, at 41 registrations.

When registering domains, registrants often use free email services to mask themselves.

The following chart shows the top free email services used by cyber attackers to register domains. The vast majority of suspicious registrations used gmail.com or qq.com (a free Chinese email service).

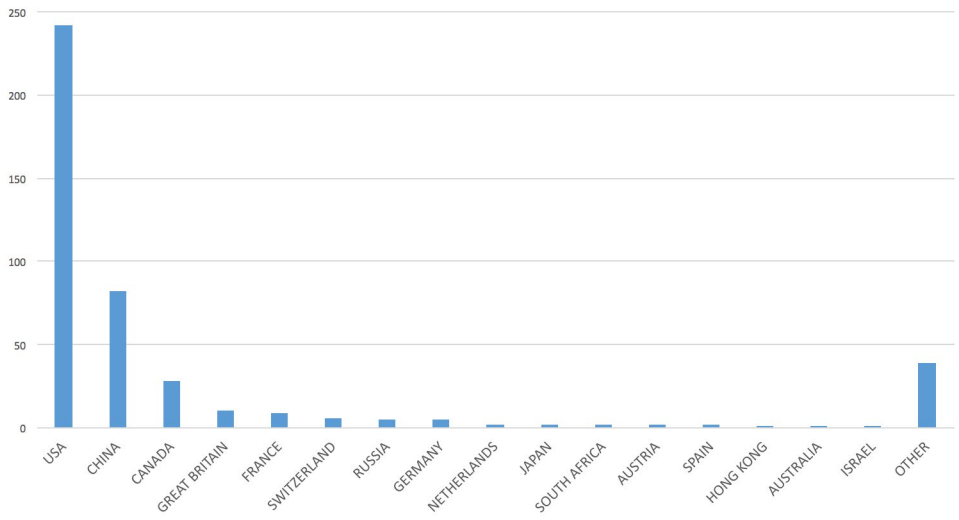

Figure 2. Suspicious domain registrations by country

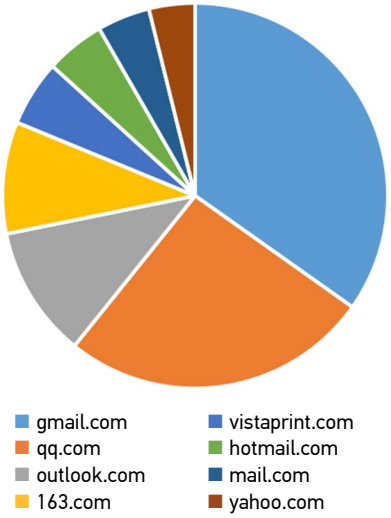

Figure 3. Top malicious registrant email domains

Mass Credential Exposures

Organizations face increasing threats from mass losses of employee IDs and passwords. Many employees will reuse corporate emails and passwords on third party sites, which are easier for adversaries to compromise than corporate networks. These credentials can then be used to infiltrate corporations. Such breaches could be mitigated by multi-factor authentication, but few companies have universally adopted this.

Large dumps of these credentials are often obtained by adversaries performing web application attacks such as SQL injection, command injection, or by compromising a website and logging all user logins. They may also be obtained by gaining access to an organization's internal network and then pivoting around until a credential repository is discovered and compromised.

Darkweb Forums and Paste sites continue to be the top sources for credentials. Users also sometimes inadvertently upload dumps to scanning services such as VirusTotal.

Our monitoring of exposed credentials for FTSE 100 companies showed that the banking vertical was the most common target, accounting for twenty-three percent of exposed credentials with 2,717 accounts.

Since last year's report, attacks on the banking industry have increased more than fivefold. The second most common target was the energy vertical, which is troubling as that it represents critical infrastructure. Damages to companies in this vertical could have catastrophic consequences for infrastructure that includes power grids, utilities, and other critical assets.

- 16,583 FTSE 100 compromised email and plain text password accounts were seen on the dark web, paste sites, hacking forums, or posted through accidental exposure. This is up significantly from last year's 5,275 compromised email and plain text password accounts.
- An average of 165.83 exposed credentials were identified across all companies. Of the 77% of companies that had credentials exposed, an average of 218 exposed credentials were found.
- Seventy-seven percent of FTSE 100 companies had exposed credentials
- Twenty-seven companies had more than 100 credential exposures
- Five companies had more than 1,000 credential exposures

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

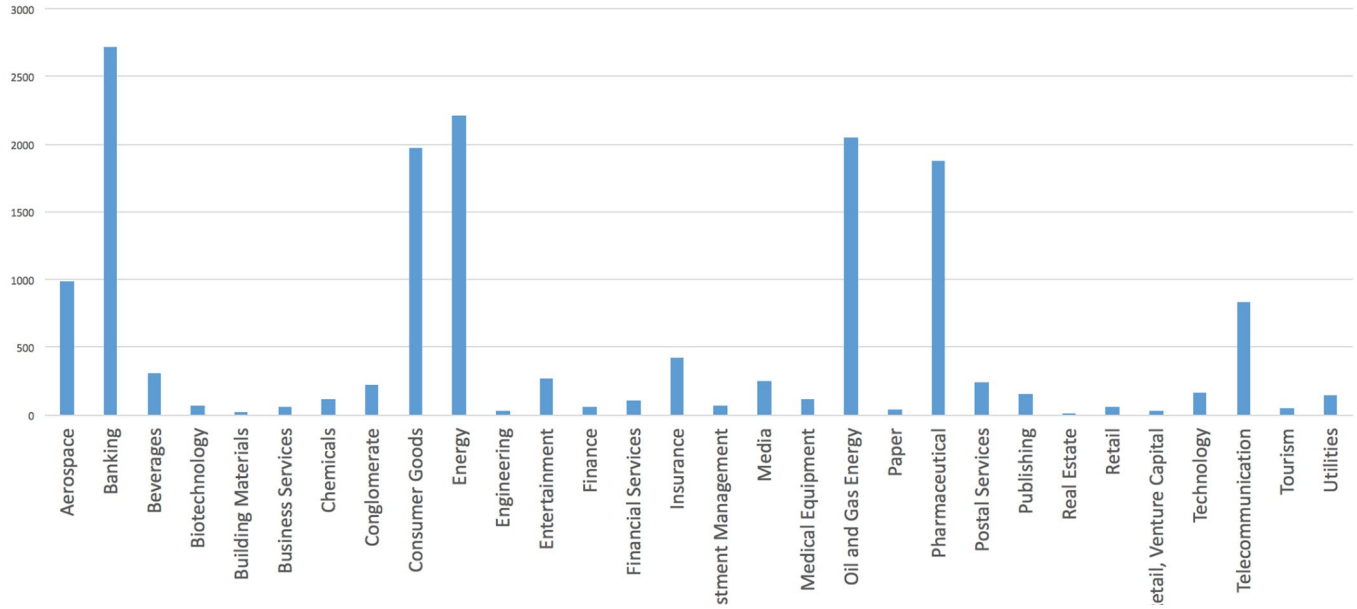

Figure 4. Potentially compromised email and plain text password combinations by vertical

Conclusions

Earlier this year more than 560 million login credentials were discovered on an anonymous online database, including roughly 243.6 million unique email addresses and passwords. Many of these credentials are from past breaches, but failure to remediate and secure compromised accounts could mean these accounts are either still compromised or at risk of being hit again. Employees should be reminded of the dangers of browsing through and logging into non-corporate websites with 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.

Additionally, monitoring domain registrations is a critical practice for businesses to understand how they might be targeted and by whom. A Threat Intelligence Platform can aid companies with identifying what other domains the registrant might have created and all the IPs associated with each domain. These IPs and domains can be routed to network security gateways to keep inbound and outbound communication to these domains from occurring.

Anomali Labs – Research and Development

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 products, ThreatStream and Anomali Enterprise. We publish threat intelligence on actors, campaigns, incidents, TTPs, and signatures as well as being the leading producer of indicator of compromise (IoC) and indicators of warning (IoW) within the Anomali Threat Intelligence Platform.

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

Disclaimers

- Our data set is limited to what is reported by registrars, which is not always accurate because actors can easily misrepresent this information
- Actual geographic location may vary due to obfuscation or deception