The OMX 30:
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 that 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.

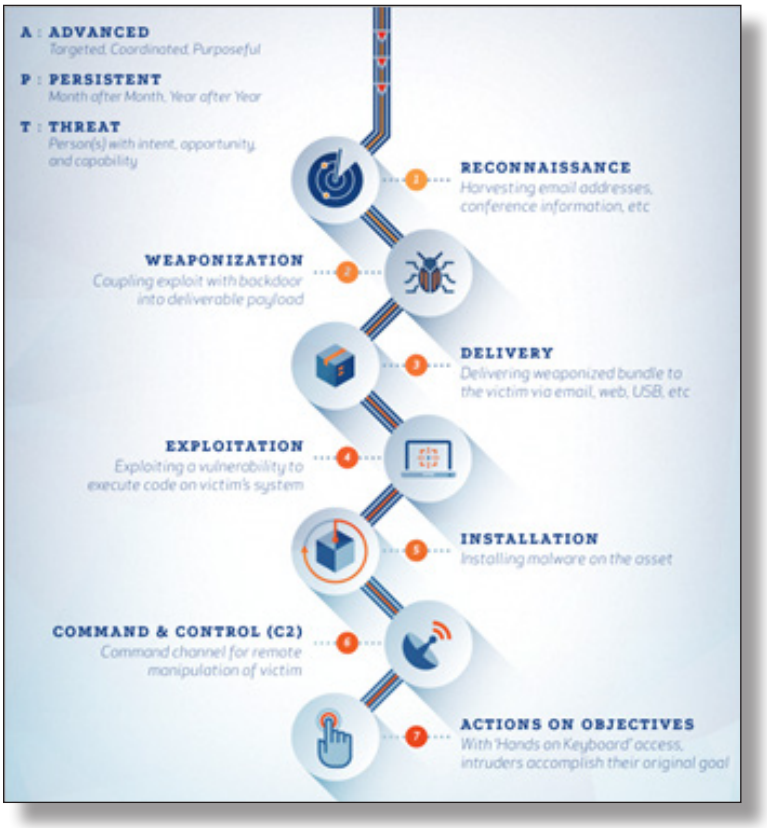


Figure 1 -- Lockheed Martin Cyber Kill Chain courtesy of SANS

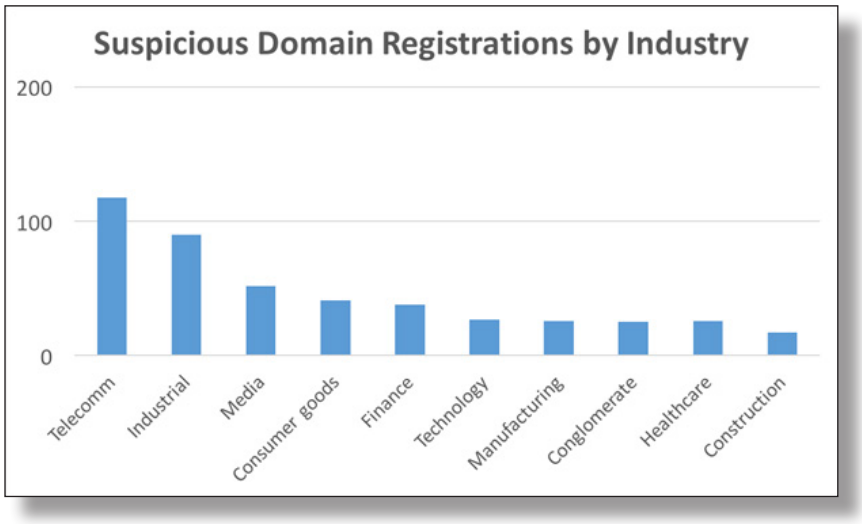
The attacker can often craft a domain name that is only slightly different from a company's domain name. This fake domain name can be leveraged as part of a social engineering-based attack with the aim of tricking users into clicking a URL and either entering credentials into a phishing website or exploiting 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.

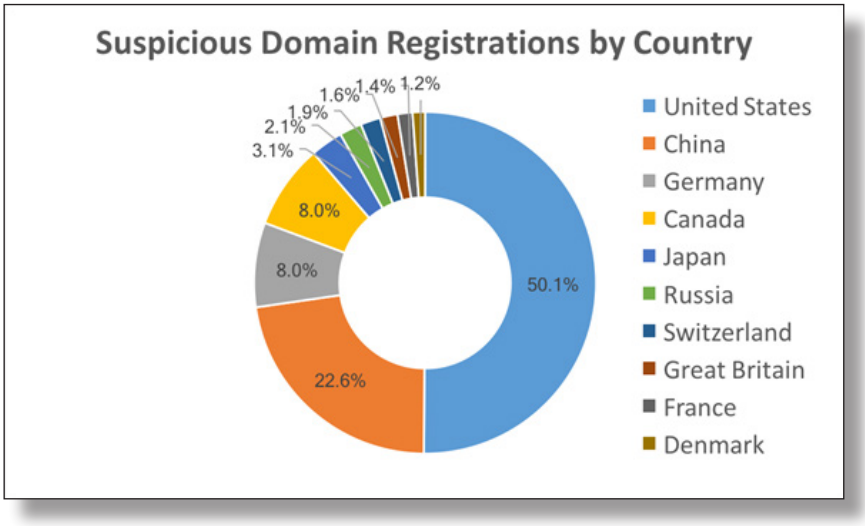
Suspicious Domain Registrations

The focus of this report is to look at the Swedish OMX largest 30 publicly traded companies (OMX 30) 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 OMX 30 collected over the last three months and our observations of this growing problem.

- A total of 479 suspicious or fraudulent domains were detected across OMX 30 enterprises.
- 90% of all OMX 30 companies had at least one potentially malicious domain registration against them. These companies had, on average, 18 suspicious domains each.



- The Telecommunications sector has the highest total number of fraudulent domains representing 12.3% of total OMX 30 suspicious sites. The rest of the top five industries are Industrial (9.4%), Media (5.4%), Consumer Goods (4.3%) and Finance (4.0%).

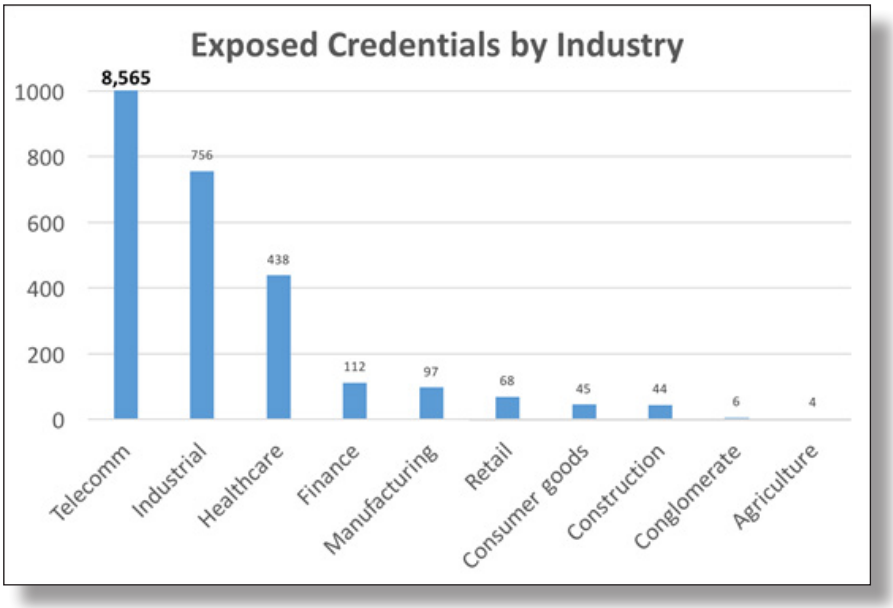


- The United States and China dominate the country of registration for these domains (50.1% and 22.6% respectively)
- Gmail is the most common email domain used to register these sites (11.8%) followed by China's qq.com (10.11%). 34.1% of potentially malicious sites for OMX 30 companies were registered using identity concealing registrars.

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 (MFA).

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.



- Over 10,000 compromised email and plain text password accounts were identified for OMX 30 organizations. Three quarters of these were found on the Darkweb, and another 2% on Pastebin. The remainder were found on hacking forums or posted through accidental exposure.

- 70% of all OMX 30 companies had at least 1 exposed email and password in plain text. 50% of companies had at least 10 exposed credentials and 20% had over 100.

- Among OMX 30 companies we see the top five industries (telecomm, industrial, healthcare, finance and manufacturing) have significantly higher exposed credentials. This is due, in part, to the proportionally higher volume of employees in these sectors. The data suggests, though, that these are also highly targeted sectors.

- The Telecommunications sector had the highest volume of exposed credentials, due to the much higher volume of total user accounts. These enterprises generally offer email addresses to consumers as part of their broadband service.

Conclusions

At least one third of the OMX-30 had credentials compromised by the Pony Password Stealer, amounting to 31 credentials stolen. Additionally, half of all OMX-30 had compromised credentials exposed via Pastebin, amounting to 183 credentials exposed. Employees need to be reminded of the dangers of using corporate email addresses and passwords to access personal websites which may weigh heavily on these statistics. 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.
