Peering Over The DAX 100 Threat Horizon

Executive Summary

German companies are globally renowned for superior build quality, skilled craftsmanship and innovation. The global rising cyber threat to critical infrastructure, intellectual property and brand reputation is of great ongoing concern to enterprise. In part the German response has been to strengthen cyber defence by most recently creating the Cyber and Information Domain Service (Cyber- und Informationsraum; CIR), which became functional in April 2017, and continued Cyber Defense Center operations (since 2011), under the authority of the Federal Office for Information Security (BSI). These efforts, in coordination with the respective internal Information Security functions, must continually advance as this landscape report details observations and findings that highlight ongoing suspected cyber threat activity across DAX 100 listed companies. Generally speaking, this echoes the wider cyber threat landscape view in which 11 of the 15 top threats observed by ENISA (Web based attacks, Web application attacks, Phishing, Spam, Denial of service, Botnets, Data breaches, Identity theft, Information leakage, and Cyber espionage) increased in 2017, according to the Threat Landscape Report 2017.

Introduction

Anomali Labs, in October 2016, produced a report titled "The DAX 100: Targeted Brand Attacks and Mass Credential Exposures," which provided a snapshot on DAX 100 suspicious domain registrations and credential exposures, highlighting the industry-agnostic cyber threat to enterprise in Germany. The purpose of this report is to update for the present day, extend the view and provide insight on the most recent observations and activity.

In September 2018, Bitkom, the German IT industry association, published a study revealing that in the last two years, cyberattacks and industrial espionage caused €43 billion ($50.2 billion USD) in losses to Germany's manufacturing sector, particularly impacting small and medium-sized companies. Moreover, a 2017 Norton Cyber Security Insights Report highlighted a significant number (38%) of German internet users affected by cybercrime; however, placing the losses at €2.2 billion ($2.5 billion USD). These estimated losses represent 1.3% (Bitkom) and 0.07 % (Symantec), respectively, of Germany's €3.3 trillion gross domestic product (GDP), which based on 2017 Eurostat data, the German economic activity totals 21.3 % of the overall European Union (EU)'s GDP. Multiple open source reporting indicators that the common types of cybercriminal activity affecting German businesses takes the form of intellectual property theft, inflicted damage from cyber attacks, or incurred costs from incident response, remediation, and recovery efforts.

This heightened cyber threat landscape increases the risk posed to a major component of the German economy consisting of the top 100 blue-chip or heavily-traded stocks referred to as "Der Deutsche Aktienindex 100", or most commonly known as the

"DAX 100". The DAX 100 was initially formed using the 30 DAX equities and the 70 MDAX (mid-cap issues calculated by Deutsche Börse) equities listed on the Frankfurt Stock Exchange. It is comprised of businesses spanning 17 industry verticals with the top five sectors consisting of Technology (14%), Chemical (12%), Manufacturing (12%), Financial Services (9%), and Real Estate (8%).

In this report, our Anomali Labs research team provides a glimpse of five threat categories that could provide attackers with an exploitable opportunity to compromise DAX 100 enterprises and its customers.

1. ***Domain Squatting.*** Domain squatting also known as cybersquatting, typosquatting, or URL hijacking is the bad faith registration or use of a domain name with the intent of profiting from the goodwill of someone else's brand or trademark. These domain name variants are used by threat actors to impersonate legitimate brands for use in social engineering attacks such as spam and phishing, malware distribution, botnet hosting, and other malicious activities intended to lure unsuspected users into engaging with the actor-controlled infrastructure.
2. ***Credential Exposure.*** Threat actors employ a variety of techniques to steal individual and corporate user's account usernames and passwords to conduct account takeovers (ATOs) or sell, trade, and freely distribute these credentials on underground forums and marketplaces or publicly accessible sites such as Pastebin-like sites. Typically, these compromised credentials are obtained from third-party data breaches resulting from misconfigurations, technical vulnerabilities, or social engineering attacks. These third-party data breaches are outside of the victim organization's infrastructure and control; hence, do not constitute poor cyber hygiene or lack of information security controls but nonetheless poses a risk of attackers obtaining unauthorized access to corporate systems and network.
3. ***Email Authentication.*** Email authentication standards, specifically Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) provides businesses a method for verifying that an email originated from the individual or company. When properly configured and deployed, SPF identifies if a server has permission to send an email from a domain and DMARC tells an email client to either reject emails that fail SPF or mark them as spam. While DKIM defines a standardized method for organizations to digitally sign outbound emails to alert recipients of unauthorized in transit modifications of the original message.
4. ***Website Security.*** The use of unencrypted Hypertext Transfer Protocol (HTTP) connections can be monitored, modified, or impersonated by malicious actors; thereby, increasing the risk to user's privacy and safety. Failure to secure web traffic especially for logins, forms, and requests for personally identifiable information (PII) can present German businesses with GDPR compliance related issues from the exposure of basic identity information and web data e.g. user's location, IP address, or cookie data, create negative publicity resulting in brand and reputational losses, and waste time and resources due to a hacked website or compromised user data. Implementation and proper configuration of the HTTPS protocol (*https://*) and HTTP Strict Transport Security (HSTS) can remedy these issues by securing web traffic and offering the level of privacy and security for gaining and maintaining user's trust and confidence while ensuring full compliance with GDPR requirements.
5. ***Dark Web Reconnaissance.*** The "Dark Web" denotes any collection of computers, or network, that create an internet which requires specific software, configuration, or authorisation to access, such as anoNet, Freenet, Riffle, or Tor. A variety of threat actor exploit the anonymity of the Dark Web to perform nefarious activities and sell or acquire illicit products and services for monetary gain. By proactively monitoring underground forums and marketplaces, businesses can detect and respond to cybercriminal activity such as the sale and distribution of unauthorized information disclosures, attack preparation, new or revised malware and hacking tools, and rogue insiders; thereby, minimizing business and security risks facing their organization.

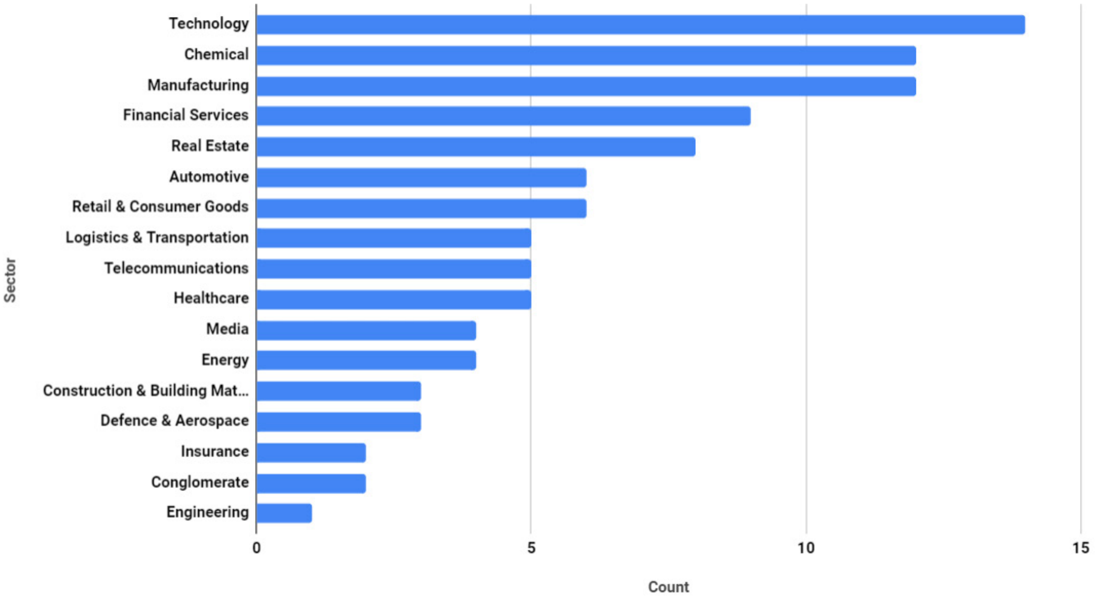

Figure 1. DAX 100 Sector Composition

The DAX 100 Enterprise's Threat Horizon

The usage of illegitimate domains to initiate the infection process or harvest account details is a commonly observed tactic by cyber threat actors across all sectors. Presented are some of the key findings in relation to squatted domains:

- A total of 4,723 suspicious or fraudulent domains were observed across DAX 100 enterprises and associated trade names.
- These companies had, on average, 27 suspicious domains per legitimate domain examined, some of which Anomali Labs suspect could be used in a targeted manner as part of a phishing campaign.
- The Manufacturing sector had the highest number of suspected fraudulent domains with almost 700 registrations (14.6% of total DAX 100 suspicious sites), followed by the Chemical sector with 623 (13.2%), Automotive sector with 577 (12.2%), Technology sector with 564 (11.9%) and the Retail & Consumer Goods sector had 394 (8.3%).

It is noted that from the prior suspicious domain analysis undertaken in 2016, the latest observations mark an increase of 280%, a concerning surge in possible suspect activity.

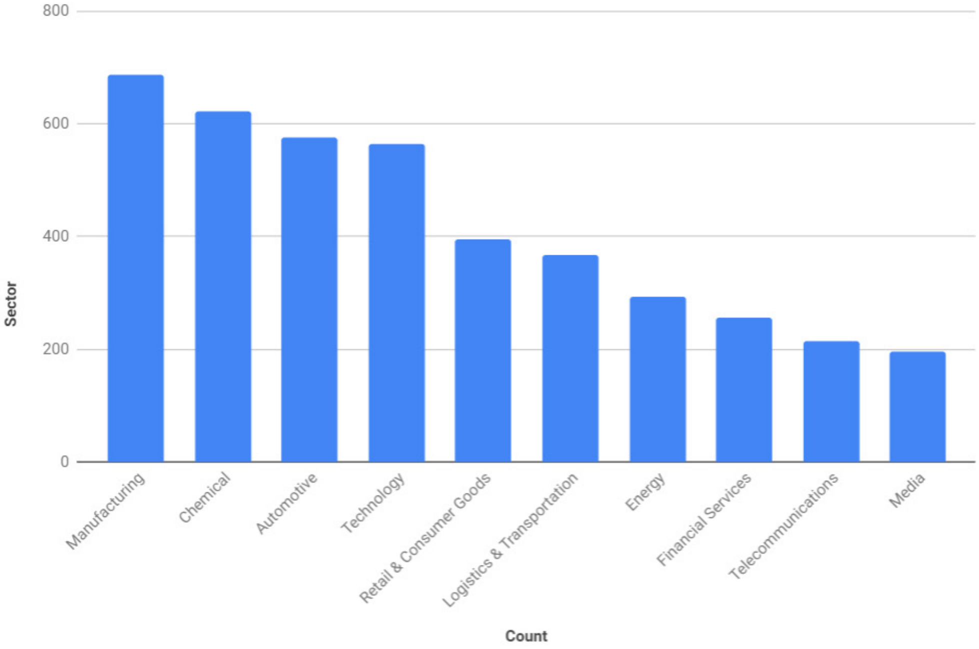

Figure 2. Top 10 DAX 100 Industries Targeted with Domain Squats

Credential Exposure

The use of compromised credentials is one of the most effective ways for an attacker to obtain unauthorized access to corporate networks, personal systems, and remain hidden for extended periods of time as they move laterally across a network, escalating privileges, extending control, and exfiltrating data. In the 2018 Verizon Data Breach Investigations Report (DBIR) report, they identified the number one "threat actions" or the actions taken by a third party that leads to a data breach was the use of stolen credentials observed in 22% or 399 out of 1,799 breaches. Most of these stolen credentials happen outside of the enterprise perimeter where employees use their corporate email address to create online accounts at third-party websites that are subsequently hacked. According to a 2017 Norton Cyber Security Insights Report, 39% of German cybercrime victims share the password of at least one online account with others and 12% use the same password across all online accounts. Therefore, continuously monitoring for compromised credentials across the Internet and Dark net locations helps reduce the potential risk of non-compliance with GDPR, which carries hefty fines and potential loss of brand reputation.

Our research into lost or stolen credentials uncovered a significant amount related to DAX 100 enterprises available on the Surface, Deep, and Dark Web:

- Amongst all the DAX 100 enterprises, there was a total of 604,255 breached accounts consisting of 560,941 unique email addresses and password pairs between 2012 and September 2018. Most of the credential exposures were discovered on Deep Web forums or non-indexed portions of the Internet, closely followed by the Dark Web or special access forums and marketplaces and ~150 Pastebin pages. The Deep and Dark Web disclosures consisted of two primary themes: advertisements for sale of data dumps and open disclosures readily available for underground community members to leverage in their attacks such as credential stuffing where automated scripts are used to test the stolen username and password pairs across multiple online accounts.
- The previous Anomali Labs analysis undertaken in 2016 found more than 76,000 exposed email and plain text password accounts for DAX 100 companies. This ~600% increase in breached accounts discovered highlights the pressing requirement for enterprises to ensure they have the visibility of appropriate channels to monitor and alert on not only credential exposures but PII and financial data.
- The top five DAX 100 enterprises with the highest number of lost or stolen credentials were in the Telecommunications sector (possible corporate

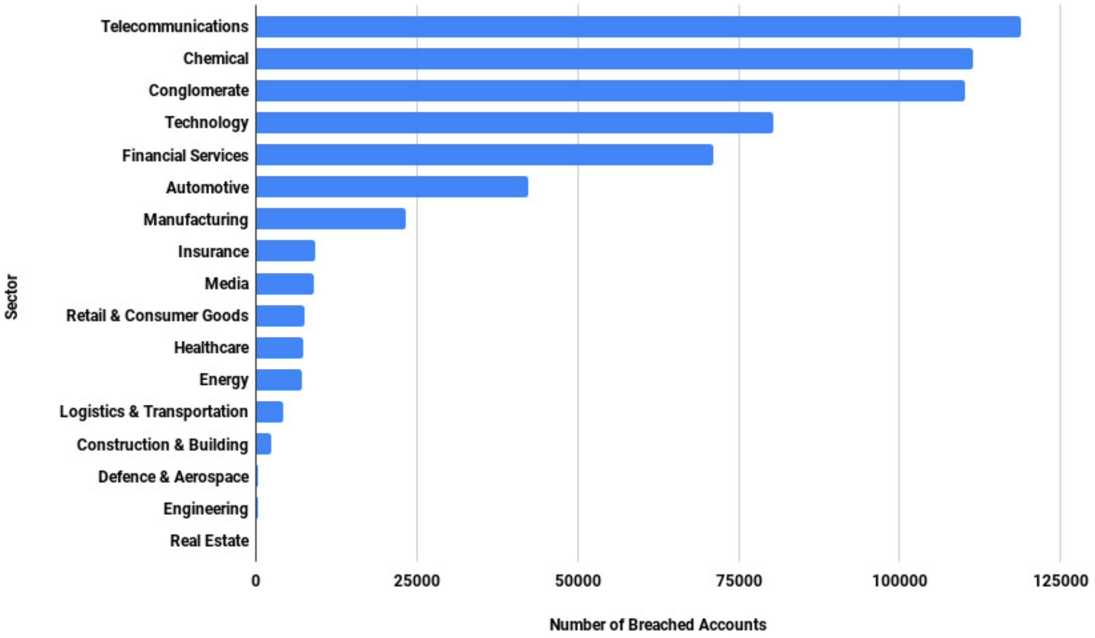

Figure 3. Total Breached Accounts Broken Down by DAX 100 Industry Verticals

credentials and those using personal/webmail services) at 118,833 (19.6%) followed by Chemical at 111,382 (18.4%), Conglomerate sector at 110,234 (18.24%), Technology sector at 80,434 (13.31%), and Financial Services sector at 71,032 (11.75%).

- Three-fourths (75%) of DAX 100 enterprises had at least one exposed email and password in plain text while close to half (48%) of these enterprises had at least 10 exposed credentials and 16% had over 100.
- Similar to our 2016 report, the Telecommunications sector remained the DAX 100 industry vertical with the highest volume of exposed credentials. This is most likely due to the much higher volume of total user accounts knowingly or unknowingly subscribing to free email services offered to consumers of these enterprises broadband service.

Email Authentication

The three email authentication standards: SPF, DKIM, and DMARC, help prevent the abuse of corporate domains by attackers impersonating your brand. The Q1 2018 Phishing Activity Trends Report by the Anti-Phishing Working Group identified an average of 249 brands per month were targeted in phishing attacks during the first half of 2018. According to Symantec, spearphishing was the number one infection vector employed by 71% of organized groups in 2017. Our study analyzed published DNS records for corporate domains of the DAX 100 to identify the policy strength and susceptibility of these enterprises to spam and phishing attacks abusing their domain names. Research uncovered many of these enterprises use some level of email authentication; however, many of the policies were insufficiently strict for preventing email forgery attacks from masquerading as DAX 100 brands.

- From January 2017 to August 2018, we found 1.7 million spam and phishing emails abusing 69 corporate domains or 51% of the DAX 100 enterprises operating in 15 out of 17 industry verticals being victimized in email spoofing attacks. During this period, the top five most abused sectors operated in Telecommunications, Automotive, Chemical, Financial Services, and Healthcare. Interestingly, the most recent spoofed emails were observed in late August 2018 impersonating companies abusing domain owners from the Chemical, Automotive, and Manufacturing sectors. We judge with near certainty that these email spoofing attacks were consistent with the lack of or insufficiently strict SPF and DMARC policies e.g. the use of DMARC records set to “p=none”, which informs receivers to take no action on all emails, forged or not, prior to reaching their inbox.
- The highest SPF adoption rates were observed in the Technology sector with 84% of domains having implemented an SPF record. The most susceptible sectors to email spoofing attacks were in the Chemical, Conglomerate and Energy, with only half (50%) of the domains having defined an SPF record.
- Overall, there was a moderate DKIM adoption rate (43%) across the DAX 100 enterprises. The highest adoption amongst sectors with four or more domains were Conglomerate (75%), Healthcare (60%), Financial Services (54%), and Manufacturing (58%). The lowest adoption rates were observed in the Construction & Building Materials (20%) and Real Estate (13%) sectors.
- Globally, DMARC remains a poorly adopted email authentication standard across all industries. Nonetheless, the rising importance of combating email-borne attacks has prompted a surge in support for raising awareness for, and promotion of DMARC adoption, including cross-sector, international support from organisations such as the Global Cyber Alliance. In our study, we found an overall low DMARC adoption rate of 21% overall for DAX 100 enterprises and less than a third of implementations used an enforcement policy of “quarantine” or “reject”. The Logistics & Transportation sector was the largest DMARC adopter at 58%. There at least five sectors: Conglomerate, Construction & Building Materials, Defence & Aerospace, Energy, and Insurance, that failed to publish a DMARC policy to their DNS records leaving themselves open to email spoofing attacks.

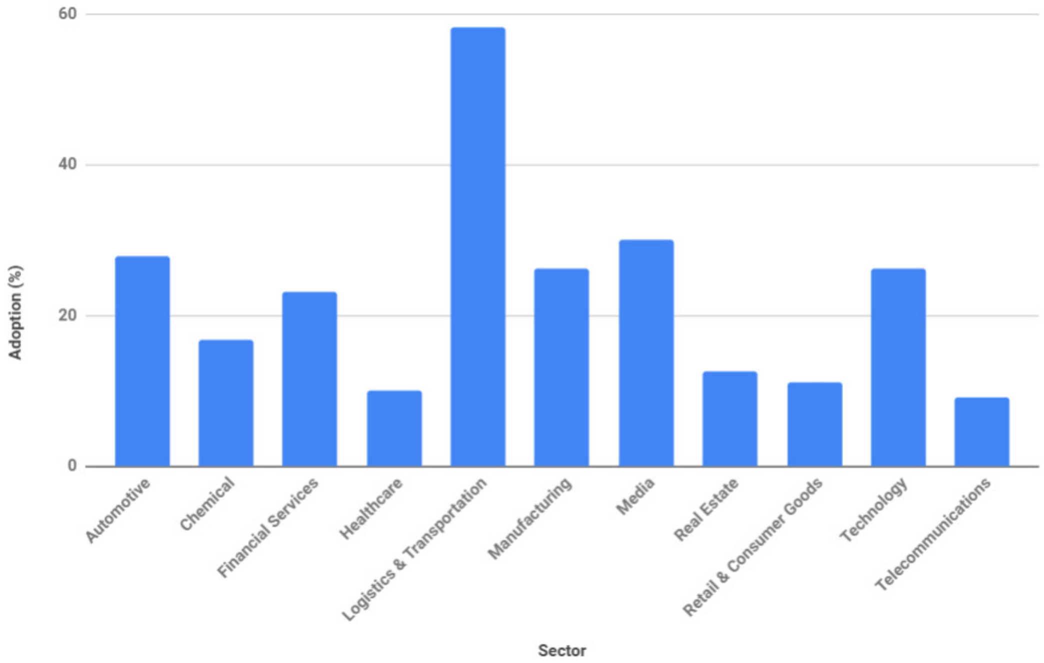

Figure 4. DMARC adoption rate amongst DAX 100 industry verticals (sectors with at least 3 companies)

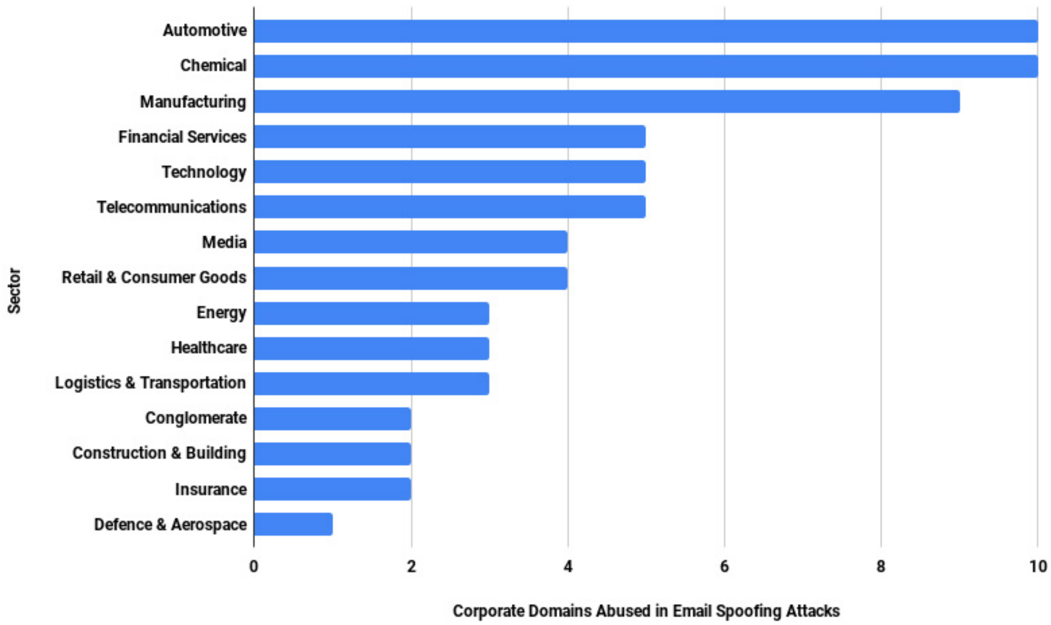

Figure 5. Sectors Abused in Email Spoofing Attacks from January 2017 to August 2018

Website Security

The unencrypted HTTP protocol does not offer data protection from interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data. By deploying HTTPS-only and HSTS protocols, including the removal of support for known weak cryptographic protocols and cipher suites, website owners create secure connections by providing authentication and encryption between a web browser and a website. When properly configured, HTTPS and HSTS implementation on all publicly accessible websites and web services can help minimize the web server's susceptibility to traffic interception, manipulation, and impersonation attacks. Failure to secure these connections can lead to privacy related risks to site visitors include browser identity, website content, search terms, and other user-submitted information.

Based on seven secure HTTP response headers and the strength and configurations of installed SSL/TLS certificates, Anomali Labs identified multiple privacy and security related risks to DAX 100 and their site visitors:

- Around 10% of websites evaluated were using the unencrypted HTTP protocol and did not redirect users to the more secure, encrypted HTTPS protocol. At least 14% of the used deprecated cipher suites: Triple DES (3DES) or RC4, which could allow malicious actors to successfully intercept or alter sensitive and privileged data while in transit. Three of these websites supported obsolete SSL/TLS protocols; two of them vulnerable to the SSLv3 POODLE attack (CVE-2014-3566) while the third site was vulnerable to SSLv2 DROWN attack (CVE-2016-0800). Exploitation of these protocol weaknesses by a remote attacker, such as a Man-in-The-Middle (MiTM) attack could allow them to decrypt and read or steal sensitive communications that includes passwords, credit card numbers, trade secrets, or financial data. Lastly, 3.5% of these sites contained certificate public keys shorter than or equal to 1024-bits, which according to NIST-800 could place sensitive data at risk of being compromised by attackers with sophisticated processing capabilities.
- Strict-Transport-Security. Of the domains reviewed, only 31% used the HTTP Strict Transport Security (HSTS) specification as defined in RFC 6797. This feature helps prevent against man-in-the-middle (MiTM) attacks as it enforces the use of HTTP over TLS encrypted communications. HSTS was not observed across any of the domains within the Conglomerate, Construction & Building Materials, Defence & Aerospace or Energy sectors. The Financial Services sector had the best HSTS opt-in with 69% of the domains using the response header.
- Content-Security-Policy. The majority (92%) of domains analysed did not have the Content Security Policy (CSP) header configured. The Telecommunications sector performed best with 50% of the domains having CSP implemented. A properly configured Content-Security-Policy can help prevent cross-site scripting (XSS) attacks by restricting the origins of JavaScript, CSS, and other potentially dangerous resources. By whitelisting sources of approved content, you can prevent the browser from loading malicious content.
- X-Frame-Options. The X-Frame-Options header was also sparsely configured, only 34% of the sites analysed. In sectors with more than four domains sampled, Financial Services (62%) and the Retail & Consumer Goods (56%) had the best implementation rates. Anomali Labs observed no presence of this header across the Defence & Aerospace and Energy sectors. An X-Frame-Options header tells the web browser whether you want to allow your site to be framed or not. By preventing a browser from framing the site can defend against attacks like clickjacking.
- X-XSS-Protection. Similarly, this response header was not widely configured, only 21% of the sites examined. Anomali Labs observed no presence of this header across the Construction & Building Materials, Defence & Aerospace, Energy, Healthcare, and the Media sectors. The X-XSS-Protection sets the configuration for the cross-site scripting (XSS) filter built into most browsers. Setting X-XSS-Protection to “FIELD” helps to prevent against common XSS attacks by filtering and blocking suspected malicious scripts. Of note, this configuration is primarily of value for users of older web browsers that do not support CSP.
- X-Content-Type-Options. Sixty-nine percent of the analysed sites did not configure the X-Content-Type-Options header. This header stops a web browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type.
- The lowest configured response headers were the Referrer-Policy (2%) and Feature-Policy (0%). The Referrer Policy governs the referrer details which should be included with the HTTP request. The Feature Policy allows site administrators to enable and disable specific browser features and APIs on their native pages and those that are embedded.

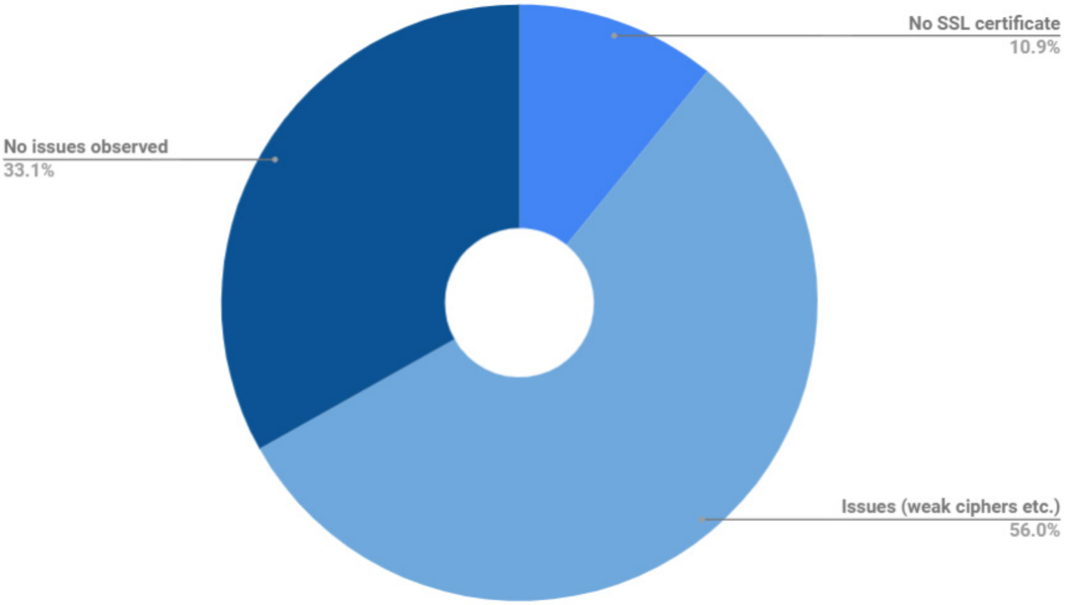

Figure 6. Breakdown of SSL certificate usage and issues amongst DAX 100 companies

Dark Web Reconnaissance

- In early 2017, Markus Koths, head of the cyber crime unit at the German Federal Crime Office, briefed at a Europol European Cybercrime Centre (EC3) conference that reported cyber crime cases in 2016 nearly doubled to over 82,000, resulting in damages of over €51 million ($55.7 million USD). Admittedly though, he stated that unreported costs could be as high as €22.4 billion ($26.07 billion), which is closer to the average annual cost of €21.5 billion ($25.02 billion USD) identified in the 2018 Bitkom study. The biggest driver for the attack increases were due to a rise in "cybercrime as a service" offerings providing hacking services and malicious software on underground forums and marketplaces or "dark net", as stated by Koths. Multiple news media reporting indicates that the German criminal underground is almost certainly the most developed in the EU and one of the major sources of botnet activity. For instance, in 2017 law enforcement operations led to arrests of black market German administrators and confiscation or neutralization of Germany-hosted infrastructure associated with "Hansa Market", "Deutschland im Deep Web" (DiDW — the largest German-speaking forum), Crimenetwork[.]biz, WebStresser (the world's largest Distributed-Denial-of-Service provider), and the Mirai botnet (which was linked to the outage of one million Deutsche Telekom customers systems in 2016).
- The maturity of the German underground requires small to large enterprises to monitor and track cybercriminal activity to stay ahead of the latest hacking tools, malware, information disclosures, and other threats against their business. Research of Deep and Dark Web posts shed light on the various discussions ranging from PII disclosures, payment card fraud related, and malicious insider recruitment posing a security and compliance risk to the DAX 100 enterprises. Additionally, we found close to 150 unique pastes on Pastebin related to breach data dumps containing compromised credentials and attack preparation data by various threat actors to include hacktivist groups affiliated with the Anonymous Collective.
- The top five mentioned DAX 100 industry verticals (excluding the Telecommunications sector which provides personal email/webmail services which could not be properly assessed in this manner) were Retail & Consumer Goods, Financial Services, Manufacturing, Conglomerate, and Technology (see Figure 8).
- A varying degree of interest exists on underground forums and marketplaces for the DAX 100 enterprises based on research of corporate domains. The data revealed that 51% of the 177 evaluated corporate domains had one or more mentions on the Deep and Dark Web while about 49% were found with no mentions.

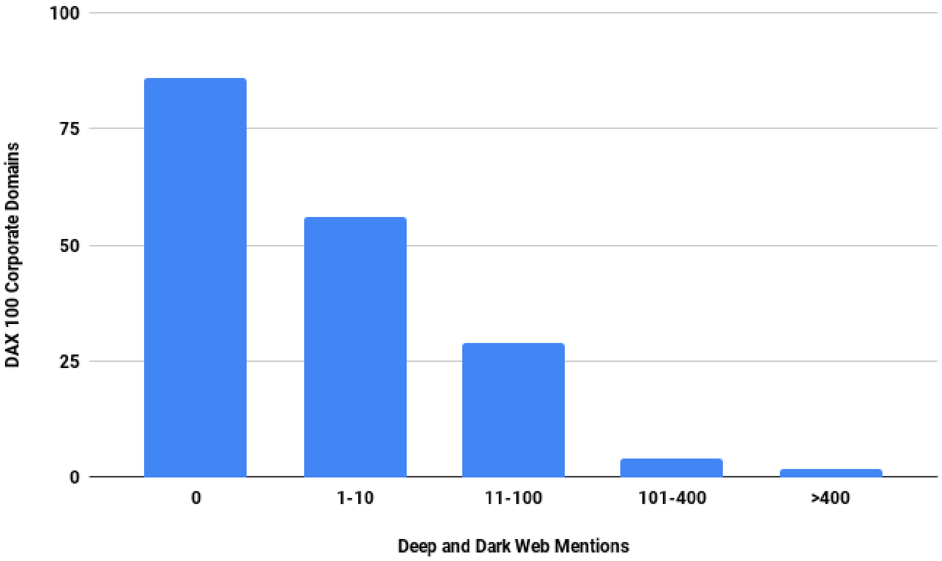

Figure 7. Deep and Dark Web Mentions of DAX 100 Corporate Domains

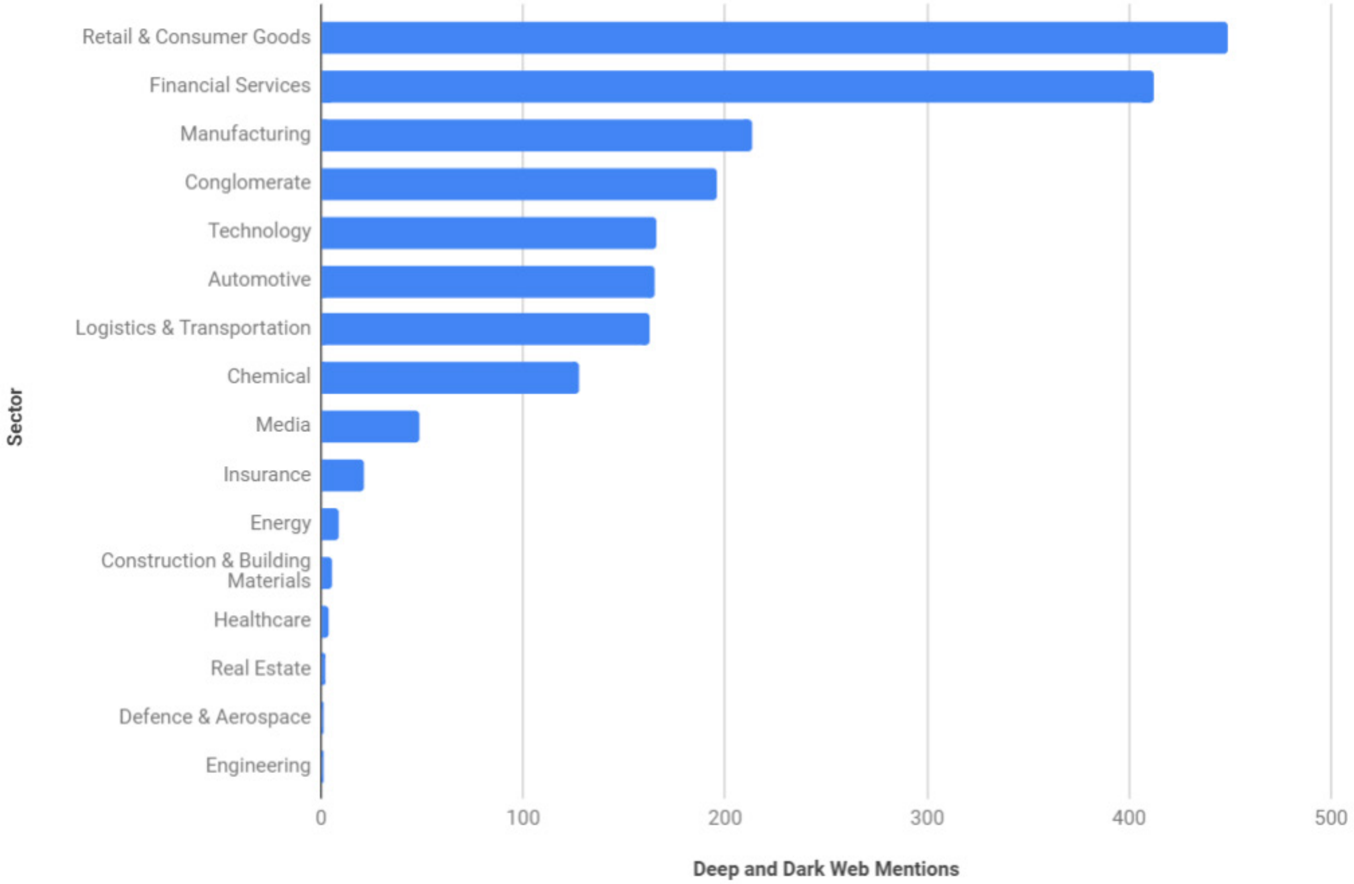

Figure 8. Deep and Dark Web Mentions Per Sector Domains

Conclusion

As the largest European Union (EU) economy, Germany remains a lucrative target for threat actors to attempt to compromise in pursuit of monetary gain, seeking a competitive advantage, or pursuing national interests. With the rapidly evolving cyber threat landscape, organizations of all sizes require key insights and complete intelligence on relevant business and security risks to protect their infrastructure and data from adversarial compromise. At the geopolitical level, divisions over immigration and a surge in populism could further the cyber threat to German entities from hacktivists and/or state-sponsored actors.

The Anomali Threat Platform offers the needed visibility and detection capabilities for small, medium, and large businesses to meet the demands of an increasingly complex threat environment to safeguard your information systems and network while successfully meeting your regulatory and legislative compliance needs.

References

- Cyber- und Informationsraum
- ENISA Threat Landscape Report 2017
- Verizon
- CERT EU
- Electronic Frontier Foundation (EFF)
- Global Cyber Alliance
- Federal Office for Information Security
- Symantec
- Symantec
- Anti-Phishing Working Group
- Reuters
- Bitkom
- Verizon Report
- Eurostat
- OWASP Secure Headers Project
- CSO Online
- EC Europa
- Business Pundit
- Scott Helme
- Reuters
- Reuters
- Bundeskriminalamt (BKA)
- Reuters
- Business Insider
- Motherboard Vice
- Cyberscoop
- Wired
- Bleeping Computer
- Schleswig-Holstein
- CERT EU
- CVE-2014-3566 (POODLE Attack)
- CVE-2016-0800 (DROWN Attack)
- DROWN Attack
- CERT Carnegie Mellon University
- CERT Carnegie Mellon University
- NIST SP800-131A