RISKIQ®

Understanding Your Attack Surface

Research into FT30 Websites

Introduction

Businesses are accelerating their digital transformation, expanding their online presence to enrich products, deepen customer relationships, and boost their brand ecosystems. However, with this rapid growth comes security challenges as web assets get created outside of corporate controls and the overall Internet presence expands to unmanageable proportions.

Cyber adversaries are taking advantage of this sprawling digital attack surface, looking for weaknesses to exploit. The attack surface has become the battle line between malicious actors and an organisation's external threat defenders and its compromise is behind many of the breaches that get reported with alarming frequency. In fact, according to the 2017 Verizon Data Breach and Incident Report, three-quarters of the incidents that lead to data breaches originate externally.

In an effort to highlight and quantify the risks which organisations have in their attack surface, we went back to the FT30 basket of companies to conduct our research. We have used this group of organisations in the past for research projects as it provides a representative sample of large UK organisations across diverse industries. The research objective was not to call out any individual company but to highlight the issues we believe all companies face.

Using our global Internet reconnaissance infrastructure, we found a total of 99,467 live websites across the FT30, an average of 3,315 websites per organisation. We analysed the collection of infrastructure components and assets that make up these web sites to identify the various types of issues that organisations must deal with in order to protect their businesses and provide a secure environment for customers. Although not an exhaustive list, we believe the following risk areas serve to illustrate the challenge.

Server and Framework Risks:

While a breach may be the result of a zero-day exploit of an unknown vulnerability, the majority are due to the successful exploitation of a known vulnerability within an organisation's web presence. Of most immediate concern are those platform components at release levels associated with known vulnerabilities (CVEs) which if discovered by malicious actors, can be exploited today. We found 5,127 at risk servers or an average of 171 per organisation and 2,045 at risk frameworks, an average of 68 per organisation.

Certificate Risks:

Moving on from servers and frameworks we looked at the security certificates associated with these sites. Certificates are the trust relationship between an organisation and its online visitors and certificate issues weaken that trust. Expired or untrusted certificates result in warning messages in the browser forcing visitors to think twice before continuing. Outdated algorithms risk transmitting data insecurely. Here we found 1,051 expired certificates or 35 per organisation and 7,503 untrusted certificates or 250 per organisation. These untrusted certificates include

WoSign and Starcom certificates which will soon be dis-trusted by the major web browsers as well as Symantec owned EV certificates which are at risk pending a resolution between Symantec and Google. In addition, we uncovered 574 OpenSSL instances or 19 per organisation that are potentially vulnerable to Heartbleed. There are still a number of older SHA-1 certificates out there, generally considered to be unsafe. We found 1,332 SHA-1's, an average of 38 per organisation.

Test Site Risks:

As part of the discovery process we identified 2,863 potential test sites or an average of 95 per organisation. These are sites with subdomain names commonly used to differentiate test sites from production ones. While most of these will be set up correctly, we're calling them out because in our work with clients we regularly come across internal use test servers that are misconfigured and as a result, discoverable on the open web, often exposing sensitive data if hacked.

Data Collection Risks:

Finally, we looked at the security of forms collecting user information. Insecure collection of personal information can affect consumers through loss and fraudulent use of their data, and organisations through loss of revenue, brand reputation, and damages. Google along with others is leading the charge for secure data collection on the Internet in all cases and is adding warnings to Chrome where that is not the case. We uncovered 13,194 pages that were collecting information through login or data input forms, an average of 440 pages per organisation. 29% of these pages were using no encryption while a further 5% were using very old encryption algorithms or expired certificates. That represents 4,465 pages or 150 pages per organisation.

Risk Type	Total Instances	Average per Organisation
Server	5,127	171
Framework	2,045	68
Expired Certs	1,051	35
Untrusted Certs	7,503	250
Open SSL Instances	547	19
SHA-1 Certs	1,332	38
Insecure data forms	4,465	150

Table 1: Summary of Risk Findings across 99,467 live websites

Web Management

We mentioned at the beginning of this report that rapid web expansion has led to web sites being created outside of corporate control. We often refer to this as shadow IT; development projects that sit with the business units or with marketing and are often outsourced to third party development teams. We can get a feel for the extent of shadow IT by looking at the number of domain registrars and certificate providers an organisation is using.

Domain Registrars:

Most central teams will use a small number of registrars to register new domains. A large proportion of domains registered with a few registrars and a long tail of other registrars is often a good indication of decentralised development activity. Our research showed that an average of 13.5 different registrars were used per organisation with the most active registrar in each case handling an average of 4,454 registrations while the least active registrar was handling an average of 3.

We also discovered a total of 4,010 domains registered with employee email addresses as the contact, an average of 134 per organisation. This practice can cause issues longer term as those employees change roles or leave the organisation and expiry notifications get missed.

Certificate Providers:

As with Domain Registrars, a long tail of Certificate Providers is a good indication of a decentralised approach to web development and deployment. From our experience, the more certificate providers the more likely it is that certificates will remain in use after their expiry or after they become obsolete. We found an average of 15 different Certificate Providers per organisation with the most active provider in each instance issuing an average of 653 certificates and the least active provider issuing an average of 1.1.

Conclusion

Gaining control of an ever-expanding web presence poses a challenge for most organisations, but it's a challenge that can't be ignored. In each case, the risk categories we highlighted were associated with a relatively small percentage of the overall web estate but as we too well know, it only takes the discovery of one exposure to provide an opportunity for an attacker. And the more you have, the more likely that one will be uncovered. While it isn't practical to eliminate all security risks, it is important to understand the full scope of the risks you have. Risks to an organisation's attack surface should be understood and evaluated along with network, endpoint and identity risks in order to gain full understanding of the risk position and prioritise remedial action.

At RiskIQ we give customers full visibility of their Internet presence along with the associated risks; those covered above and many more. To find out more about RiskIQ Digital Footprint™ visit https://www.riskiq.com/products/digital-footprint/.

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com