CYCOGNITO

EXECUTIVE BRIEF

Anybody Got a Map?

The Danger of Subsidiary Sprawl and Unknown Unknowns in External Attack Surface Management

Executive Summary

We just came off a banner year for mergers and acquisitions, which, combined with uncertain M&A trends this year, leaves a ticking time bomb in many organizations. Already overburdened CISOs and security teams will have their work cut out for them as they try to get a handle on a constantly fluctuating attack surface - we found that the average attack surface grew or shrank by 5% every month.

Part of that fluctuation in attack surface size comes from potentially vulnerable web apps. Web apps make up approximately 1 out of every 10 exposed assets of organizations but can be the vector for substantial risk, either because they are vulnerable to a slate of evergreen and unpatched vulnerabilities or because they contain valuable personal identifiable information (PII).

While security managers rightfully focus much of their attention on patching, patching, patching, we found that 11% of identified issues could only be solved by changes in security practices (or better user behavior around authentication). Combined with the possibility of web app access to PII, bad password practices could leave consumers and employees valuable PII exposed in plaintext.

Introduction

CyCognito, founded in 2017 by ex-intelligence agency reconnaissance experts, uses proprietary machine learning, natural language processing, and data sources for automated reconnaissance. CyCognito's External Attack Surface Management (EASM) solution automatically finds and maps and attributes external digital assets with context - the way threat actors see them - on an adjustable cadence, providing superior visibility and risk detection with reduced resource requirements. Below we will discuss the results of CyCognito Labs' examination of customers' attack surfaces over the last 12 months. These customers are roughly a 50/50 split between large enterprises and small- to medium-sized companies.

Shedding Light on Subsidiaries and Attack Surface Size

- On average, each organization has 95 subsidiaries. For the purposes of this research, "subsidiaries" means any entity owned by a parent company, regardless of whether they are called a business unit, brand, standalone company, etc. CyCognito discovers and classifies these subsidiaries as part of our asset discovery process using natural language processing to look across open source sites, financial reports, and more.

- Organizations were initially unaware of 10-to-30% of their subsidiaries. This may seem surprising - how could a company be unaware of what subsidiaries fall under its corporate umbrella? - but modern companies may have gone through decades of mergers and acquisitions, leaving behind unknown and neglected cyber assets. These unknown and under-addressed subsidiaries carry a lot of the overall risk.

- Global merger and acquisition deals reached 62,000 globally in 2021, up 24% from 2020. Much of this activity was driven by demand for modern business practices shadow IT assets and more risk to an organization from the unknown assets within its attack surface.

- On average, the size of an organization's attack surface fluctuates by 5.5%. This fluctuation isn't necessarily a problem - a well-managed attack surface can grow and shrink month to month as new assets are added, discovered, and retired once they are no longer useful. The most important factor is an organization's awareness of the change in size and ability to adjust its security posture accordingly.

- If not properly managed, monthly changes in attack surface size can complicate the job of the CISO or security leader considerably. Not only are they responsible for monitoring and improving the overall security posture of the organization,they must stay on top of regular fluctuations in the attack surface size (for example, caused by a team signing on with a new software or service or from an office location closure) as well as larger changes that come with strategic shifts in the business.

95
Average number of subsidiaries each organization has

Organizations were initially unaware of
10-30%
of their subsidiaries

5.5%
Average amount that an organization's attack surface fluctuates in a given month

Web Apps

A web application (commonly referred to as web app) is any application or service that is stored on a remote server and delivered over the Internet to a browser. Because of how easily they can be accessed from any device, web apps have become essential to modern workplaces. Many organizations create and use their own homegrown web apps to provide a unique experience to their customers or streamline internal operations. However, web apps often represent security risks tied to unpatched vulnerabilities and potential exposure of sensitive data.

Of the organizations we examined, we found an average of 5,000 web apps per organization. These web apps made up 6 to 7% of the organization's total attack surface. This was consistent across industries, including technology (6.8%), media (6.8%), and finance (6.6%).

Each sub-organization or subsidiary organization at each customer has an average of 8.8 SQL injection and/or cross-site scripting issues at any given time.

By their very nature, web apps can provide footholds for attackers. Given the sheer variety of web apps, you might think that the vulnerabilities that affect them would be varied and difficult to categorize, but our data showed that just six web app related vulnerabilities accounted for approximately 90% of all web app issues. Open source JavaScript web apps also contribute to over 60% of identified issues.

Web apps aren't just a risk because they can give attackers a foothold into your systems - they also provide direct access to personally identifiable information (PII) that can be exploited, leaked, or sold on cybercriminal marketplaces. We found PII in 9% of the web apps we surveyed and in 8% of the average organization's web apps. Of course, some sectors by their very nature are more likely to have PII stored in their web apps - for example, we found that on average 17% of healthcare organizations' web apps contain PII.

Identifying and knocking out these most common vulnerabilities can be an easy win for security teams looking to shore up their attack surface.

Unsafe Authentication

- We found that not everything boils down to web apps or software vulnerabilities: across the organizations we surveyed, we found over thirty-three thousand assets that transmitted and stored users' information, including credentials, in plaintext.
- Recent research into password habits by password manager vendor Bitwarden revealed that despite years of effort from security experts to enforce better password practices, more than 8 in 10 (85%) of Americans reuse passwords across multiple sites.
- With statistics like that, it's no surprise that even though vulnerable software issues account for 84% of identified critical and high severity issues, we found that unsafe authentication accounts for 11% of these issues.

We use "unsafe authentication" as an umbrella term (see below). It doesn't all come down to bad password practices on the part of users. Some issues, like a lack of account takeover (ATO) and anti-botnet protection or a lack of corporate single-sign-on (SSO) solution can be remedied by changing corporate security practices. Even issues like sites accepting default credentials or weak passwords can be remedied once they're identified.

Top Web App Security Risks:

- **Vulnerable Open Source JS Library - jQuery** - some versions of the jQuery JS library don't validate inputs by default. An attacker can use this vulnerability to sneak in malicious functions or code, which jQuery will execute.
- **Unmaintained Asset** - we noticed a significant number of vulnerable assets were vulnerable because they were unmaintained and forgotten by their security teams. Unmaintained assets may still contain valuable information or loose permissions that attackers can use to burrow deeper into systems.
- **Vulnerable Open Source JS Library - JQuery-UI** - some versions of the JQuery-UI JS library are vulnerable to a cross site scripting (XSS) vulnerability that could allow attackers to inject their own code when a web app loads.
- **Vulnerable Open Source JS Library - Bootstrap** - some versions of the Bootstrap JS library are vulnerable to a cross site scripting (XSS) vulnerability that could allow attackers to inject their own code when a web app loads.
- **Clickjacking** - this occurs when multiple deceptive interactive layers are placed over a web application. The user thinks they're clicking on a safe item or window, but their click is hijacked by a bad actor to launch another attack. It's also known as "user interface (UI) redressing."

What is Unsafe Authentication?

- Default credentials
- Login web pages not protected ATO tech / anti-bot
- Weak passwords
- Login web pages not covered by corporate SSO

Conclusion

Our research makes it clear that organizations are facing down rapidly fluctuating attack surfaces exacerbated by subsidiary sprawl, a frenetic pace of mergers and acquisitions, and overworked security teams. Their attack surface is likely to contain valuable web apps that come with vulnerabilities giving attackers footholds into their network and access to sensitive data. In the face of such an overwhelming volume of issues, it is more important than ever that organizations have a clear picture of their attack surface, complete with straightforward steps to address and eliminate the most critical issues affecting their assets. The need for External Attack Surface Management solutions is only growing.

For more information on CyCognito's External Attack Surface Management solutions, go to cycognito.com/how-it-works, or schedule a demo at cycognito.com/demo-video.

Of the organizations examined, we found an average of

5000

web apps per organization

6-7%

of an organization's attack surface is made up of web apps

Six web app related vulnerabilities accounted for approximately

90%

of all web app issues

More than

85%

of Americans reuse passwords across multiple sites

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO