RISKIQ®

The Anatomy of an Attack Surface: Five Ways Hackers are Cashing In

To keep up with the breakneck speed of modern business, organizations are moving customer and partner interactions online. Unfortunately, increased risk of cyber attack and the associated consequences like data theft, operational disruption, brand erosion, and employee and customer compromise have become a natural side effect of this digital transformation. With the boundaries between what's inside the firewall and what's outside becoming less and less discernible, an organization's attack surface—everything it needs to worry about defending—now begins inside the corporate network and extends all the way to the outer reaches of the internet. Internet visitors taking advantage of all these new digital touchpoints available to engage with brands and other users are also in the crosshairs of hackers, who view their clicks, traffic, credentials, and computers as commodities to be harvested and traded and use the brands they love as bait.

For security teams, the sheer depth and breadth of what they need to defend may seem daunting, but thinking about the Internet from an attacker's perspective —a collection of digital assets that are discoverable by hackers as they research their next campaigns—can put the massive scope of their organization's attack surface into perspective. In this report, we'll highlight five areas that we feel help to better frame the challenges faced in keeping the Internet a safe environment, all of which underline a need to broaden awareness of the potential risks involved to foster a more informed approach to cyber defense.

With the boundaries between what's inside the firewall and what's outside becoming less and less discernable, an organization's attack surface—everything it needs to worry about defending—now begins inside the corporate network and extends all the way to the outer reaches of the internet.

1. The Global Attack Surface is much bigger than you think

And growing every day. We deployed our web-crawling infrastructure, which each day executes and analyzes more than 2 billion HTTP requests, takes in terabytes of passive DNS data, collects millions of SSL Certificates, and monitors millions of mobile apps, to map the scope of this attack surface over a two-week period.

- RiskIQ observed 3,495,267 new domains (249,662 per day) and 77,252,098 new hosts (5,518,007 per day) across the internet over a two week period, each representing a possible target for threat actors.

Modern websites are made up of many different elements—the underlying operating system, frameworks, third-party applications, plug-ins, trackers, etc., all designed to deliver a user experience that people have come to expect, as well as reduce the time to market and derive maximum value from user interactions. As in the PC environment, this commonality of approach is attractive to malicious actors as a successful exploit written for a vulnerability or exposure on one site can be reused across a large number of sites.

As an example, Content Management Systems (CMS) are popular amongst web developers for creating dynamic sites that are easy to maintain and update. Their ubiquity makes them a popular target for hackers as we've seen many times in the past. Over a two week period our research found:

- 13,297 WordPress plugins in the Alexa top 10,000 (most visited websites)
- 12,536 CMS instances in the Alexa top 10,000
- 1,713,556 WordPress plugins overall
- 1,814,997 CMS instances overall

Common Vulnerabilities and Exposures (CVE's) are classified by severity on a scale of 1 to 10 using the Common Vulnerability Scoring System (CVSS), where 7 to 8.9 represent high vulnerabilities and 9 to 10 represent critical vulnerabilities. Focusing on these high and critical vulnerabilities, our research showed:

- 3,390 of the Alexa top 10,000 domains were running at least one potentially vulnerable web component.
- 6,303 potentially vulnerable web components in total were found in the Alexa top 10,000
- 1,036,657 potentially vulnerable web components were found overall

While some of these instances will have patches or other mitigating controls to prevent the identified vulnerabilities and exposures from being exploited, many will not.

2. Sometimes hackers know more about your attack surface than you do

Most organizations lack a complete view of their Internet assets. In our dealings with new customers, we typically find 30 percent more assets than they thought they had. There are two significant contributors to this lack of visibility; shadow IT and mergers and acquisitions (M&A).

Where IT can't keep pace with business requirements, the business looks elsewhere for support in the development and deployment of new web assets. The security team is frequently in the dark with regards to these shadow IT activities and as a result, cannot bring the created assets within the scope of their security program. Unmanaged and over time, orphaned assets form the Achilles heel of an organization's attack surface. They are not regularly patched or security tested and the operating systems, frameworks, and third-party applications of which they are comprised can quickly age and become vulnerable to common hacking tools.

When you merge with another company, their vulnerabilities become your vulnerabilities. Mergers and acquisitions often bring with them incomplete and inaccurate lists of public facing digital assets that further exacerbate the problem.

Digital assets can be broken down into many different types, each with associated risks that must be understood and managed. Some of the key asset types are hosts, domains, websites, certificates, 3rd party applications and 3rd party components.

To highlight the scope of the challenge large organizations face in defending their digital assets, we conducted research on the FT30 basket of companies. Summarizing the results, on average each organization has:

- 5,322 hosts
- 9,896 dormant websites (parked, defensively registered, etc.)
- 3,846 live websites, 3,201 of which are currently serving content
- 596 live websites hosted on Amazon, 67 hosted on Azure (20 percent of total)
- 38 mail servers
- 1,766 registered domains
- 616 web pages collecting PII, 35 percent doing so insecurely
- 4 websites with expired certificates and 3 websites using old, untrusted encryption algorithms
- Content Management Systems (CMS's) - 96 instances of Wordpress and 56 instances of Drupal
- 120 websites with a potential critical score CVE (CVSS score 9-10)
- 228 websites with a potential high score CVE (CVSS score 8-9)
- 123 test sites. Some of these should be exposed on the Internet but in our experience, many should not.

These assets comprise a large and complex attack surface that needs to be understood and actively managed to reduce the low-hanging fruit available for cybercriminals to exploit.

3. The hidden attack surface: Hackers don't have to compromise your assets to attack your organization or your customers

Social engineering through impersonation remains a top tactic for threat actors. Impersonating domains, subdomains, landing pages, websites, mobile apps, and social media profiles are all used, many times in combination, to trick consumers and employees into giving up credentials and other personal information or installing malware.

- In Q1 2018, RiskIQ identified 26,671 phishing domains impersonating 299 unique brands, 40 percent of which were financial services brands
- Phishing tactics have become increasingly sophisticated, often leveraging multiple digital elements as we can see in our recent coverage of a MyEtherWallet phish: https://www.riskiq.com/blog/labs/myetherwallet-android/

Apart from their own assets, organizations must be on the lookout for impersonating or affiliating assets created to target their customers and employees. Early detection and takedown of infringing assets are one of the most effective ways of disrupting targeted campaigns.

4. The mobile attack surface: You have much more to worry about than just the Apple and Google Play mobile app stores

The general perception is that there are a small number of mobile app stores but the reality is somewhat different. There are a large number of secondary and affiliate stores primarily serving the Android market which provide an opportunity for malicious actors to compromise legitimate apps and launch fake apps while hiding in the vastness of the app store ecosystem. Our Q1 2018 mobile app research revealed:

- 21,948 blacklisted mobile apps across 120 mobile app stores and the open internet. This equates to 1.5 percent of all new apps detected. 8,287 of those were detected in the Google Play store
- 46 percent of all feral apps (mobile apps not hosted in a store) were blacklisted. Users are often directed to these apps through mobile and social phishing campaigns
- 86 percent of apps blacklisted claimed the READ_SMS permission, which allows the app to read messages and can be used for any number of nefarious purposes, including circumventing two-factor authentication

Organizations must do more to monitor the app store ecosystem for stores hosting their apps without permission and for apps impersonating their brand(s). Users should stick to the primary app stores where possible and be vigilant in researching apps they wish to download. They should question whether the developer looks legitimate, whether the user reviews indicate anything concerning and whether the permissions being asked for seem excessive for the functionality the app needs to provide its service.

5. Cryptocurrency Miners are the latest attack surface compromise

While spyware, ransomware and other forms of malware still proliferate, cybercriminals are augmenting their activities by stealing computer resources rather than information. With the exponential growth in the value of cryptocurrencies, crypto mining is now a lucrative pursuit. The primary challenge facing cryptocurrency prospectors is that mining requires an extreme level of computing power, which can be prohibitively expensive — Fundstrat reported that the cost of mining a single Bitcoin reached about $8,038, and the cost of mining other coins are not far behind. To get around it, actors are siphoning computing resource from unwitting users across the internet; hosting crypto mining scripts on the websites of highly visited sites which then execute in the web browsers of visitors to those sites. From our research we found:

- 50,000+ websites have been observed running Coinhive in the past year
- An average of 495 new hosts running cryptocurrency miners each week over the past 26 weeks.
- 326 Drupal injections on hosts running Coinhive, suggesting that this is one of the ways sites are being infected.
- Across the websites belonging to the FT30, we found 11 instances of cryptocurrency miners

Some of the crypto mining scripts we found have been active for over 160 days, suggesting that organizations are failing to detect them.

Summary

Traditionally, the security strategy of most organizations has been a defence-in-depth approach starting at the perimeter and layering back to the assets that should be protected.

However, there are disconnects between that kind of strategy and the attack surface as presented in this report. In today's world of digital engagement, users sit outside the perimeter along with an increasing number of exposed corporate digital assets—and the majority of the malicious actors. As such, companies need to adopt security strategies that encompass this change.

RISKIQ

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ