RISKIQ®

Analysis of an Attack Surface:

Five Ways Hackers are Targeting Organizations

Contents

Key Insights

The Global Web-Based Attack Surface is Much Bigger Than You Think

Across the internet over two weeks, RiskIQ observed:

2,959,498
New Domains
(211,392 per day)

772,786,941
New Hosts
(55,199,067 per day)

Of the Alexa top-10,000 domains:

2,480
2,480 are running at least one potentially vulnerable web component

8,121
There are 8,121 potentially vulnerable web components overall

Sometimes Hackers Know More About Your Attack Surface Than You Do

On average, each organization in the FTSE-30 has:

324
Expired certs

25
SHA-1 certs

743
Potential test sites

28
Insecure login forms

385
Total insecure forms

46
Web frameworks with known vulnerabilities

80
PHP 5.x instances (EOL end of the year)

664
Web servers at release levels with known vulnerabilities

Key Insights (cont.)

The Hidden Attack Surface: Hackers Don't Have to Compromise Your Assets to Attack Your Organization or Your Customers

21,496

RiskIQ identified 21,496 phishing domains in Q1 2020 across 478 unique brands

720,188

RiskIQ identified 720,188 instances of domain infringement in Q1 2020 across 170 unique brands

350%

Phishing attacks immediately grew 350% after the COVID-19 outbreak

317,000

RiskIQ noted 317,000 new websites related to COVID-19 over just two weeks

The Mobile Attack Surface: You Have Much More to Worry AboutThan Just the Apple and Google Play Mobile App Stores

170,796

170,796 blacklisted mobile apps existed across 120 mobile app stores and the open internet in 2019

25,647

Only 25,647 (15% of the total) blacklisted apps were in the Google Play Store in 2019

JavaScript Threats: A New Frontier of Cybercrime

+30%

In March, with COVID-19 forcing a spike in online shopping, RiskIQ detected a 30% increase in Magecart skimmers

2,552

RiskIQ has detected 2,552 Magecaert attacks in 2020

Introduction:

The Digital Transformation a Decade in the Making

Businesses are undergoing a digital transformation demanding rapid migration to the cloud and expanded adoption of web, mobile, and social platforms. These initiatives, which expand organizations' digital presence far across the internet, were already exposing the limitations of network security controls like firewalls, DLP, and network monitoring. According to the Verizon Data Breach report, external-facing web applications, into which network security tools lack visibility, comprised the vector category most commonly exploited in hacking-related breaches.

This digital transformation, already challenging long-held views of cybersecurity, was sent into hyperdrive by COVID-19. Almost overnight, workforces and business operations were decentralized and flung all over the world even farther than before, widening protection gaps and turning security protocols on their heads. Personnel, now forced to work from home, moved the edges of their organization's digital attack surfaces along with them.

In this paper, we'll highlight five areas that we feel help to frame the challenges faced in going beyond network security controls to discovering unknowns and investigating threats outside the firewall. All five of these areas underline a need to extend security programs outside the perimeter to foster a more informed approach in this new age of cyber defense.

The COVID Effect

With much of the $80 trillion global economy being run out of homes, attackers now have far more access points to probe or exploit, with little to no security oversight. IT teams for companies who moved to a WFH format are feverishly standing up new systems, new access, and new channels, but in the process, they're likely succumbing to human error, such as critical misconfigurations. Adding to this ballooning attack surface area, once things normalize and IT teams can create established processes, many of the systems set up as IT patches during the COVID crisis will be forgotten and left exposed.

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, even into the homes of employees.

For IT security teams, the sheer depth and breadth of what they need to defend may seem daunting. However, 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 area of their organization's attack surface into perspective.

1. The Global Web-Based Attack Surface is Much Bigger Than You Think

The internet is like a boundless tapestry that's ever-expanding in all directions and growing every day. Each of its components—websites, IP addresses, components, frameworks, and code—are individual threads that are all woven together to create the web as we know it. Being a part of this tapestry isn't a choice; if an organization has an internet presence, it is interwoven with every other entity on the web, including attackers. Those who understand how these connections work, good guy or bad guy, are the ones who win.

To show the scale of the internet-wide attack surface, RiskIQ deployed our global collection technology, which extracts terabytes of internet data to map the billions of relationships between internet-exposed infrastructure worldwide, in order to assess digital risk. These systems make daily scans of hundreds of unique ports and service banners across the entire IPv4 space and execute billions of HTTP requests to take in passive DNS data and extract web components such as SSL certificates, tracking code, and cookies.

Across the internet over two weeks, RiskIQ observed:

2,959,498

New Domains

(211,392 per day)

772,786,941

New Hosts

(55,199,067 per day)

Each of these represents a possible target for threat actors.

Modern websites are made up of many different elements—the underlying operating system, frameworks, third-party applications, plugins, trackers, etc. All these elements come together to deliver a user experience that people have come to expect while reducing the time-to-market. 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 many sites.

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

13,222

WordPress plugins in the Alexa top 10,000 most visited websites

4,780

total CMS instances in the Alexa top 10,000

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 represents high vulnerabilities, and 9 to 10 represents critical vulnerabilities. Focusing on these high and critical vulnerabilities, our research showed that:

2,480 **of the Alexa top 10,000 domains were running at least one potentially vulnerable web component**

8,121 **potentially vulnerable web components in total were found in the Alexa top 10,000**

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. RiskIQ typically finds 30% more assets in our dealings with new customers than they thought they had.

There are two significant contributors to this lack of visibility:

- Shadow IT
- Mergers and acquisitions (M&A)

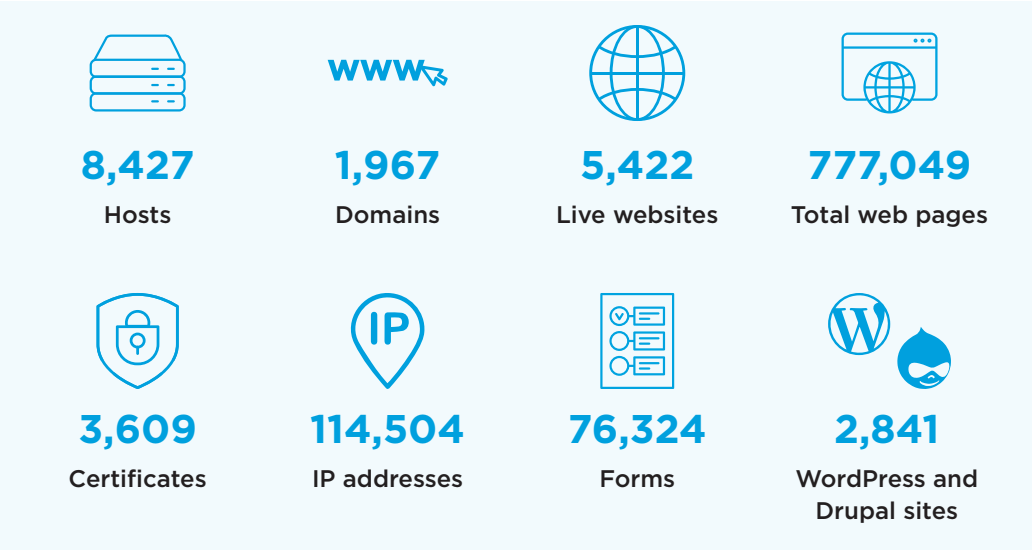
However, with much of the world now suddenly working remotely—and likely to remain remote after the pandemic—it's shadow IT that will become one of the biggest monsters for security teams to slay in the coming weeks, months, and even years.

When an organization's IT can't keep pace with its business requirements, the business looks elsewhere for support in the development and deployment of new web assets. As staff quickly set up workstations from home, and business units rework processes that were previously contained within the corporate network, supporting infrastructure may now sit outside the purview of their security teams. As a result, they cannot bring the created assets within the scope of their security program. Over time, unmanaged orphaned assets form the Achilles heel of an organization's attack surface. These assets are not patched or tested, and their operating systems, frameworks, and third-party applications can quickly age and become vulnerable to even common hacking tools.

There are many different types of digital assets that require security oversight. Some of the common asset types are hosts, domains, websites, certificates, third-party applications, and third-party components.

To highlight the scope of the challenge large organizations face in defending their digital assets, we conducted research on the companies that comprise the FTSE-30, a group of 30 large-cap organizations in the UK.

Summarizing the results, each organization has on average:



The mad dash by IT teams to stand up new systems outside the firewall to enable a remote workforce has expanded attack surfaces quicker and more radically than ever before. VPN usage surged 112% over just six weeks, and RiskIQ noted a 26.11% increase in Microsoft Remote Access Gateway instances, peaking around March 20 when stay-at-home orders took full effect.

Threat actors know these internet-connected services can be easy inroads to corporate networks and are always scanning for vulnerable services to attack. To counter hackers, security teams must have visibility into the IPv4 space so they can develop a full inventory of digital assets connected to them outside their internal network and flag assets that become vulnerable so they can be patched and put under management.

On average, each FTSE-30 organization has:

114,504
IP addresses

45
Mail servers

7,790
Cloud-hosted apps (Amazon and Azure)

26
Potentially vulnerable Citrix Netscaler instances

8
Potentially vulnerable Palo Alto GlobalProtect instances

9
Potentially vulnerable Pulse Connect instances

25
Potentially vulnerable Fortinet instances

1,464
Remote access service instances

Each digital asset in an organization's attack surface, shadow IT or not, has associated risks that must be understood and managed. On average, each FTSE-30 organization has:

324
Expired certs

25
SHA-1 certs

743
Potential test sites

28
Insecure login forms

385
Total insecure forms

46
Web frameworks with known vulnerabilities

80
PHP 5.x instances (EOL end of the year)

664
Web servers at release levels with known vulnerabilities

3. The Hidden Attack Surface: Hackers Don't Have to Compromise Your Assets to Attack Your Organization or Your Customers

Social engineering via 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 2020, RiskIQ identified 21,496 phishing domains impersonating 478 unique brands, 34% of which were financial services brands.
- In Q1 2020, RiskIQ identified 720,188 instances of domain infringement across 170 unique brands.
- The global response to COVID-19 revealed a host of new opportunities for threat actors, with FBI cybercrime reports quadrupling during the pandemic. As concern over the outbreak was sweeping the globe, attackers got to work to take advantage of it. Phishing attacks immediately grew 350%.
- RiskIQ noted 317,000 new websites related to "COVID-19" or "coronavirus" in the two weeks between March 9 and 23, and Google blocks millions of COVID-19 scam emails daily. Many of these messages promise treatment or a cure for the virus, while others offer promotions, discounts, and free products.

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 very different. Apple treats its App Store like Fort Knox and rarely hosts dangerous apps. Meanwhile, Google's security controls are improving despite allowing troublesome apps to enter the Play Store at a rate it finds acceptable. For example, the number of blacklisted apps in the Play Store dropped an impressive 76.4% in 2019.

However, there are a large number of secondary and affiliate stores primarily serving the Android market. These provide an opportunity for malicious actors to compromise legitimate apps and launch fake apps while hiding in the vastness of the app store ecosystem.

In 2019, RiskIQ discovered:

- 170,796 blacklisted mobile apps across 120 mobile app stores and the open internet. Of these, 25,647 of these were found in the Google Play Store.
- 25,647 of these were found in the Google Play Store.

Because the two leading app stores are inhospitable for malicious apps, threat actors must turn elsewhere to turn a profit. However, there are hundreds of stores across the world in which threat actors can comfortably sell their wares. They can also make their apps available as feral apps across the open web, outside of stores altogether.

- 46% 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% of blacklisted apps 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

The most prolific stores of blacklisted apps in 2019 were:

1. **9Game.com**
   61,669
2. **Google**
   25,647
3. **Zhushou**
   25,091
4. **Feral apps**
   12,079
5. **Vmallapps**
   5,972

This hidden mobile threat landscape is a branding and consumer trust nightmare for businesses. Whether they have an official mobile presence or not, brands must be aware of this mobile app landscape to understand the entirety of their mobile attack surface. Monitoring primary stores like the Apple App Store and Google Play Store is essential. Still, having visibility into apps in lesser-known app stores across the world and the web is paramount.

5. JavaScript Threats: A New Frontier of Cybercrime

Just a decade ago, the world's JavaScript was a nearly untapped wellspring of victims and cash for attackers. Now, it's a new frontier for cybercrime that covers 95% of all websites on Earth.

Because they execute in the victim's browser, JavaScript threats fall outside the corporate network and beyond the purview of traditional security controls. Realizing they were operating in a blind spot for security teams, innovative threat actors seized the opportunity and started picking apart the JavaScript of websites worldwide.

E-commerce is particularly vulnerable to this onslaught, with web-skimmers intercepting consumer credit card numbers across a massive swath of websites. In March, with COVID-19 forcing a spike in online shopping, RiskIQ detected a 30% increase in Magecart skimmers.

So far in 2020, RiskIQ has detected 2,552 Magecart attacks, or 425 per month.

Also, with the rise in value of cryptocurrency, attackers have returned to stealing users' CPUs to mine coins, stealthily placing their cryptominers in the JavaScript of victimized websites. So far, in 2020, RiskIQ has detected cryptocurrency miners on 963 distinct hosts.

Summary:

Extend Your Security Outside the Firewall with RiskIQ

Traditionally, the security strategy of most organizations has been a defense-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.

The rush to migrate to the cloud and warp-speed adoption of web, mobile, and social platforms badly exposed the limitations of internal network security controls. The COVID-19 pandemic, which has scattered workforces and business operations across the country, has made these controls almost obsolete and Internet-wide visibility imperative. Attackers now have far more access points to probe or exploit, with little to no security oversight.

With RiskIQ's Internet Intelligence Graph, customers have access to a pre-computed relationship database of internet intelligence updated daily. Tapping into the Graph provides a full picture of the entire internet to show your own organization's internet attack surface, including known, unknown, and attacker-owned assets. This view includes external third-party infrastructure and resources your organization, users, and customers depend on.

Lots of "outside the firewall" security companies claim to give you visibility into this new dispersed and rapidly-growing internet attack surface. Unfortunately, they only have a cursory view of the web and only know about known assets their customers provide them. RiskIQ deeply understands the internet and how its threads weave together. Contact us today to find out how we can help you understand and defend your attack surface in this new era of cybersecurity.

About RiskIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75%of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

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

sales@riskiq.net

1 888.415.4447

Learn more at riskiq.com