IONIX

WHITEPAPER

WHAT'S HIDING IN YOUR EXTERNAL ATTACK SURFACE?

THE HIDDEN THREATS INTRODUCED BY THIRD PARTIES

OVERVIEW

Security incidents originating from digital supply chain risks are on the rise. As modern web applications become increasingly reliant on 3rd party web services and content, such risks will pose a growing threat to organization's online infrastructure. This paper provides a detailed overview of these risks, and a systematic approach risk reduction with an advanced Attack Surface Management (ASM) platform. By automating discovery, risk assessment, threat prioritization, accelerating remediation, and automating protection – security teams can effectively improve their security posture.

In the coming years, it is predicted that the majority of security incidents will stem from third-party vulnerabilities.

In fact, the recent uptick in supply chain attacks has prompted executive leaders to put greater focus oncybersecurity. Many organizations are beginning to incorporate cybersecurity standards into their enterprise risk management strategies and procurement qualifications as well.

In turn, cybersecurity teams need to develop, maintain and enforce policies and practices around their ecosystem and digital supply chain. These practices must include continuous discovery and mapping of all assets and connections, including those of third parties, as well as continuous risk assessment of these connections. Controls must include the ability to detect and alert on risky or broken connections, coupled with automated remediation when feasible.

Modern web applications are increasingly reliant on 3rd-party web services and content.

THE MODERN ATTACK SURFACE

Modern web apps and websites are amalgams of code and content delivered from multiple sources into the users' browser. It is common for pages in popular websites to have the browser load content from 50 or 100 different sources. This content includes user trackers, site monitoring and analysis, ads, fonts, scripts, images, and embedded social media and other widgets. Some of this content will be delivered from sources that are owned and actively managed by the site owner, but many sources will be third parties that the site owner does not actively manage.

Pages in popular websites commonly load content from 50 and even 100 different sources.

These third-party assets and sources create an ecosystem connected to an organization's online properties (websites and applications). These assets are typically connected to the web property via various HTML tags, chains of scripts, and, with the advent of CDNs and cloud computing, via chains of DNS records that may direct the browser to retrieve content from "files.mycompany.com" (a DNS record pointing to a specific S3 bucket), or "app.mycompany.com" (a DNS record pointing to a specific Azure web app). These too are part of the ecosystem.

THE NEW NORMAL OF CONNECTED ASSETS

Beyond the indispensability of cloud providers and CDNs in hosting and delivering applications, if an organization has any public sites, it will leverage:

- Third-party user tracking
- Site analysis and monitoring
- Embedded social media
- Advertising

in order to deliver the best possible user experience. Because these solutions are readily available from third-party providers, it is unlikely the organization will develop them in-house. In addition, it is common for the framework used for the site structure itself to contain connections to third parties.

It’s worth noting, in this context, that the term “third party” does not convey the true depth and extent of its presence in the ecosystem. A script or a bit of HTML loaded from a partner will often call additional scripts or other content from their partners, who in turn may do the same. In one example, a researcher at AKAMAI found a single chain of 40(!) calls to reach the final asset that was included in a page from Monster.com.

Monster.com link required a chain of 40 calls to reach the final distination.

From a security standpoint, it is important to note that your online ecosystem comprises not just the resources that are explicitly referenced by your first-party HTML code or your DNS records. The complete online ecosystem expands through long chains of references that can include connections and assets from providers that the site owner does not have a direct relationship with. A breach anywhere along these chains could lead to a compromise of your sites and ultimately your users, customers, and business. In what follows we’ll use the term “third party” inclusively, so as to refer to any nonfirst-party resource or asset that’s called when loading content for an organization.

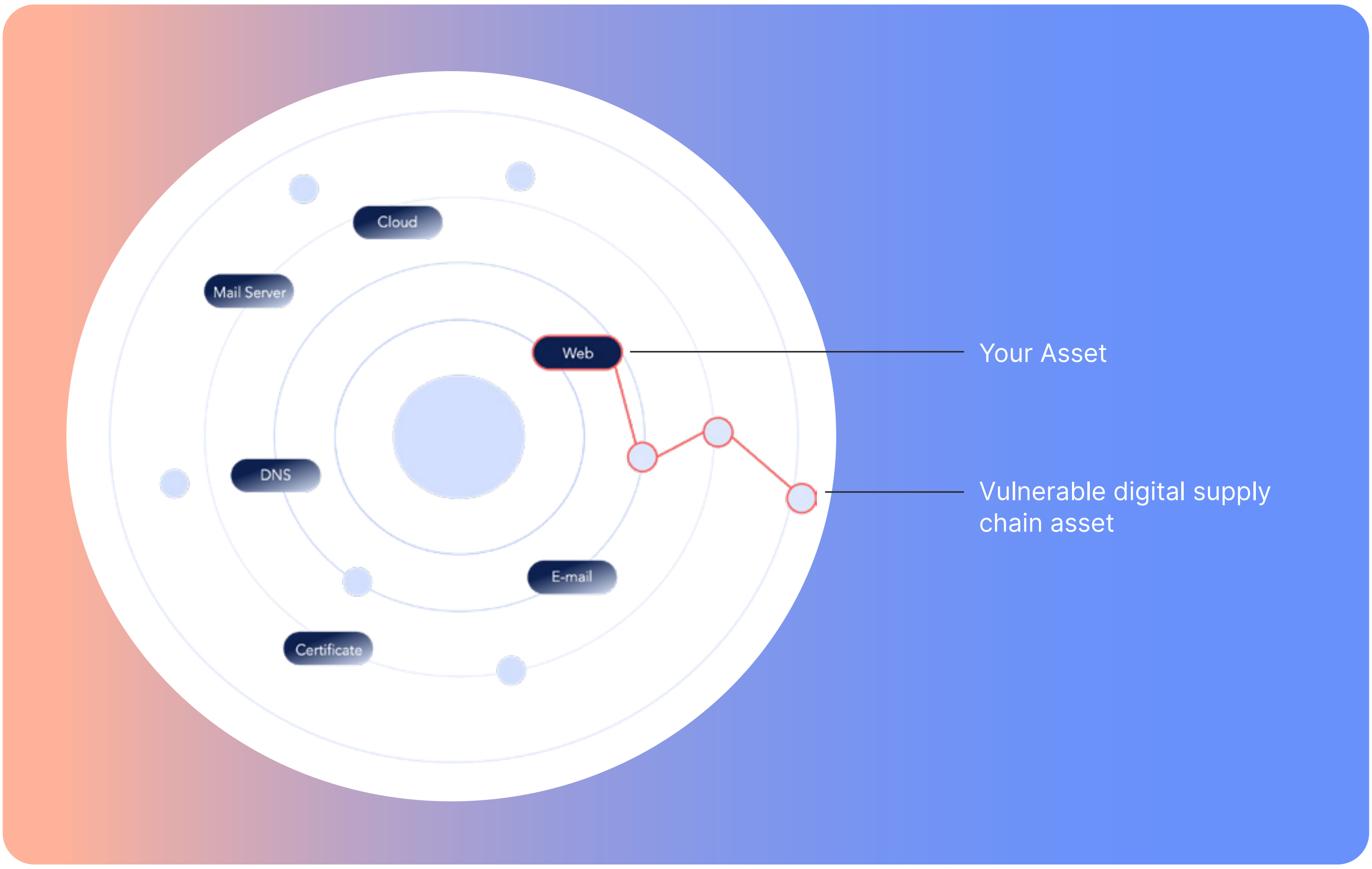
For medium and large enterprises, IONIX found that the ratio of unique third-party FQDNs to unique first-party FQDNs is about 3:2. The number of unique connections is easily a 6:1 ratio to the number of firstparty assets. These connections are conduits of risk and exploits, and, due to the sheer number of them, technologies need to be put to use to help discover and secure them.

RISK PROPAGATION THROUGH DIGITAL SUPPLY CHAIN CONNECTIONS

It is remarkable, but not surprising, that supply chains have been largely overlooked by enterprise cybersecurity groups. Third-party assets and connections aren't seen by organizations' perimeter security tools. It's only the user's browsers and apps that make a network connection with them, so WAFs and Firewalls do not see these connections. Besides, it's been hard enough to keep track of an organization's own inventory of websites and maintain a consistent perimeter security around these, so very few enterprises have been systematically engaged in discovering, assessing or monitoring third-party assets across their online presence.

It is also worth noting that despite growing awareness of the need to do it, relatively few organizations have set standards around even the most obvious known-to-berisky connections—third-party script inclusions—even though cross-site scripting has been on the top 10 OWASP list for as long as it has existed. Even less have found any effective technology for centrally monitoring script inclusions organizationally across their websites. The tools simply have not been there. Handling script security has been left to the developers who, with little effort, can establish guardrails and limit the damage any one script inclusion could cause. But IT and cybersecurity teams have, by and large, not concerned themselves with this challenge. And the obscurity of this challenge, coupled with this neglect, have precipitated the explosion of Magecart attacks.

Script inclusion is decidedly *not* the only third-party connection



that carries a risk. If an attacker takes control of an image or font source for your website, they can easily deface it, but they can do much more. And these are, by no means, all the ways in which web content served by your websites can refer your users' apps and browsers to load and process malicious content from third-party sources. There are dozens of other ways. One particularly attractive conduit for breaching organizations through their supply chain has been the cloud. The use of most cloud services to deliver content online requires companies to use DNS CNAME records to map some meaningful FQDN (www.mycompany. com) to the canonical name of their instance of the cloud service ("mycompany.com.azurewebsites.com" or "mycompany.com.s3.amazonaws.com"). Now, beyond the fact that these cloud resources are generally outside any organizational firewalls and require cloud-native modes of protection that may or may not be centrally or effectively managed, these resources are also fungible.

A dev shop might spin up an instance of a service for testing or a short lived campaign, then destroy it. When that happens, any connection to that service remains "dangling" until reference to that CNAME is removed, or until someone else sets an instance of the service with the same canonical name. Cloud providers have little or no controls concerning the canonical names customers choose for their service, beyond keeping names unique. So, malicious users are trying, and in many cases succeeding, in finding these dangling connections, i.e., canonical names referenced by DNS CNAME records, registering services with those names, and then using that connection either to serve illicit content on an organization's domain in order to bypass anti-spam or URL filtering, thereby damaging the organization's reputation and potentially making it also legally liable, or to do worse.

Once any of these connected assets are compromised, so are you. Beyond defacements that inflict damage to your brand's reputation, exploits can be set to harvest user data as well as manipulate trusted users' data entry. If this is not enough, the road from there is very short to installing persistent malware on your users' devices. And then your data centers are next in line. In fact, exploiting vulnerable third-party connections is today perhaps the path of least resistance for breaching most organizations.

A SYSTEMATIC APPROACH TO ATTACK SURFACE MANAGEMENT

As is always the case, a strategy for securing the attack surface will require a combination of technology and human processes. The technology will be used primarily for collecting and synthesizing information, while the processes will focus on taking preemptive or remediate action.

Discovery

Let's start with the obvious: there's no security without visibility. In the same way that IT security requires asset discovery, the first step in attack surface security is that of supply chain discovery, at enterprise scale. Cybersecurity analysts need a tool that will be able to list for them, in near real time, all of the websites that currently embed some Facebook social plugin, or that download fonts from Adobe, or that download some script from Tabula. Without such tools, companies will not be able to respond effectively even when a specific exploit has been disclosed somewhere within their digital supply chain.

Now, knowing what connects with what, even at the webpage level, is not enough. The tool should collect enough metadata about connected third-party assets so as to be able to tell, for instance, if and which cloud service they're implemented on. The security analyst might find it relevant that the third-party asset their site was directing users to download scripts from is some S3 bucket. She might want to list all the S3 buckets from which any scripts are loaded. Note that attack surface discovery must include the continuous discovery of the organization's own firstparty online assets. Effective discovery is the iterative, recursive discovery of Nth-level connections and connected assets ultimately emanating from first-party assets. Thus any solution that provides asset discovery can be expected to excel in first-party online asset discovery.

Assessment

Perhaps the most crucial part of any solution is the subsequent assessment of discovered assets. Security teams need some level of analysis on the security posture of assets in their supply chain, i.e. If my site is loading script from an S3 bucket, I need to know that that bucket does not allow anonymous access. The tool should provide this analysis. If, instead, the third-party asset is some server running Apache, I need to know that the version it's running does not have critical known vulnerabilities that will allow attackers to take over the server and modify the scripts my users are loading. In general, third-party assets can only be assessed as "black boxes". By definition, an organization may not have any kind of privileged access to these assets. This requires the organization to adopt scanning capabilities that operate non-destructively and yet, in a way, that mimic reconnaissance tools attackers might use. Beyond using such tools to discover the cloud service and/or components that are used in building sites, additional care needs to be put to the cryptographic characteristics of the asset: does it use TLS or does it allow HTTP? Is it using a valid certificate from a trusted source? DNS is of particular interest here: what's the resolution tree for the FQDN of the asset? Does it resolve consistently? Does it resolve at all?

This last point is pertinent to the specific case of broken connections. Broken connections are ones where the referenced connected asset is not reachable. Now, there can be more or less innocuous reasons for a broken connection. The least innocuous broken connection is where the FQDN or IP address that referenced asset resolves to (via CNAME or DNS records) are available for taking over. These broken connections must be signaled immediately, because after a malicious takeover, it might be nearly impossible to tell the difference.

But most importantly, any vulnerabilities discovered within the supply chain have to be accounted for in calculating the real risks they pose to the first-party assets that connect to them. Any attack surface security platform needs to derive from these vulnerability assessments a prioritized risk score for the organization and each asset, with clear steps that can be taken to remediate the vulnerabilities and eliminate the risks.

Alerting & Remediation

As suggested above, information is valuable only if it informs action. In the case of supply chain vulnerabilities, the current state of the art precludes, in most cases, completely automatic responses to address the root cause. This is true for many cases when vulnerabilities are found in first-party assets—e.g., you often can't automatically force a website to upgrade its webserver, and it is even more true when the root cause is a vulnerability detected in a third-party asset where that asset is not under the control of the organization, and the connection to that asset cannot be completely severed without a detailed analysis followed by a code change. Nonetheless, a set of standard operating procedures must be developed to address issues, and these procedures need to be backed by a flexible, highly-configurable, rules-based alerting and notification system that can group findings by resolution flow, set thresholds based on risk levels or other parameters, and initiate action by sending notifications, alerts, and remediation steps to the right systems (often SIEM and SOAR systems) or personnel (via SMS, email etc) for further coordinated action. Of course, when some remediation steps can be automated, either by the platform itself, or somewhere downstream, the value can be immense. At IONIX, the platform supports automatic mitigations against distinct high-risk broken connections.

THE IONIX PLATFORM

The IONIX platform is a first of its kind solution providing visibility, security and risk assessment, as well as alerting and remediation. It delivers unmatched discovery capabilities that go beyond discovering organizations domains and first-party assets to discover unlinked shadow IT. Because of its focus on asset AND connection discovery, it's the only system available today that will allow security and operations personnel, at a click of a button, to list all the assets that e.g., load images from a no-longer-trusted partner, or have hyperlinks to a site that no longer exist. It offers high-value, actionable vulnerability and misconfiguration assessments for cloud, web, PKI, TLS and DNS infrastructures across the supply chain, and it offers highly-flexible notification, alerting, and programmatic access. It also offers automatic mitigation for some of the most insidious vulnerabilities.

While the system requires no installation to discover and assess an organization's ecosystem, and while every finding is accompanied by a specification of the steps needed for a resolution, IONIX's veteran security team can assist clients in setting up alerts and notifications, and in formulating and implementing organization-specific remediation flows.

IONIX's unique risk assessment capability uilizes multi-faceted and contextualized criteria, including:

Cloud Infrastructure
Cloud infrastructures provide IT with agility and scalability. However, the scale of these assets can lead to configuration and maintenance errors that create vulnerabilities.

Web
Scripts and other objects incorporated into web properties may be hosted or served from vulnerable infrastructures.

DNS
Internal and external DNS infrastructures are used by the organization and related parties. As DNS is the basis for every online communication, DNS misconfiguration or security issues can result in loss of data or access.

Public Key Infrastructure
Public Key Infrastructure (PKI) is a vital layer within the security framework. PKI misconfiguration issues expose the organization to trust and reputation damage,regulatory violations, and risk of data losses.

IONIX ATTACK SURFACE MANAGEMENT

Our platform perfroms a continuous process of discovery, assessment, remediation and visualization.

- Continuous Discovery Discover and map any asset and its connection to your enterprise. Our unique approach to discovery uncovers, maps, and assesses the complete online ecosystem connected to your organization.
- Prioritize Risks Assess the risk of every asset and connection based on multi-faceted and contextualized criteria (PKI, DNS, TLS, Cloud configuration errors, known exploits of web resources, etc.)
- Accelerate Remediation Reduce false positives and accelerate remediation with severity-ranked action items and built-in playbooks presented in a web-based dashboard.
- Automatic Defense against takeovers with Active Protection feature that freezes exploited assets until your team can remediate the issue.
- Advanced Reporting Comprehensive reporting for internal, external, connected, login and managed domain inventories; PKI, Cloud, DNS, TLS, web, network and mobile assessments; vulnerability and misconfiguration analysis; attack surface reduction progress, and executive summaries.
- Streamline Integration with existing tools via API or native integrations including Microsoft Azure Sentinel, ServiceNow, Atlassian JIRA, Splunk, Cortex XSOAR, and more.

GET STARTED TODAY

Contact our team to get a complete assessment of your environment, or get free discovery today.

sales@ionix.io | Learn more at ionix.io