Managing Domain Attack Surfaces in the Financial Sector with WhoisXML API

Posted on September 14, 2021

While the cybersecurity landscape constantly evolves, the targets remain consistent. Among the hardest hit by cyber attacks is the financial services industry. In Verizon's 2021 Data Breach Investigations Report (DBIR), for instance, 65% of security incidents in the industry resulted in confirmed data disclosure.

Mitigating this problem begins by determining where the threat actors are attacking from—inside or outside? Identifying attack vectors is also pertinent.

Threat actors in the financial sector vary. Some are institution insiders and partners, while 56% are external parties. The top attack vectors are phishing and other social engineering campaigns.

One of the keys to a digitally safer financial industry is properly managing as many external attack vectors as possible. External Attack Surface Management (EASM) Solutions that uncovers and addresses vulnerable and dangerous Internet-facing assets, can help achieve this feat.

External Attack Surface Management in the Financial Sector

WhoisXML API's EASM Solutions gives financial institutions a complete view of what's happening in the Domain Name System (DNS) and the Internet and which occurrences can affect them. EASM Solutions can help users discover, validate, prioritize, and monitor external digital assets using a four-step process.

Step #1: Asset Discovery

In the asset discovery stage, EASM Solutions comprehensively catalogs digital assets relevant to

the organization. These could include domain names, subdomains, and IP addresses.

In the financial industry, actual WHOIS, IP, and DNS data relevant to the top 10 financial companies on Forbes 2021 Global 2000 uncovered thousands of external digital assets. These assets were only added since Forbes published the list on 13 May 2021. The breakdown is presented below.

Number of Domains	Number of Subdomains	Number of Related IP Addresses	Total Number of Assets Discovered
14,098	5,758	596	20,452

On average, about 2,045 assets were added to the attack surface of each financial institution in the past four months.

Step #2: Asset Attribution and Validation

The next phase can involve properly processing the assets and looking for anomalies based on context derived from geolocation, WHOIS, DNS, network infrastructure, and other data sources.

Domain Ownership Attribution

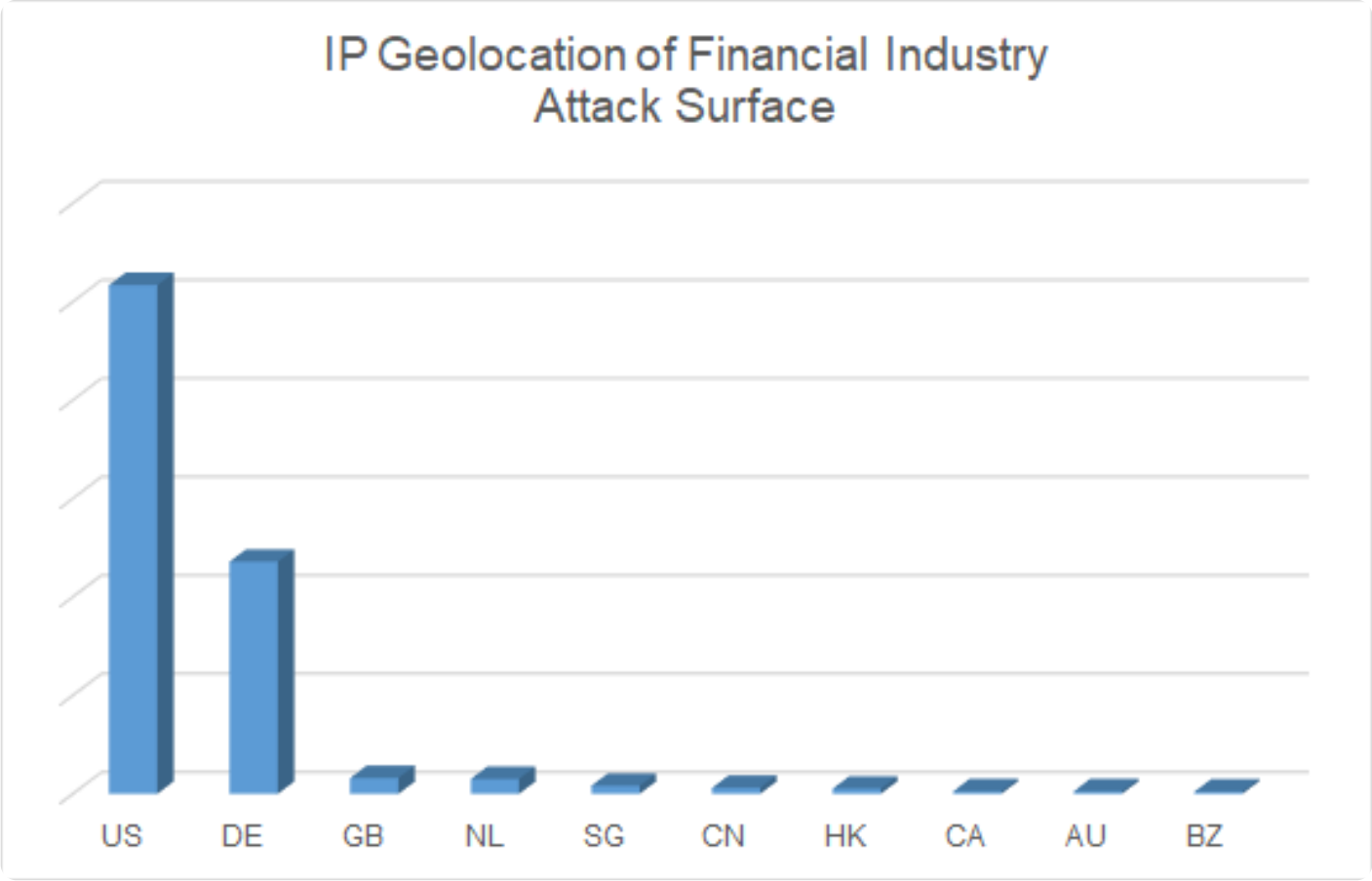
One of the first steps is to see which assets are under the organization's control and which aren't.

Analyzing WHOIS registrant records can help with attribution. From a sample of the financial industry's newly discovered assets, public attribution was nonexistent. Even when most of the companies had public WHOIS records, none of the domains in the sample matched their registrant email addresses.

IP Geolocation Validation

An external asset that resolves to an IP address geolocated outside an organization's scope could pose a risk. This danger becomes more pressing for financial companies that only serve specific locations. The top 10 financial institutions, for example, operate in China and the U.S.

However, the IP geolocation of the discovered assets in the financial sector is distributed across 36 countries. While most of the IP addresses are based in the U.S., only 0.60% belonged to China. Almost a quarter were geolocated in Germany.

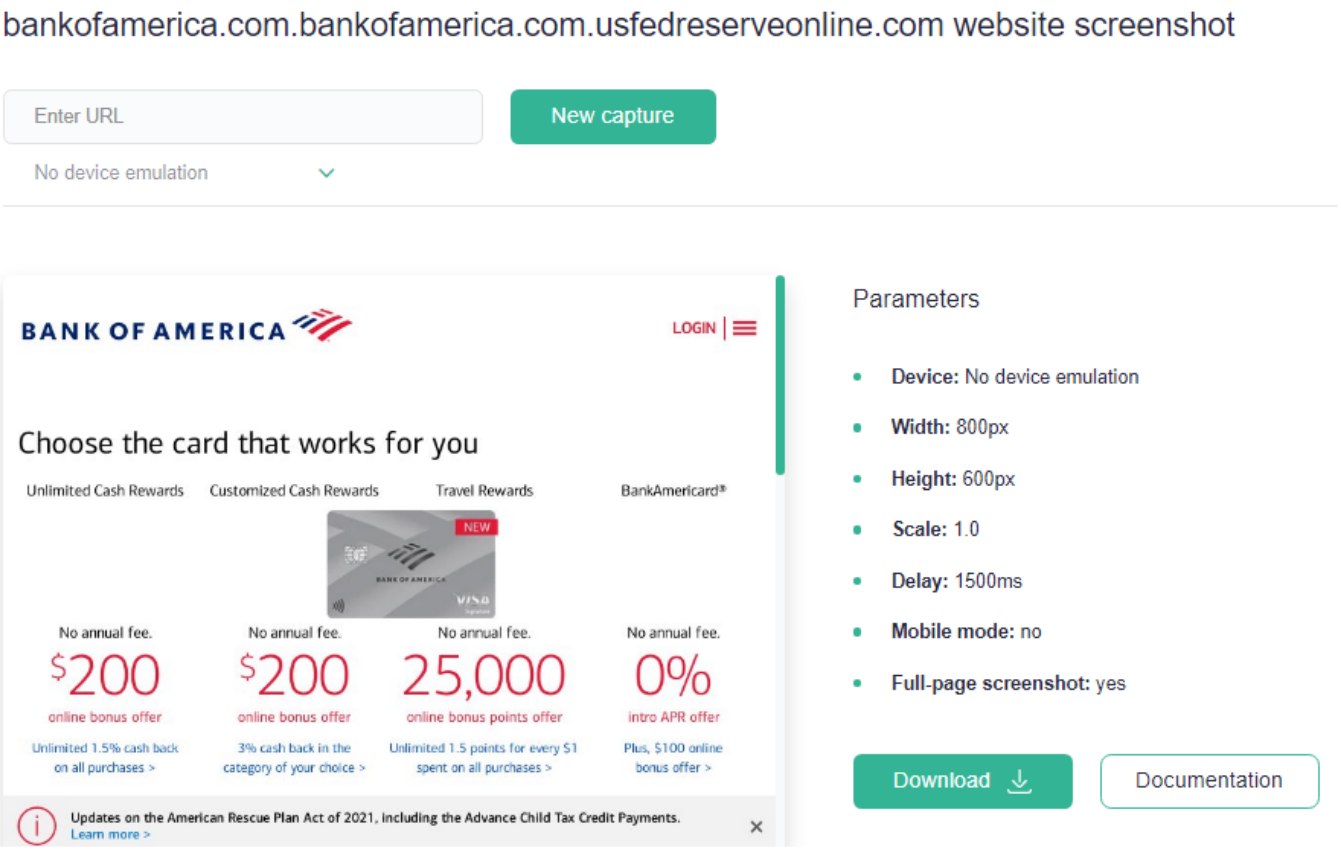


Remediation Prioritization

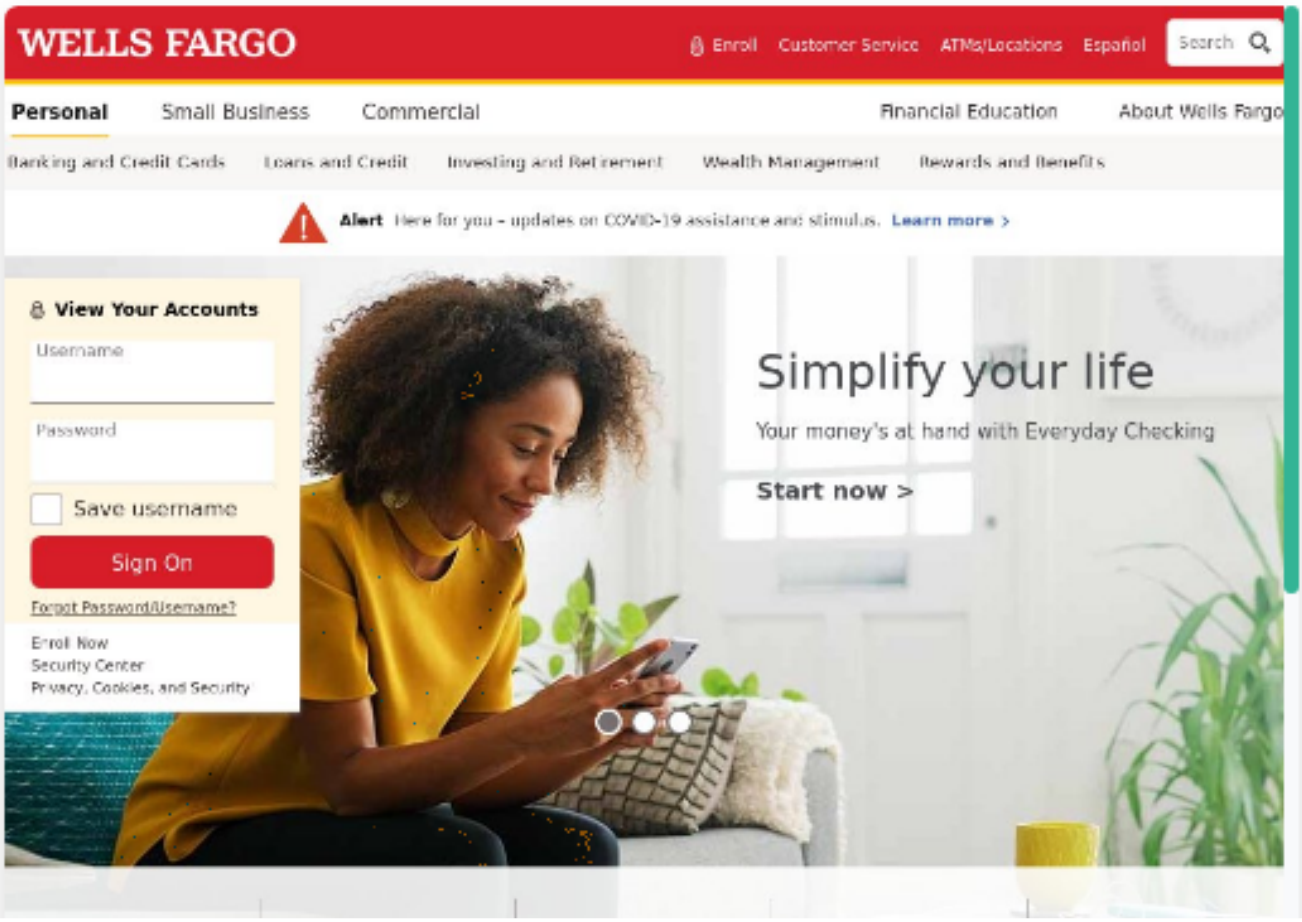
To efficiently manage one's attack surface, proper allocation of resources is crucial. Prioritize assets according to how critical their risks and vulnerabilities are. From a sample of the financial

sector's domain attack surface, for instance, 473 domains and subdomains have already been flagged as malicious.

Blocking and investigating these properties should be the top priority. The investigation includes finding out which malicious domains and subdomains still host live content. In the financial industry, that could mean pages that look like those that belong to the imitated organization, such as the content hosted by these malicious domains:

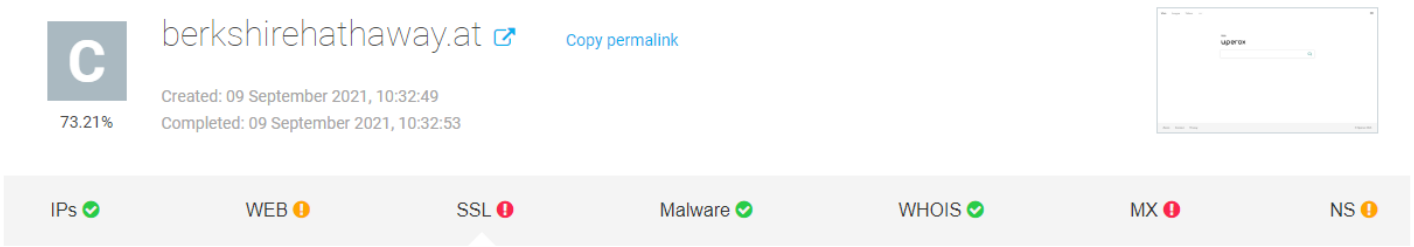


wellsfargolog.in website screenshot



These domains should take precedence over others, as they possibly posed an imminent threat (at the time of writing) to the spoofed companies' clients, employees, and other stakeholders.

Next to malicious properties, financial institutions may want to check domains with infrastructure misconfigurations. For example, we found a domain with multiple configuration issues.



These are some of the problems detected by the Threat Intelligence Platform (TIP):

- No SSL certificates
- Sender Policy Framework (SPF) is not configured
- Domain-Based Message Authentication, Reporting, and Conformance (DMARC) is not configured
- Mail server is blacklisted
- Does not follow the standard nameserver and Start of Authority (SOA) configurations

Properties on the attack surface that have similar issues may be accorded high priority as well.

Step #4: Continuous Monitoring

All discovered assets are then placed under monitoring. Changes to their availability, WHOIS records, and DNS resolutions are a few aspects to look out for. These assets can be placed under Domain Monitor to get notified of any modifications to their registration details.

Cybersquatting domains and subdomains that were inactive in the past may start resolving and hosting content, so monitoring them is crucial to effectively manage one's attack surface.

The monitoring stage also includes surveilling new assets that could be added to an organization's attack surface. At this point, financial companies circle back to the first stage of domain attack surface management.

To recap, the finance-related assets uncovered during the first phase of EASM were added between 13 May and 8 September 2021. Some of the properties have already been used in malicious campaigns. More might be added in the next few weeks, making early detection of possible attack vectors crucial.

Effective and efficient domain attack surface management may help reduce the number of successful security incidents against financial institutions.

Discovering, validating, prioritizing, and monitoring the external attack surface of the financial sector are key security processes. WhoisXML API's EASM Solutions, with its customizable components and massive volume of IP, DNS, and domain intelligence sources, is at the top of each phase.