RiskIQ for Financial Services

RiskIQ empowers financial services security teams to respond quickly to external threats targeted at their employees, customers, and brand. RiskIQ illuminates unknown digital attack vectors across web, social, and mobile channels that include phishing websites, shadow IT, rogue mobile apps, fake social media profiles, and domain infringement.

In Q1 2016, RiskIQ found evidence of 37 financial industry brands being targeted by a single threat actor.

FINANCIAL SERVICES ORGANIZATIONS USE RISKIQ TO REDUCE THEIR DIGITAL ATTACK SURFACE AND SOLVE PROBLEMS ASSOCIATED WITH:

COMPLIANCE WITH INDUSTRY REGULATIONS AND POLICY

NIST, NERC, FISMA, PCI, and Critical Security Controls

To comply with regulatory requirements, financial institutions must perform periodic risk assessments considering changes not only to their internal environment, but also external-facing digital infrastructure. RiskIQ uncovers unknown digital assets and adds them to the asset inventory of the organization and then continuously monitors the inventory for compromise, unsanctioned changes, and compliance. With a comprehensive list of external-facing digital assets, a bank's security team can ensure an up-to-date asset inventory, complete with ownership information and status, and provide required compliance documentation.

PHISHING

RiskIQ found and took down a domain hosting 240 different phishing sites targeting a single major bank

Financial services organizations are some of the hottest targets for phishing schemes since they're the closest to a threat actor's primary goal—money. RiskIQ scans the internet for evidence of phishing, looking for unofficial sites that use an organization's logo, branding, copied phrasing, and marketing language. RiskIQ virtual user technology experiences websites like a real user would, and can provide information about what would happen if a customer were to be tricked into visiting the site. RiskIQ can also open suspected phishing emails that are submitted by users and customers, follow the links, and analyze their impact.

RiskIQ automates the discovery and analysis processes around phishing investigations and allows security and incident response teams to mitigate its impact faster than ever before.

MOBILE APP SECURITY

RiskIQ eliminated 16 rogue mobile application threats for a major bank in Q1 2016

RiskIQ continuously scans hundreds of mobile app stores and millions of apps to safeguard brand reputation and customers by detecting malware, application tampering, and brand impersonation. For each financial organization, RiskIQ creates a complete inventory of mobile assets that are related to the bank, official and unknown, across the global mobile app ecosystem. This process includes monitoring for new apps, existing apps, app updates, and rogue or fraudulent apps.

By using RiskIQ, financial organizations can easily find, analyze, and mitigate threats to their mobile apps. The platform will find official, unofficial, and rogue apps across hundreds of mobile app stores and monitors them for malware or compromise. If unauthorized apps are found, RiskIQ expedites corrective action with each app store directly inside the platform.

SOCIAL

RiskIQ found multiple profiles impersonating a major financial services firm

Recently, threat actors impersonated a large bank's customer service Twitter account saying it was the secondary support profile setup to take on overflow from the primary one. Its tweets included a link for the user to click to "solve" their issue, which directed them to a phishing site masquerading as the official site.

With RiskIQ virtual user technology, organizations can find and shut down social impersonators like this by continuously discovering and monitoring social media profiles—both legitimate and fraudulent. They can then detect and eliminate social media-based threats against the organization, its employees, and its customers.

.com

DOMAIN INFRINGEMENT

RiskIQ discovered and took down multiple infringing domains being used in tech support scams and browser locker attacks on customers of a major bank

Threat actors can register domains using trusted financial services brand names to drive monetizable traffic to other sites, phish for login credentials or payment card data, and distribute malware. RiskIQ searches DNS zone files for both exact matches to branded terms and close spelling variants (typosquatting) within domain names not belonging to an organization.

In addition, RiskIQ virtual user technology automatically maps out an organization's websites and infrastructure and distinguishes legitimate sites from third-party registrations—even those falsely claiming brand association in their WHOIS data.

THREAT INVESTIGATION

More than 80% of attacks are related to external threats

In a matter of minutes, security analysts can use RiskIQ PassiveTotal to build additional context and indicators related to suspicious incidents and financial fraudsters. For example, looking at a fraudulent URL in PassiveTotal, an analyst can see several unique data points:

- A historical view of the IP resolution for this domain
- Correlated web and analytics trackers to a particular threat actor
- WHOIS registrant/registrar information related to the domain
- Tags associated to the indicator that show that the domain is in RiskIQ's blacklist and that it is active

Teams leveraging RiskIQ can consolidate tools and disparate data sets and easily identify threat actors' infrastructure. Once found, security teams can block and report the infrastructure, and set monitors to alert on changes to that infrastructure or the appearance of related new infrastructure.