SOLUTION BRIEF

BloxOne™ Threat Defense for Banking and Financial Services

The Banking and Financial Services Challenge

The banking and financial services industry has almost always been one of the top three targets for cybercriminals. In 2019 the financial services industry remained the most targeted sector in the United States and in many other countries around the world. It has been estimated that financial institutions may lose between $100 to $300 billion annually from cyberattack activity. Cybercriminals targeted financial institutions to breach and defraud a variety of financial systems to include those for card processing, interbank transfers, electronic banking systems, and automated teller machine (ATM) networks.

Financial services customer data is highly prized by cybercriminals and they remain relentless in their efforts to acquire it. Sensitive information can be used to breach other networks, create fake identities, and further compromise both enterprise and consumers.

Important Banking and Financial Services Use Cases

Banking Trojans

The acquisition of threat intelligence is quite important to banks as this can help you identify and protect against many of the trojans and malware that are targeted at banks and financial institutions. Our research recently covered banking trojans such as Ursnif that recently targeted Germany and Italy, the Dridex banking trojan, the Dreambot banking trojan which was quite active in eastern Europe, and the GootKit banking trojan. Ursnif gains initial entry into banks through malicious spam campaigns that use compressed Microsoft Word documents embedded with malicious macros which, in turn, deliver Ursnif malware. Dridex similarly uses malicious emails with Microsoft Office document attachments which in turn use macros with hardcoded URLs to download and execute Dridex payloads. Dreambot extends Ursnif's functionality with the ability to communicate over Tor to further obscure communication traffic. All of these target financial institutions and their customers to steal authentication information and steal funds.

Phishing Emails

Bank employees are often exposed to targeted attacks via phishing emails which offer malicious links with alternate routes to malware laden websites. Using threat intelligence on DNS can prevent users from being directed to those malicious websites if they click on those phishing links. In addition, employees can be restricted from going to certain categories of websites using content filtering at the DNS level.

DNS Tunneling

Of course, DNS tunneling allows attackers that have successfully compromised banks to gather data and then exfiltrate it within a string of DNS queries. This appears to follow the DNS standard and hence bypasses all of the bank's other DNS solutions. This attack vector can also be mitigated by the use of a foundational security solution.

DNS Based Attacks

In the finance industry, attacks which directly leverage the domain name system (DNS) remain prevalent as most institutions receive multiple DNS attacks over a typical year. DNS, of course, is the critical infrastructure for internet communications. DNS translates easy-to-understand domain names into the IP addresses that the internet requires for connection. DNS attacks and related deception come in many flavors. Domain Name System changer malware modifies the DNS settings of a system and allows cyber attackers to modify your router to misdirect your users to cyber attacker controlled websites. This attack is usually transparent to your users and seems to work as a standard DNS resolver. Even with the best cyber hygiene, such an attack can be impossible to detect without foundational security.

Rapid Threat Investigation and Triage

Last, and perhaps most important, is the need for security operations teams to quickly triage incidents when they do happen, so that they can contain the threat and remediate efficiently. This requires comprehensive visibility, threat and network context and an integrated security ecosystem, with well correlated data. This helps your security operations center team substantially reduce research and remediation times in the face of ongoing attacks.

One Bank's Success with Foundational Security

One major U.S. bank chose the BloxOne Threat Defense architecture to help protect both cloud-based and on-premise services and applications. This bank has moved aggressively to defend against the tide of rising cybersecurity threats that continue to impact the banking industry and chosen foundational security to help secure their enterprise and their workers. This bank has thousands of employees across multiple locations in the United States. Their enterprise utilizes resources resident both in the cloud and within the bank's on-premises operations.

Infoblox integrated with the bank's existing security architecture and helped prevent a broad range of threats to the bank's ongoing operations.

BloxOne Threat Defense enabled the bank to identify and prevent DNS-based attacks across all of their cloud-based and on-premise assets. The BloxOne Threat Defense hybrid architecture gave them one architecturally efficient, centralized point of control and high visibility to any traffic that seeks to resolve a domain name with DNS services. Now the blocking of known threats and traffic can be done earlier in the cycle at the DNS level. This off-loads a significant workload from the bank's NGFWs, Web Gateway, and IDS/TPS so that these tools can focus on what they are designed for and can allow Infoblox to handle the known threats at the earliest time of potential network compromise. This preserves the processing power and improves the ROI for the other security tools in the bank's environment.

Foundational security gave them the ability to reduce cyber incidents, minimize their risk further, and strengthen their compliance initiatives. The value and technical advantages of foundational security are well understood by the bank and considered to be important to their overall operations. Of critical importance, the bank also gains the benefits of stronger protection for the brand and reputation.

Protecting Banks and Financial Services Institutions with BloxOne Threat Defense

BloxOne Threat Defense protects enterprise users, devices and systems no matter where they are, strengthening and optimizing your security posture from the foundation up. Our hybrid architecture extends protection across your on-premises, remote locations, and teleworking environment. It detects and blocks phishing, exploits, ransomware, and other modern malware, and it prevents workers from accessing objectionable content restricted by policy. Unique patented technology prevents DNS-based data exfiltration, to keep protected data safe, monitors for advanced threats (including lookalike domains) and automates incident response so that your security ecosystem can remediate any incidents quickly.

Infoblox controls enforce your policies and protect all of the employees in a financial institution, both on-premise and remote. Using DNS as an essential control point ensures that every Internet request is inspected to determine if it is malicious, as identified by our integrated threat intelligence, analytics, and machine learning. DNS also gives you scalable web and content filtering and reduces your overall threat defense costs.

Other important BloxOne Threat Defense capabilities for banking and finance include protection against Lookalike Domains, Domain Generation Algorithms, Fast Flux, DNS Tunneling, Content Filtering, and DOH (DNS over HTTPS), and more.

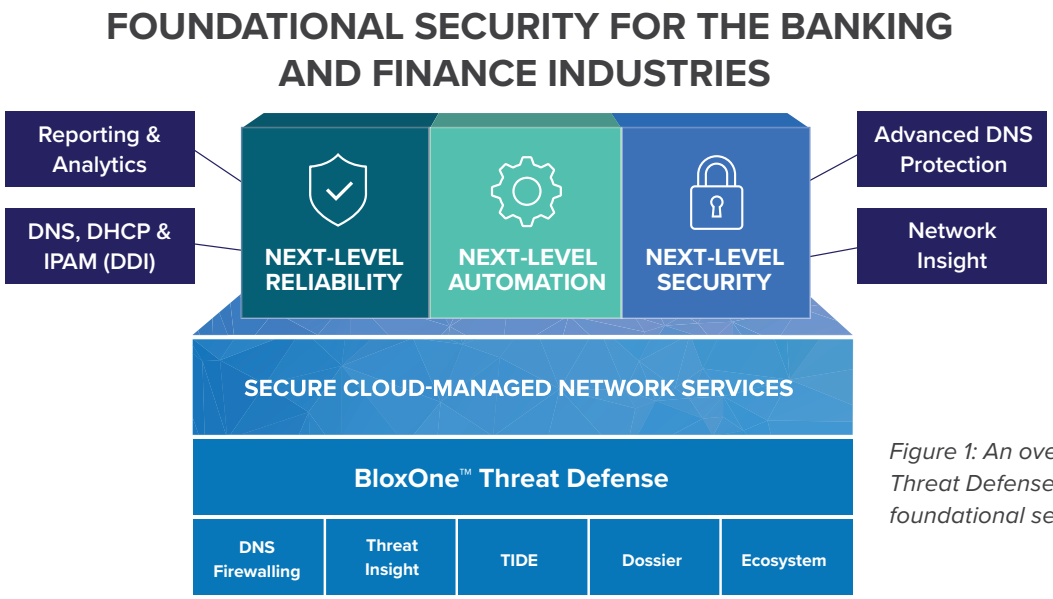

Figure 1: An overview of BloxOne Threat Defense and its key foundational security components

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com