SOLUTION NOTE

BLOXONE® THREAT DEFENSE FOR BANKING AND FINANCIAL SERVICES

Infoblox BloxOne Threat Defense proactively protects financial institutions by combining original DNS-based threat intelligence with DDI intelligence, blocking communication to adversary infrastructure used by malware, ransomware, phishing, lookalikes, and other forms of cyber attacks.

THE BANKING AND FINANCIAL SERVICES CHALLENGE

The banking and financial services industry has consistently been among the top three targets for cybercriminals. In 2022, more than 60 percent of global financial institutions with at least $5 billion in assets experienced cyberattacks[1]. During the same period, 64 percent of financial institutions reported an increase in attacks that exploited vulnerabilities in applications. These incidents included techniques aimed at destroying data held by the institution, which could support ransomware attacks or prevent access to forensic data after an attack. Furthermore, they observed a wide range of attacks, including banking trojans, phishing emails, waterhole attacks (embedding malicious code in a website or mobile app used by financial customers), ransomware, trojans, and more.

Cybercriminals focused their threats on financial institutions to breach and defraud various financial systems, such as those used for card processing, interbank transfers, electronic banking systems, and automated teller machine (ATM) networks. Financial services customer data is highly valuable to cybercriminals, who remain relentless in their efforts to obtain it. They can use this sensitive information to breach other networks, create fake identities, and further compromise both enterprises and consumers.

IMPORTANT BANKING AND FINANCIAL SERVICES USE CASES

Banking Trojans

The acquisition of threat intelligence is quite important to banks as it can help identify and protect against many of the trojans and malware targeting these financial institutions. Infoblox research has covered banking trojans such as Ursnif, observed targeting Germany and Italy; the Dridex banking trojan; the Dreamboat 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.

1 https://www.contrastsecurity.com/cyber-bank-heists-report

All of these target financial institutions and their customers to steal authentication information and funds. As online banking continues and new mobile services emerge, banking trojans that leverage false domains will continue to be a problem for the industry and their customers.

Phishing Emails

Bank employees often experience exposure 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 bypasses all of the bank's other DNS solutions. The use of a foundational security solution can also mitigate this attack vector.

DNS Based Attacks

In the finance industry, attacks that 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 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.

Suspicious Domains

Given the high risk associated with financial institutions, relying on existing tools alone to block known threats isn't enough. By being pre-emptive and protecting against suspicious domains (domains that haven't been confirmed as malicious but whose infrastructure and activity indicate malicious intent), banks can get ahead of attacks, blocking these domains long before they have an opportunity to activate within a network.

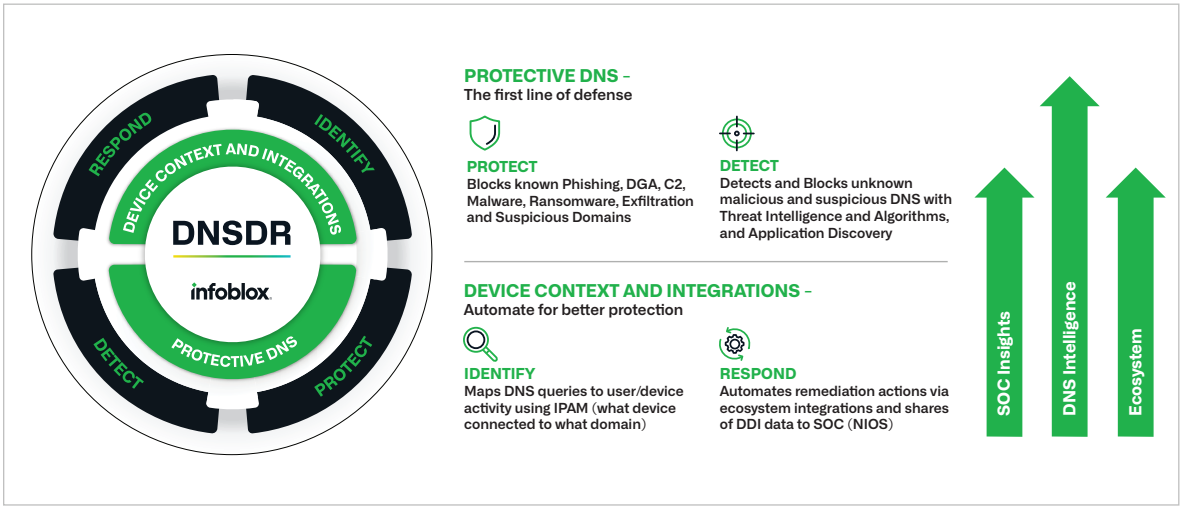
Lookalike Domains

Banking institutions are among the top targets of lookalike campaigns, including typo squats that deceive consumers into giving up their credit card or login information and multi-factor authentication (MFA) phishing attacks used to compromise banking employees. Aside from the obvious monetary implications, there is also a direct impact on the brand reputation of banks, so it's become imperative to take a more offensive approach to protecting against lookalike attacks.

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 it 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.

PROTECTING BANKS AND FINANCIAL SERVICES INSTITUTIONS WITH DNS DETECTION AND RESPONSE



Infoblox arms financial institutions with a DNS Detection and Response solution – BloxOne Threat Defense. It detects and blocks phishing, exploits, ransomware, and other modern malware, preventing workers from accessing objectionable content restricted by policy. Unique patented technology prevents DNS-based data exfiltration, keeps protected data safe, monitors for advanced threats (including lookalike domains), and automates incident response for quick remediation via ecosystem integrations.

BloxOne Threat Defense provides complete coverage, enforcing policies and protecting all employees, whether on-premises or 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 provides scalable web content filtering, helping to reduce overall threat defense costs. Other important BloxOne Threat Defense capabilities for banking and finance include protection against Lookalike Domains, Suspicious Domains, Domain Generation Algorithms, Fast Flux, DNS Tunneling, Content Filtering, and DOH (DNS over HTTPS), and more.

A LEADING ASIAN BANK IDENTIFIES AND REMEDIATES THREATS MORE EFFECTIVELY THROUGH EXTENSIVE AUTOMATION

BUSINESS CHALLENGE

- As with all financial institutions globally, this leading Asian Bank remains a popular target for malicious cyber attacks; its core challenge involved strengthening its security posture to counteract these emerging threats
- Prevent data infiltration and exfiltration techniques and detect and block exploits, phishing, ransomware and other modern malwares

Products:

- BloxOne® Threat Defense

SOLUTION

- Installed BloxOne® Threat Defense in the bank's data center over incumbent legacy security product from a leading router and switch vendor
- Adopted pervasive automation and ecosystem integration to drive efficiencies in SecOps

Industry: *Financial Services*
Location: *Asia Pacific*
Company info: *350+ branches*

"To me, no other solution vendor is providing the level of DNS security that Infoblox is with BloxOne® Threat Defense."

CISO,
A Leading Asian Pacific Bank

RESULTS

- Achieved access to real-time network and threat intelligence
- Secured IoT and other devices, apps, virtual machines and switch ports centrally and automatically
- Provided resiliency and redundancy

A MAJOR EUROPEAN BANK MODERNIZES NETWORK ARCHITECTURE AND ENHANCES CYBERSECURITY POSTURE

BUSINESS CHALLENGE

- The emergence of DNS as the key enabler of the digital business has led to this major bank ranking continuous uptime high among their list of priorities
- While the bank has been maintaining secure core DDI capabilities over the long term, it needed to simplify/centralize network management, enhance its cybersecurity posture, and begin migrating network operations to the cloud to guarantee availability of its online services to customers 24×7

Products:

- BloxOne® Threat Defense
- NIOS DDI

SOLUTION

- Modernized network architecture, rolling out Infoblox DDI worldwide
- Deployed BloxOne® Threat Defense—the on-premises version of the Infoblox cybersecurity solution—to harden core DDI operations in ways that boost network security comprehensively

RESULTS

- Modernized network infrastructure steadily
- Centralized network management
- Increased security threat response time by two-thirds faster at lower cost
- Increased visibility into network resources and operations

Industry:	*Financial Services*
Location:	*EMEA*
Company info:	*30,000+ employees globally*

"The online presence of <our bank> must always be available via the various channels, without ever faltering. Infoblox helped us address the challenge."

Senior Service Owner,
Network Security and Connectivity
A Major European Bank

A MAJOR SOUTH AMERICAN BANK SELECTS NIOS DDI AND BLOXONE THREAT DEFENSE TO CONTINUE ITS GROWTH AS A BANKING LEADER

BUSINESS CHALLENGE

- The growing number of financial projects posed significant challenges as their outdated technology hindered scalability, infrastructure management, and project activation
- Meeting regulatory demands and safeguarding against cyber threats

Products:

- NIOS DDI
- BloxOne® Threat Defense

SOLUTION

- NIOS DDI allowed this bank to centralize DNS, DHCP, and IPAM services, streamlining operations and automating infrastructure provisioning through a user-friendly portal
- BloxOne Threat Defense bolstered this bank's security posture and improved control and visibility over DNS and network records

RESULTS

- Improved quality and agility to deliver resources to the business
- Accelerated the delivery of products to members and end users
- Improved provisioning times: From 5 days to 15 minutes

Industry: *Banking*
Location: *South America*
Company info: *1,000+ branches*

"Infoblox accelerated delivery of our products to associates and end users. Provisioning a machine previously took five days,on average. Today, we can do it in 15 minutes. It is more flexible and agile."

Infrastructure Analyst
A Major South American Bank

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240216v1