Solution Brief

THE STAKES HAVE CHANGED: TIME FOR BANKS TO REASSESS THE RISKS

Weaponization of IoT Botnets Increase the Risk of DDoS Attacks to Your Business

Dark Side of Digital Transformation

The banking industry continues to automate processes, introduce digital products that improve the customer's experience and leverage new, fintech services in the value chain. But digital transformation has a dark side: increased vulnerability. A study by McKinsey suggests the increased operational risk of digital innovation threatens 6% of the net profit for a retail bank.[1]

As banks have invested in transaction migration and web and mobile technologies to attract digital customers, they have also expanded their potential attack surface. These vulnerabilities have not gone unnoticed by cyber adversaries. Witness interbanking compromises and theft (e.g., the SWIFT system), renowned hactivist group Anonymous' siege on the world's banking infrastructure known as Oplcarus and well publicized, successful Distributed Denial of Service (DDoS) attacks against banks such as Lloyds, Halifax Bank of Scotland and TSB Bank.

DDoS Attacks Have Changed: Has Your Protection?

Concurrent with the digital transformation of banking, DDoS attacks have also evolved. Reflection/amplification vectors and the weaponization of the Internet of Things (IoT) botnets — such as the Mirai botnet attacks — has changed the risk equation. The size of DDoS has increased dramatically, with some reaching 800Gbps. And though most attacks are less than 2Gbps (88%), this is still plenty large enough. A 2016 FS-ISAC Survey found most financial organizations have less than 1 Gbps of Internet bandwidth.

The vulnerability of any organization to the modern day DDoS attack was driven home by the recent Mirai botnet attacks against DNS service provider Dyn. The weaponization of IoT botnets, the potential size and greater sophistication, was known in the security community — but the collateral damage got the media's attention as the impact included well-known services such as PayPal, Twitter, GitHub, Amazon, Netflix, and Spotify. The uncomfortable truth: Interconnectedness, essential to operating today's banking organization, brings more risk.

The modern day DDoS attack is frequently a dynamic combination of volumetric, TCP state exhaustion and application layer attack vectors. In Arbor Networks' 12th annual *Worldwide Infrastructure Security Report* (WISR 2017), 67% of respondents have experienced a multi-vector DDoS attack. A 'low and slow' application layer

—

Industry

Financial Services: Banking

Challenges

- The digital transformation of banking, the interconnectedness of services, continues to increase vulnerability.
- IoT-based botnets are increasingly being used to launch large and complex DDoS attacks – and financial institutions such as banks are common targets.
- It's not just about stealing money. Highly valuable personal information, service availability and brand are also at risk.
- Misconceptions linger and current protections struggle with increasingly sophisticated attacks.

Solution

- Arbor's fully-managed, intelligently integrated in-cloud and on-premise DDoS protection solutions provide comprehensive protection from modern day DDoS attacks – so you can maintain service availability.
- Leverage Arbor's ATLAS Intelligence Feed to arm all Arbor solutions with global threat intelligence.

ARBOR® NETWORKS

The Security Division of NETSCOUT

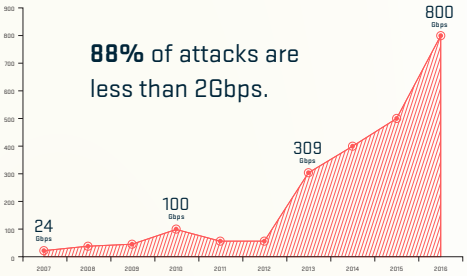

Figure 1 *Peak Attack Size*

—

Arbor Availability Protection System (APS)

- Provides always on, in-line protection from network and application layer DDoS attacks and advanced threats;
- Provides in-bound and out-bound threat identification and mitigation;
- APS mitigation platforms and capacities range from 2U appliances (1 Gbps-40 Gbps) to virtual machines (sub 1 Gbps).

Arbor Cloud DDoS Protection Service

- Arbor Cloud is a fully managed DDoS protection service providing up to multi-Tbps of global protection.
- Arbor Cloud Signaling™ provides instant, intelligent communication between on-premise Arbor APS and Arbor Cloud for comprehensive, layered, DDoS protection.

A recent Javelin Study found that account takeover incidence and losses rose notably in 2016. Total ATO losses reached $2.3 billion, a 61% increase from 2015, while incidence rose 31%.[3]

attack presents just as much risk as an 800Gbps volumetric attack.

And DDoS attacks are frequently used as cover for multi-part, long-running attack campaigns targeting personal information. A 2015 Kaspersky Labs study found 74% of advanced attacks used DDOS as a diversion.[2] To top it off, attacks have become easier to launch. And as usual, banks are in the cross-hairs. In Arbor Networks' 12th annual WISR, 41% of banks reported DDoS attacks.

Risky Thinking About DDoS Protection

The dramatic increase in the size, frequency and complexity of DDoS attacks, begs the question: When was the last time you reassessed your risk of a DDoS attack? Common misconceptions about what constitutes effective DDoS protection plague proper risk analysis. For example:

- Firewalls, load balancers, WAFs and IPS are not designed to protect against all DDoS attacks. These stateful devices are themselves vulnerable to TCP state exhaustion DDoS attacks — and routinely fail during attacks. According to Arbor's 12th annual WISR 53% of Enterprises reported their firewalls/IPS failing during a DDoS attack.
- Most on-premises protection can be easily saturated given DDoS attack techniques such as reflection/amplification or IoT botnets for hire. Even though 88% of attacks are less than 2Gbps, these can still overwhelm most banks' Internet circuits.
- ISPs are required to stop large volumetric DDoS attacks — but they struggle to detect smaller, application layer attacks. 74% of attacks last for less than 30 minutes. Automation is vital for effective on-premises protection.

Adversaries also continue to evolve, honing the tools of their trade. DDoS attacks have become ever more sophisticated, planned and coordinated — witness the rise in ransomware and DDoS extortion attempts. Dynamic, multi-vector attacks were effectively deployed against financial institutions in 2012 with Operation Ababil.

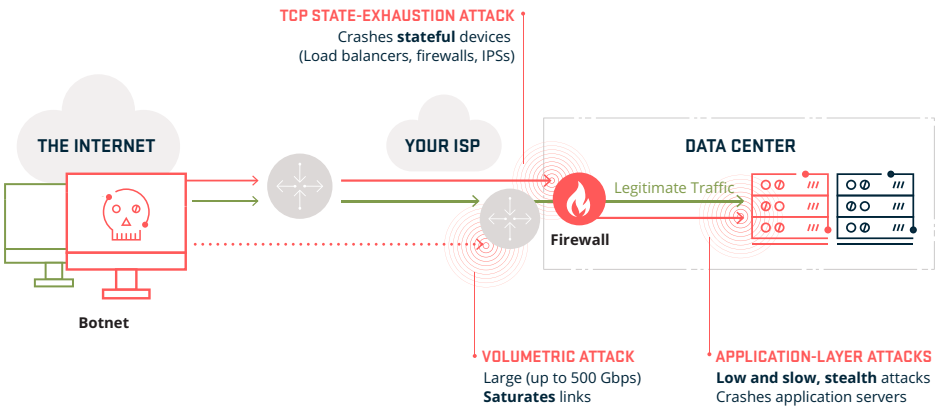

Figure 2 *The modern day DDoS attacks consists of a dynamic combination of 1) Volumetric 2) TCP-stat exhaustion and 3) Application-layer attack vectors.*

Today's IoT based botnets such as Mirai are capable of launching much larger and more complex multi-vector attacks.

To add fuel to the fire, the ease with which complex DDoS attacks and weaponized IoT botnets can be purchased, or services hired, puts serious attacks within easy reach of virtually any potential adversary. And when DDoS is increasingly used as a diversion when stealing money or valuable information, you have a recipe for disaster.

Now is the time for banking organizations to reassess their risk of DDoS attacks and re-evaluate their protection strategies.

Layered, Automated Protection with Continuous Threat Intelligence

To stop the modern day DDoS attack which utilizes a dynamic combination of volumetric, TCP state exhaustion and application layer attack vectors, industry best practices recommend a layered, automated protection strategy backed by continuous, timely threat intelligence.

Arbor's DDoS Protection solution offers a fully integrated combination of in-cloud and on-premise DDoS attack protection products and/or services:

1. Arbor APS or Flow Based Detection to stop in-bound network, application-layer and state exhaustion attacks on-premise, in front of firewalls and key communication gateways;
2. Cloud Signaling™ to intelligently link to in-cloud mitigation before on-premise protection and internet circuits are overwhelmed with large attacks;
3. Arbor Cloud and 24/7 SOC to mitigate volumetric attacks upstream before on-premises gateways and security systems are overwhelmed;
4. ATLAS Intelligence Feed to continuously feed all mitigation options to stay protected from the latest threats (e.g., Mirai botnet derivatives).

Unique Threat Intelligence

DDoS is frequently part of larger attack campaigns that include the planning of tactics, techniques and procedures (TTPs) long before a victim is even targeted. A campaign is an ongoing set of operations, much of it automated, against well-researched targets. And adversaries frequently circle back — particularly if they have been successful. The good news is that these techniques and tactics leave a trail.

For over 16 years Arbor Networks has had unique visibility into global threats. The ATLAS Intelligence Feed (AIF) is built on data from over 300 ISPs providing global threat intelligence. About one third of all Internet traffic flows thru ATLAS or an Arbor product. (A current representation of some of this data came be seen on the Digital Attack Map at **digitalattackmap.com**.) ASERT security experts augment this data with additional research and historical perspective, for example, the origins and trajectory of Mirai malware.

The AIF continuously arms all Arbor on-premise and cloud-based solutions with actionable threat intelligence. Timely AIF threat intelligence helps more rapid, automatic mitigation of DDoS attacks.

Following the online theft of £2.5m from 9,000 Tesco Bank accounts, Financial Conduct Authority (FCA) chief executive Andrew Bailey "told members of Parliament (MPs) that he is concerned about the cyber security of banks due to the complexity of their IT systems. The more complex banks' IT systems are, the more potential "points of entry" are available for criminals..."[4]

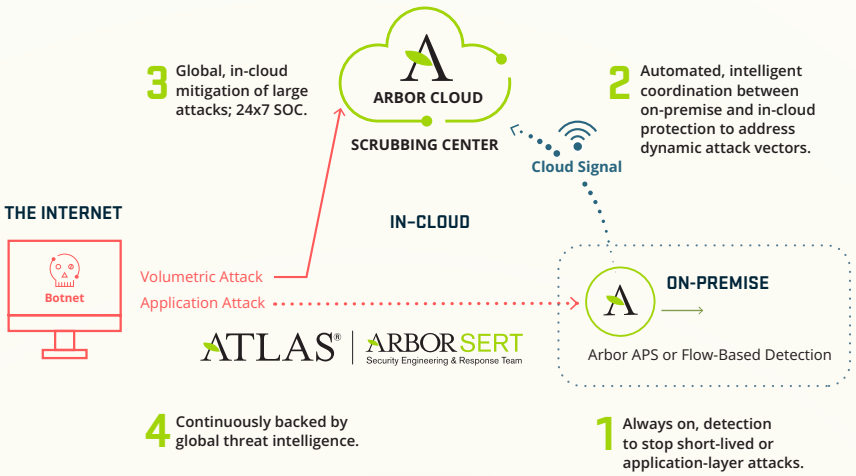

Figure 3 *Need Title Here*

Arbor ATLAS: Global Visibility and Threat Intelligence

Over the past 16 years more than 300 ISPs have participated in ATLAS, providing Global Visibility and Threat Intelligence to businesses worldwide.

Arbor's Security Engineering and Response Team (ASERT) leverages ATLAS to conduct threat research, help customers mitigate DDoS attacks and create ATLAS Intelligence Feeds (AIF). AIFs continuously arm all Arbor DDoS protection products and services.

Quantifying the Risk of Cyber Attacks

There are a number of risk frameworks, from NIST, ISO, CERT, ISACA, and others. While all recognize the business need to quantify risk, they for the most part leave quantification up to the organization. What is clear is a compliance based approach to enterprise security is not enough.

While certainly helpful in meeting compliance regulations these frameworks fall short in helping businesses to quantify risk. Most are silent on how to analyze and compute risks in a business sense: ergo, a cost benefit analysis.

The NIST 800-30 "Guide for Conducting Risk Assessments" relies on too much qualitative criteria and cannot help a business prioritize risks for their specific operations and business environment. You could 'meet' all the NIST guidelines and still be at significant risk from DDoS or other advanced attacks. The more recent Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) has been criticized as too black and white.

"The tool's yes-and-no question-and-answer format leaves no room for banks and credit unions to provide open-ended responses that could better explain their current levels of cybersecurity maturity" John Carlson, vice chairman of the Financial Services Sector Coordinating Council.[5]

One emerging risk assessment methodology is **Factor Analysis of Information Risk (FAIR)**. FAIR provides for the measurement, management and communication of information risk in terms of value to the business. FAIR can be leveraged on top of existing, compliance frameworks. A practical understanding and analysis of information risk in terms of dollars and cents can enable more well-informed business decision making.

No matter what framework or risk assessment methodology you use, accurate results depend on three things: 1) knowledge of the latest DDoS attacks trends (i.e. size, frequency and complexity); 2) best practices in DDoS defense (i.e., an intelligent combination of in-cloud and on-premise protection backed by continuous threat intelligence) and 3) understanding that not all assets are equal in value and will have a different risk profile.

Summary

Digital transformation and interconnectedness of services are critical for the business of banking; they also increase vulnerability. The risks and costs of a breach, service unavailability, incident recovery, ransomware and extortion are greater than ever. More sophisticated tools and techniques in the hands of determined attackers means now is the time to reevaluate the risks to your operations and assets.

Arbor's integrated in-cloud and on-premise solutions represent the industry's most comprehensive, effective DDoS protection. Easy to deploy, use and armed with campaign intelligence from ATLAS, Arbor's complete solution enables you to more efficiently protect your monetary and information assets — and better safeguard your bottom-line.

> "In 2013, cyber was the 15th top risk, with only 6% of responses naming it in their top three business risks. By 2014, it jumped to 8th place with 12%. In 2015, it was the most significant mover, climbing to 5th place with 17% of responses. Last year (2016), cyber emerged for the first time into the top three in 3rd position with 28% and although still in third place this year, the number of responses is up to 30%, only one point behind the number two risk, market developments."[6]

—

Additional Resources

Overview of Arbor DDoS Protection Solution

ATLAS Attack Map

[1] *Broeders, Henk and Somesh Khanna, "Strategic choices for banks in the digital age," McKinsey&Company, January 2015.*

[2] *"Denial of service: How businesses evaluate the threat of DDoS attacks," Kapersky Labs, 2015.*

[3] *Pascual, Al, Kyle Marchini, and Sarah Miller, "2017 identity fraud: Se-curing the connected life," Javelin, February 1, 2017.*

[4] *Ashford, Warwick, "Financial Conduct Authority concerned about cyber secu-rity of banks," Computer-Weekly.com November 9, 2016.*

[5] *Carlson, John, "FFIEC Cyber Tool Needs Urgent Revamp. FFIEC BankInfoSecurity, January 15, 2016.*

[6] *Pascual, Al, Kyle Marchini, and Sarah Miller, "2017 identity fraud: Securing the connected life," Javelin, February 1, 2017*

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

SB/STAKESHAVECHANGED/EN/0417-LETTER

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842