Solution Brief

ARBOR NETWORKS
The Security Division of NETSCOUT

DIGITAL TRANSFORMATION OF HEALTHCARE PRESENTS SECURITY CHALLENGES

Expanding and Increasing Reliance on IT Networks Presents Greater Risk

The Changing Stakes of Network Security

Increasingly interconnected digital technologies are continuing to transform healthcare. Trends such as interoperability, remote monitoring, distributed sites of care, mobility and cloud access, wearables and Internet of Things (IoT) enabled devic-es are all changing the way care is provided — and the underlying infrastructure. Along with the opportunities comes increased responsibility to protect the network. More endpoints and increasing connectivity also means more threat surfaces and greater risk of and impact from cyber-attack.

"For connected medical and IoT devices constantly exchanging data via a network connection, a DDoS attack will completely derail their operation. Cloud-based EHR and email systems are also rendered unusable, preventing clinicians from accessing with critical patient information and putting patients and their protected health in-formation (PHI) at risk."[1]

Cyber criminals are taking advantage:

- Ransomware used in concert with DDoS is nearly triple 2016's numbers: 14 percent of breached organizations experienced a combined attack.[2]
- U.K. government blames North Korea for WannaCry ransomware that crippled the National Health Service. U.K. Security Minister Ben Wallace told BBC radio: "North Korea was the state that we believe was involved in this world-wide attack on our systems. We can be as sure as possible."[3]
- "2016 was a record year for US Healthcare breaches — affecting hospitals, dental clinics, and senior care facilities, among others — with the top 10 breaches netting criminals in excess of 13 million records, and the Dark Web literally flooded with "fullz" (full packages of personally identifiable information) as well as patient insurance information."[4]

With more sophisticated malware running on large botnets, distributed denial of service (DDoS) attacks are at the forefront of these threats. DDoS is now a dynamic com-bination of different, simultaneous attack vectors used as part of a campaign to install ransomware or stealthy malware aimed at stealing valuable patient information and other data. Arbor Networks' 12th annual *Worldwide Infrastructure Security Report*, found 67% of respondents experienced a multi-vector DDoS attack, up from 56% the year before.

INDUSTRY

Healthcare

CHALLENGES

- As healthcare organizations pursue digital transformation they increase threat surfaces and network vulnerability.
- DDoS continues to evolve. IoT-based botnets can launch large and complex DDoS attacks – and healthcare organizations are tempting targets.
- The attackers' aims go beyond network availability to include ransomware, theft of valuable personal data and access to connected systems.
- Misconceptions linger and current protections struggle with increasingly sophisticated DDoS attacks.

SOLUTION

- Arbor's fully managed, intelligently automated, in-cloud and on-premises DDoS protec-tion 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.

[1] *hitinfrastructure.com/news/protecting-health-it-infrastructure-from-ddos-attacks*

[2] *www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode*

[3] *www.bloomberg.com/news/articles/2017-10-26/u-k-government-watchdog-slams-health-service-over-wannacry)*

[4] *https://www.csoonline.com/article/3189869/data-breach/healthcare-records-for-sale-on-dark-web.html*

The Weaponization of IoT for Modern-Day DDoS Attack

Sophisticated malware and the exploitation of the Internet of Things (IoT) botnets has re-sulted in the virtual weaponization of these devices for DDoS attacks. In 2016 LizardStressor malware running on an IoT botnet of 10,000 IoT devices (primarily webcams), generated sustained attacks of over 540 Gbps. The Mirai botnet, designed specifically to infect IoT devices, and released 'into the wild' last year, is estimated to have compromised more than half a million IoT devices worldwide and generated attacks in excess of 620 Gbps. But run-of-the-mill volumetric attacks are not the only threats from the new breed of botnets. Both of these botnets can launch the equivalent of the modern-day DDoS attack.

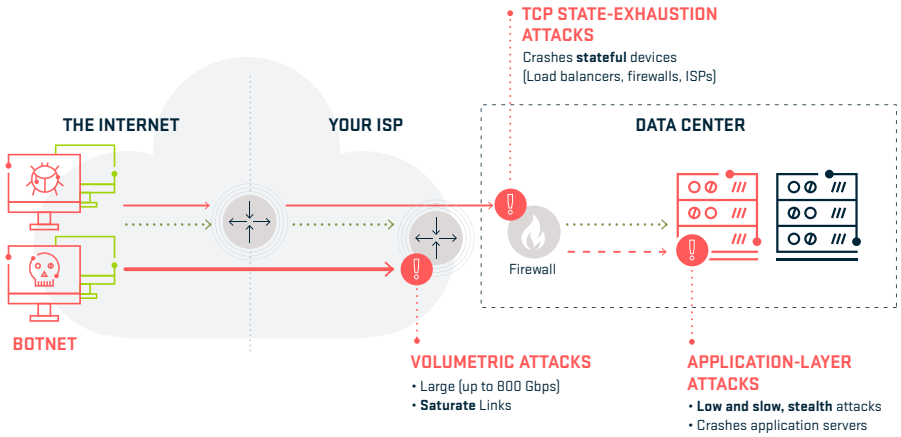

Figure 1 *The modern-day DDoS attack*

The modern-day DDoS attack is frequently a dynamic combination of volumetric, TCP state exhaustion and application layer attack vectors. Volumetric attacks are designed to saturate internet facing circuits. TCP-State exhaustion attacks can target the very defenses, firewalls and IPS, intended to protect against cyber-attack.

Application layer attacks target business critical services running application such as HTTP/HTTPs. According to Arbor Networks' 12th annual WISR, 25% or respondents suffered attacks targeting the application layer. A 'low and slow' application layer attack presents just as much risk as an 800Gbps volumetric attack. To be effective a DDoS attack only has to saturate the bandwidth of your internet connection. Arbor Networks' 12th annual WISR, found 67% of respondents have experienced a multi-vector DDoS attack, up from 56% the year before.

Making matters worse, sophisticated DDoS botnets now conduct massive phishing operations, deliver ransomware, or help gain entry to other, connected systems. They can be used as cover for multi-part, long-running attack campaigns targeting valuable patient or financial information.

Risky Thinking About DDoS Protection

When was the last time you reassessed your risk of a DDoS attack? Common misconceptions about 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 43% 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. Traffic in the in-famous DDoS attack on Children's Hospital in Boston hit 27 Gbps — 40 times typical traffic volumes. Even though 88% of attacks are less than 2 Gbps, these can still overwhelm the Internet circuits of most healthcare organizations.[5]

13%

increase in denial-of-service attacks on the healthcare industry this past year.

WWW.HEALTHCAREITNEWS.COM/NEWS/DENIAL-SERVICE-ATTACKS-HEALTHCARE-POISED-EXPLODE

THE 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)

THE 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

ATLAS Intelligence Feed (AIF) continuously arms all Arbor solutions with timely, actionable, threat campaign intelligence

[5] *www.cio.com/article/2682872/healthcare/how-boston-childrens-hospital-hit-back-at-anonymous.html*

- 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.

DDoS attacks have become more sophisticated, planned and coordinated — witness the rise in ransomware and DDoS extortion attempts. Today's IoT based botnets such as Mirai can be used to launch DDoS attacks to coverup multi-part, long-running attack campaigns targeting PII (Personally Identifiable Information) and PHI (Protected Health Information). And when multi-vector DDoS is used as a diversion for stealing valuable healthcare information, you have a recipe for disaster.

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

Protecting Your Patients and Organization Requires Intelligently Automated, Layered Protection

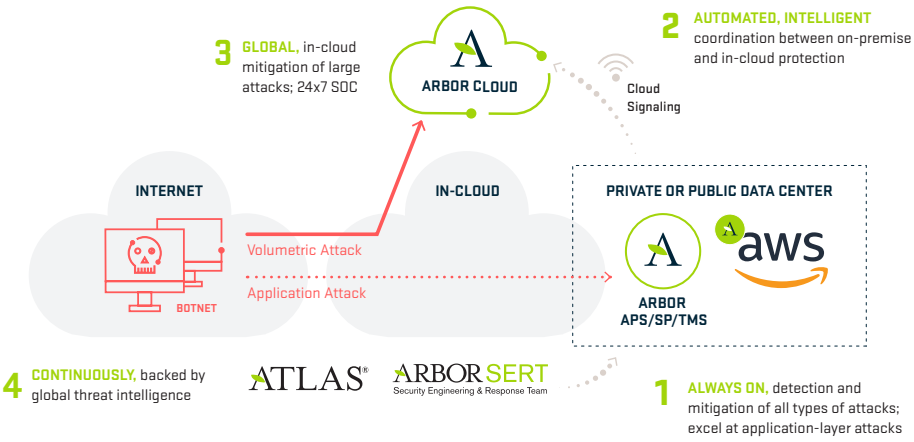

Figure 2 *Unified, intelligently, automated DDoS protection products and services: armed with global visibility and actionable threat intelligence*

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

Arbor APS

to stop In-line, always-on, installed in private or hosted data centers (e.g. Amazon Web Services), in front of firewalls and key communication gateways; can automatically stop in-bound network, application-layer and TCP-state exhaustion attacks.

Cloud Signaling™

to automatically and intelligently link to Arbor Cloud, in-cloud mitigation before on-premise protection and internet circuits are overwhelmed by large attacks.

Arbor Cloud

24/7 SOC to automatically mitigate volumetric attacks upstream before on-premises gateways and security systems are overwhelmed.

ATLAS Intelligence Feed

to continuously feed all mitigation options to stay protected from the latest threats (e.g., Mirai botnet derivatives).

HACKERS HIT

320%

more healthcare providers in 2016 than in 2015, per Department of Health and Human Services data.

WWW.HEALTHCAREITNEWS.COM/NEWS/DENIAL-SERVICE-ATTACKS-HEALTHCARE-POISED-EXPLODE

ARBOR ATLAS: GLOBAL VISIBILITY AND THREAT INTELLIGENCE

Over the past 16 years more than 400 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.

Intelligent Automation is the key to effective protection.

A DDoS campaign is an on-going set of threat tactics, techniques and procedures (TTPs), much of it automated – like botnets, against well-researched targets. Automation effects speed of mitigation, the efficient use of scarce resources, both investments in technology and talent, and the capacity to stay up-to-date on the latest DDoS TTPs.

Unique, Automated Global Threat Intelligence

For over 16 years Arbor Networks has had unique visibility into global threats. The ATLAS Intelligence Feed (AIF) is built on data from over 400 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. ASERT security experts augment this data with additional research and historical perspective, for example, the origins and trajectory of Mirai botnet malware to determine the 'reputation' of IPs and DNS.

The American Hospital Association has observed that healthcare cybersecurity measures must be flexible and resilient enough to address threats that are likely to be constantly evolving and multi-pronged. The AIF continuously arms all Arbor on-premise and cloud-based solutions with actionable threat intelligence. Timely AIF threat intelligence aids more rapid, automatic mitigation of DDoS attacks.[6]

New Methods of Quantifying Risk

There are a number of risk frameworks, from NIST, ISO, CERT, ISACA, and others. While all recognize the business need to assess risk, they for the most part leave quantification up to the organization. What is clear is a compliance based approach to security is not enough. For example, you could "meet" all the NIST guidelines and still be at signifi-cant risk from DDoS or other advanced attacks.

One emerging risk analysis methodology is Factor Analysis of Information Risk (FAIR). FAIR provides for the quantitative measurement, management and communication of information risk in terms of the value to the business. A practical understanding and analysis of information risk in terms of dollars and cents can enable more well-informed business decision making. To see an example of how to conduct a FAIR-based risk analysis of DDoS attack and how different Arbor solutions can reduce the risk refer to the "Additional Resources" in the side bar.

Quantifying the Risk of Cyber Attacks

There are a number of risk Common Security Frameworks (CSF), from NIST, HITRUST, CERT, ISACA, and others. While certainly helpful in meeting compliance regulations these frameworks fall short in helping organizations to quantify risk 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 HITRUST CSF was developed in collaboration with healthcare and information security professionals but it too focuses on providing a comprehensive set of baseline security controls — not quantifying risk.

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. (See example Cost-Benefit Analysis of Connecting Home Dialysis Machines Online to Hospitals in Norway.) 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 TTPs); 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 val-ue and will have a different risk profile.

Anthem and certain Blue Cross and Blue Shield companies who had members with data stored on Anthem's databases agreed to pay $115 million to settle a class action lawsuit stemming from a data breach announced by Anthem in February 2015.

WWW.TOPCLASSACTIONS.COM/LAWSUIT-SETTLEMENTS/LAWSUIT-NEWS/822522-ANTHEM-DATA-BREACH-CLASS-ACTION-SETTLEMENT/

[6] *www.beckershospitalreview.com/healthcare-information-technology/top-five-healthcare-it-trends-for-2017.html*

Summary

Healthcare organizations are leveraging digital transformation to improve services and become more efficient. Increasing interoperability and supporting innovations such as telemedicine, mobility and cloud access, wearables and IoT devices is placing an ever greater burden on network security teams. The risks and costs of a breach including potential regulatory penalties, service unavailability, incident recovery, ransomware and extortion are greater than ever. Now is the time to re-evaluate the risks to your operations and assets.

Arbor's integrated in-cloud and on-premise solutions represent the industry's most comprehensive, up-to-date DDoS protection. Easy to deploy and constantly armed with up-to-date threat intelligence from ATLAS, Arbor's complete solution enables you to more efficiently protect critical assets, from electronic health records to the growing array of software-based medical equipment and wearables.

ADDITIONAL RESOURCES

Overview of Arbor DDoS Protection Solution

ATLAS Attack Map

FAIR White Paper

Arbor 2016 Report: Mirai Botnet

ARBOR NETWORKS

The Security Division of NETSCOUT

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

North America 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

www.arbornetworks.com

SB/HEALTHCARE/EN/0318-LETTER