Tuesday, May 13, 2014
1:00-2:00 EDT

Is Your Credit Union Prepared for a DDoS Attack?

AffirmX

neustar

RISK WATCH WEBINAR

INTRODUCTION

Dennis Dollar
Principal Partner
Dollar & Associates
Former NCUA Chair

RISK WATCH WEBINAR

PANELISTS

Jane Pannier
Senior Vice President, In-House Counsel
AffirmX

Susan Warner
Market Manager, Security Solutions
Neustar

Jesse Boyer
Vice President, Product Development
AffirmX

The Problem of DDoS

Susan Warner,
Market Management,
Security Solutions, Neustar, Inc.

AffirmX

Is Your Credit Union Prepared for a DDoS Attack?

neustar®

A Dangerous World

AffirmX

neustar®

What is Denial of Service?

- When a server is overloaded with connections, new connections can no longer be accepted.
- Occurs systems flood the bandwidth or resources of a targeted system, usually one or more web servers.
- Distributed Denial of Service (DDoS) occurs when multiple compromised systems (for example a botnet) flooding the targeted system(s) with traffic

"DDoS is like 15 large men trying to fit through a revolving door all at once - nothing moves."

Graham Cluely,
UK Security Expert,
Writer, Speaker


LET'S TAKE
THIS INSIDE
VAPESTICK

Partial DDoS Timeline

Patelco Confirms Five-Hour DDoS Takedown

Texas Credit Union Hit by DDoS Attackers

Largest Ever DDoS Cyber Attack Hits US and European Victims

Mega DDoS Attacks of 800Gbps Expected Within a Year

DDoS Update: Credit Unions in the Crosshairs

Iranian Hacker group claims credit for DDoS Attack on Nasdaq

AffirmX

neustar

Why the Revival?

If You Build It, They Will Come

- Ecommerce/online stores
- Customer support/ service
- Digital marketing
- Partner/Vendor Mgt
- Remote workforce and internal communications

Our customers' demands for a superior online experience makes us vulnerable

AffirmX

neustar®

Anyone Can DDoS

- $5 - $50 per hour depending on site size
- Days, Weeks or Months!
- Years of DDoS Attack experience
- Training in DDoS protection methods!

All companies are vulnerable – not just large, high-profile or risk industries.

AffirmX

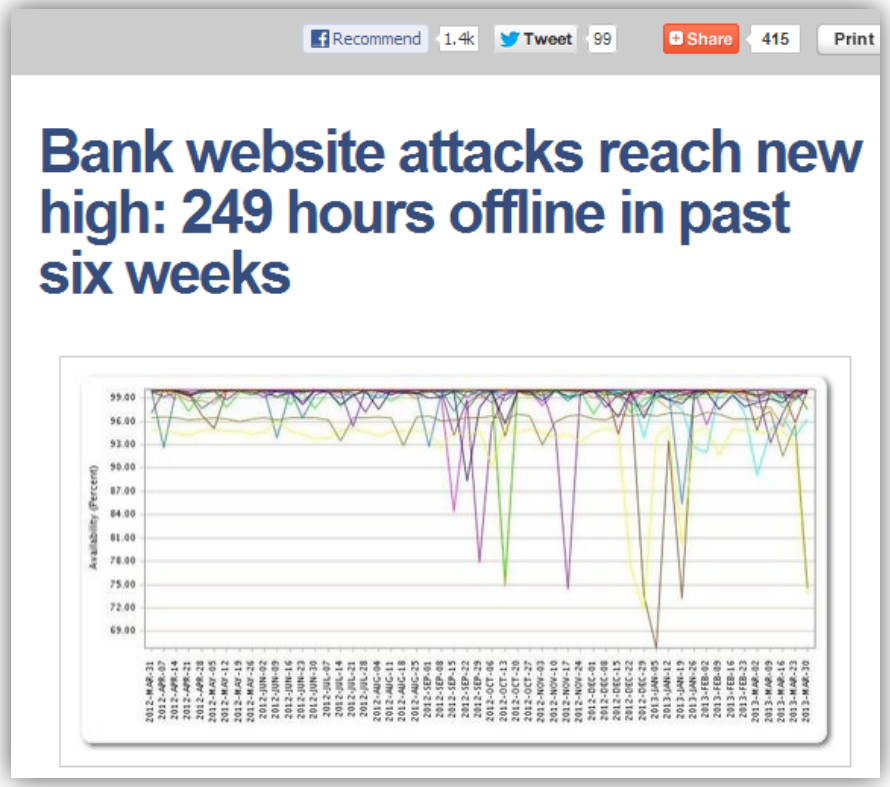
neustar®

The Reality of DDoS Attacks

- **More than 3,000 attacks happen every day**
- ✓ Attacks are increasingly more complex and harder to mitigate
- ✓ The attacks by Al Quassam were 1/3 the size of what they could have been
  - ✓ Attacks came in at 230 Gbps
  - ✓ Botnet was sized at being able to generate potentially 600+Gbps

AffirmX

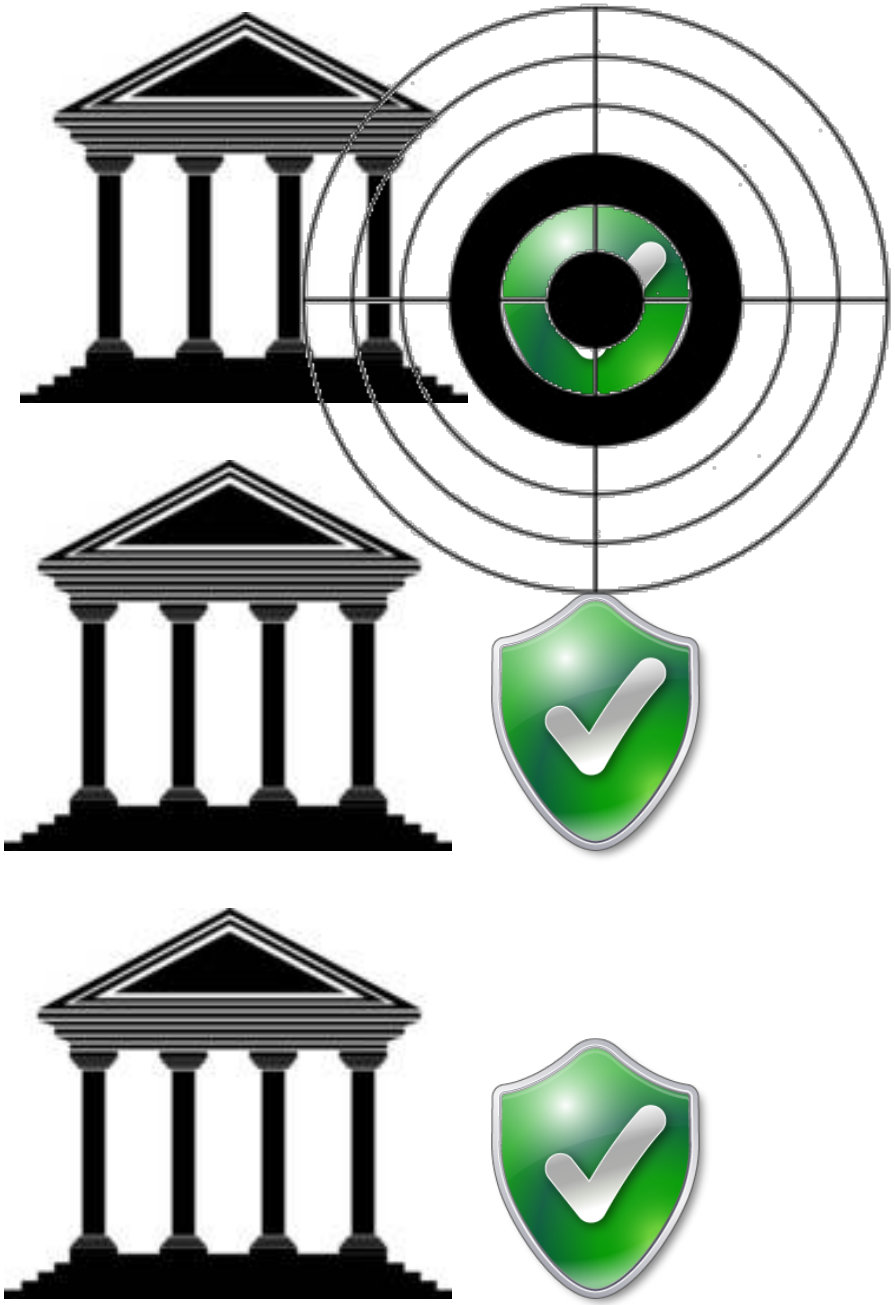
neustar



In early 2013 U.S. banks knocked offline a total of 249 hours.

If DDoS cost banks an average of $50K per hour

$12,450,000 was lost from January - March



AffirmX

neustar

2014 THE DANGER DEEPENS

Neustar Annual DDoS Attacks and Impact Report

Surveyed 450
IT, Networking,
& Security
Professionals
across all industries

AffirmX

neustar

75 Financial IT, Networking, & Security Professionals

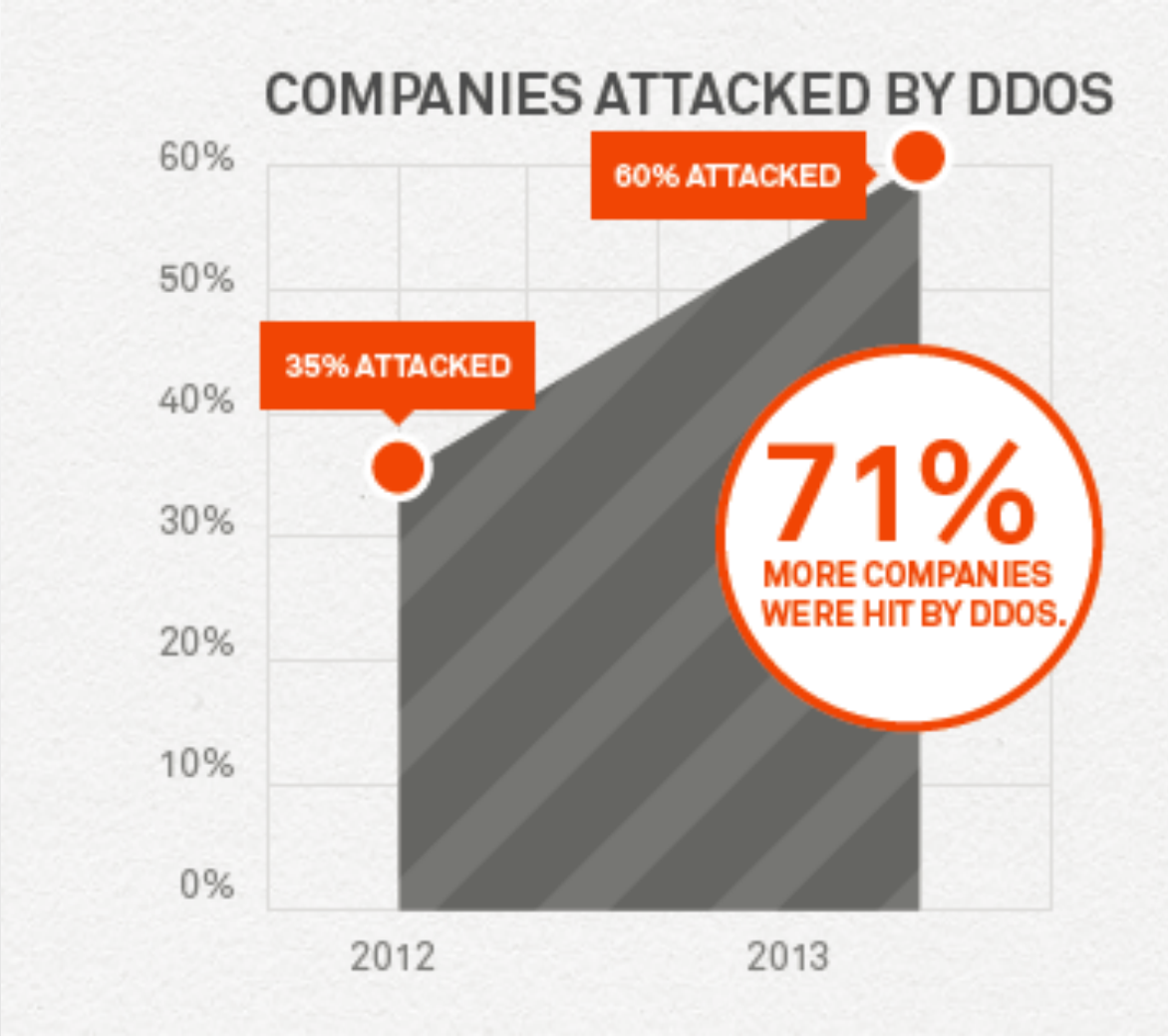
AffirmX

neustar

What's the temperature?

93% of Financial Organizations
say DDoS is as great or a larger threat than last year

Have you been attacked?



How many times were you attacked?

How many attacks?	
Just once- 13%	Monthly- 10%
2-5 times- 34%	Weekly- 14%
6-10 times- 12%	Lost count -18%

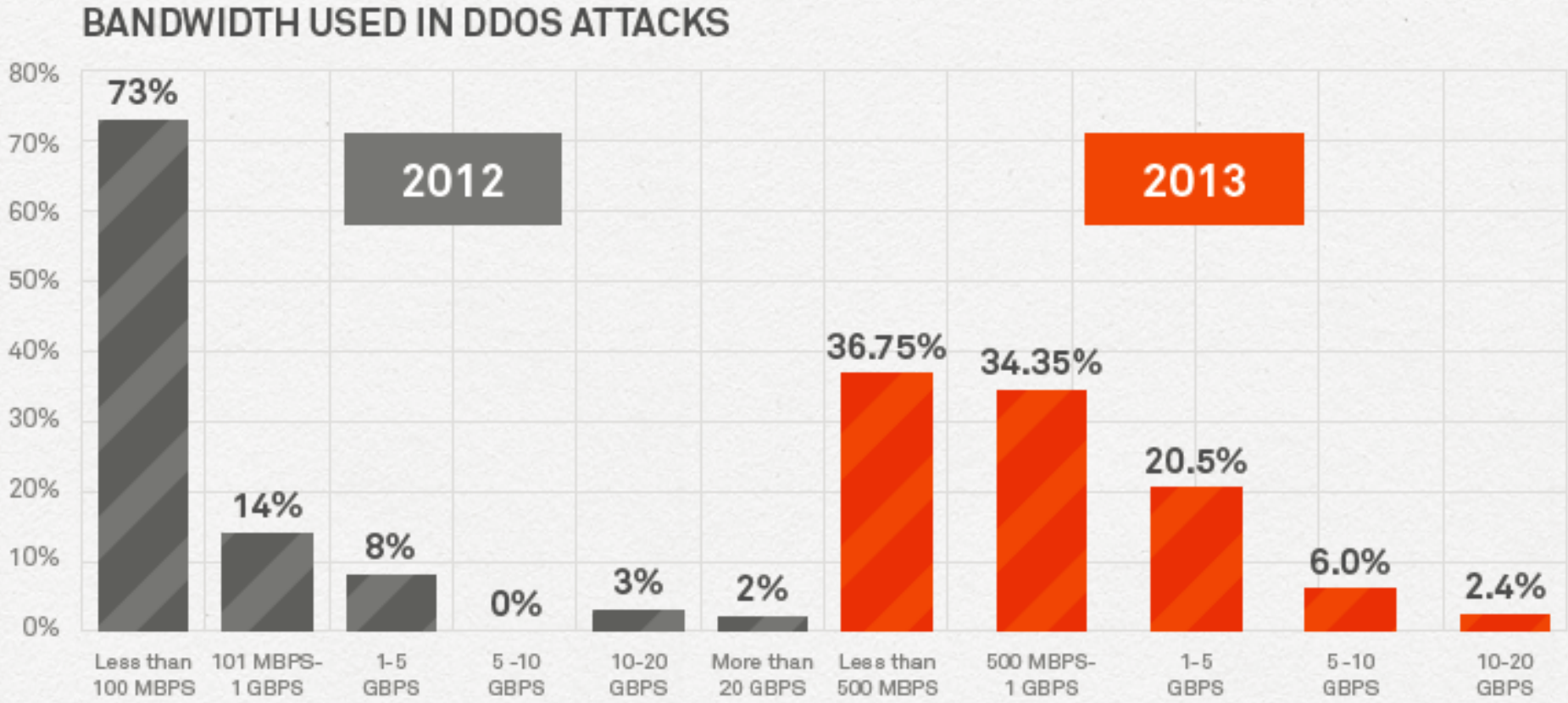
87%

Attacked Multiple Times

AffirmX

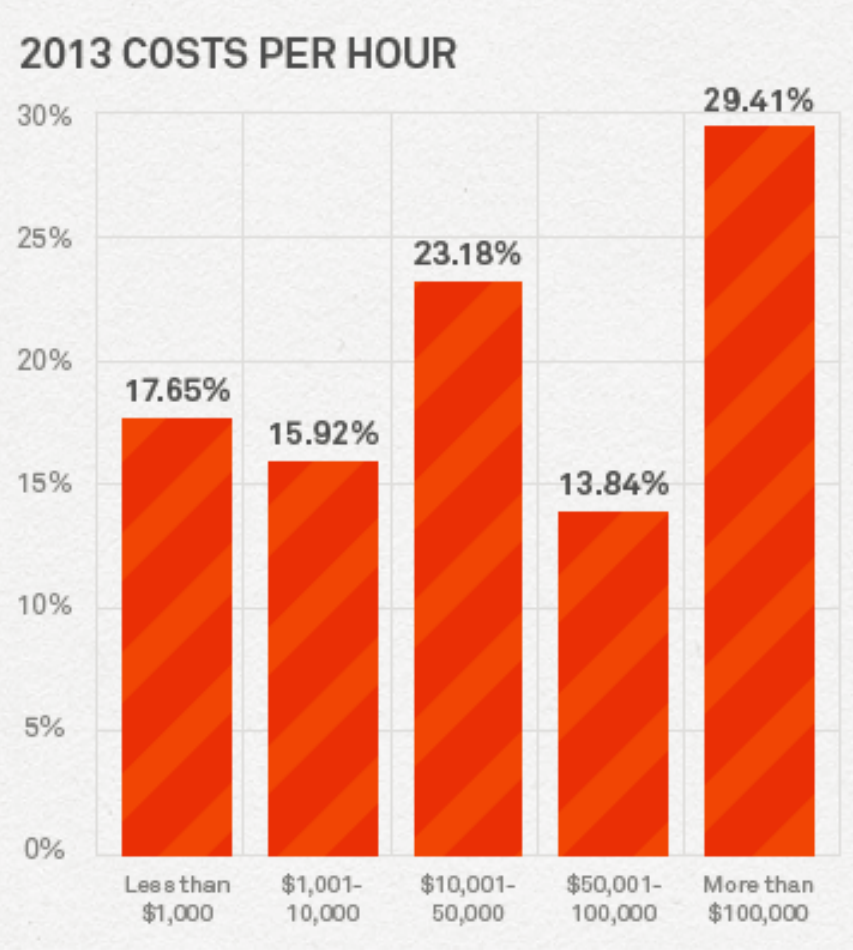
neustar

How large were the attacks?

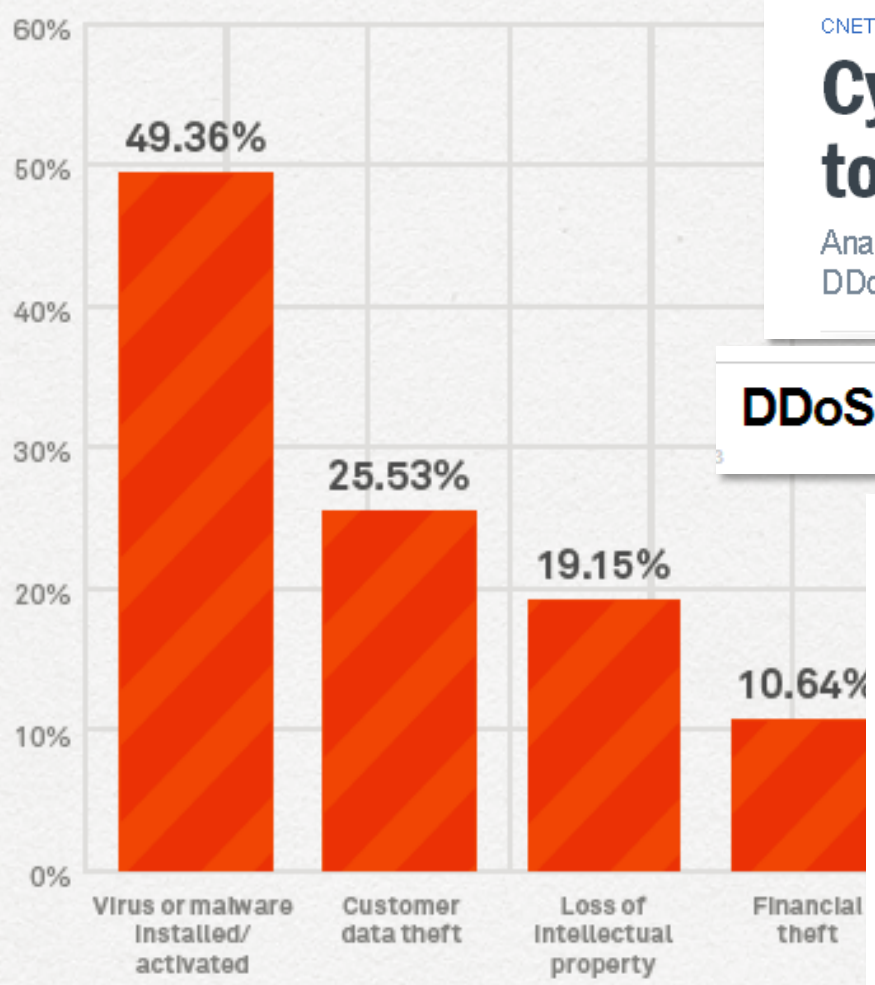


Impacts

How much does downtime cost financial?



When DDoSed and breached?



CNET › News › Security & Privacy › Cybercrooks use DDoS attacks to mask theft of ...

Cybercrooks use DDoS attacks to mask theft of banks' millions

Analyst says three unidentified US banks have been hit with "low powered" DDoS attacks to cover fraudulent wire transfers.

DDoS Attack on Bank Hid $900,000 Cyberheist

News

Deep cyberattacks cause millions in losses for U.S. banks

Hackers used DDoS attacks prior to attacking wire payment applications

By Jeremy Kirk

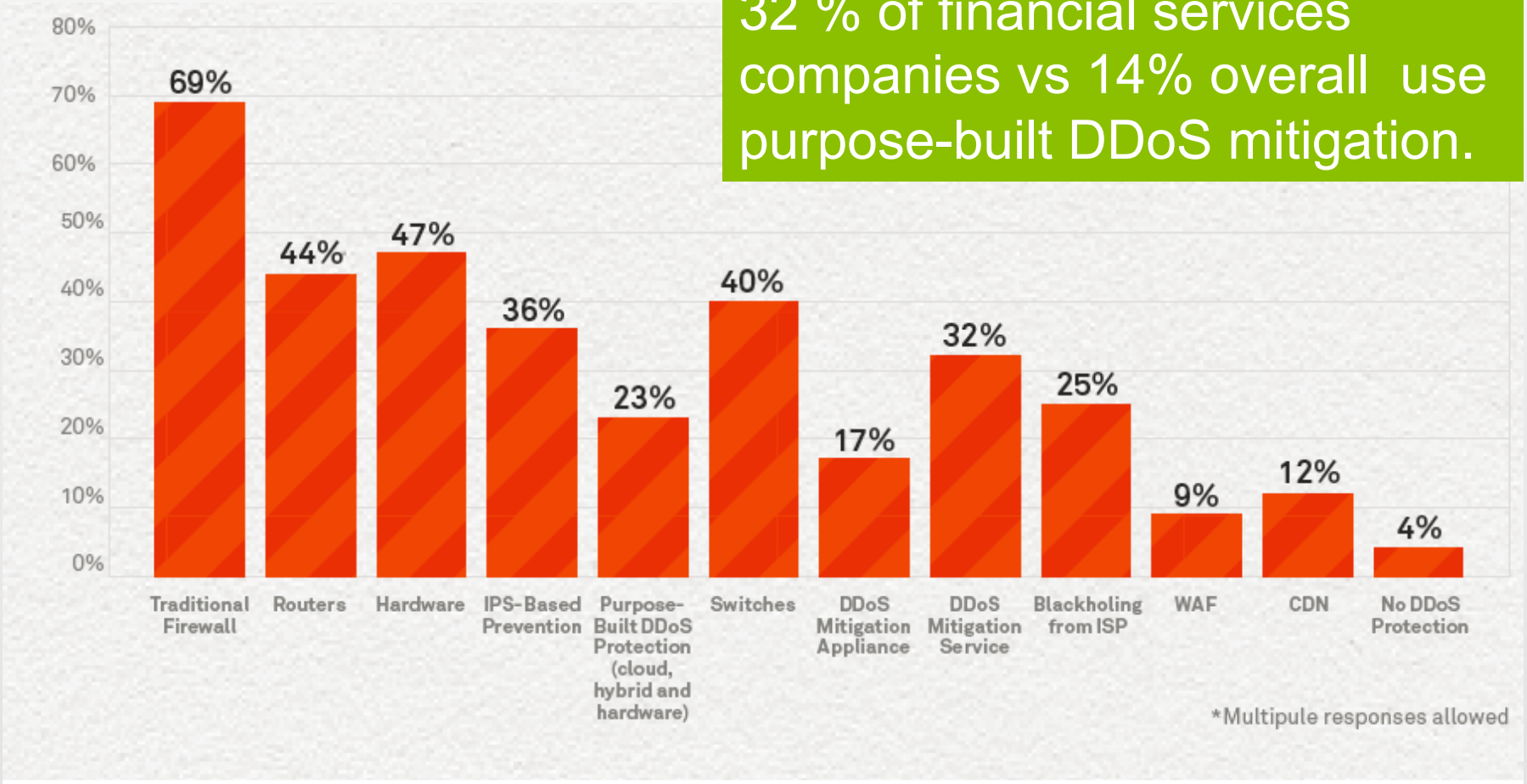
August 22, 2013 11:20 PM ET 3 Comments

Share 31 g+1 Like 37 More

IDG News Service - At least three U.S. banks have lost millions of dollars after fraudsters gained control of payment applications that control wire transfers.

DDoS protection solutions?

32 % of financial services companies vs 14% overall use purpose-built DDoS mitigation.



Key Takeaways

- DDoS continues to be a threat for all industries but especially for banks and credit unions
- DDoS is often used as a distraction or smokescreen for other malicious activity
- As organizations add protection, attackers adjust their targets downstream until they find vulnerabilities


2014 Neustar Annual DDoS Attacks and Impact Report | Financial Services Brief

THE BIGGEST TAKEAWAY: Financial institutions are now far more likely to have DDoS-specific protection than companies in other industries.

2014 Neustar Annual DDoS Attacks and Impact Report: A Neustar Financial Services Brief

Financial services companies risk higher revenue losses and lead the way in implementing DDoS-specific protection solutions.

These are the findings of a Neustar survey of nearly 450 companies in North America, across numerous industries: financial services, technology, retail, government/ public sector, health care, energy/utility, telecommunications, e-commerce, Internet services and media.

Financial services leads in adopting DDoS protection

The wave of attacks initiated by Al Quassam against US financial institutions from late 2012 through 2013 was like nothing the IT and Security industry had seen before. Large, debilitating DNS reflection attacks brought banks to a standstill—impacting their revenues and customer confidence.

Moreover, criminals are increasingly using DDoS as a diversionary tactic or "smokescreen" to access more valuable assets like intellectual property and funds. In fact, one bank suffered a $9 million cyberheist in which the attackers used DDoS to distract the security teams.

In April 2014, the FDIC issued a letter with the expectation that all FDIC-supervised banks have plans and take specific steps to mitigate the risks associated with DDoS attacks: "DDoS attacks may be a diversionary tactic by criminals attempting to commit fraud."

The industry has fought back and is now showing other sectors how forward-thinking solutions can help. This is one key finding in Neustar's 2014 DDoS Attacks and Impact Survey. Over 440 North American companies, including 75 financial institutions, shared their DDoS experiences of 2013, which the survey report compares to 2012 findings.

- Download the full report and financial briefing at www.neustar.biz

AffirmX

neustar

IT Operational Preparedness:

A 7 Point Approach

Jesse Boyer,
Vice President, Product Development
AffirmX

AffirmX

neustar

7 Point Approach to Preparedness

1. **Conduct a company-wide DDoS risk assessment:**
   - The first step in a good defense is to conduct an enterprise risk assessment. This allows you to assess the probability of a DDoS attack and identify your most likely targets.
   - It also helps determine the impact of an attack and estimate the potential loss to your organization (downtime, e-commerce impact, connectivity, communications and other factors.)
   - You can also better ensure that you invest in the right IT security and risk-reduction activities.

7 Point Approach to Preparedness

2. Create an action plan to prepare for and respond to DDoS attacks:

- Once an attack occurs, it is too late to determine how to respond and what the next steps should be.
- An action plan documents how to prepare for an attack and what to do when one occurs.
- Your plan should include different severity levels and responder actions, depending on the attack's impact.
- For example, you will respond differently to an attack that takes down the entire company, as opposed to a strike affecting only one web server.

7 Point Approach to Preparedness

3. **Know your infrastructure components inside and out:**
   - It is important to know all resources and equipment on your network, along with the strengths and weaknesses of each component.
   - Periodically test and document the protection capabilities of the equipment and the network as a whole.
   - This will give you a better understanding of what kind of attacks you can withstand (such as a small attack originating from a single IP address), and if you need to outsource to protect against more complex attacks.

7 Point Approach to Preparedness

4. Understand ISP options for DDoS mitigation:

- It pays to communicate clearly with your internet service provider (ISP), particularly if it's also affected by a DDoS attack.
- Understand your ISP's options for defending against DDoS attacks and confirm your understanding of any Service Level Agreements (SLA).
- If your organization is multi-homed, all your ISPs would need to participate.
- Problems with ISP-only Defense

7 Point Approach to Preparedness

5. Implement general rules to help mitigate DDoS attacks:

- There are some general rules to help defend against a DDoS attack. They should only be used as a guide, since they will not stop all attacks, especially some of the more complex varieties.
- Examples:
  - Turn down all unnecessary ports and protocols
  - Implement an IP blacklist
  - Block invalid and malformed packets
  - Configure and harden network equipment

7 Point Approach to Preparedness

6. **Conduct a post-attack analysis after a DDoS attack:**
   - While it's crucial to have a plan in place to address a DDoS attack, it is equally important to perform a post-attack analysis.
   - Some of the items to consider:
     - the type of attack that happened;
     - which equipment helped you mitigate, even it was only partially successful; and
     - what attack traffic had the most impact and why?
   - This will lead you to consider if you need to purchase better equipment. If that's not in the budget, you may want to think about out-sourcing to a security service provider.

7 Point Approach to Preparedness

7. Leverage monitored and managed services:

- Partnering with a managed security provider has real benefits. Such providers have deep experience in dealing with DDoS attacks and offer a wide array of equipment and resources.
- You can use their services on demand—for example, a DNS redirect service—or have them monitor your network 24/7 for signs of attacks.
- To mitigate the most complex attacks, you need costly equipment. A managed service offers it, when and if you need it.

7 Point Approach to Preparedness

1. Conduct a company-wide DDoS risk assessment
2. Create an action plan to prepare for and respond to DDoS attacks
3. Know your infrastructure components inside and out
4. Understand ISP options for DDoS mitigation
5. Implement general rules to help mitigate DDoS attacks
6. Conduct a post-attack analysis after a DDoS attack
7. Leverage monitored and managed services

AffirmX

neustar

Regulatory Compliance Considerations

Jane Pannier,
Executive Vice President, In-House Counsel
AffirmX

AffirmX

neustar

NCUA PART 748, APPENDIX B Risk Response Programs

- At a minimum, your response program should include procedures to:
  - Assess the nature and scope of the incident;
  - Notify the appropriate NCUA Regional Director or state supervisory authority as soon as possible;
  - File a SAR if the incident involves Federal criminal violations and notify appropriate law enforcement authorities;
  - Take appropriate steps to contain and control the incident; and
  - Notifying members when required or warranted.

Member Notification

- If you determine that misuse of the information by an unauthorized party has occurred or is reasonably possible and the information involves sensitive member information, you must notify the affected members as soon as possible.
- Notice can be delayed if an appropriate law enforcement agency provides you with a written request to delay the notification

Member Notification

- The misused information must be “sensitive member information”.
- Sensitive member information means a member’s name, address or telephone number, **in conjunction with** the member’s social security number, driver’s license number, account number, credit or debit card number, or PIN or password that would permit access to the member’s account.

Member Notification

- If you can determine specifically which member's information has been accessed, you need only provide notification to those members.
- If you are not able to identify specific members, but can narrow those affected down to a particular group of members, you need only notify the members of that group.

Member Notification

- **The notice provided to the members must include:**
  - A general description of the incident and the type of member information that was subject to the unauthorized access or use;
  - A general description of what you have done to protect their information from further unauthorized access;
  - A telephone number members can call for more information;

Member Notification

- A reminder to members to be vigilant for the next 12 to 24 months and to promptly report any incidents of suspected identity theft.
- When appropriate, the notice should also include:
  - A recommendation that the member review account statements and immediately report any suspicious activity
  - A description of fraud alerts and an explanation of how to place a fraud alert on their credit reports
  - A recommendation that the member obtain periodic credit reports in order to delete any fraudulent information

Member Notification

- An explanation of how the member may obtain a free credit report; and
- Information about the availability of the FTC's online guidance regarding the steps a member can take to protect against identity theft and encourage the ember to report any incidents of identity theft to the FTC and provide the FTC's website address and toll-free phone number.

Delivery of the Member Notice

- NCUA encourages credit unions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of members that include contact information for the reporting agencies.
- The member notice may be delivered in any manner that is designed to ensure that the member can reasonably be expected to receive it.

Q&A

RISK WATCH WEBINAR

Q&A

Jane Pannier
Senior Vice President, In-House Counsel
AffirmX

Susan Warner
Market Manager, Security Solutions
Neustar

Jesse Boyer
Vice President, Product Development
AffirmX

For more information:

affirmx.com
888.972.3624

neustar.biz
855-898-0036