AGILITY
2016
SOLUTIONS FOR AN APPLICATION WORLD
Anatomy of an Attack
Understanding the means and motivations around attacks

Gary Newe
An Unprecedented Year in Security

TARGET CEO FIRED - CAN YOU BE FIRED IF YOUR COMPANY IS HACKED?

SECURITY BREACH
83 million households and businesses

FORTUNE
Frank Blake concluded his stellar run as CEO of Home Depot with a smooth succession plan. But will his reputation be singed by the company’s gigantic data breach?

THE NEW YORK TIMES
Bank Hacking Was the Work of Iranians, Officials Say

PNC

CAPITAL ONE BANK

EBAY INC: TO ASK EBAY USERS TO CHANGE PASSWORDS

BBC NEWS
eBay faces backlash on hack delays

© 2016 F5 Networks
Not All Security Challenges Are Technical
3 of top 5 “most challenging” security concerns aren’t technical

- Increasing attack sophistication: 58%
- Employees underestimate importance: 52%
- Complexity of solutions: 42%
- Budget too small: 41%
- Data leakage from personal devices accessing apps in the cloud: 37%

Twin Forces Are Impacting the Security Landscape

Cloud and Mobility

- Apps deployed across data center, SDN, public cloud, and SaaS environments
- Multi-device mobility is now the norm
- Mobile apps surpass desktop apps

Threat Evolution and SSL Obfuscation

- Encryption used in 32.8% of traffic
- 68% of IT: zero-day attacks greatest threat, “Targeted attacks are the new normal” (Forrester Research)
- $9.4M average cost to restore reputation (Ponemon)
The Evolution of the Application
The Evolution of the Application

1995

Users

Apps

Client/Server

Centralized Apps

HTML App

1995

40M

20K
The Evolution of the Application

<table>
<thead>
<tr>
<th>Year</th>
<th>Users</th>
<th>Apps</th>
<th>Used Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>40M</td>
<td>20K</td>
<td>HTML</td>
<td>Client/Server, Centralized Apps</td>
</tr>
<tr>
<td>2000</td>
<td>400M</td>
<td>9.5M</td>
<td>SOAP, JAVA, SSL</td>
<td>Internet Applications, Data Confidentiality</td>
</tr>
</tbody>
</table>
The Evolution of the Application

<table>
<thead>
<tr>
<th>Year</th>
<th>Users</th>
<th>Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>40M</td>
<td>20K</td>
</tr>
<tr>
<td>2000</td>
<td>400M</td>
<td>9.5M</td>
</tr>
<tr>
<td>2005</td>
<td>1B</td>
<td>58M</td>
</tr>
</tbody>
</table>

- **1995**: Client/Server, Centralized Apps
- **2000**: Internet Applications, Data Confidentiality
- **2005**: Mobile Devices, Mobility Malware Threats
The Evolution of the Application

1995
- Users: 40M
- Apps: 20K
- Client/Server
- Centralized Apps

2000
- Users: 400M
- Apps: 9.5M
- Internet Applications
- Data Confidentiality

2005
- Users: 1B
- Apps: 58M
- Mobile Devices
- Mobility Malware Threats

2010
- Users: 2B
- Apps: 207M
- Public Cloud
- Website Availability Threats
The Evolution of the Application

<table>
<thead>
<tr>
<th>Year</th>
<th>Users</th>
<th>Apps</th>
<th>Technology</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>40M</td>
<td>20K</td>
<td>HTML, JAVA,</td>
<td>Client/Server, Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SOAP, SSL</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>2000</td>
<td>400M</td>
<td>9.5M</td>
<td>HTML, SOAP,</td>
<td>Internet Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SAML, SSL</td>
<td>Data Confidentiality</td>
</tr>
<tr>
<td>2005</td>
<td>1B</td>
<td>58M</td>
<td>FLASH, SSL,</td>
<td>Mobile Devices,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SAML, XML,</td>
<td>Mobility Malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FLASH, AJAX</td>
<td>Threats</td>
</tr>
<tr>
<td>2010</td>
<td>2B</td>
<td>207M</td>
<td>HTML 5, ITIL</td>
<td>Public Cloud, Website</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOBILE VIDEO</td>
<td>Availability Threats</td>
</tr>
<tr>
<td>2015</td>
<td>3.2B</td>
<td>1B</td>
<td>MOBILE VIDEO</td>
<td>Hybrid Cloud, Blended</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ITIL, CONTAINERS</td>
<td>Threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IOT, NANO/MICRO,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LEARNING, CONTAINERS</td>
<td></td>
</tr>
</tbody>
</table>
Understanding Motivations of Cyber Criminals

<table>
<thead>
<tr>
<th>GOAL</th>
<th>CYBER CRIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organized crime/cyber crime</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company ransom/risk of reputation</td>
</tr>
<tr>
<td>Buys data to compromise key companies</td>
</tr>
<tr>
<td>Willing to move to another target if protection is robust</td>
</tr>
</tbody>
</table>
Understanding Motivations of Cyber Criminals

**CRIME PAYS***

<table>
<thead>
<tr>
<th>Stolen assets/Criminal activity</th>
<th>Payout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit card numbers</td>
<td>$5–$10 for virgin account</td>
</tr>
<tr>
<td>Bank credentials</td>
<td>$80–$700</td>
</tr>
<tr>
<td>Bank transfers</td>
<td>10%–50%</td>
</tr>
<tr>
<td>Social security number</td>
<td>$30–$50</td>
</tr>
<tr>
<td>Zero-day exploits</td>
<td>$1,000–$100,000</td>
</tr>
<tr>
<td>Exploits for known vulnerabilities</td>
<td>$500–$2,000</td>
</tr>
<tr>
<td>Malware (pay per install)</td>
<td>Up to $1.50 (U.S. victims)</td>
</tr>
</tbody>
</table>

* Source: Alert Logic

**CYBER CRIME**

<table>
<thead>
<tr>
<th>GOAL</th>
<th>Organized crime/cyber crime</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HOW</th>
<th>Company ransom/risk of reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Buys data to compromise key companies</td>
</tr>
<tr>
<td></td>
<td>Willing to move to another target if protection is robust</td>
</tr>
</tbody>
</table>

© 2016 F5 Networks
Understanding Motivations of Cyber Criminals

<table>
<thead>
<tr>
<th>GOAL</th>
<th>Organized crime/cyber crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOW</td>
<td>Company ransom/risk of reputation</td>
</tr>
<tr>
<td></td>
<td>Buys data to compromise key companies</td>
</tr>
<tr>
<td></td>
<td>Willing to move to another target if protection is robust</td>
</tr>
</tbody>
</table>
## Understanding Motivations of Cyber Criminals

<table>
<thead>
<tr>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GOAL</strong></td>
<td><strong>Spread a message and promote a political agenda</strong></td>
</tr>
<tr>
<td>Organized crime/cyber crime</td>
<td></td>
</tr>
<tr>
<td><strong>HOW</strong></td>
<td></td>
</tr>
<tr>
<td>Company ransom/risk of reputation</td>
<td></td>
</tr>
<tr>
<td>Buys data to compromise key companies</td>
<td></td>
</tr>
<tr>
<td>Willing to move to another target if protection is robust</td>
<td>Deface websites, dump company-specific internal information</td>
</tr>
<tr>
<td>Can gain sympathy quickly</td>
<td></td>
</tr>
</tbody>
</table>
# Understanding Motivations of Cyber Criminals

<table>
<thead>
<tr>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
<th>GAIN INTELLECTUAL PROPERTY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GOAL</strong></td>
<td><strong>HOW</strong></td>
<td><strong>Competitive advantage and information warfare</strong></td>
</tr>
<tr>
<td>Organized crime/cyber crime</td>
<td>Spread a message and promote a political agenda</td>
<td></td>
</tr>
<tr>
<td><strong>HOW</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company ransom/risk of reputation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buys data to compromise key companies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willing to move to another target if protection is robust</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Penetrate company defenses and successfully exfiltrate data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recent attacks have been 200+ days installed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Well-funded and well-resourced</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anatomy of an Attack
Anatomy of an Attack

RECONNAISSANCE
Identification, target selection, and organization to determine methods that will work with the highest degree of success.
Anatomy of an Attack

RECONNAISSANCE
Identification, target selection, and organization to determine methods that will work with the highest degree of success.

WEAPONIZATION AND PACKAGING
Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).
Anatomy of an Attack

<table>
<thead>
<tr>
<th>RECONNAISSANCE</th>
<th>Identification, target selection, and organization to determine methods that will work with the highest degree of success.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELIVERY</td>
<td>Transmission of the payload. Initiated by user via malicious web presence, or opening of a malicious PDF file.</td>
</tr>
<tr>
<td>WEAPONIZATION AND PACKAGING</td>
<td>Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).</td>
</tr>
</tbody>
</table>
Anatomy of an Attack

RECONNAISSANCE
Identification, target selection, and organization to determine methods that will work with the highest degree of success.

DELIVERY
Transmission of the payload. Initiated by user via malicious web presence, or opening of a malicious PDF file.

WEAPONIZATION AND PACKAGING
Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).

EXPLOIT
The malicious payload gains foothold by exploiting vulnerability of zero-day vector.
# Anatomy of an Attack

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RECONNAISSANCE</strong></td>
<td>Identification, target selection, and organization to determine methods that will work with the highest degree of success.</td>
</tr>
<tr>
<td><strong>DELIVERY</strong></td>
<td>Transmission of the payload. Initiated by user via malicious web presence, or opening of a malicious PDF file.</td>
</tr>
<tr>
<td><strong>WEAPONIZATION AND PACKAGING</strong></td>
<td>Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).</td>
</tr>
<tr>
<td><strong>EXPLOIT</strong></td>
<td>The malicious payload gains foothold by exploiting vulnerability of zero-day vector.</td>
</tr>
<tr>
<td><strong>INSTALL</strong></td>
<td>Often a remote access Trojan. Usually stealthy in operation, allowing persistence or “dwell time” to be achieved.</td>
</tr>
</tbody>
</table>
## Anatomy of an Attack

<table>
<thead>
<tr>
<th><strong>RECONNAISSANCE</strong></th>
<th><strong>WEAPONIZATION AND PACKAGING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification, target selection, and organization to determine methods that will work with the highest degree of success.</td>
<td>Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DELIVERY</strong></th>
<th><strong>EXPLOIT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission of the payload. Initiated by user via malicious web presence, or opening of a malicious PDF file.</td>
<td>The malicious payload gains foothold by exploiting vulnerability of zero-day vector.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>INSTALL</strong></th>
<th><strong>COMMAND AND CONTROL (C2)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Often a remote access Trojan. Usually stealthy in operation, allowing persistence or “dwell time” to be achieved.</td>
<td>Adversaries control assets within your organization, and tell the controlled asset “what to do next.”</td>
</tr>
</tbody>
</table>
Anatomy of an Attack

**RECONNAISSANCE**
Identification, target selection, and organization to determine methods that will work with the highest degree of success.

**DELIVERY**
Transmission of the payload. Initiated by user via malicious web presence, or opening of a malicious PDF file.

**EXPLOIT**
The malicious payload gains foothold by exploiting vulnerability of zero-day vector.

**INSTALL**
Often a remote access Trojan. Usually stealthy in operation, allowing persistence or “dwell time” to be achieved.

**WEAPONIZATION AND PACKAGING**
Takes many forms, including: web application, off-the-shelf or custom malware, documents (PDF, Office).

**COMMAND AND CONTROL (C2)**
Adversaries control assets within your organization, and tell the controlled asset “what to do next.”

**ACT**
Adversary exfiltrates data, identifies more targets, expands footprint, and obtains valuable data.
How Are the Sources of Attacks Changing?
How Are the Sources of Attacks Changing?
How Are the Sources of Attacks Changing?

STATE SPONSOR

ORGANIZED CRIMINAL
How Are the Sources of Attacks Changing?

- STATE SPONSOR
- ORGANIZED CRIMINAL
- WELL-MEANING INSIDER
How Are the Sources of Attacks Changing?

- STATE SPONSOR
- ORGANIZED CRIMINAL
- WELL-MEANING INSIDER
- MALICIOUS INSIDER
Network Threats
Network Threats

27% OF ATTACKS ARE FOCUSED HERE

90% OF SECURITY INVESTMENT
Network Threats

- 27% of attacks are focused here
- 90% of security investment

Application/User Threats

- 78% of attacks are focused here
- 10% of security investment
Today’s Threat Landscape

CLIENT-SIDE ATTACKS
- Malware
- Stolen user credentials/fraud
- Man in the browser

NETWORK ATTACKS
- Botnet/SPAM
- DNS amplification/cache poisoning
- Recon. port scan
- Network DDoS attacks

SESSION ATTACKS
- Man in the middle
- Man in the browser
- Attacks against SSL vulnerabilities
- Application DDoS attacks

APPLICATION ATTACKS
- DNS attacks
- Business logic abuse
- Application vulnerability exploits
- Application DDoS attacks
- Business logic abuse

OWASP Top 10

© 2016 F5 Networks
Today’s Threat Landscape

CLIENT-SIDE ATTACKS

USER ACCESS AND CREDENTIALS

NETWORK ATTACKS

SESSION ATTACKS

APPLICATION ATTACKS

APPLICATION PROTECTION

USER ACCESS AND CREDENTIALS

Malware

User

Stolen user credentials/fraud

Phishing

Botnet/SPAM

DNS amplification/cache poisoning

Recon. port scan

Network DDoS attacks

Man in the middle

Attacks against SSL vulnerabilities

Application DDoS attacks

Business logic abuse

DATA

DATA

ATTACKS ARE DISPROPORTIONATELY TARGETING THESE AREAS

OWASP Top 10

© 2016 F5 Networks
Today’s Threat Landscape

- Stolen user credentials/fraud
- Phishing
- Network DDoS attacks
- Application vulnerability exploits
- Recon. port scan
- Network DDoS attacks
- Attacks against SSL vulnerabilities
- Application DDoS attacks
- Business logic abuse
- Malware
- DNS amplification/cache poisoning
- Application SSL attacks
- Application DDoS attacks
- Application SSLv3 attacks

ATTACKS ARE DISPROPORTIONATELY TARGETING THESE AREAS
Today’s Threat Landscape

ATTACKS ARE DISPROPORTIONATELY TARGETING THESE AREAS

CLIENT-SIDE ATTACKS

USER ACCESS AND CREDENTIALS

NETWORK ATTACKS

SESSION ATTACKS

APPLICATION ATTACKS

LAYER 7 APPLICATION PROTECTION

DATA

OWASP Top 10

© 2016 F5 Networks
Today's Threat Landscape

USER ACCESS AND CREDENTIALS

Stolen user credentials/
fraud
Phishing

APPLICATION ATTACKS

Application
vulnerability
exploits
Application
DDoS attacks
Application
vulnerability
exploits

NETWORK ATTACKS

SSL ENCRYPTION
AVAILABILITY

Botnet/SPAM
DDoS
DNS attacks
Application
DDoS attacks
Application
vulnerability
exploits

SESSION ATTACKS

Recon.
port scan
Attacks against
SSL vulnerabilities

Malware
Botnet
Spam

CLIENT-SIDE ATTACKS

User
Mal in the
browser
Mal in the
browser

DATA

Malware
Stolen user
credentials
fraud
Phishing
SSL ENCRYPTION
AVAILABILITY

User
Mal in the
browser
Mal in the
browser

DATA

SSL ENCRYPTION
AVAILABILITY

ATTACKS ARE DISPROPORTIONATELY TARGETING THESE AREAS

OWASP Top 10

© 2016 F5 Networks
How Can You Mitigate Attacks?
How Can You Mitigate Attacks?

**LARGE RETAIL COMPANIES**

**ATTACK**
Attackers stole credentials from a third-party vendor

**HOW TO MITIGATE**
Apply better/stronger authentication to remote access technologies (VDI/SSL VPN)
# How Can You Mitigate Attacks?

<table>
<thead>
<tr>
<th>LARGE RETAIL COMPANIES</th>
<th>ONLINE PAYMENT SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ATTACK</strong></td>
<td><strong>HOW TO MITIGATE</strong></td>
</tr>
<tr>
<td>Attackers stole credentials from a third-party vendor</td>
<td>Apply better/stronger authentication to remote access technologies (VDI/SSL VPN)</td>
</tr>
<tr>
<td>Aimed at password change functionality of the payment site</td>
<td>Enabled discovery of automated attacks against this critical application function</td>
</tr>
</tbody>
</table>
## How Can You Mitigate Attacks?

<table>
<thead>
<tr>
<th>LARGE RETAIL COMPANIES</th>
<th>ONLINE PAYMENT SERVICE</th>
<th>BANKING AND FINANCIAL SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attackers stole credentials from a third-party vendor</td>
<td>Aimed at password change functionality of the payment site</td>
<td>Attacked by a multipronged DDoS attack</td>
</tr>
<tr>
<td>HOW TO MITIGATE</td>
<td>HOW TO MITIGATE</td>
<td>HOW TO MITIGATE</td>
</tr>
<tr>
<td>Apply better/stronger authentication to remote access technologies (VDI/SSL VPN)</td>
<td>Enabled discovery of automated attacks against this critical application function</td>
<td>Scrubbing services and mitigation of a computational attack</td>
</tr>
</tbody>
</table>
The Hybrid Threat

Mobile phone retail company breach with a DDoS smoke screen

• DDoS attack before giant data breach
• 2.4M customers’ data stolen from web application attack
• More commonplace threat for Internet connected businesses
  • Especially those that house sensitive data
  • For example, credit cards or personal information

Average Attack Size

- 1–10 Gbps: 38%
- 10–50 Gbps: 20%
- 500–999 Mbps: 23%
- Over 50 Gbps: 6%
- Unknown: 12%
Attack Threats: Pay up or Else!

April–May 2015: Emails sent to legitimate businesses with the threat of massive DDoS attacks

- DD4BC claims ~400 Gbps
- Extortion demands starting at 25 Bitcoins
- Initially targeted Bitcoin, payment providers, banks, and now moving to other targets
- UDP amplification attacks (NTP, SSDP, DNS), TCP SYN floods, and layer 7 attacks

Sample from actual email

```
Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. At least, don't expect cheap services like CloudFlare or Incapsula to help...but you can try. :)
```
Web App Attacks Adversaries Use

“This year, organized crime became the most frequently seen threat actor for web app attacks.”

Verizon 2015 Data Breach Investigations Report

Source: Verizon 2015 Data Breach Investigations Report
Vulnerability Likelihood

- Insufficient Transport Layer Protection: 70%
- Brute Force: 56%
- URL Redirector Abuse: 47%
- SQL Injection: 5%
- Insufficient Authorization: 29%
- URL Redirector Abuse: 26%
- SQL Injection: 16%
- Insufficient Authorization: 24%
- SQL Injection: 15%
- Insufficient Authorization: 11%
- SQL Injection: 11%
- SQL Injection: 8%
- SQL Injection: 6%
- SQL Injection: 6%
- SQL Injection: 6%
- SQL Injection: 5%
What Are Advanced Security Threats?

**Volumetric denial of service**
- Difficult to screen out at high rates
- Denies legitimate user access to site

**Computational or consumption attacks**
- Artificially inflate SaaS consumption
- Require a deep understanding of what items induce delay or fault within an application

**Browser-based malware**
- Exists wholly outside the perimeter
- Delivers various malicious programs to users’ computers

**Spear phishing**
- Targets specific organizations, seeking unauthorized access to confidential data
- Perpetrators out for financial gain, trade secrets, or military information

**Monitoring saturation attacks**
- Overwhelm SIEM tools to disguise malicious inbound actions
- Mask data exfiltration

**Advanced persistent threats (APTs)**
- Targeted cybercrime of stealth over prolonged duration
- Low-and-slow to avoid detection

A NEW SECURITY PERIMETER IS REQUIRED!
Application Attacks Hurt Your Business

Evolving Security Threats

Cyber Security Intelligence Index
Application Attacks Hurt Your Business
Evolving Security Threats

$7.7M
Average cost of cyber crime per company\(^1\)

99
Successful attacks per year per company\(^1\)

81M
Monitored cyber attacks Worldwide\(^2\)

Source 1: Ponemon Institute, 2015 Cost of Cyber Crime Study, 2 IBM Security Services, 2015 Cyber Security Intelligence Index

© 2016 F5 Networks
Application Attacks Hurt Your Business

Evolving Security Threats

$7.7M
Average cost of cyber crime per company

99
Successful attacks per year per company

81M
Monitored cyber attacks Worldwide

Damages brand reputation.
Results in significant downtime and revenue loss.
Compromises sensitive enterprise, employee, and customer data.
Breaches compliance required to conduct business online.

Source 1: Ponemon Institute, 2015 Cost of Cyber Crime Study, 2 IBM Security Services, 2015 Cyber Security Intelligence Index
Comprehensive Security Across Hybrid Environment

Incorporate Threat Feeds in Cloud-Based, Network, and App Security Services

Threat Intelligence Feed

- Scanner
- Anonymous Proxies
- Anonymous Requests
- Botnet
- Attackers

Cloud Scrubbing Service

- Volumetric attacks and floods, operations center experts, L3-7 known signature attacks, IP Reputation

Network

- Network attacks: ICMP flood, UDP flood, SYN flood
- DNS attacks: DNS amplification, query flood, dictionary attack, DNS poisoning, IP Reputation

Next-Generation Firewall

Corporate Users

Network and DNS

- Multiple ISP strategy

Application

- SSL attacks: SSL renegotiation, SSL flood
- HTTP attacks: Slowlows, slow POST, recursive POST/GET, IP Reputation

Financial Services

E-Commerce

Subscriber

© 2016 F5 Networks
Monitoring and mitigating attacks while reducing false positives requires a 24/7 staff of skilled DDoS analysts

- Full provisioning and configuration
- Proactive alert monitoring
- Identification and inspection of attacks
- Custom and script mitigation

Service level agreements time to:
- Notify, mitigate, escalate

Security Operations Center (SOC)
- Tier II DDoS Analysts and Above
- Availability and Support
- Active DDoS Threat Monitoring
Connecting the Dots

IP Addresses
61.160.232.202

Same Attack
Elastic Search (CVE-2014-3120)

Same Bot Attribute
User Agent + HTTP Headers Anomaly
Web Application Firewall

Proven Security Effectiveness as a Convenient Cloud-Based Service

Protect web applications and data from layer 7 attacks
Enable compliance, such as PCI DSS
Provide WAF service backed by 24x7x365 support from experts

L7 Protection:
- Geolocation attacks
- DDoS
- SQL injection
- OWASP Top Ten attacks
- zero-day threats
- AJAX applications
- JSON payloads

VA/DAST Scans
Policy can be built from third-party DAST

© 2016 F5 Networks
Protect Web Apps, Anywhere

Easily Extend WAF Protections to SaaS and Cloud Apps
Global Threat Intelligence
Global Threat Intelligence

Security Force

• Threat Research and Intelligence Team
• Security Operations Center
• Security Incident Response Team (SIRT)
• Security Architects and Security Consulting
Global Threat Intelligence

- Worldwide coverage
- Global scope and scale
- Regional focus
- 24x7 team
- Sensors and honeynets

Security Force

- Threat Research and Intelligence Team
- Security Operations Center
- Security Incident Response Team (SIRT)
- Security Architects and Security Consulting

- Owned and third-party intelligence
- Darknet and other sources
- Vulnerability testing
- Research tools
**Best Practices in Protecting Your Apps**

- Most attacks are at the application layer with little security investment.
- Many times DDoS attacks are smoke screens for app attacks.
- Integrated security protects an app instance, WAFs protect all apps based on policy.
- Virtual and cloud WAFs will continue to grow.
- Apps migrated to clouds will be exposed to more attacks.
- Mitigate app attacks using a WAF no matter app location.

**LEAVE NO APPS UNPROTECTED**
Recommendations
Recommendations

Strong focus on risk management
Recommendations

- Strong focus on risk management
- Consider the sources for attacks
Recommendations

- Strong focus on risk management
- Consider the sources for attacks
- Reduce the impact of user-facing threats
Recommendations

- Strong focus on risk management
- Consider the sources for attacks
- Reduce the impact of user-facing threats
- Develop strong application security
# Recommendations

<table>
<thead>
<tr>
<th>Strong focus on risk management</th>
<th>Consider the sources for attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the impact of user-facing threats</td>
<td>Develop strong application security</td>
</tr>
<tr>
<td>Improve visibility across threat vectors</td>
<td></td>
</tr>
</tbody>
</table>
Give Feedback – Get Points!

- Add class to your personal schedule.
- Survey will pop up in Mobile App.
- Answer the multiple choice.
- Submit your question to complete.
- Receive 5 points!
SOLUTIONS FOR AN APPLICATION WORLD