Advanced Threat Protection with F5 and FireEye

Gary Fisk, CISSP | Solutions Architect
FireEye
Welcome

• Security Trends from the Front Lines
• Advanced Threat Protection – FireEye
• F5 and the ‘SSL Blind Spot’
• Security vs. Enterprise Networking
• Conclusion
FireEye and The Cyber Security Marketplace:
“...And you do what, now?”

Source: Momentum Partners.
Expertise Earned on the Front Lines

- First responders to the world’s most consequential breaches
- Offer proactive and reactive services
- Hundreds of intelligence and malware experts
- Unmatched knowledge of advanced attacker techniques
- Our consultants wrote the book (literally) on incident response
47% of organizations detected the breach on their own.

This percentage is growing from the previous year, where 31% of victims discovered the breach on their own.

Source Data: M-TRENDS 2016
M-TRENDS: INTERNAL DETECTION VS EXTERNAL NOTIFICATION

<table>
<thead>
<tr>
<th>Year</th>
<th>Internal Detection (%)</th>
<th>External Notification (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>47%</td>
<td>53%</td>
</tr>
<tr>
<td>2014</td>
<td>31%</td>
<td>69%</td>
</tr>
<tr>
<td>2013</td>
<td>33%</td>
<td>67%</td>
</tr>
<tr>
<td>2012</td>
<td>37%</td>
<td>63%</td>
</tr>
<tr>
<td>2011</td>
<td>6%</td>
<td>94%</td>
</tr>
</tbody>
</table>
The typical incident saw attackers present for **4+ months**

The longest time we detected attackers had been present in the victim’s environment was 2,982 days (over 8 years).

M-TRENDS 2016: MEDIAN DAYS BEFORE DISCOVERY
WHAT IS WORKING?

- **Segment sensitive data on its own network**
  Ensures that attackers cannot easily move from one segment of the network to another.

- **Improve control over powerful accounts**
  Requires the most powerful accounts to be checked in / out prior to usage, usually protected by two-factor authentication.

- **Promote a “Security Culture”**
  Senior executives set the tone in any successful initiative. Security orgs often need increased support for new controls like two-factor access, incident response plan testing, etc.

- **Focus on phishing prevention**
  Phishing (luring users to click on malicious e-mail attachments) is still the #1 method that attackers use to compromise organizations. Most orgs are not well-protected.

- **Require two-factor authentication for remote access**
  Prevents attackers from using stolen passwords to access resources. Most companies prioritize remote access to e-mail and networks (virtual provide networks).

- **Only permit pre-authorized programs to run on servers**
  Critical systems like servers generally only need to run a small set of software—yet they are often allowed to run arbitrary programs. “Whitelisting” technology can prevent this.

- **Test the incident response plan**
  Fewer than 20% of organizations test response plans with a cross-functional team on an annual basis.

- **Use new technology to block advanced malware**
  New technologies can proactively execute and test web downloads in a secure environment (known as a “sandbox”) to find malware that traditional signature-based models miss.
The typical incident saw attackers present for **4+ months**

The longest time we detected attackers had been present in the victim’s environment was 2,982 days (over 8 years).
FireEye Advanced Threat Protection
FireEye Adaptive Defense

TECHNOLOGY
- Identifies known, unknown, and non-malware based threats
- Integrated to protect across all major attack vectors
- Patented virtual machine technology

INTELLIGENCE
- Discovered 22 of the last 40 zero-days
- Line intel from incident response
- Millions of network and endpoint sensors
- Hundreds of intel and malware experts
- Hundreds of threat actor profiles

EXPERTISE
- "Go-to" responders for security incidents
- Hundreds of consultants and analysts
- Unmatched experience with advanced attackers
FireEye Continuous Threat Prevention Process

Signature-less and multi-flow virtual machine-based approach that leverages superior threat intelligence

Multi-vector inline known and unknown threat prevention

Remediation support and threat intelligence to recover and improve risk posture

Containment, forensics investigation and kill chain reconstruction
Detection And Prevention – Technology

ANALYZE

2 MILLION OBJECTS PER HOUR

DETONATE

EXPLOIT

MALWARE DOWNLOAD

CALLBACK

LATERAL TRANSFER

EXFILTRATION

CORRELATE

Within VMs Across VMs Cross Enterprise

© F5 Networks, Inc

© FireEye, Inc
FireEye Platform: Magic of MVX

1. FireEye Hardened Hypervisor
   - Custom hypervisor with built-in countermeasures
   - Designed for threat analysis

2. Multi-modal Virtual Execution
   - Multiple operating systems
   - Multiple service packs
   - Multiple applications
   - Multiple file-types

3. Threat Protection at Scale
   - Over 2000 simultaneous executions
   - Multi-stage analysis

Nearly 200 execution environments

MVX Core
FireEye Intelligence — A Global Defense Community

REAL-TIME INFORMATION SHARING

DYNAMIC THREAT INTELLIGENCE

RISK AND CONTEXT TO PRIORITIZE RESPONSE

TACTICAL AND STRATEGIC INTELLIGENCE WITH ATTRIBUTION THAT IS APPLICABLE AND ACTIONABLE TO YOUR ORGANIZATION

4,000 CUSTOMERS IN 67 COUNTRIES

10M+ VIRTUAL MACHINES

5M+ ENDPOINTS
FireEye Threat Intelligence: Strategic + Tactical = Actionable

FireEye combines Mandiant Threat Intel + FireEye Labs data to provide actionable information about security threats.

Help us to understand:
- Who’s attacking you?
- What data do they typically target?
- What are the indicators of compromise?
- Which vulnerabilities are they targeting?
- What is the risk of this type of attack?

**Strategic ‘Human Curated’ Threat Intel**
- Threat Actor Profiles
- Intentions
- Tools, Techniques, and Procedures
- Focuses on planning, decisions

**Tactical ‘Machine Generated’ Threat Intel**
- IPs
- URLs, Domains
- MD5s
- Focuses on detection, triage, response
The SSL Dilemma
Encryption Protects Privacy ... Even For Cyber-Criminals

Increasing Share of Internet Traffic

New Applications Drive Adoption

- 29% of Internet traffic is encrypted today
- 65% of Internet traffic will be encrypted by 2017

Evading Detection with Encryption

Growth of Malware that Uses SSL

- 29 reported malware families use SSL
- 2000+ malicious SSL certificates in 1 year

Sources: Sandvine, SSL Blacklist
Industry Trends Driving Encrypted Traffic

An increasing share of network traffic is being encrypted

**DRIVING CHANGE**

- Insider threat (Snowden)
- Increased customer awareness (PFS, Heartbleed)
- New regulatory and compliance requirements
- Evolving cryptography and new standards
- Everything is connected (IoT)

**WARNING**

- Insider threat (Snowden)
- Increased customer awareness (PFS, Heartbleed)
- New regulatory and compliance requirements
- Evolving cryptography and new standards
- Everything is connected (IoT)

**ENCRYPTED TRAFFIC**

- 30% Annual Growth

**TODAY**

- 25%

**2017**

- 50%

1 Netcraft
The SSL Security Challenge

Network Security Tools Cannot Inspect Encrypted Traffic

- Designed to Prevent ‘Man-in-the-Middle’ Interception
- Firewall
- IPS
- DLP
- MVX

Inbound Exploits and Malware Outbound Callbacks

Encrypted Callbacks Are More Prevalent

- Malware Families with SSL Callbacks
  - Dyre
  - Shylock
  - KINS
  - Dridex
  - Gootkit
  - 24+ others

Regulatory Compliance & Privacy Policies

Exploits Malware

Firewall

https://

FireEye
SSL/TLS Overview

How does SSL work?

Client Hello

Server Hello

Key Exchange (Encrypted Session key)

Change CipherSpec ‘Finished’

Establish Security capabilities (protocol version, Cipher suites, Session ID, compression, random No.)

Client verifies server Cert

Client Cert if requested by Server (optional)

Server sends Certificate, key exchange

Verify Client Cert (optional)

Client finish

Secure Data Exchange

Client End Point

Server End Point
SSL Visibility
Making SSL-Encrypted Traffic visible

Client End Point

Client Hello

Server Hello

Key Exchange

Change CipherSpec ‘Finished’

Client-Side Secure Data Exchange

SSL Visibility
F5 BIG-IP

Security Infrastructure

Server End Point

Client Hello

Server Hello

Key Exchange

Change CipherSpec ‘Finished’

Server-Side Secure Data Exchange
Internet Trends and Challenges

• SSL growth is not stopping

• Impacts ability to identify behaviors or recognize exfiltration across all ports

• Up to 80% performance degradation with SSL on NGFWs, etc.

• New SSL protocols and ciphers can break aging security products

• Moving and modifying certificates is a risky business
Typical Architecture - built for little/no Encryption
New Architecture for SSL/TLS Visibility

SSL/TLS
Decryption
Re-encryption

BIG-IP

IPS
FW
DLP
FEYE
WAF

SVR

Scale-Out

Inspection Zones:
100% Visibility
“AIR GAP”
(Separate/Secure Network)
F5 SSL Intercept Solution

- Purpose built, all-in-one SSL Intercept appliances
- Provides security solutions with visibility into SSL/TLS encrypted traffic
- Key Features
  - SSL visibility at high performance
  - Policy based service chaining of security solutions
  - Load balancing of SSL traffic flows across security devices
  - Centralized and simplified management of certificates, encryption keys
  - Selective decrypt / encrypt of specific traffic flows
  - Flexibility of deployment
How Security Vendors See Enterprise Networks
Technology trends create opportunity and complexity

- Mobility
- ‘Software defined’ everything
- Internet of Things
- Advanced threats
- SDDC/Cloud
- Everything is webified
Advanced Threat Protection with F5 and FireEye

- **Scale** FireEye for demanding environments
- **Failover** protection for service availability
- **Find** hidden threats in encrypted traffic
- **Protect** keys for data privacy
- **Lowest TCO** and quickest ROI

All backed by world-class support and professional services
Thank You
Why BIG-IP in Front?

Cipher Diversity
- HW implementation
- F5 developed drivers/ciphers
- Bulk Throughput

SSL
TLS

2K or 4K Keys
Strong Ciphers (TLS 1x)

F5 Silverline
DDoS, WAF

Security Services with Visibility
- Firewalls: Network, WAF, DNS, DDoS
- Access Control, SSO, SAML, SSL VPN
- Forward Proxy, Web Filtering
- Anti-BOT (IPI), Anti-Fraud (Websafe)
- IPS, FireEye, DLP, etc. (external)

1K Keys
SSL
TLS
Weak Ciphers (SSL V3)

TMOS
FPGA
CAVIUM

#1 Performance/Scale
- Sessions, Connections
- Unmatched anywhere

LTM

Servers
Key Use Cases

• Customer needs to load balance and do SSL inspection across multiple FireEye Appliances (NX, EX, PX)
• Customer wants to enable SSL/TLS Inspection across their organization
• If customer needs to load balance more than 3+ FireEye Appliances F5 is the recommended solution.
SSL/TLS Basics and why F5 is the BEST out in front

- Reduces more point products in the daisy chain
- Uses existing infrastructure smarter- i.e Investment Optimization
  - Rightsize your Firewall
  - Scale out IPS or other services
- Be careful with the outbound Air Gap use case
  - Great new features in v12

- Client negotiates the Cipher so…
  - Broad Cipher Diversity is Required (ideally in Hardware)
  - OR software Ciphers are a new attack (DDoS) vector
  - F5 writes our own drivers for our crypto cards
  - F5 builds our own SSL/TLS stack (NetScaler does not)
  - NetScaler and all Firewalls have LIMITED Cipher support
  - SSL V3 is not secure – remove or minimize it
Perimeter Services

- Network firewall with ICSA and EAL4+
- On-premises network DDoS mitigation
- DNS firewall
- SSL visibility
FireEye Advanced Threat Protection

- Block web-based malicious files
- Block malicious web communication
- Advanced malware detection
- Reduce false positives
Secure Access

- Secure access from any device
- SSL VPN
- Context-aware access and control
- Federated platform
Threat Intelligence

- Silverline cloud-based platform
- Cloud-based DDoS scrubbing
- Volumetric DDoS mitigation
- WAFaaS
This deployment mode employs two BIG-IP creating a decryption zone in between for inspection (Sandwich Architecture)

- **Ingress BIG-IP** (BIG-IP 1) to decrypt the HTTPS traffic from the Client
- **Egress BIG-IP** (BIG-IP 2) to re-encrypt the HTTPS traffic to Web Server

**OUTBOUND Request**

- Client HTTPS traffic to server is decrypted by Ingress Big-IP and is passed through the Inline FireEye NX to inspect and uncover any threats.
- Egress Big-IP aggregates and re-encrypts the client decrypted HTTPS traffic after it exits the FireEye before sending it to the server

**INBOUND Response**

- Server HTTPS traffic to client is decrypted by Server-side Big-IP and state fully passed through the FireEye NX for Inspection.
- The Client side Big-IP re-encrypts this traffic back to Client
F5 – FireEye Value Proposition

In 2016, the Internet will reach an inflection point where more than half the traffic is encrypted. Typical network architectures are built for little or no encryption. A security service chain simply consists of a set of security services, such as firewalls or IPS that are intelligently connected through the BIG-IP to provided SSL visibility and to help with scalability and uptime.

**CUSTOMER SCENARIOS**

- Use SSL Intercept for visibility and scale into SSL traffic with FireEye for APT threats.

**DESIRED SOLUTION CAPABILITIES**

- Find hidden threats with SSL Visibility
- Scale security services with defense-in-depth and scale-out for growth
- Single point of control across security solutions for greater efficiencies
- Bypass URL dynamically and statically
- Dynamically detect SSL on any port
Solution Overview

Visibility and Control

Scale SSL across multiple security devices that are either blind or challenged with SSL performance to defend against encrypted threats.