Sourcefire and ThreatGrid

A new perspective on network security
Agenda

An overview of traditional IPS solutions

Next-Generation IPS Requirements

Sourcefire Next-Generation IPS

Advanced Malware Protection

ThreatGRID
If you knew you were going to be compromised, would you do security differently?
It’s no longer a question of “if” you’ll be breached... it’s a matter of “when”?. 
How do they do it?

Hacker Houses contracted to infiltrate our organization

<table>
<thead>
<tr>
<th>Survey</th>
<th>What is the antivirus solution currently used? What are the countermeasures?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write</td>
<td>Create malicious code specially designed for the customer’s environment.</td>
</tr>
<tr>
<td>Test</td>
<td>Test malicious code against a security solution replica.</td>
</tr>
<tr>
<td>Execute</td>
<td>Launch the attack.</td>
</tr>
<tr>
<td>Accomplish</td>
<td>Data exfiltration. Strategic data removal.</td>
</tr>
</tbody>
</table>
Problems with Traditional IPS Technology

- Doesn’t give you much information to go on
- Requires you to spend weeks tuning
- Gives you a false sense of security – the IPS is your “Silver Bullet”
- Overwhelms you with irrelevant events

- Results:
  - IPS is minimally effective or isn’t used
  - Massive amounts of time spent on tuning policies/signatures
  - Companies exploited
Getting most of IT security with your Next-GEN IPS

- Identify the attackers and hosts that really matter for company’s business
- Receive contextual awareness info about critical attacks: who, when, how, why and when
- Gain full network visibility in terms of:
  - Applications used: Google, AIM, Facebook
  - Endpoint types: Windows, Apple, Linux
  - Files transferred throughout the network (who was the first one to access a specific malware file; what is the origin of the outbreak?)
  - Connections (who owns this IP, what’s the origin country? How much data did he access/transfer?)
Who is SourceFire?

Founded in 2001
- Led by cyber-security-focused individuals
- Security from Network to Endpoint to Cloud
  - Market leader in (NextGen)IPS
  - Groundbreaking Advanced Malware Protection solution
- Innovative – 52+ patents issued or pending
  - Pioneer in NextGenIPS, context-driven security, advanced malware protection
  - World-class research capability (VRT)
- Owner of major Open Source security projects:
  - Snort, ClamAV, Razorback
- Bought by Cisco on October, 2013
Open Source SNORT

- Created in 1998 by Marting Roesch
- Snort combines the benefits of signature, protocol, and anomaly-based inspection.
- Snort is the most widely deployed IDS/IPS technology worldwide.
- With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.
- World’s largest threat response community
- Owned and controlled by Cisco/Sourcefire
- Interoperable with other security solutions
Cisco ASA with FirePOWER Services
Industry’s First Adaptive, Threat-Focused NGFW

Cisco ASA
- World’s most widely deployed stateful firewall
- Identity-Policy Control & VPN
- Best in class with availability & clustering
- TCP normalization, TCP Intercept, NAT, Routing

Sourcefire
- Industry-leading next-generation IPS
- Application Visibility and Control
- Built-in network profiling
- URL Filtering to enforce Acceptable Use Policy
- Advanced Malware Protection
- FireSight Analytics & Automation
ASA + Sourcefire = Cisco ASA FirePOWER Services

- Clustering & High Availability
- Intrusion Prevention (subscription)
- Network Firewall Routing | Switching
- Application Visibility & Control
- Advanced Malware Protection (subscription)
- Built-in Network Profiling
- URL Filtering (subscription)
- Identity-Policy Control & VPN
- FireSIGHT Analytics & Automation

CISCO ASA
FireSIGHT Management Center

- Centralized management and analysis
- Customisable reports, alerts, dashboards
- Centralised policy administration
- High availability
- Available both as hardware/virtual appliances
- Automatically discovers and catalogues all network devices and services
- Features automated tuning – adjust policies automatically
- Associates users with security and compliance events
- Mandatory for any Sourcefire installation!
# Sourcefire Network Discovery – Gaining Full Network Visibility

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>EXAMPLES</th>
<th>FirePOWER Services</th>
<th>TYPICAL IPS</th>
<th>TYPICAL NGFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Attacks, Anomalies</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Users</td>
<td>AD, LDAP, POP3</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Web Applications</td>
<td>Facebook Chat, Ebay, Gmail</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Application Protocols</td>
<td>HTTP, SMTP, SSH, Telnet</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>File Transfers</td>
<td>PDF, Office, EXE, JAR, CAB</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Malware</td>
<td>Conficker, Flame</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Command &amp; Control Servers</td>
<td>C&amp;C Security Intelligence</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Client Applications</td>
<td>Firefox, IE10, BitTorrent</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Network Servers</td>
<td>Apache 2.4, IIS7,</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Windows, Linux, Mac</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Routers &amp; Switches</td>
<td>Cisco, Juniper</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>iPhone, Android</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Printers</td>
<td>HP, Xerox, Canon</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>VoIP Phones</td>
<td>Cisco, Avaya</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>VMware, Xen, RHEV</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
Sourcefire Context Explorer - Network Discovery
Impact Assessment

- Relies on information obtained from passive discovery: OS, client and server apps
- Correlates all intrusion events to an impact of the attack against the target.
- Allows analyst to focus on the smaller subset of events that they could be vulnerable to.

<table>
<thead>
<tr>
<th>IMPACT FLAG</th>
<th>ADMINISTRATOR ACTION</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately, Vulnerable</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate, Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vuln mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know, Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know, Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>0</td>
<td>Good to Know, Unknown Network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
Application Control

- Control access for applications, devices or users
- Enforces an application acceptable use policy across the enterprise
- Identifies over 3000 apps, devices and more
- Can use OpenAppID – an application-focused detection language module for Snort that enables users to create, share and implement application detection.
URL Filtering

- Blocks non-business-relates sites using URL categories
- Can be based on users, user groups, subnets, etc.
IPS Policies

- Sourcefire can automate IPS policy tuning.
- Can recommend signatures/event configurations based on the results obtained from network discovery.
- By default, one can apply some standard IPS policies (connectivity over security, balanced connectivity and security, etc.)
**Indication of Compromise (IOC)**

- IOC tags a host that is susceptible of being infected with malware.
- IOC data can give you a clear, direct picture of the threats to your monitored network as they relate to its hosts.
ASA + Sourcefire = Cisco ASA FirePOWER Services NSS Labs Results

- Best Threat Effectiveness
- Highest throughput
- Most Sessions
- Best Value (lowest TCO/protected Mbps)

"For the past five years, Sourcefire has consistently achieved excellent results in security effectiveness based on our real-world evaluations of exploit evasions, threat block rate and protection capabilities."

Vikram Phatak, CTO NSS Labs, Inc.

Top Ratings (8260)*
- 98.9% detection & protection
- 34Gbps inspected throughput
- 60M concurrent connections
- $15 TCO / protected Mbps
ASA with FirePOWER Services
**Licensing – Subscription Packages**
- 1 and 3 years terms
- Application Visibility and Control is part of the default offering
- Application Visibility and Control updates are included in SMARTnet
Advanced Malware Protection – Attack Continuum Model

Visibility and Context

**Attack Continuum**

**BEFORE**
- Discover
- Enforce
- Harden

**DURING**
- Detect
- Block
- Defend

**AFTER**
- Scope
- Contain
- Remediate

**BEFORE**
- Firewall
- Patch Mgmt
- App Control
- VPN
- IAM/NAC

**DURING**
- IDS
- FPC
- Antivirus
- Email/Web
- Forensics

**AFTER**
- AMD
- Log Mgmt
- SIEM

**Visibility and Context**
Advanced Malware Protection – Protection Framework

1-to-1 Signatures  Spero  Device Flow Correlation  Dynamic Analysis
Ethos  IOCs  Advanced Analytics
Advanced Malware Protection – Retrospective Framework

**Typical Analysis**

- File
- Analysis Stops After Initial Disposition
- 1-to-1, Fuzzy, Machine Learning, Sandboxing, etc;
  Disposition = CLEAN
- Actually...
  Disposition = BAD
  ... too late!

**Continuous Analysis**

- File
- Analysis Continues
- Initial Disposition = CLEAN
- Retrospective Alert sent later when Disposition = BAD

- When you can’t detect 100%, visibility is critical
- Sleep techniques
- Unknown protocols
- Encryption
- Performance
Advanced Malware Protection Cloud Intelligence

- 1.6 million global sensors
- 100 TB of data received per day
- 150 million+ deployed endpoints
- 600+ engineers, technicians, and researchers
- 35% worldwide email traffic
- 13 billion web requests
- 24x7x365 operations
- 40+ languages

Automatic Updates every 3-5 minutes

180,000+ File Samples per Day
FireAMP Community, 3+ million
Advanced Microsoft and Industry Disclosures
Snort and ClamAV Open Source Communities
Honeypots
Private and Public Threat Feeds
Dynamic Analysis
Advanced Malware Protection Deployments

**Endpoint AMP**

- Local Connector
- No local definitions (sort of)
- No updates
- Minimal resource usage
  - Approx 30 MB RAM
  - 150 MB HDD
    - 1GB if using TETRA Engine

- Detection Engines
  - 1-1
  - SPERO
  - ETHOS
  - Advanced Analytics
  - Dynamic Analysis
- Trajectory Data

**Network AMP**

![Image of Network AMP]

- SHA256, SPERO, ETHOS
- Clean, Malware, Unknown

---

**Edit File Rule**

- Application Protocol
- Direction of Transfer
- Action
  - Block Malware
  - Spam Analysis for MSE
  - Dynamic Analysis
  - Reset Connection

**Selected File Categories and Types**

- Category: Dynamic Analysis Capable
- Category: System Files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables
- Category: Archive
- Category: Office Documents
Third-party integration with Sourcefire

Cisco Identity Services Engine
- relies on APIs to quarantine attacker’s IP address using Endpoint Protection Services
- quarantines attacker based on Sourcefire intrusion events

F5 Networks – BIG IP
- connects to BIG IP and creates iRules on demand in order to protect virtual servers
- denies attacker access to virtual-server, based on Sourcefire intrusion events

Remote SSH Command Remediation
- can be used with any 3rd party vendor in order to block the IP address of the attacker
- includes the capability to run in privilege mode
- High-speed, automated analysis and adjustable runtimes
- Does not expose any tags or indicators that malware can use to detect that it is being observed
- Can observe a greater number of behaviors
- Video playbacks
- Glovebox for malware interaction and operational troubleshooting
- Process Graph for visual representation of process lineage
- Threat Score & Behavioral Indicators
- Search and correlate all data elements of a single sample against billons of sample artifacts collected and analyzed over years (global and historic context)
- Enable the analyst to better understand the relevancy of sample in question to one’s environment
- Architected from the ground up with an API to integrate with existing IT security solutions (Automatically receive submissions from other solutions and pull the results into your environment)
**amp ThreatGrid Report Sample**

For a live session visit us @Datanet / Cisco Connect

---

**Behavioral Indicators**

<table>
<thead>
<tr>
<th>Description</th>
<th>Threat Score</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Modified a File in a System Directory</td>
<td>90</td>
<td>90</td>
<td>100</td>
</tr>
<tr>
<td>Path: <code>C:\Windows\system32\drivers\PROCRES.FS</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Name: <code>procexp.exe</code></td>
<td>1348</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HTTP Traffic**

**DNS Traffic**

**TCP/IP Streams**

<table>
<thead>
<tr>
<th>Stream</th>
<th>Src. IP</th>
<th>Srv. Port</th>
<th>Dest. IP</th>
<th>Dest. Port</th>
<th>Transport</th>
<th>Artifacts</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream 0</td>
<td>172.16.1.1</td>
<td></td>
<td>172.16.94.27</td>
<td></td>
<td>ICMP</td>
<td>0</td>
<td>+37.212s</td>
</tr>
<tr>
<td>Stream 1</td>
<td>172.16.94.27</td>
<td></td>
<td>224.0.0.22</td>
<td></td>
<td>IGMP</td>
<td>0</td>
<td>+39.273s</td>
</tr>
</tbody>
</table>

**Processes**

<table>
<thead>
<tr>
<th>Process Name</th>
<th>PID</th>
<th>File Actions</th>
<th>Registry Actions</th>
<th>Analysis Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>procexp.exe</td>
<td>1348</td>
<td>3</td>
<td>14</td>
<td>Is target sample.</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>620</td>
<td>3</td>
<td>0</td>
<td>Process activity after target sample started.</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1032</td>
<td>3</td>
<td>0</td>
<td>Process activity after target sample started.</td>
</tr>
</tbody>
</table>
Short video – AMP
KEY TAKE-AWAY POINTS

ASA with FirePOWER Services

IPS Intrusion Prevention System
AVC Application Visibility and Control
URL filtering
AMP for networks and endpoints
File trajectory and file retrospections
Passive network discovery
Indication of Compromise

AMP Threat Grid

Malware Analysis & Threat Intelligence
believe in more | believe in security
Thank you!