AN INTELLIGENT APPROACH TO STOPPING ADVANCED THREATS

Peter Gyenese
Security Channel Leader, Central and Eastern Europe

p.gyenese@hu.ibm.com

hu.linkedin.com/pub/peter-gyenese/52/681/351/
How do we (humans) protect ourselves from threats?

- Skin, the physical barrier, 1st layer of defense
- Cellular counter attack – layer 2.
- Antibodies – layer 3.

The immune cells must communicate and cooperate effectively!
Introducing the IBM Threat Protection System

A dynamic, integrated system to disrupt the lifecycle of advanced attacks and help prevent loss


DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM
Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network

**Trusteer Apex Malware Protection**

- Prevent malware installs
  - Verify the state of applications
  - Block exploit attempts used to deliver malware

- Prevent mutated exploits
  - Verify the state of network protocols
  - Block unknown exploits with behavioral heuristics

**On the Endpoint**

- Exploit Disruption
- Malware Quarantine
- User Protection

**Prevent control channels**
- Stop direct outbound malware communications
- Protect against process hijacking

- Prevent active beaconing
  - Stop malware and botnet control traffic with real-time reputation and SSL inspection

**Prevent credential loss**
- Block keyloggers
- Stop credential use on phishing sites
- Limit reuse of passwords

**On the Network**

- IBM Security Network Protection XGS

- Prevent malicious apps
  - Block access to malicious websites
  - Prevent web application misuse

Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network.
Continuously monitor security-relevant activity from across the entire organization

Predict and prioritize security weaknesses before adversaries do

- Use automated vulnerability scans and rich security context
- Emphasize high-priority, unpatched, or defenseless assets requiring attention

Pre-Attack Analytics

IBM Security QRadar Vulnerability Manager

Detect activity and anomalies outside normal behavior

- Correlate and baseline massive sets of data
- From logs, events, flows, user activity, assets, locations, vulnerabilities, external threats, and more

Real-time Attack Analytics

IBM Security QRadar SIEM

IBM Security QRadar Security Intelligence Platform
Quickly investigate breaches, retrace activity, and learn from findings to remediate weaknesses

**Post-Attack Incident Forensics**

Reduce the time to fully discover what happened and when it occurred

- Index and reconstruct attack activity and content from full-packet network data
- Apply search engine technology and advanced visualizations

**Rapid Response Integrations**

Quickly expand security coverage to prevent further harm

- Share indicators across control points
- Dynamically apply customized rules

**IBM Security Framework Integrations**

**Emergency Response Services**

Help prepare for and withstand security breaches more effectively

- Gain access to key resources that can enable faster recovery and help reduce incident business impact

**IBM Security QRadar Incident Forensics**

**IBM Emergency Response Services**
Leverage threat intelligence with product integrations that draw upon human and machine-generated information

Global Threat Intelligence

- Combines the renowned expertise of X-Force with Trusteer malware research
- Catalog of 70K+ vulnerabilities, 22B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis
Q2 quarterly X-Force report published on 9 June

Web Applications remain a concern

<table>
<thead>
<tr>
<th>Mapping of 2013 findings to the OWASP Top 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of scanned web applications with threat</td>
</tr>
<tr>
<td>0%</td>
</tr>
<tr>
<td>6%</td>
</tr>
<tr>
<td>17%</td>
</tr>
</tbody>
</table>

Figure 1. Common vulnerabilities found occurring in web applications tested by the IBM Hosted Application Security Management (HASM) service, compared to the OWASP Top 10 for 2013

Spam bots “live” on XP workstations

Table: Top 10 countries where spam originates, 4Q 2013 through 1Q 2014

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spain</td>
<td>10.1%</td>
</tr>
<tr>
<td>Italy</td>
<td>6.2%</td>
</tr>
<tr>
<td>United States</td>
<td>6.2%</td>
</tr>
<tr>
<td>India</td>
<td>5.7%</td>
</tr>
<tr>
<td>Germany</td>
<td>4.5%</td>
</tr>
<tr>
<td>Romania</td>
<td>4.4%</td>
</tr>
<tr>
<td>Argentina</td>
<td>4.3%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>3.4%</td>
</tr>
<tr>
<td>Russia</td>
<td>3.1%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>3.0%</td>
</tr>
<tr>
<td>Other</td>
<td>49.1%</td>
</tr>
</tbody>
</table>

How to prepare your staff for incident response.

The “return” of image spam

Figure 5. Percentage of image spam, 1 December 2013 through 1 March 2014

Percentage of image spam

1 December 2013 through 1 March 2014

- First attack on 5 Dec
- New attack on 21 Dec
- New attack on 24 Feb
Share, analyze, and act upon information gathered from an ecosystem of third-party products

IBM Security Partner Ecosystem Integrations

IBM works with a broad set of technology vendors who provide complementary solutions and are integrated with our security products

Strengthen the threat protection lifecycle

- Leverage a vibrant ecosystem of security products
- Increase visibility, collapse information silos, and provide insights on advanced attacks

**IBM Security Partner Ecosystem**

90+ vendors and 400+ products

**Planned Advanced Threat Protection Integrations:**
- Trend Micro Deep Discovery
  IBM XGS Quarantine and Blocking
- FireEye Web Malware Protection System
  IBM XGS Quarantine and Blocking
- Damballa Failsafe
  IBM XGS Quarantine and Blocking
- Palo Alto Firewalls
  Trusteer Apex integration

**Additional Example QRadar Partners:**

- Cisco
- Blue Coat
- Proofpoint
- Juniper
- Qualys
Examples of breaking the attack chain through integrated intelligence

**ATTACK CHAIN**

**Break-in**
Attacker sends a phishing email to an unsuspecting user, a link is clicked, an exploit is sent to the browser

**Latch-on**
Remote employee executes untrusted code from an attachment, which tries to download and install malware

**Expand**
Attacker finds a way in and tries to search for usernames and passwords to access critical systems

**Gather**
Internal system attempts to access and export data from critical resources

**Exfiltrate**
Malware made its way through an unprotected system and attempts to quietly siphon out data

- XGS prevents the remote exploit from reaching the vulnerable browser and alerts QRadar to the intrusion attempt
- Apex prevents malware from installing, shares an event to QRadar through the cloud, and enforces an XGS quarantine rule
- XGS prevents the attempt to scan internal systems, while QRadar detects abnormal traffic patterns on the network
- QRadar detects user logins and database activity revealing abnormal access to sensitive servers
- QRadar detects the slow data transfer, sends a quarantine rule to XGS, while Incident Forensics records attack activity
IBM is uniquely positioned to offer integrated protection

1. Smarter Prevention
   - Trusteer Apex Endpoint
     - Malware Protection
   - IBM Security Network Protection XGS
     - Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS
   - Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration

2. Security Intelligence
   - IBM Security QRadar
     - Security Intelligence
   - Threat Monitoring and Intelligence Services
     - SIEM enhancements (SOC) new cyber threat intelligence

3. Continuous Response
   - IBM Security QRadar
     - Incident Forensics
   - Integrated forensics module with full packet search and visual reconstruction of threat actor relationships
   - IBM Emergency Response Services
     - Increased global coverage and expertise related to malware analysis and forensics

4. Global Threat Intelligence
   - IBM X-Force Threat Intelligence
     - New virtual real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force

5. Open Integrations
   - Ready for IBM Security Intelligence Ecosystem
     - New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors

DYNAMIC PROTECTION AND ANALYTICS PLATFORM

SECURITY PARTNER ECOSYSTEM
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.