Tell Me Your IP and I Will Tell You Who You Are

Noa Bar-Yosef
Sr. Security Strategist
Imperva
www.imperva.com

OWASP
Oct. 29, 2010
 Agenda

- Different attacks, different sources
- Applying IP Intelligence – determining what, how and why
- Your IP Intelligence toolbox
- Summary
Data At Risk

Total publicly stolen data records by external hackers in the US since 2005.

Source:
http://www.privacyrights.org/ar/ChronDataBreaches.htm#2
The Value of Data

molodec

- Join Date: Jun 2010
- Posts: 27
- Репутация: -3
- Сфера: Stuff, CC, Cashing

Sell CC base

- Have 2 bases:
  - EU (1.3k valid)
  - USA (>2k valid)

Prices and conditions of deal ----> 402860090

Yesterday, 09:47 AM

Peks

- Он в блэке на соседних площадках. В частност...
The Rise of Industrialized Hacking

Roles
- Researching Vulnerabilities
- Developing Exploits
- Growing Botnets
- Exploiting Targets
- Consuming

Optimization
- Direct Value – i.e. IP, PII, CCN
- Command & Control
- Malware Distribution
- Phishing & spam
- DDoS
- Blackhat SEO

Automation
- Growing Botnets and Exploiting Vulnerabilities
- Selecting Targets via Search Engines
- Templates & Kits
- Centralized Management
- Service Model
It’s Not Going to Stop

$1 TRILLION

The amount of money rolled in the hacking industry.

Source:
Joseph Menn, Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, January 2010
More Hacking Motivations - Competitors

- Data theft
  - Intellectual property
  - Company secrets
  - Business plans

- Blackmail
  - Employee details
  - Company tradings
  - DoS

- Corporate espionage
More Hacking Motivation – Nation States

■ Advanced Persistent Threats (APT)
  ▸ Politically motivated
  ▸ Cyber-warfare
  ▸ Government espionage

■ When Hactivism Meets Industrialization
  ▸ Stuxnet?!
Different Hack Sources – Common Ground

- Formalized Attack Tools
- Formalized Attack Services
- Automation
The Security Solution

- Quickly prevent the “Known Bad”
- Focus analysis on the “Unknown Bad”
  - Mixture of sources
  - Different threat levels
  - Varied sophistication
IP Addresses - First Impression (1)

Connection Aggregators

- Large organizations, ISPs
- A single IP represents a group of unrelated sources
IP Addresses - First Impression (2)

- Masquerading
  - Proxies, relays, TOR
  - The IP address does not represent the true source
IP Addresses - First Impression (3)

- Hopping
  - Dynamic allocation
  - Attacker can alternate between addresses during a single session
IP Addresses – On a Second Look (1)

- Persistent connections for home users (Cable, DSL)
  - 65% of dynamically allocated addresses persist for more than a day
  - 15% for more than a week

IP Addresses – On a Second Look (2)

■ Many attacks do not go through aggregators (i.e. home users)
  ▸ IPv4 is still not exhausted
    ▪ <15% of available IPv4 addresses were used in Q3 2009 (Akamai)
    ▪ Only 60% of available addresses are allocated with a growth rate of 11% per year (IP2Location)

■ Not all hopping activity matters
  ▸ Usually within the same country or area

■ IPv6?
Introducing IP Intelligence

What IP Intelligence is:

- **Gather information** – obtain enough information about individual IP addresses
- **Analyze retrieved information** – analyze what can be used to assist in security decisions and influence them
- **Apply Intelligently** - apply the information in automated decision engines or manual forensic analysis
Gathering IP Information

- **Inherent Information**
  - Type of allocation (Dynamic/Static)
  - Ownership (ISP/Individual)
  - Geo Location

- **Reputation-based**
  - Known infections
  - Reported nefarious behavior
Aspects of IP Intelligence

Geo Location

Thwarting masquerading

Connection and Allocation Attributes

Reputation

WHAT?

HOW?

WHY?
Geo Location - What

■ Assign a physical geographical location to a network address

■ Different levels of granularity
  ▶ Country (usually reliable)
  ▶ City ("Greater Area")
  ▶ POP
Geo Location – How (1)

- Explicit Registrar Information
- Network Analysis
  - Route
  - Timing
Geo Location – How (2)

■ Degree of Accuracy

<table>
<thead>
<tr>
<th>Geography</th>
<th>Your IP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continent:</td>
<td>asia</td>
</tr>
<tr>
<td>Country:</td>
<td>il</td>
</tr>
<tr>
<td>Country CF:</td>
<td>99</td>
</tr>
<tr>
<td>Region:</td>
<td>hamerkaz</td>
</tr>
<tr>
<td>State:</td>
<td>99</td>
</tr>
<tr>
<td>City:</td>
<td>petach tikva</td>
</tr>
<tr>
<td>City CF:</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong>: ISRAEL TEL AVIV, TEL AVIV</td>
</tr>
<tr>
<td><strong>Latitude / Longitude</strong>: 32.067 LATITUDE, 34.957 LONGITUDE</td>
</tr>
<tr>
<td><strong>Connecting through</strong>: AIMFRVA-LTD</td>
</tr>
<tr>
<td><strong>Time Zone</strong>: UTC +02:00</td>
</tr>
<tr>
<td><strong>Net Speed</strong>: COMP</td>
</tr>
<tr>
<td><strong>IDD Code</strong>: 972</td>
</tr>
<tr>
<td><strong>Weather Station</strong>: ISRA0026 - TEL AVIV-YAFO</td>
</tr>
</tbody>
</table>

**Your IP Address**
- **Countries**: Israel
- **Region**: 02 (Hamerkaz)
- **Global Cities**: Ashdod
- **ISP**: Golden Lines Cable
- **Organization**: Golden Lines Cable
- **Netspeed**: Cable/DSL
- **Domain Name**: 012.net.il
Geo Location – Why (1)

- Business Logic Attacks
  - Unexpected geographic locations
  - Functionality limitations
    - EU regulations restrict access of personal information from outside the EU
Geo Location – Why (2)

- Fraud Detection
  - Unusual geographic locations
  - Simultaneous access from different locations
  - Account differences
    - Physical location
    - Shipping
    - Billing
Geo Location – Why (3)

- Analyze distributed attacks
  - Manually or automatically
  - Examples:
    - Scalping Attack
    - Comment Spam
Geo Location – Why (4)

- Influence Fuzzy Decisions
  - Flag as: suspicious, malicious or benign
- May require further investigation
  - Adaptive authentication
  - Reduced functionality
Connection and Allocation - What

- Allocation
  - Dynamic
  - Static
- Connection
  - Dial-up
  - Cable
  - T1
- Speed
Connection and Allocation - How

- Network Analysis
  - Route
  - Timing
Connection and Allocation – Why

- Dynamic allocations are usually not servers
  - According to Microsoft the vast majority (96%) of SMTP traffic originating from dynamically allocated addresses is spam.

- Dynamic allocations are usually not aggregators
  - Easier to detect brute force attacks
  - Expected application events rate is low
    - Regardless of connection speed
Thwarting Masquerading - What

- Identify attackers hiding their true source
- Hiding places
  - Network relays (SOCKS Proxy)
  - Anonymous proxies
  - TOR network (Onion routers)
Thwarting Masquerading – How (1)

- Blacklist known IP masquerading addresses
  - TOR servers
  - Anonymous proxy computers
Thwarting Masquerading – How (2)

- Detect discrepancies between information implied by IP address and the actual request
  - “Accept Language”
    - Value is local (en-us) but address is foreign
    - Value is foreign but address is local
  - Response time
    - In accordance to what is implied by location
  - Abnormal path
    - Analyze BlueCoat headers
Thwarting Masquerading – Why
Reputation – What (1)

- Listings of IP addresses with bad reputation
  - Compromised servers
  - Botnet C&C servers
  - Infected servers
  - Infected computers
  - Active spam sources
  - Crawlers
  - ...
Reputation – What (2)

- Listings of IP addresses with impeccable reputation
  - Legitimate search engine bots
  - Aggregators (Akamai, Limelight)
Reputation – How

- “Real-time” feeds for blacklists
  - Information should be updated and queried with high frequency (at least hourly)
  - Aging mechanisms must be applied

- Honeypots

- Community effort

- Dynamic Allocation
  - Usually static for days
Reputation – Why (1)

- Form spam / Comment spam
  - Identify potentially vulnerable resources
  - Block access by known active spamming sources

- Business Logic Attacks
  - Reduced functionality for known infected sources
  - Require extended authentication
Reputation – Why (2)

- Automation
  - Challenge for anti-automation

- Block active attack sources
  - 0-days can be blocked based on who is actually using them.
IP Intelligence Tools
Geo Location Tools (1)

- Two major form factors
  - Online service
    - Forensic analysis
    - Non-stream applications (email)
    - e.g. Quova
  - On-premise database with API
    - Online security decisions
    - e.g. Maxmind
Geo Location Tools (2)

- Different levels of granularity
  - Connection and allocation
  - Proxy detection
Reputation Data (1)

- Multiple providers
  - Different data sets and information
  - Specialize towards specific type of malicious activity
    - Spam
    - Botnet
    - ...

- Data provided in various forms
  - Web Service
  - Incoming feed
  - On premise database/ appliance shielded by an API
Reputation Data (2)

- Various data attributes
  - Raw data – use with discretion
  - Processed data
  - Gradual score

- Data includes various indicators
  - A measurement for intensity of malicious activity
  - Activity duration information (last seen, first seen, etc.)
Reputation Data (3)

- Non-commercial sources
  - Dshield (www.dshield.org)
  - ShadowServer (www.shadowserver.org)
Reputation Data (3)

- Commercial providers
  - Verisign (iDefenceLabs)
  - RSA
  - McAfee (TrustedSource)
  - CommTouch
  - ThreatMetrix
  - Cyveillance
  - Unspam
Putting It All Together
IP Intelligence – Step #1

- Incorporate IP Intelligence into your security process
  - Geo Location as a forensic tool
  - Incorporate Geo Location into many frameworks
    - Supported by log aggregators
    - SIEMs can be customized
IP Intelligence – Step #2

Integrate with IP reputation services at different points

- Some vendors (FW, WAF) offer it
- Some reputation vendors offer their own independent solution
- Most email protection solutions already have their integration out of the box
IP Intelligence – Step #3

Evaluate which vendor provides the most suitable solution for you

- Form factor
  - High speed streaming
  - Manual forensic process
- Focus of data
  - Spam
  - Web attacks
  - Bot infection
- Data attributes
  - Raw data
  - Processed, scored feed
Changes in threat landscape make the use of IP Intelligence valuable for detecting and mitigating attacks.

- Quickly identify known bad and keep your focus on complex issues
- Mitigate 0-day attacks before they are well-analyzed and have specific protection
- Fight online fraud with tools that help evaluate transactions and user behavior.
IP Intelligence – Summary (2)

- Commercial tools of various shapes and different purposes are available
  - Some are forensic analysis-oriented. Others can integrate with online security devices
  - Some vendors provide packaged solutions
Q & A

info@imperva.com