What Is ROI for Attackers

- Researchers subverted a botnet's command and control infrastructure (proxy bots)
  - Modified its spam messages to point to the Web server under researcher control
- That server mimicked the original Web page from the spam emails
  - A pharmacy site
  - A greeting card download site


Most-targeted E-mail Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Freq</th>
</tr>
</thead>
<tbody>
<tr>
<td>hotmail.com</td>
<td>8.47%</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>5.05%</td>
</tr>
<tr>
<td>gmail.com</td>
<td>3.17%</td>
</tr>
<tr>
<td>aol.com</td>
<td>2.37%</td>
</tr>
<tr>
<td>yahoomail.com</td>
<td>1.12%</td>
</tr>
<tr>
<td>sbglobal.net</td>
<td>0.89%</td>
</tr>
<tr>
<td>mail.ru</td>
<td>0.89%</td>
</tr>
<tr>
<td>shawe.ca</td>
<td>0.61%</td>
</tr>
<tr>
<td>wanadoo.fr</td>
<td>0.61%</td>
</tr>
<tr>
<td>mail.com</td>
<td>0.58%</td>
</tr>
<tr>
<td>Total</td>
<td>23.99%</td>
</tr>
</tbody>
</table>


Spam Conversion Pipeline

- How many spam emails reach recipients:
  - Open a few email accounts themselves and append them to email delivery lists in spam messages
- How many emails result in Web page visits:
  - Must filter out defense accesses
- How many users actually buy advertised products or download software:
  - No "sale" is finalized
- Ethical issues abound


Spam Filter Misses

<table>
<thead>
<tr>
<th>Spam Filter</th>
<th>Pharmacy</th>
<th>Postcard</th>
<th>April Fool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail</td>
<td>0.0068%</td>
<td></td>
<td>0.0025%</td>
</tr>
<tr>
<td>Yahoo</td>
<td>0.0017%</td>
<td>0.0005%</td>
<td>none</td>
</tr>
<tr>
<td>Hotmail</td>
<td>none</td>
<td>none</td>
<td>0.0002%</td>
</tr>
<tr>
<td>Rambler</td>
<td>0.18%</td>
<td>none</td>
<td>N/A</td>
</tr>
<tr>
<td>Total</td>
<td>0.0068%</td>
<td>0.0005%</td>
<td>0.0025%</td>
</tr>
</tbody>
</table>

For More on Botnets

http://www.shadowserver.org
http://www.honeynet.org/papers/bots/
http://www.honeynet.org/papers/ff

Can’t protect applications from within themselves
  o Exploits can turn off defenses
Can’t protect the OS from within itself
  o Exploits can turn off defenses
  o Rootkits can hide any sabotage from users
May not be able to trust users
  o They may be uninformed
  o They may be malicious – OK for their computer
    but risk for the others they communicate with
  o Digital right management issues

What Problem Are We Solving?

What is Trusted Computing

Attestation
  o Means of ensuring someone (user, remote computer) of the system’s trustworthy status
    o Usually means authentic/approved apps
  o Root of trust needed to store keys
  o Trusted path (allows user to have confidence in the system)
    o Chain of trust (like for certificate authorities)
Separation
  o Secure storage (data/keys)
  o Protection of processes
The rest is policy
  o That’s the hard and controversial part

Trusted Path

Communicated Assurance

We need a “trusted path”
  o For user to communicate with a domain that is trustworthy.
    o Usually initiated by escape sequence that application cannot intercept: e.g. CTRL-ALT-DEL
    o Could be direct interface to trusted device:
      o Display and keypad on smartcard

We need a “trusted path” across the network.
  Provides authentication of the software components with which one communicates
What Can We Do with TC?

- Clearer delineation of security domains
  - We can run untrusted programs safely
    - Run in domain with no access to sensitive resources
    - Such as most of your filesystem
    - Requests to resources require mediation by TCB (trusted computing base), with possible queries to the user through trusted path.

Mediating Programs Today

- Why are we so vulnerable to malicious code today?
  - Running programs have full access to system files
  - Why? NTFS and XP provide separation
    - But many applications won’t install, or even run, unless users have administrator access
  - So we run in “System High”

Corporate IT Departments’ Solution

- Users don’t have administrator access even on their own laptops
  - This keeps end users from installing their own software, and keeps IT staff in control
  - IT staff select only software for end users that will run without administrator privileges
  - But systems still vulnerable to exploits in programs that cause access to private data
  - Effects of “Plugins” can persist across sessions

The Next Step

- But, what if programs were accompanied by third party certificates that said what they should be able to access?
  - IT department can issue the certificates for new applications
  - Access beyond what is expected results in system dialogue with user over the trusted path

Red / Green Networks

- Butler Lampson of Microsoft and MIT suggests we need two computers (or two domains within our computers)
  - Red network provides for open interaction with anyone, and low confidence in who we talk with
  - We are prepared to reload from scratch and lose our state in the red system

Red / Green Networks

- The Green network provides high accountability, no anonymity, and we are safe because of the accountability
  - But this green system requires professional administration
  - A breach anywhere destroys the accountability for all
Somewhere Over the Rainbow
- But what if we could define these systems on an application by application basis
  - There must be a barrier to creating new virtual systems, so that users don’t become accustomed to clicking “OK”
  - But once created, the TCB prevents the unauthorized retrieval of information from outside this virtual system, or the import of untrusted code into this system
  - Question is who sets the rules for information flow, and do we allow overrides (to allow the creation of third party applications that do need access to the information so protected)

A Financial Virtual System
- I might have my financial virtual system. When asked for financially sensitive data, I hit CTRL-ALT-DEL to see which virtual system is asking for the data
- I create a new virtual system from trusted media provided by my bank
- I can add applications, like Quicken, and new participants, like my stock broker, to a virtual system only if they have credentials signed by a trusted third party

How Many Virtual Systems
- Some examples:
  - Open, untrusted, wild Internet
  - My financial virtual system
  - My employer’s virtual system
  - Virtual systems for collaborations
    - Virtual Organizations
  - Virtual systems that protect others
    - Might run inside VM’s that protect me
    - Resolve conflicting policies
    - DRM vs. Privacy, etc

What do we need for TC
- Trust must be grounded
  - Hardware support
    - How do we trust the hardware
    - Tamper resistance
    - Embedded encryption key for signing next level certificates
    - Trusted HW generates signed checksum of the OS and provides new private key to the OS

Non-Maskable Interrupts
- We must have hardware support for a non-maskable interrupt that will transfer program execution to the Trusted Computing Base (TCB) when user demands it
  - This invokes the trusted path

The Hardware Basis
- Trusted computing is proof by induction
  - Each attestation stage says something about the next level
  - Just like PKI Certification hierarchy
- One needs a basic step
  - On which everything is built
  - Hardware is that step
**Trusted Platform Module (TPM)**

- Basically a key storage and cryptographic functionality device
- Capabilities:
  - Generation of new keys
  - Storage and management of keys
  - Use of keys for cryptographic functions

**Remote Attestation with TPM**

- Sign something with EK
  - Compromises user privacy since different sessions can be linked together
- Using remote CA
  - AIK is generated and signed by a remote CA

**Secure Storage with TPM**

- Users’ data can be encrypted by TPM–generated and TPM–protected keys (binding keys)
  - Not every key can be stored on TPM but it can be protected by keys that are stored on TPM
- Eventually, every binding key is secured by the TPM’s Storage Root Key (SRK)
Secure Storage with TPM

- Two ways to protect data with TPM:
  - **Data binding**: encrypting with a binding key
  - **Data sealing**: data is encrypted, bound to a specific TPM platform and a particular configuration
    - Take data, a binding key and requested PCR values as input, then outputs a sealed data package.
    - To decrypt this package, one must be running the same TPM, have the key, and the current PCR value has to match with the value used in the sealing process.
    - E.g., one seals a Word document with a binding key, and PCR values indicating that Microsoft Word and Symantec antivirus were loaded. To read that document, other users must have access to the key, use Microsoft Word and Symantec antivirus, in the same TPM.

OS Support for Trusted Computing

- **Separation of address space**
  - So running processes don’t interfere with one another
- **Key and certificate management for processes**
  - Process tables contain keys or key identifiers needed by application, and keys must be protected against access by others
  - Processes need ability to use the keys

OS Support for Trusted Computing

- **Fine-grained access controls on persistent resources**
  - Protects such resources from untrusted applications
  - The system must protect against actions by the owner of the system (!!!)

Discussion – Risks

- Trusted computing is a tool that can be misused
  - If one party has too much market power, it can dictate unreasonable terms and enforce them
- Too much trust in trusted computing
  - Attestation does not make a component trustworthy (vulnerabilities may still exist, component may still misbehave)

Discussion – Benefits

- Allows systems to be developed that require trustworthy remote components
  - Provides protection of data when out of the hands of its owner
- Provides isolation and virtualization beyond local system
  - Provides containment of compromise

Equal Opportunity for Discrimination

- Trusted computing means that the entities that interact with one another can be more certain about their counterparts
- This gives all entities the ability to discriminate based on trust
- Trust is not global – instead one is trusted “to act a certain way”
Equal Opportunity for Discrimination

- Parties can impose limits on what the software they trust will do
- That can leave less trusted entities at a disadvantage
- Open source has fewer opportunities to become “trusted”

Privacy and Anti-Trust Concerns

- Strong DRM systems require trust in the systems that receive and process protected content
  - Trust is decided by the provider of the content
  - This requires that the system provides assurance that the software running on the system is software trusted by the provider

Privacy and Anti-Trust Concerns

- The provider decides its basis for trust
  - Trusted software may have features that are counter to the interests of the customer
    - Imposed limits on fair use
    - Collection and transmission of data the customer considers private
    - Inability to access the content on alternative platforms, or within an open source OS

Trusted Computing Cuts Both Ways

- The provider–trusted application might be running in a protected environment that doesn’t have access to the user’s private data
  - Attempts to access the private data would thus be brought to the users attention and mediate through the trusted path
  - The provider still has the right not to provide the content, but at least the surreptitious snooping on the user is exposed.