Trust-based Collaboration

Session 4A: Law Enforcement Engagement Practices
Opinions expressed are my own.

Dave Piscitello

APTLD 72
September 2017
Agenda

- Typical Attack Landscape
- Today’s Intervention-Mitigation Timeline
- Intervention-Mitigation Today
- Trusted Intervener Frameworks
- Public-Private Partnerships
- Accelerating Due Process
Setting Context:

Chronology of a typical attack

User receives spam with malicious attachment

Malicious attachment self-installs, connects to criminal host to download malware installer

Malware installer downloads attack-specific malware

Attacks ensue: Phishing, Data Theft, Ransomware, Account theft...
Attackers Operate at Internet Pace: Botnet-facilitated Attacks

<table>
<thead>
<tr>
<th>Pre-Attack</th>
<th>Hour 0</th>
<th>Hours 1-12</th>
<th>Day 1+… Months later…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet operator registers domain names for command and control host names</td>
<td>Botnet operator leases botnet for criminal use attack begins</td>
<td>Consumers affected by botnet facilitated crimes</td>
<td>Victims notify local LE of fraud/loss</td>
</tr>
<tr>
<td>Botnet building begins: Malware infected computers are enlisted into botnet</td>
<td></td>
<td></td>
<td>Private sector actors work with LE, service providers to disrupt or dismantle botnet</td>
</tr>
</tbody>
</table>

Private sector actors identify, investigate and contain botnet

LE obtains court order or MLATs for multi-jurisdiction interdiction

Botnet activity disrupted
Debunking popular myth…

Attackers aren’t *smarter* than responders.

They *are* able to

move faster than responders,

more economically, and

act unencumbered by

law, jurisdiction, contract, interpretation.
The advantages are staked in favor of attackers

Attackers create *their own* attack infrastructure on infected or compromised devices or servers.

Attackers compromise legitimate infrastructures to operate covertly or to encumber investigations.

Attackers don’t need approval, permission, budgets, licenses, or court orders.
<table>
<thead>
<tr>
<th>JURISDICTION</th>
<th>What is the prevailing jurisdiction of content hosting, DNS hosting, domain registration, alleged perpetrators?</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAW</td>
<td>Is this a criminal activity in all relevant jurisdictions?</td>
</tr>
<tr>
<td>CONTRACT, INTERPRETATION</td>
<td>Is a contracted party in breach of an obligation? According to whose interpretation?</td>
</tr>
</tbody>
</table>
Intervention Today: Trust-based Collaboration

- Private- and public sector investigators cooperate 24x7 using trusted communications channels
- Information sharing
  - Malware, phishing, spam samples
  - Host names, URLs, addresses, geo-location
  - Activities of persons of interest (e.g., social media posts)
  - Points of contact (targets, victims, operators, investigators)
- Coordination or hand off
  - Mitigating DDoS by squelching sources
  - Providing evidence of AUP violation to operator for action
  - Triage actions, e.g., block listing, sinkhole, blackhole routing
Trust is Earned

- New participants earn nominations from existing members and are vetted prior to admission
  - Personal references,
  - Prior collaboration,
  - Cryptographic competency
  - Reputation
- Individuals put own reputation and membership at risk when they nominate
- Strict codes of conduct
- Self-policing model
Is trust-based collaboration effective?

Yes. *It reduces the attack surface in several ways:*

- Sharing “data feeds” forms the bases for blocklisting
- Sharing malware samples expedites remediation
- Sharing intelligence improves dossiers on suspected criminal actors
- Reduces time from threat identification to containment or mitigation
- Gives participating law enforcement agents insights other than direct complaints

BUT... it is not a “universal” solution
The APWG AMDoS concept or framework could be applied to other realms. Transparent, accountable vetting process for interveners
Next Challenge: Evolving to formal Public-Private Partnerships

<table>
<thead>
<tr>
<th>Trust-based collaborative communities</th>
<th>Public-Private Trust Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaves ethically. Does not lie.</td>
<td>Provides a transparency and accountability framework that serves the public interest.</td>
</tr>
<tr>
<td>Distinguishes fact from opinion.</td>
<td>Provides disclosure and public review frameworks.</td>
</tr>
<tr>
<td>Is prepared to share data to corroborate what he claims is fact.</td>
<td>Acknowledges that sharing is bidirectional.</td>
</tr>
<tr>
<td>Is willing to admit failure or fault and hold herself accountable.</td>
<td>Is willing to be held publicly accountable.</td>
</tr>
<tr>
<td>is willing to course correct.</td>
<td>Is agile, willingly seeks conflict resolution. Thoughtfully considers multi-stakeholder input.</td>
</tr>
</tbody>
</table>
If we are to effectively intervene or mitigate cybercrime, we must accelerate due process to operate at Internet pace.

Image: https://www.flickr.com/photos/controlarms/
Questions?

Visit us at icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann

Visit me:

@securityskeptic
Facebook.com/securityskeptic
LinkedIn.com/in/securityskeptic/
www.securityskeptic.com