# *Law Enforcement Engagement & Incident Response Handling: NANOG Engagement*


*Paul Ferguson*
*Advanced Threats Research*
*Trend Micro, Inc.*

# *What is the problem?*

- “Web Threats” have become the de facto “low hanging fruit for cyber crime (e.g. compromised webpage with malicious iFrame redirection or JavaScript, leading to “drive by” infections);
- Literally thousands of compromised websites/webpages, leading to thousands of compromised users & botnet zombies;
- All too often, the contact information for the “owners” of compromised websites is incorrect or outdated.
- Which tends to leave a huge procedural mess…

# *As a Security Company, Our Primary Goal: Protect Our Customers*

# *…which means:*

- A Large Staff of Researchers Who:
  - Implement & manage honeypots, sandboxes, reverse-engineer binaries;
  - Incorporate new AV signatures;
  - Incorporate known malicious hosts & URLs into blocking databases for immediate “in-the-cloud” product integration (shorter time-to-implement);
  - Try to notify the owners of compromised websites to remove malicious content
    - Harder, takes time, sometimes impossible (e.g. sheer volume)

# *Our Secondary Goal: Find the Criminals*

# *…which means:*

- A Few Staff Researchers Dedicated to:
  - Working with Law Enforcement
  - Working with the National CERTs/CSIRTs
  - Etc.

# *Make No Mistake:*

- We should never “dumb down” the language that we use to describe this activity – it is criminal.
- In the future, we need to make sure that we refer to these activities as criminal activity -- not some “old school” reference that lessens the language of the crime (e.g. miscreants, hackers, etc.)

# *Some of the Activity We Are Seeing is Now Organized Crime*

- Criminals follow the money.
- And we can expect MUCH more of the same in the near future.
- In fact, even more clever, more convoluted, and more challenging…
- There is apparently enough low-hanging fruit, however, that digital crime is "…enjoying an upswing in sophistication."
- …and basically operating in the open without concern that they will be found or prosecuted.

# *Goals & Desired Results*

- Better two-way communications for all stakeholders:
- Law Enforcement:
  - FBI Cyber Crime Division, U.S. Secret Service, U.S. Treasury Department (IRS), International LEOs (e.g. InterPol, Scotland Yard/London Met, etc.), DHS (US-CERT.gov)
- NGOs (Non-Governmental Organizations)
  - CERT.org, Registries/Registrars, ICANN, the RIRs, Network Operations forums (e.g. NANOG), Financial Institutions (e.g. Banking Security contacts)
- National & Organizational CERTs & Incident Response Teams
  - US-CERT.gov, other FIRST.org –affiliated CERTs
- Develop operational processes to engage & communicate with these organizations, exchange intelligence, in semi- real-time, etc. (e.g. not nsp-sec.)

# *Law Enforcement*

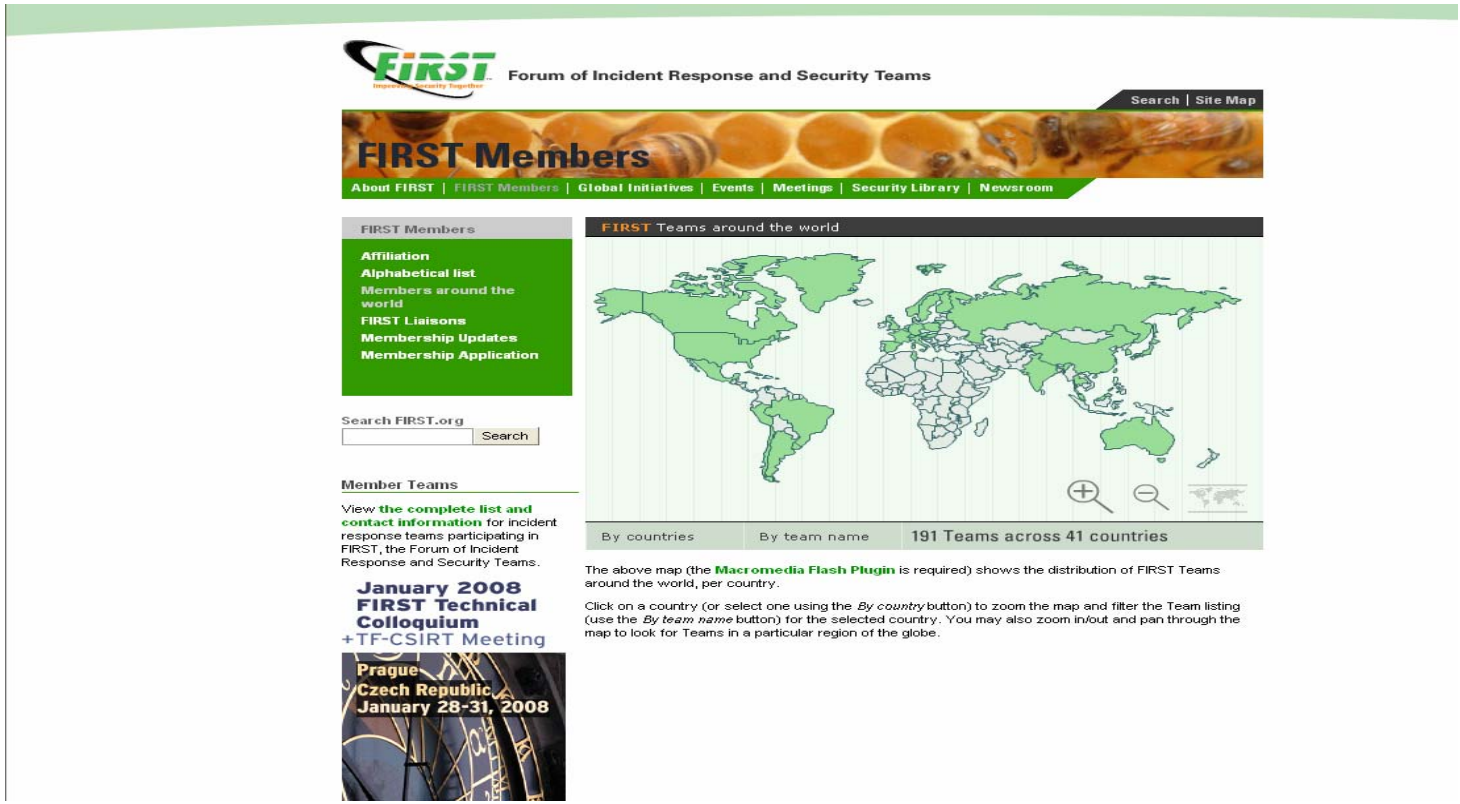
- Need more focus/relationships with International LEO & U.S. local and regional LEO – we (and others) are actively working on this engagement.
- Develop a mechanism for reporting cyber crime which engages the ISPs who may unwittingly be involved (abuse@ contacts do not necessarily seem to be working in most cases)
- Need to also heavily involved in “mutual investigation” exchanges where we can privately (in a limited fashion) engage participants.

# *NGOs*

- Already have some “piecemeal” working relationships with NGO security organizations, but need to be a bit more focused & concerted.
  - Suggest we actively use the FIRST.org affiliate list of CERTs/CSIRTs as a baseline, as well as develop an S.O.P. for all external incidents which warrant notification.
  - Also, actively engaging security-related contacts at various financial institutions, etc. (e.g. Banks, PayPal, eBay, Visa, etc.)

# CERT Contacts

- Use the FIRST.org contact list. It works.



# *ISP and Network Operations Engagement:*

- Not an easy path, but must be done.
- Continual dialogue, understand ISP concerns, etc.
- Some IETF RFCs to note:
  - RFC 2142: Mailbox Names for Common Service, Roles and Functions
  - RFC 3013: Recommended Internet Service Provider Security Services and Procedures
- Unfortunately, not all service providers follow (or are aware of) these guidelines…

# *Develop Relationships with Corporate Abuse & Fraud Contacts*

- Already in process:
  - eBay, PayPal, Google, Yahoo!, AOL, ISPs, etc.
- An ongoing effort…with myriad challenges, problems with engagement.
- Need to develop an processes to immediately interact with these organizations
  - Working on it?

# *The Biggest Challenge: Internal Process*

- Not just “process”, but also “discipline”.
  - When it comes to security stature, discipline is everything.
  - A disciplined process is everything.
- We MUST develop discipline, adhere to our processes, etc. or the Bad Guys™ stay ahead of us.
- NANOG is uniquely positioned to take a leadership role in a program encompassing these principles, and “pull” the rest of the ISP community in this direction
- (Discussion point here.)

# *Summary*

- We’re on the right path, but need some “course corrections”.
- Security notification process is a dire need of attention, industry-wide.
- A larger, organized effort needs to be for most of these external issues.
- Need the NANOG community to “act as one voice” with internal engagement
- Comments and concerns welcomed.
- Discussion.
- Solicitations and suggestions welcome.

***Fin.***

*Questions?*