Prevalence of Malicious DNS and Proposed Solutions

Christopher Davis and Zachary Hanif

Introduction
Chris Davis

- Emerging Threats & University of Toronto Fellow
- IPTrust, DefIntel, Damballa...
- Mariposa, Conficker, Storm...

Introduction
Zach Hanif

- IPTrust, Georgia Tech, GTRI
- Mariposa, Zeus, many other APTs
- Machine Learning, Big Data (Hadoop, Cassandra...)
- Many additional Botnet takedowns and sinkholes

What Are We Doing Now

- 60-80k malware samples processed daily
- 5 separate malware analysis systems
- 10’s of thousands of bad domains per day
- Tracking > 20k active Botnets

The Problem

- Malware is custom designed to evade detection, stay resident, and display coordinated action
- Anti-virus solutions are generally ineffective
  - “...8 out of 10 pieces of malicious code are going to get in.” -Graham Ingram, AUSCERT
  - “Every second, 14 adults become the victim of cyber crime.” -Symantec via theregister.co.uk

Scope of the Problem

- Majority of banks
- Fortune500
- Many international government departments
- Airlines
- Hotel chains
- Oil and gas companies
- Utilities and infrastructure

High Profile Botnet Compromises

- Sony
- RSA
- Google
- Nasdaq
- Dalai Lama
- Mitsubishi Heavy Industries
- UN, International Olympic Committee

Current Response

- Anti-virus
- IDS/IPS - not designed to detect compromises
- Court ordered domain takedowns - too many bad domains, and other issues.
  - See “Guidance for preparing domain name orders, seizures, and take downs” - Dave Piscitello (ICANN)
- NXD mailing list - good but small scale

Proposed Solution

- 100% public benefit non-profit - Malicious domain clearing house / registrar
  - ICANN backed
  - Emerging Threats sponsored
  - Community support (ISC, Dagon, Wesson, etc...)

Goals/Mission

- Analyze immense amounts of malware to identify malicious domains
- Identify, analyze, validate, confirm
- Sinkhole C2s & identify victims
- Notify victims & provide free remediation assistance
- Remove, in a coordinated fashion, malicious domains from registrars

Clearing House Offerings

- Daily bad domain feed (zero error)
- EPP/RPP bad domain transfers/sinkholing
- Bad actor DB with credential and login data for LEO
- Peer reviewed analysis
- Move the bad traffic off your pipe

Technical Challenges

- Identify malicious domains with zero error
  - C2 / Compromised domain
- Bad domain transfer mechanism and fees
- Sinkhole robustness and victim identification
- Victim notification and remediation
  - Must maintain victim privacy while being able to work towards resolution

Social Challenges

- Registrar/registry buy-in
  - Simply cannot work without this support
- Requires substantial support from the community
  - Needs ISPs, NGOs, CERTs, etc for remediation and customer notification
  - Large industry partners (Google, Microsoft, etc)

First Steps

- Provide a per-registrar feed of C2 domains and evidence of their maliciousness
- Support the Snort/Suricata projects through custom rulesets
- New TLD monitoring
    - Easier to prevent an issue then root it out after the fact

Q&A