Indicator Expansion Techniques – Tracking Cyber Threats via DNS and Netflow Analysis

United States Computer Emergency Readiness Team
(US-CERT)
Detection and Analysis
January 2011

Homeland Security

Background

As the number or compromises escalates and our visibility into the network grows it becomes imperative to create automated Operational solutions to feed your Computer Network Defense machine.

Tracking cyber threats through the coupling of DNS data and netflow analysis allows for a much higher level of confidence in identification of malicious activity.

Homeland Security

Tools of the Trade

- The model to be discussed is currently a working concept. The model leverages the following tools
  - Linux
  - Apache
  - MySQL
  - PHP
  - PERL
  - SiLK
  - DNS Tracking DB
  - Various passive DNS feeds

Homeland Security

Approach

- An historical archive (repository) of domain/IP address pair with timestamps
  - validated malicious
  - suspicious
  - Unknown

- Maintain a Master List of vetted malicious domains
  - second level
  - third level
  - fourth and fifth level

- Run Master List of domains against internal repository
  - Create hash of domain/IP pair

Homeland Security

Approach Cont . . .

- Run Master List of domains against external passive DNS sources
  - Create hash of domain/IP pair

- Compare lists between external and internal domain/IP pair
  - Comparing the two paired lists is a safe and accurate methodology for quickly identifying new IP addresses and/or new domain/IP address pair

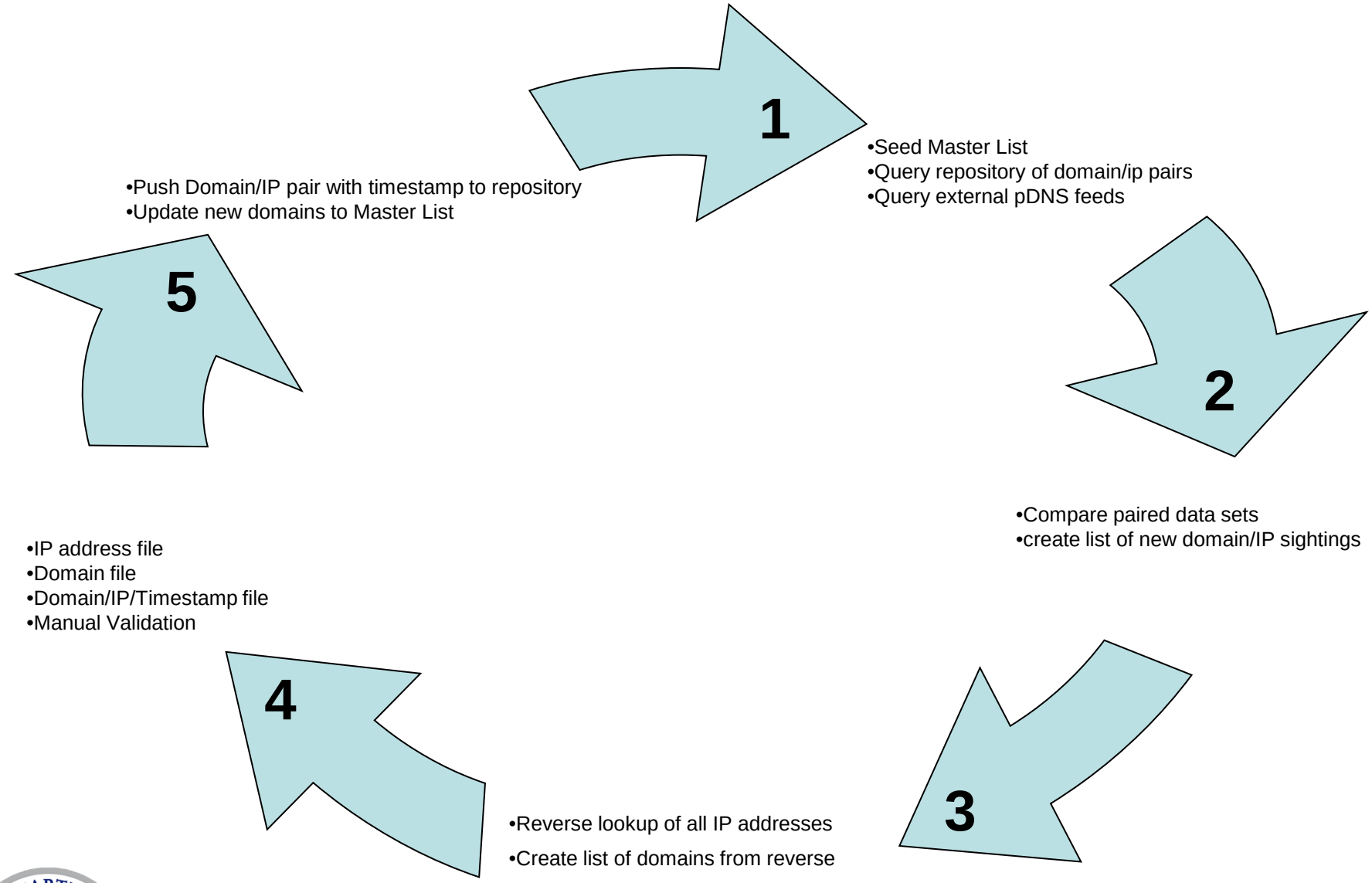
- Run all the identified IP addresses through external passive DNS sources
  - The final outputs
    - Compared list
    - IP address list
    - domain list
    - domain/IP address/timestamp list

Homeland Security

Approach Cont . . .

- Manual validation of all lists
  - Watch for anomalies (dictionary)
  - run away domain lists (vhosts)
- push new vetted findings of domains/IP addresses/timestamps to internal repository
- update master list with new domains

Homeland Security



Homeland Security

Indicators Expansion

- Command and Control Infrastructure
  - *.cars.com (badguy Command and Control domain)
  - *.bikes.org (badguy Command and Control domain)
  - 192.168.2.33 (badguy Command and Control IP)
  - 192.168.2.34 (badguy Command and Control IP)
  - 10.0.2.105 (badguy Command and Control IP)
  - 127.0.0.4 (Domain Parking)

Homeland Security

Indicators Expansion cont …

- wicked.55chevy.cars.com was identified in malware and resolved to 192.168.2.34 on August 6, 2011
  - Second level domain is registered by ‘joebob@mercy.com’

- Passive DNS research on *.cars.com
  - wicked.55chevy.cars.com|192.168.2.34|2011-05-04
  - wicked.55chevy.cars.com|127.0.0.4|2011-05-25
  - 60Dynamic88.cars.com|127.0.0.4|2011-06-07
  - 62GrandPrix.cars.com|127.0.0.4|2011-07-08
  - wicked.55chevy.cars.com|192.168.2.34|2011-08-06
  - wicked.55chevy.cars.com|127.0.0.4|2011-08-07
  - 68GTO.cars.com|127.0.0.4|2011-08-07
  - 55mercury.cars.com|192.168.2.33|2011-08-07

Homeland Security

Indicator Expansion cont …

- Passive DNS research
  - On August 25, 2011 scott.r2addict.bikes.org (new identified domain registered by ‘bob@comfort.com’ resolves to IP address 127.0.0.4
    - scott.r2addict.bikes.org|127.0.0.4|2011-08-25
    - scott.r2addict.bikes.org|10.0.2.105|2011-09-01
    - scott.r2addict.bikes.org|127.0.0.4|2011-09-08
    - scott.r2addict.bikes.org|192.168.2.34|2011-09-09
    - wicked.55chevy.cars.com|192.168.2.34|2011-09-09
  - On September 9, 2011 both scott.r2addict.bikes.org and wicked.55chevy.cars.com resolve to 192.168.2.34 validating a link between the two domains
  - From a single malware sample we now have identified 6 malicious domains, 3 Command and Control IP’s and an unusual parking methodology

Homeland Security

Applying Netflow ‘Current’

- All IP address sets are manually updated and maintained on a SAN using a custom written PERL script called ‘set_manager.pl’
  - The script uses several ‘rw’ SiLK options including but not limited to pmapfilter, rwsetbuild, rwsetintersect
- A daily cron executes a separate script called ‘ipstore_manager.pl’
- Traffic analysis is conducted typically within a 24 hr period of the creation of the store
- Domain research is conducted manually and depending on the date of resolution flow traffic analysis could be on activity that is dated

Homeland Security

Applying Netflow ‘Future’

- To be Integrated in Operational workflow in near future
- All indicators will be managed in the Indicator DB (to replace Master List) and ‘set_manager.pl’
- DNS Tracking DB content will be accessible through Indicators DB interface
  - Allows for easier domain and IP address set management
  - Scripts can parse and properly bucket IP address sets according to their categorization allowing for more accurate traffic stores

Homeland Security

Applying Netflow ‘Future’ Cont …

- Write a wrapper to identify malicious netflow traffic based on the timestamp of domain/IP address pair
  - Spawned from Ed Stoner’s work ‘DNS and Flow’ presentation in 2010
  - Allows for more accurate and targeted netflow query in automation (reduces false positives)

Homeland Security

Technical comments or questions

US-CERT Security Operations Center

Email: soc@us-cert.gov

Phone: +1 888-282-0870

Media inquiries

US-CERT Public Affairs

Email: media@us-cert.gov

Phone: +1 202-282-8010

General questions or suggestions

US-CERT Information Request

Email: info@us-cert.gov

Phone: +1 703-235-5110

* Information available at http://www.us-cert.gov/contact.html

Homeland Security

Questions?

Homeland Security