Security in knowledge

Advanced Malware Sinkholing

Silas Cutler

Dell SecureWorks

Joe Stewart

Dell SecureWorks

RSACONFERENCE2013

Session ID: END-R35B

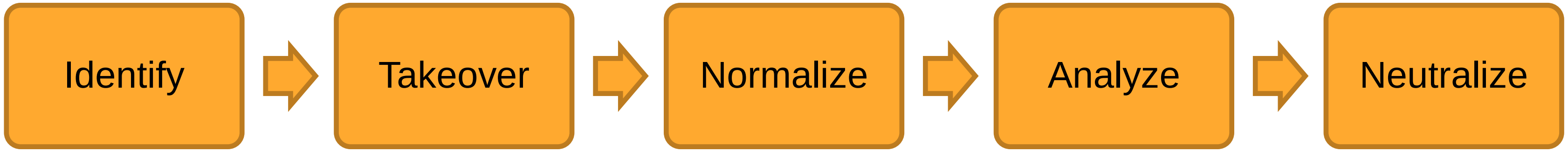
Session Classification: Advanced

Objectives

- Define the types of sinkholes
- Understanding sinkholing operations
- Recognize challenges of sinkhole data analysis
- Identify gained actionable intelligence
- Comprehend risks and threats

Rethinking Sinkholing

- Breaking away from the Sinkholing == Neutralizing mentality
- Objective remains the same: disrupt communications between the malware command and control server
- What is the “Sinkholing Lifecycle”?
  - “No Data Left Behind” mentality
    - How can I make my malware sandbox fuel my sinkhole?
    - Reanimation



Identify → Takeover → Normalize → Analyze → Neutralize

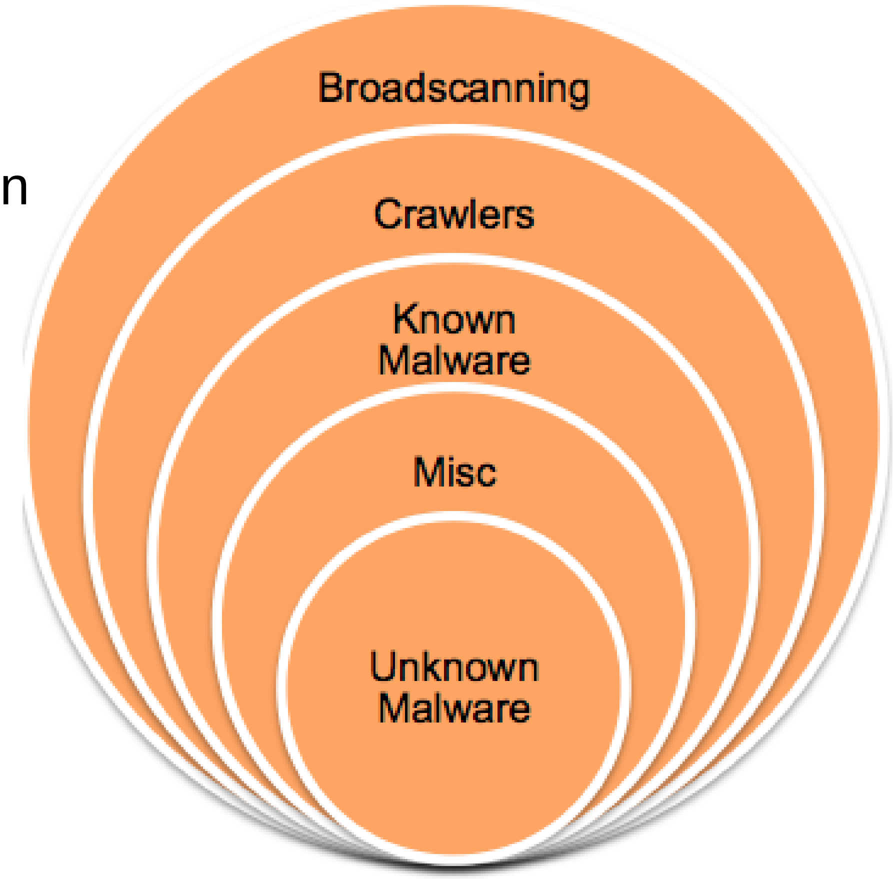
- What can we discover from analysis of these domains?

Setup and Acquisition

- Building a better setup
  - Name server, capturing system, processing system
    - DNS server holds zones for each of our domains with a wild card entry, which points to our sinkhole
    - Capturing system is doing full packet logging
    - Processing system is processing all PCAP files and BIND logs from the systems through Proximity
- Main methods for acquiring domains:
  - Legal
    - Domain takeovers (Brand infringement)
    - Partnerships with registrars
  - Domain Drops
    - Capturing Malicious Domains when they expire

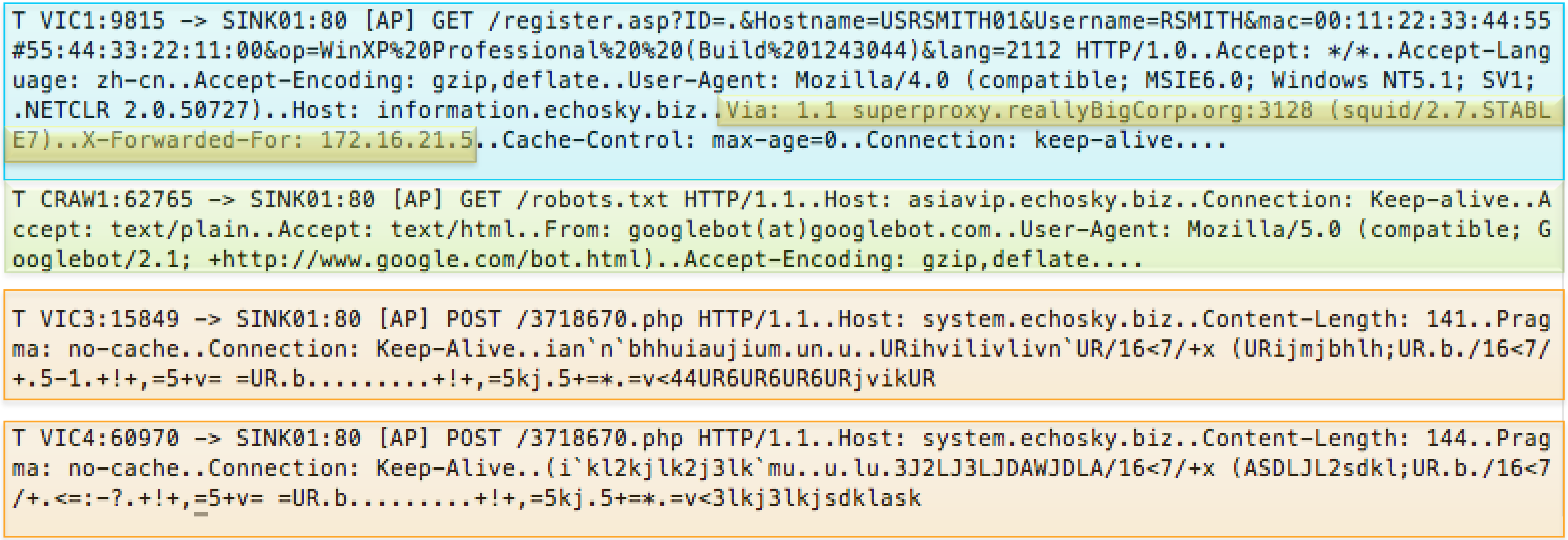
Operations

- Identify and classify all incoming connections
  - Sorting
  - Identify the known and unknown malware
  - Classify incoming IP to associated domain
- Monitoring



Operational Tricks

- Identifying Victim through decoding phone home requests
- Finding the needles in the hay stack



```
T VIC1:9815 -> SINK01:80 [AP] GET /register.asp?ID=.&Hostname=USRSMITH01&Username=RSMITH&mac=00:11:22:33:44:55
#55:44:33:22:11:00&op=WinXP%20Professional%20%20(Build%201243044)&lang=2112 HTTP/1.0..Accept: */*..Accept-Lang
uage: zh-cn..Accept-Encoding: gzip,deflate..User-Agent: Mozilla/4.0 (compatible; MSIE6.0; Windows NT5.1; SV1;
.NETCLR 2.0.50727)..Host: information.echosky.biz..Via: 1.1 superproxy.reallyBigCorp.org:3128 (squid/2.7.STABL
E7)..X-Forwarded-For: 172.16.21.5..Cache-Control: max-age=0..Connection: keep-alive....
```

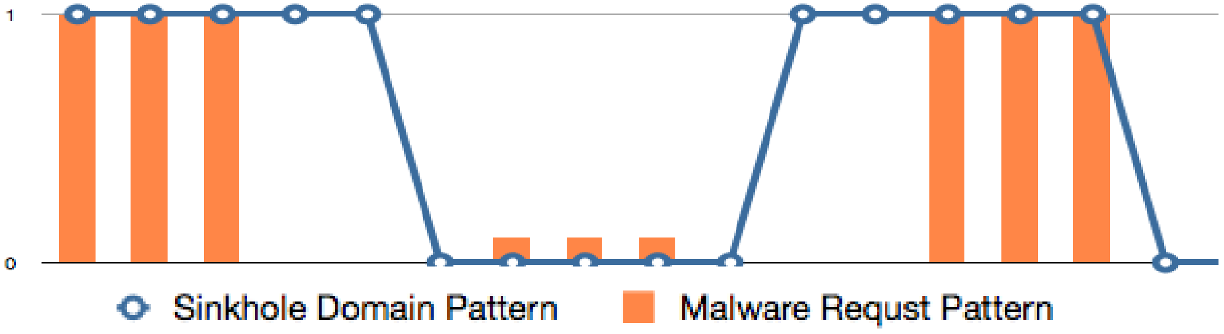
```
T CRAW1:62765 -> SINK01:80 [AP] GET /robots.txt HTTP/1.1..Host: asiavip.echosky.biz..Connection: Keep-alive..A
ccept: text/plain..Accept: text/html..From: googlebot(at)googlebot.com..User-Agent: Mozilla/5.0 (compatible; G
ooglebot/2.1; +http://www.google.com/bot.html)..Accept-Encoding: gzip,deflate....
```

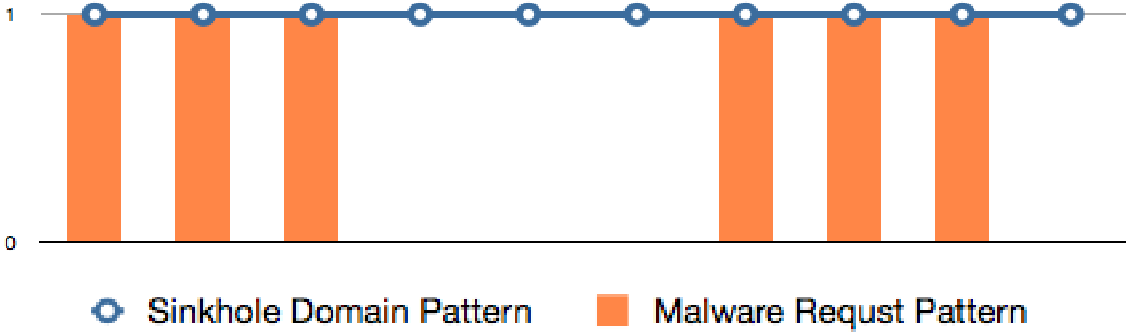
```
T VIC3:15849 -> SINK01:80 [AP] POST /3718670.php HTTP/1.1..Host: system.echosky.biz..Content-Length: 141..Prag
ma: no-cache..Connection: Keep-Alive..ian`n`bhhuiaujium.un.u..URihvilivlivn`UR/16<7/+x (URijmjbhlh;UR.b./16<7/
+.5-1.+!+,=5+v= =UR.b.........+!+,=5kj.5+=*.=v<44UR6UR6UR6URjvikUR
```

```
T VIC4:60970 -> SINK01:80 [AP] POST /3718670.php HTTP/1.1..Host: system.echosky.biz..Content-Length: 144..Prag
ma: no-cache..Connection: Keep-Alive..(i`kl2kjlk2j3lk`mu..u.lu.3J2LJ3LJDAWJDLA/16<7/+x (ASDLJL2sdkl;UR.b./16<7
/+.<=:-?.+!+,=5+v= =UR.b.........+!+,=5kj.5+=*.=v<3lkj3lkjsdklask
```

Operation Tricks (Cont.)

- Domain “bumping” w/ Proximity Flux Echo





Proximity

- Toolkit for managing Public Safe Host Sinkhole
- Automates most of Operations
  - Anomaly Detection
  - Filtering
  - Reporting
  - Statistics
  - Storage
- Reads in PCAP Files and BIND9 DNS logs
- Databases all incoming connections
- Perl / MySQL
- Open Source

Risks and Threats

- Retaliation
  - Data floods
  - Data theft / Compromise of Sinkhole
- Legal / Authorities
  - Staying within boundaries of hosting / ISP ToS
  - Take down requests
  - Blue on blue domain hijacking
- Victim Disclosure
  - i.e. No good deed goes unpunished

Take Away Points

- Two primary types of sinkholes
- Operations are a daily task that require careful analysis
- Through analysis of traffic, we can identify new malware families and victims.
- Risks are ever present from external threats from both threat actors and the misinformed
- The data and intelligence makes up for the risks and costs of operations

Resources

- GitHub / Source: http://github.com/silascutler/Proximity
- Mailing List: https://oid.tisf.net/mailman/listinfo/proximity
- “How Big is Big? Some Botnet Statistics”
  - http://www.abuse.ch/?p=3294
- “How Domain Name Registrars can can help us in the war against botnets”
  - http://www.simplysecurity.com/2011/05/16/how-domain-name-registrars-can-help-us-win-the-war-against-the-botnets/

Contact

- Silas Cutler
  - Email: Silas@CounterThreatUnit.com
  - Web: www.SilasCutler.com
  - Twitter: @silascutler
- Joe Stewart
  - Email: jstewart@CounterThreatUnit.com
  - Web: www.JoeStewart.org
  - Twitter: @joestewart71

Security in knowledge