HIDDENSALAMANDER

Alerting and Characterization of Botnet Activity in TURMOIL

Briefers:
(S//REL) High Level Goals

⊙ Detect (all!) botnet activity on our sensors

- Alert **only** when activity is relevant and time-sensitive
  » Involves entities/commanding of high interest
  » Involves protected areas
  » Could initiate defensive action

- Generate metadata **always**
  » Aids in attribution and retrospective analysis

- Enrich metadata as much **as possible**
  » Alleviate the need for in-depth knowledge of actors or malware
(S//REL) Approach

HIDDENDATA

1. Analyze Packets
   - Post-Process
     - Light Decrypt (future)
   - Decode, Detect Encryption, ...

2. Gather specialized knowledge

3. Apply generic Knowledge
   - Apply 5-tuple metadata, SID, SIGAD, ...

4. Process Payload for "targets", BotlIDs, channels, nicknames, add directionality...

5. Track C2 (IP and SID) over a period of activity, document bots

6. Track over Event's time

7. Summarize Activity
   - Report Overall "Event"

8. Report Instance
   - Alert on single event

Similar to Traditional "Phishing Activity"
(S//REL) Concept/Idea Behind It

- **Support Attribution**
- **Association**
- **Discovery**
(S//REL) What we offer today

- An extensible botnet processing service
  - Capabilities are added via configuration or specialized processors
- The ability to track events spanning across 5-tuples
  - Enables production of Event Summaries and Enrichment
- Geographical dispersion
  - SIGINT perspective, currently at SCS sites and MHS (prototype)
- TURMOIL augments Defensive Efforts two fold
  - Early warning Tips for defensive action (to NETEZZA, then TUTELAGE)
  - Metadata for characterization and to support attribution (to GMPLACE and RONIN, then CYBERCLOUD and MARINA).
(S//REL) Progress over the last year

🔗 Advancements

- Zeus RC4 encrypted processing flow
- Base64 decoding e.g. BEB v1.8 target IP extraction
- Limited Metadata Enrichment
  » Case Study to support QBOT activities
- Deployment to F6 sites and a second system at MHS
- Established ASDF to GMPLACE for GHOSTMACHINE analytics
- Established flow to NETEZZA (TURQI) for validation
- Defined Botnet Lifecycle Model for categorizing enrichment metadata
(S//REL) Current Development Focus

- Attain analyst validation
  - Ingest into GM and creating Views
  - End-to-end dataflow validation
- Improve Metadata Enrichment capabilities
  - Define generic model to create metadata PCRE rules
  - Refine Enrichment Model for Malware
- Improvements to function as a framework/service
  - Greater focus on metadata enrichment
- Provide dynamic AEG tasking
- Re-factor Tasking and Tips to fit botnets
  - Update Tip format to closely align with extracted data
- Add specialized packet processors
  - Mariposa
  - Looking for opportunities
(S//REL) Future Work

♫ Initial development
  - Initiate promotion (to XKS) or collection flows
  - Re-factor SEG to make Metadata Enrichment more flexible
  - Redesign the Analytic to provide more valuable Summaries
    » Possibly detect point of origin of Herder commanding

♫ Biggest Challenges
  - Currently have no means to track peer-to-peer botnet activity
    » May look to current TURMOIL Fast Flux capabilities for ideas
  - Encrypted bots defeat most attempts at tracking and reporting
    » Possible candidate for TURMOIL Re-Injection flow
The Components

- **BotDiscoveryAeg**
  - Not A Snort based Application.
  - Ingests translated Snort signatures and tasks the FSPF.
  - Emulates Snort behavior as closely as possible.

- **RC4Aeg/RC4Seg**
  - Highly specialized components aimed at detecting RC4 Encrypted Zeus activity

- **MariposaAeg (Currently in development)**
  - Highly specialized – detects and decodes a particular encoding.

- **BotDiscoverySeg**
  - De-dups on SID/5 Tuple for Tipping and MARINA.
  - De-dups on SID/IP/Port for BotAnalyticSeg.

- **BotAnalyticSeg**
  - Summarizes Event Metadata from BotDiscoverySeg.
  - Provides metadata to RONIN.

- **CIDR Block/SID Filter**
  - Filters Tip Events based on IP information OR SID.

- **cwbBot**
  - Translates Tip messages to adhere to TRAFFICTION schemas.
(S//REL) Current Dataflow

Events

Passive Collection Sensor

ASDF Summarized Output

How to Use it?

NETZEZZA

TurQi
Turnabout Query Interface

ingest
normalize
aggregate
write

GMPLACE

consume
display

DB/WEB

CYBERCLOUD
(TS//SI//REL) Prototype View - POUNDSAND

**POUNDSAND Prototype Incubator**

### Queries

- **Welcome**
- **BotNet Family**

#### Botnet Families

- LT: VILNIUS, Donbot, Control Channel
- IQ: ASSULAYMANIY, Donbot, Control Channel
- RU: MOSCOW, Donbot, Control Channel
- LY: TRIPOLI, Donbot, Control Channel

#### Bots

- LB: BEIRUT, Donbot
- TM: ASHGABAT, Donbot
- LB: BEIRUT
- LB: BEIRUT
- IQ: ASSULAYMANIY
- IQ: BAGHDAD
- NL: AMSTERDAM
- TM: ASHGABAT
(TS//SI//REL) HIDDENSALAMANDER Outputs

Who?
What else can we tell today?
ROLE of the IPs involved: Is it a Bot Controller? Bot Victim? Target?
Who is the Target of this activity? (for certain botnets)
Who has this Bot Controller been commanding (over time)?
What botnet families are active in this region? How active?

What?
What will we tell tomorrow?
What “Attack” commands are active that we could use to exploit?
What type of botnet activity is seen in this region? For this bot family?
- (e.g. Increased “Infections” in US, or, most BadBot activity is “Reconnaissance”)
What actual [server, filename, command, IP, url] did they send/grab/connect to?
## Optional Payload Details

<table>
<thead>
<tr>
<th>Stage Name</th>
<th>Stage Instance</th>
<th>Optional Attribute</th>
<th>Optional Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Display/Adjust Bot Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Redirect Traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flush DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mode Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connect to Server</td>
<td>Server IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Infection/Exploit</strong></td>
<td>Update</td>
<td>Server IP</td>
<td>Web Address</td>
</tr>
<tr>
<td></td>
<td>Download</td>
<td>Server IP</td>
<td>Web Address</td>
</tr>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>DNS/IP/Host Resolve</td>
<td>A Record (multiple)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Display Network Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Display System Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Scan Enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Scan Disable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Harvest</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C&amp;C Communication</strong></td>
<td>Disconnect</td>
<td>Server IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connect</td>
<td>Server IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log In</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log Out</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current Bot Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove Bot</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terminate Bot</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Attack</strong></td>
<td>Execute File</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DDOS</td>
<td>Type (Syn, Http…)</td>
<td>Target IP</td>
</tr>
<tr>
<td></td>
<td>Open File</td>
<td>File Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat Execute Command</td>
<td>Command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute Command</td>
<td>Command</td>
<td></td>
</tr>
</tbody>
</table>
“Categorizing” Existing Signatures

Most popular bot signature analyst repositories:
- BLUESMOKE: Snort Rules
- XKEYSCORE: Fingerprints

Requires author to add extra detail to the existing signature

Requires front end tools to add extra fields to their GUIs for analyst input
- Suggested that the Lifecycle Stage Group and Stage Instance be required for submission for botnet signatures
- Other attributes may be optional for submission
Bot Characterization Proposed Flow

Analysts will develop signatures and include required metadata for submission.

TURMOIL HS will generate bot protocol tasking and accept tasking from repositories.

Metaldata Produced and Consumed

[Hidden Salamander]

Map-Reduced Job Results Available

CyberCloud produces analytic results from all incoming data sources. RONIN provides immediate hardware characterization info.

Analyst Search Results Available

GoGadget displays analytic results from CyberCloud and detailed metadata for the analyst.
Questions???
Example

- **Command Found:**
  20;3000;10;0;0;30;300;20;20;2000;3000#flood http #1#xK3_2893BC90

- **How alert describes it:**
  
  IP SRC/DEST: 1.1.1.1 / 2.2.2.2
  PORT TO/FROM: 234/123
  SIGAD/CASN:
  SID: 12345
  SIGNATURE NAME: BEB:BlackEnergy_DDoS_X_of_Y
  TIME: 00:00:00

- **How summary describes it today:**
  
  IP SRC 1.1.1.1 PORT: 123 [ROLE: C2]
  IP DEST a.a.a.a PORT: 234 [ROLE: BOT]
  b.b.b.b ...
  z.z.z.z ...
  SIGAD/CASN:
  SID: 12345
  SIGNATURE NAME: BEB:BlackEnergy_DDoS_X_of_Y
  TIME: 00:00:00 – 00:00:10
  FAMILY: BEB
  Total Events: 51
Example

Command Found:
20;3000;10;0;0;30;300;20;20;2000;3000#flood http#1#xK3_2893BC90

How Summary describes it (tomorrow):
IP SRC 1.1.1.1 PORT: 123 [ROLE: C2]
IP DEST a.a.a.a PORT: 234 [ROLE: BOT]
   b.b.b.b ..
      z.z.z.z ...
SIGAD/CASN:
SID: 12345
SIGNATURE NAME: BEB:BlackEnergy_DDoS_X_of_Y
FAMILY: BEB
TIME: 00:00:00 – 00:00:10
Total Events: 51
CONFIGURATION / BOTID: xK3_2893BC90
ATTACK / DDOS / COMMAND: 20;3000;10;0;0;30;300;20;20;2000;3000#flood http#1#xK3_2893BC90
ATTACK / TARGET:
Example #2

.command found:
JOIN :#marCh2#<crlf>:TESTING1.Virus.HERE 332 virus-squadIr #marCh2# :!N Zend.marCh2
http://[REDACTED]/page/file.jpeg aFile.exe 1<crlf>

How alert describes it:
We don’t want alert! It’s insignificant for defensive activity!

how summary describes it today:
IP SRC 1.1.1.1 PORT: 123 [ROLE: C2]
IP DEST a.a.a.a PORT: 234 [ROLE: BOT]
  b.b.b.b ..
  Z.Z.Z.Z ..
SIGAD/CASN: 
SID: unknown!!!
SIGNATURE NAME: botnet/quantumbot/possible_download1 (XKS Fingerprint-derived)
TIME: 00:00:00 – 00:00:10
FAMILY: IRC_GEN
Total Events: 3
Example

 несколькo:
JOIN :#marCh2#<crlf>:TESTING1.Virus.HERE 332 virus-squadlr #marCh2# !NAZELmarCh2
http://[REDACTED]/page/file.jpeg aFile.exe 1<crlf>

How Summary describes it (tomorrow):
IP SRC 1.1.1.1 PORT: 123 [ROLE: C2]
IP DEST a.a.a.a PORT: 234 [ROLE: BOT]
  b.b.b.b ..
  z.z.z.z ...
SIGAD/CASN:
SID: unknown!!!
SIGNATURE NAME: botnet/quantumbot/possible_download1 (XKS Fingerprint-derived)
FAMILY: IRC_GEN
TIME: 00:00:00 – 00:00:10
Total Events: 3
CONFIGURATION / BOTID /NICKNAME: virus-squadlr
C&C COMMS / CONNECT / CHANNEL: #marCh2#
C&C COMMS / CONNECT / SERVER: TESTING1.Virus.HERE
INFECTION / UPDATE / COMMAND: !NAZELmarCh2 [REDACTED] aFile.exe 1