72 Hrs of Incident Response

an I.R. lifecycle
with pwrcycle
CV: pwrccycle

I've worked for the 3 largest DDoS companies:

- Prolexic (bought by Akamai)
- Verisign (DDoS SOC)
- Defense.net (bought F5 Networks)

Apple's SIRT

- Flashback: Largest Mac Botnet
- Pintsized: ATP Malware targeting Silicon Valley companies
- iOS “In-App Purchases” hack via DNS Change/Hijacking
Incident Response Preparation

Know thy self:

( Obligatory Sun Tzu quote, presented as a Bash If statement):

If [ ( know_yourself=1) and ( know_enemy=1 ) ] ;
    echo “you need not fear the result of a hundred battles.”;
elif [ ( know_yourself=1) and ( know_enemy=0 ) ]
    echo “for every victory gained you will also suffer a defeat”;
elif [ ( know_yourself=0 ) and ( know_enemy=0) ] ;
    echo “you will succumb in every battle.”
fi
 Incident Response Timeline

Day 1.  {Friday before a long weekend}

Noon  - You’re at lunch, it begins & you don’t know.
1pm   - Support tickets, Twitter/Reddit complaints
2pm   - Press Reports (Gawker/NYTimes)
3pm   - Internal recognition of a problem
4pm   - Gather Facts
5pm   - Conf Call (Circle the Wagons)
<table>
<thead>
<tr>
<th>Internal</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems - NOC</td>
<td>+ Users - Twitter, Reddit</td>
</tr>
<tr>
<td>Networking - Net. Eng.</td>
<td>- Forums</td>
</tr>
<tr>
<td>Database - Application</td>
<td>- Support Tickets</td>
</tr>
<tr>
<td></td>
<td>+ Hosting Provider</td>
</tr>
<tr>
<td></td>
<td>- Logging &amp; Graphs</td>
</tr>
</tbody>
</table>
Circle the Wagons Conf. Call

Internal Stakeholders. (No more than 10 people)
1. Business - VP of something
2. Database - Application Owner
3. Systems - NOC (Servers/LBs/DNS/Monitoring)
5. Security - SOC/SIRT (PCI, HIPAA, PII)

Sales, Dev., Marketing, Kibitzers
Incident Response Timeline

Day 2. {Groundhog Day}

6pm-6am - Implement a solution.
9am - Test Changes (separate IP)
Noon - Go live vs the attack
1pm - Conf Call (hopefully 2nd and last call)
5pm - End of day update
Incident Response Timeline

Day 3. {... and there was much rejoicing}

9am  - New Attack
Noon - Review of solution vs new attack.
1pm  - {Back to day 2?}
5pm  - Final Event report.
Incident Response Preparation

Know thy self:

Logging
- User-Agent & Referer

Graphs
- Network, CPU, RAM

pcaps
- Network Taps/Spans & on server
What to say publicly:

1. Publicly acknowledge the problem.
2. Tell people you are taking action to fix it.
3. Tell them when to expect an update.

“There is an issue with the {website/app/etc}.”
“We are conducting maintenance.”
“We will have an update {soon}.”
Change Control Control

1. DNS
   - Password to {Register/GoDaddy/etc}?
   - TTL (1 hr or 24 hrs?)

2. Who holds the HTTPS Cert & Key?

3. Who’s in charge?
   - Who authorizes changes?
   - Who authorizes “It’s working.”?
Links

Ten Strategies of a World-Class Computer Security Incident Response Team
by Carson Zimmerman @ Schmoocon 2013
https://www.shmoocon.org/speakers_2013#strategies

China's Man-on-the-Side Attack on GitHub
Tuesday, 31 March 2015
http://www.netresec.com
http://netres.ec/?b=153DB4E
http://netres.ec/?b=153DB4E
DDoS Attack Types

UDP Reflection Floods

- DNS : port 53
- NTP : port 123
- SSDP : port 1900
- CharGen : port 19