THE HARD PROBLEMS IN SECURITY
(WE STILL CAN’T GET THE BASICS RIGHT)

Ming Chow
Email: mchow@cs.tufts.edu
Twitter: @0xmchow
A LIST OF BRIGHT SHINY OBJECTS SEEN IN SECURITY PRODUCTS AND STARTUPS (OR BUZZWORD HELL)

- APTs
- Machine Learning
- Comprehensive cybersecurity
- Real-time monitoring
- Behavioral analysis
- Next-gen <FILL IN THE BLANKS> (thanks Russell butturini)
- Xgen
- Cloud-enabled
Changing Yahoo passwords will be just the start for many users. They'll also have to comb through other services to make sure passwords used on those sites aren't too similar to what they were using on Yahoo. And if they weren't doing so already, they'll have to treat everything they receive online with an abundance of suspicion, in case hackers are trying to trick them out of even more information.

The company said as much in an email to users that warned it was invalidating existing security questions — things like your mother’s maiden name or the name of the street you grew up on — and asked users to change their passwords. Yahoo also said it was working with law enforcement in their investigation and encouraged people to change up the security on other online accounts and monitor those accounts for suspicious activity as well.

"Here are the 61 passwords that powered the Mirai IoT botnet" (top right picture): [http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html](http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html). Source code: [https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ecec1de8b245bcd5ff802/mirai/bot/scanner.c](https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ecec1de8b245bcd5ff802/mirai/bot/scanner.c)


The data set includes 100 separate internal penetration test engagements spanning 75 unique organizations. The top four attack vectors are based on utilizing stolen credentials.


---

**The Approach**

The following table represents the top five attack vectors used by Praetorian between 2013 and 2016 as part of a complete corporate network compromise kill chain. This list was last updated in June 2016 and is based on a review of 100 reports.

<table>
<thead>
<tr>
<th>RANK</th>
<th>FINDING</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Weak Domain User Passwords</td>
<td>66%</td>
</tr>
<tr>
<td>2</td>
<td>Broadcast Name Resolution Poisoning (aka WPAD)</td>
<td>64%</td>
</tr>
<tr>
<td>3</td>
<td>Local Administrator Attacks (aka Pass the Hash)</td>
<td>61%</td>
</tr>
<tr>
<td>4</td>
<td>Cleartext Passwords Stored in Memory (aka Mimikatz)</td>
<td>59%</td>
</tr>
<tr>
<td>5</td>
<td>Insufficient Network Access Controls</td>
<td>52%</td>
</tr>
</tbody>
</table>

*Table 1:* Praetorian's top internal findings based on frequency of occurrence in kill chain
~1M German Telekom routers have been knocked offline. One of the main models is vulnerable a nasty SOAP RCE bug: isc.sans.edu/forums/diary/P...

FWIW, exploit appears to be textbook OS command injection, subject of every OWASP Top 10 / CWE Top 25 list dating back to 2007
SO HOW DID YOUR EXPENSIVE SECURITY PRODUCT DO?

WannaCry: 75,000 detections in 99 countries — so far. Did they not have AV, or it just didn’t work? Billions wasted each year on crap.

$81,000,000,000 later: "survey found 35% of companies suffered 2 or more breaches in the last 12mo. 3 in 5 expect to be breached in 2017..."

Sources: https://twitter.com/jeremiahg/status/863183321408393222
https://twitter.com/jeremiahg/status/866783974311444480
### Top 10 vulnerability categories overall

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>% APPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Leakage</td>
<td>72%</td>
</tr>
<tr>
<td>Cryptographic Issues</td>
<td>65%</td>
</tr>
<tr>
<td>Code Quality</td>
<td>62%</td>
</tr>
<tr>
<td>CRLF Injection</td>
<td>53%</td>
</tr>
<tr>
<td>Cross-Site Scripting</td>
<td>50%</td>
</tr>
<tr>
<td>Directory Traversal</td>
<td>49%</td>
</tr>
<tr>
<td>Insufficient Input Validation</td>
<td>44%</td>
</tr>
<tr>
<td>Credentials Management</td>
<td>41%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>32%</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>25%</td>
</tr>
</tbody>
</table>

### Percentage of applications passing OWASP Top 10 policy

<table>
<thead>
<tr>
<th></th>
<th>DID NOT PASS</th>
<th>PASSED</th>
</tr>
</thead>
<tbody>
<tr>
<td>v7 - 2016</td>
<td>61.4%</td>
<td>38.6%</td>
</tr>
<tr>
<td>v6 - 2015</td>
<td>67.7%</td>
<td>32.3%</td>
</tr>
</tbody>
</table>

### Percentage of applications passing CWE/SANS Top 25 policy

<table>
<thead>
<tr>
<th></th>
<th>DID NOT PASS</th>
<th>PASSED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>65.8%</td>
<td>34.2%</td>
</tr>
</tbody>
</table>

Source: Veracode’s State of Software Security 2016
@ramonkrikken @Veracode 50% of web apps tested in 2016, have XSS vulnerabilities-
@Gartner_inc #GartnerSEC

6:40 AM - 13 Jun 2017

2 Retweets  1 Like
SQLi prevalence on first scan

All first static scans between 2013 and first half of 2017.

Mean: 31.9%
SD: 0.36%

Fix rate by application on 3rd scan

https://www.slideshare.net/SarahGibson17/sympathy-for-the-developer
THE MOST COMMON ATTACKS AND SECURITY ISSUES ARE THE MOST DIFFICULT TO SOLVE TOO

- Phishing and social engineering
- SQL Injection
- Password reuse
- Distributed Denial of Service (DDoS)
- Attribution
- Writing secure code
- Connecting and communicating with non-technical folks and the policymakers (policy)
BUT WE HAVE AN INFATUATION WITH THE SEXIEST ATTACKS

Source: “Fortune 100 InfoSec on a State Government Budget” by Eric Capuano, presented at the Speaker Workshops, Packet Hacking Village at DEF CON 25. https://docs.google.com/presentation/d/1Np57U13aly15Glw76Qv0l6CWw4PlmPtQPxg4Cdj8r20/edit#slide=id.p
Work Smarter - **Know Your *Actual* Threats**

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels."

- John C. Inglis, Former Deputy Director, National Security Agency 2015.07.09

<table>
<thead>
<tr>
<th>Agent</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrel</td>
<td>927</td>
</tr>
<tr>
<td>Bird</td>
<td>461</td>
</tr>
<tr>
<td>Snake</td>
<td>84</td>
</tr>
<tr>
<td>Raccoon</td>
<td>76</td>
</tr>
<tr>
<td>Rat</td>
<td>41</td>
</tr>
<tr>
<td>Marten</td>
<td>23</td>
</tr>
<tr>
<td>Beaver</td>
<td>15</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>13</td>
</tr>
<tr>
<td>Human</td>
<td>3*</td>
</tr>
</tbody>
</table>

Credit: [http://cybersquirrel1.com/](http://cybersquirrel1.com/)  
*(the only reputable source on ‘Cyber Squirrel 1’ Ops)*

Source: “Fortune 100 InfoSec on a State Government Budget” by Eric Capuano, presented at the Speaker Workshops, Packet Hacking Village at DEF CON 25.  
[https://docs.google.com/presentation/d/1Np57Ul3al5Glu76Qv0l6CWw4PjmtQPxg4Cdj8r20/edit#slide=id.p](https://docs.google.com/presentation/d/1Np57Ul3al5Glu76Qv0l6CWw4PjmtQPxg4Cdj8r20/edit#slide=id.p)
Where we fail

- Algorithms & Protocols
  (sometimes)
- Engineering & Implementation
  (often)
- Systems & Applications
  (almost always)
SO WHAT OPTIONS DO WE HAVE?

(Photo is from Matt Blaze and Sandy Clark’s talk “Crypto War II: Updates from the Trenches” at The Eleventh HOPE Conference)
WHAT’S THE POINT?

• We (still) can’t even get the basics right.
• We are still battling vulnerabilities known for decades.
• We need to rethink and think hard about the basics issues and what’s really important.
• We need to keep it simple; complexity is an enemy of security (one of the “Trinity of Trouble” –Gary McGraw).
WHAT WE REALLY NEED TO DO

• “Be more boring.”
• Inform and talk to those who are curious
• Build relationships with especially those in policy or in government.
  • Sadly, these are not new messages. First channeled to me by Ed Felten at the USENIX Annual Conference in 2004!
• Invest in training and mentoring developers.
• Invest in training and mentoring the younger generation, especially those in K-12 and undergraduates.
The fundamental flaw exploited in WannaCry — ransomware that infected hundreds of thousands of machines in under a week in May — had already been patched by Microsoft at the time of the attack. The infected machines had all put off updating their systems. NotPetya, which spread about three weeks later, used the same flaw.

Most high-profile research is in novel attacks, previously unseen security flaws in software and large — sometimes nation-driven — political actors. But most attacks use well-worn techniques like phishing and other forms of fraud and security vulnerabilities that have long since been patched.

BUT IT MAY BE TOO LATE?

Source:
https://twitter.com/gdead/status/892547412308480032

Bruce Potter
@gdead

This is a sign that we (sec/IT pros, tech execs, and academia) have failed & now pay the price. Legislation is a heavy hand and it will hurt

Pwn All The Things @pwnallthethings
Senators introduce IoT Cybersecurity Improvement Act; requires USG’s IoTs be patchable; have no hard-coded passwords scribd.com/document/35526...

5:47 PM - 1 Aug 2017
2 Retweets 4 Likes
REFERENCES

- https://twitter.com/ErrataRob/status/800161662900772866
- https://twitter.com/kennwhite/status/803274803243286528
- https://twitter.com/SushiDude/status/803401771158749184
- https://isc.sans.edu/forums/diary/Port%207547%20SOAP%20Remote%20Code%20Execution%20Attack%20Against%20DSL%20Modems/21759/