Proven Security Solutions for Higher Education

Visit Us at Start up Alley for EDUCAUSE 2017!

Andrew Scheifele, PhD
Salty Cloud, PBC

• We deliver unique, proven-at-scale info-sec solutions

• Built from bottom up in EDU for EDU

• Purpose-built for highly distributed and regulated environments

saltycloud.com

Salty Cloud is a Public Benefit Company
Saltycloud Team

• Leadership Team - serial SaaS startup experience, worldwide product launch experience at scale

• Product developers have extensive DevOps security background:
  
  • CISSP, CIFI, GCIH-G, GREM, GREM-G, GCIA, GSSP-JAVA, GXPN, CNSS/NSA 4011, GSEC x2, GWAPT x3
Saltycloud Products

- **DORKBOT**
  - Automatically scan and assess vulnerabilities on high-risk web applications

- **STACHE**
  - Securely store and share encryption keys and other sensitive credentials

- **ISORA**
  - Easily conduct scalable organization-wide risk assessments

- **SENF**
  - Quickly identify sensitive numbers across systems

- **PANOPTICON**
  - Efficiently consolidate and automate incident management. Security Orchestration, Automation and Reporting (SOAR) workflow
Cyber Crime Costs Projected To Reach $2 Trillion by 2019

IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'

Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021

Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020
<table>
<thead>
<tr>
<th>Company/Event</th>
<th>Date/Details</th>
<th>Breach Size (Millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo (Aug '13, revealed Dec '16, updated Oct '17)</td>
<td></td>
<td>3,000</td>
</tr>
<tr>
<td>River City Media (Feb '17)</td>
<td></td>
<td>1,370</td>
</tr>
<tr>
<td>Yahoo (2014, revealed Aug '16)*</td>
<td></td>
<td>500</td>
</tr>
<tr>
<td>MySpace (May '16)**</td>
<td></td>
<td>427</td>
</tr>
<tr>
<td>Friend Finder Network Inc (Oct '16)</td>
<td></td>
<td>412</td>
</tr>
<tr>
<td>US Voter database (Dec '15)</td>
<td></td>
<td>191</td>
</tr>
<tr>
<td>Adobe (Sep '13)</td>
<td></td>
<td>152</td>
</tr>
<tr>
<td>eBay (Mar '14)</td>
<td></td>
<td>145</td>
</tr>
<tr>
<td>Equifax (May-Jul '17, reported Sep '17)</td>
<td></td>
<td>143</td>
</tr>
<tr>
<td>Heartland (Jan '09)</td>
<td></td>
<td>130</td>
</tr>
<tr>
<td>LinkedIn (Jun '12, revealed May '16)</td>
<td></td>
<td>117</td>
</tr>
<tr>
<td>VK (Jun '16)</td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>
Web Application Attacks Remain The #1 Source of Data Breaches

- Web Attacks Increasing 35% yr/yr
- SQLi remains the #2 source of web application attack breaches
- SQLi Attacks increasing 28% yr/yr
- Web App vulnerability market > $600 Million and estimated to be $1.2 Billion by 2019

1. Verizon Data Breach Investigation Report (DBIR) 2017 (excluding bot-net activity)
3. IDC 2016
Dorkbot - Intro

- Dorkbot is a hosted service that efficiently and automatically identifies potentially high-risk web applications and tests them for vulnerabilities.
- Only verified vulnerabilities are sent along to campus security.
- Notifications include a screen shot demonstrating the vulnerability as well as remediation instructions.
- From March to October 2017 over 250 campuses have signed up for the Dorkbot service.
Dorkbot - Findings

Overall
- Mean: 24
- Median: 11

Month 1
- Mean: 8
- Median: 4

n = 4003 Verified Vulnerabilities across 168 campuses
Individual Campus Example
(12 weeks/ 88 Verified Vulnerabilities)
Initial User Feedback

“You are a shining light in the choppy sea of security products that want our time & money”

- Meh
- “Better than services I’ve paid for”
- “Pretty good for a free service”
- “Wow - this really fills a gap in my DefSec toolkit”

- 53% of users: “Wow - this really fills a gap in my defensive security toolkit”
- Net Promotor Score (NPS) = 65%
- 74% for those with at least 1 vulnerability
- How they describe Dorkbot: Actionable, easy, no false positives, automatic, priceless, increased visibility, increased awareness, it just works…
- How they describe alternatives: bloated, expensive, confusing reports, cryptic findings, extortion, manual, more effort…

n = 74 responses
Dorkbot is Differentiated From Other Commercial Vulnerability Scanners

- Dorkbot uses publicly available information to map clients’ web presence and identify potential vulnerabilities.
  - **No lengthly and bandwidth consuming spidering required**

- Webpages with putative vulnerabilities are automatically penetration tested to verify the presence of the vulnerability.
  - **No more false positives**

- Verified vulnerabilities are sent to client in actionable format including: offending URL, screenshot demonstrating vulnerability, and remediation instructions.
  - **No more cryptic, bloated reports**
Dorkbot Summary

• Dorkbot was successful in automatically scanning domains for at risk webpages and pen-testing to verify putative vulnerabilities.

• Dorkbot identified numerous high risk vulnerabilities including top breach culprits (eg, XSS, SQLi, LFI, RFI) across campuses.

• Dorkbot was able to give campuses greater inside into web pages and applications running on their domains.

• Dorkbot was well received and regarded with value relative to traditional web application vulnerability scanners.
Thank you!

Proven Security Solutions for Higher Education

Salty Cloud offers scalable cloud-based security applications engineered to protect highly distributed & regulated environments.

- **DORKBOT**: Automatically assess vulnerabilities on high-risk web apps.
- **ISORA**: Easily conduct scalable organization-wide risk assessments.
- **SENF**: Quickly identify sensitive numbers on devices.
- **STACHE**: Securely share & store sensitive data.
- **PANOPTICON**: Efficiently manage incidents and consolidate system data.

saltycloud.com
Salty Cloud is a Public Benefit Company