Can Correlations Protect Web Applications?

Ofer Shezaf,
Product Manager, Security Solutions
HP ArcSight
ofr@hp.cm
## About Myself

<table>
<thead>
<tr>
<th>I live in</th>
<th>Kibbutz Yiftah, Israel</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>I create security products</th>
<th>Currently, Product Manager for Security Solutions at HP ArcSight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prior to that did security research and product management at Breach Security &amp; at Fortify</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I am an application security veteran</th>
<th>OWASP leader and founder of the OWASP Israeli chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Leads the Web Application Firewall Evaluation Criteria project</td>
</tr>
<tr>
<td></td>
<td>Wrote the ModSecurity Core Rule Set</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I really try to learn what information security is</th>
<th>Read my blog at <a href="http://www.xiom.com">http://www.xiom.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Be ready to some philosophy of science and cognitive psychology</td>
</tr>
</tbody>
</table>

They Paid My Trip!
The Web Attacks You Haven’t Heard about and Really Matter

Correlations to the Rescue

Current WAF Implementations

Using SIEM correlations
THE WEB ATTACKS YOU HAVEN’T HEARD ABOUT AND REALLY MATTERS
Meet the Time Magazine most influential person:

Survey Results

The Auto Voter System

Found out Some of Google’s Most Searched Keywords

1. rohm and haas
2. jesse jackson
3. 坉
4. monarch butterfly biosphere reserve
5. sc education lottery

Hot Searches (USA)

- Whitney Casey
- FBI jobs
- lol niggers
- gas stations
- comic book stores
- debt counseling
- grocery stores
Those Damn Rappers
(and Politicians)

Kanye West falls victim to hacker

January 27, 2009

Web User

Hip-hop star Kanye West is the latest celebrity to have had his online presence compromised.

The Grammy Award-winning singer has had his MySpace, his Google Mail and his Twitter accounts all hacked.

West said that someone is using all three services to spread malicious rumors about him including one that he was open to considering a career as a bisexual porn star.

On his blog he pleaded to decease, "Please I need a break," he wrote. "Let me have a break,

Lil Kim Facebook Hacked

January 28th, 2009 by Casilda
Tagged as: Lil Kim

Arghhh. He is so inconsistent and purposely misleading! I am sorry Sean. He is one for the Congressional position and he KNOWS it (that's the inconsistency)... he matters on matters like LIFE, honesty, ability, etc... all those things you are as opposed. He knows you fit all of his, and conservatives', and Alaskan's criteria. He is fighting for you. Does he want someone OFF experienced and capable and still, I am so sorry he does this.
### SEO and Comments Spam

<table>
<thead>
<tr>
<th>Subject</th>
<th>Author</th>
<th>Posted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>oXZcqrp kwpRef</td>
<td>aqoygtecSu</td>
<td>Solutions Directory</td>
</tr>
<tr>
<td>ZwCRyOotQLGTot</td>
<td>kspxzprn</td>
<td>WHID 2008-32: Yahoo HotJobs XSS</td>
</tr>
<tr>
<td>5G6evGTqvp</td>
<td>Cjkapzfjq</td>
<td>Black Cat, White Cat</td>
</tr>
<tr>
<td>5G6evGTqvp</td>
<td>Cjkapzfjq</td>
<td>Black Cat, White Cat</td>
</tr>
<tr>
<td>5G6evGTqvp</td>
<td>Cjkapzfjq</td>
<td>Black Cat, White Cat</td>
</tr>
<tr>
<td>5G6evGTqvp</td>
<td>Cjkapzfjq</td>
<td>Black Cat, White Cat</td>
</tr>
<tr>
<td>satisfactory job</td>
<td>Zohh1ep</td>
<td>Ivan Ristic releases a ModSecurity book!</td>
</tr>
<tr>
<td>satisfactory job</td>
<td>Zohh1ep</td>
<td>Ivan Ristic releases a ModSecurity book!</td>
</tr>
</tbody>
</table>

**Comment:**

sttxnomx
6eQzfR7lx on 20 June 2012 - 2:42pm

http://www.michael-kors-us.com/ womens apparel michael kors bags
michael kors mens watches michael kors bags michael kors shoes michael kors purses

Delete Edit Reply Approve
Auction Sniping

OWASP

JoyBidder eBay Auction Sniper

Item # 120536870931

Info

Porsche : 911
Current Price: USD 20200.00 Reserve Not Met
Time Left: 4d 8h 48m
Shipping: N/A
Seller: IdanielHh92 ( 41 | 100%)

Bid

Max Bid: 20300 USD (Enter 20300 or more)

Bidder:

Place bid Now
Place bid 15 seconds before auction ends

Bid Close

33 bids

Current bid: US $20,200.00 Reserve not met
Your maximum bid: US $ (Enter US $20,300.00 or more)

Place bid Watch this item

Get low monthly payments
Exclusive: Google's Click Fraud Rate is Less than 2% of $36 Billion!

It's $720 Million for god sake!
Web Scraping

Action
- Go to URL: http://www.ncbi.nlm.nih.gov
- Submit form with 'pubmed-key'
- Get a list of links like 'Carragge E,
  Title: Extract data like 'Does minor
  Journal: Extract data like '1: Spine
  Author: Extract data like 'Carragge
  Abstract: Extract data like 'STUDY

My Robots

C:\Downloads\Internet\irobot-eval\pubmed

Local Robots
- baidu.irm
- checkmails.irm
- hotornot.irm
- pubmed.irm

Recent Robots
- C:\Downloads\Internet\irobot-eval\pubmed.irm

Adventages:
1) Don't need to copy
2) Abstracts are save
3) Build abstract col

It includes:
- Go to URL: http://
  Select infowith
And I did not have time for

Ticket Scalping

Automated Stock Trading

Game Bots
And the Usual Lengthy Attacks

- Slow rate Reconnaissance
- Brute Force
- Distributed Denial of Service
What’s Common to Those Attacks?

Hard to Detect

Any single request looks benign

Only together they can be identified as malicious

Behavior is borderline

Need high certainty to respond

May not be allowed, business-wise, to block
CORRELATIONS TO THE RESCUE
Follow Sequences

Multi-Stage Attacks

HTTP Session Tacking

5 or more failed logins in a minute from same source

Attempted brute force attack

Attempted brute force attack + Successful login

User access violation: compromised account

OWASP
The Open Web Application Security Project
Consider the Environment

Source Reputation

Date & Time

Target Assets & Vulns

Users & Roles
Statistics & Behavior Analysis

Profile Behavior to Detect Anomalies

Overall site usage patterns

Specific users behavior

Determine False Positive Prone Rules

Signatures
Aggregate Indicators

Conclusive Answer

- Correlation Results
  - Rate
  - Environment
  - Behavioral

- Multiple Detection Engines
  - Signatures
  - Anomalies

- Low confidence results
CURRENT WAF IMPLEMENTATIONS
I say only good things

I am limited to what’s publicly available or disclosed by companies specifically for this project

If I get customers input (from you...) I will add it
All WAFs

Application Profile Learning

But Does it work?
• Multi-Layered Analysis for Accurate Decision Making
• Threat Intelligence

• Anti-Automation:
  – Rate or latency based detection
  – Latency based detection
  – Challenge Response
• IP Intelligence
• Signature based line learning

https://www.youtube.com/watch?v=H2PQBlhxL9I
• Bi-directional traffic inspection correlation
• Excessive Access Rate Detection

https://www.trustwave.com/web-application-firewall/#learn
(registration required)
Thanks to Matthieu Estrade for the information
• Anomaly scoring
• Messages aggregation
• Inbound & outbound correlation
• Bad robots

```
SecRule REQUEST_FILENAME|ARGS_NAMES|ARGS|XML:/*
  \bselect\b.{0,40}\buser\b"
...
setvar:tx.sql_injection_score=+%{tx.critical_anomaly_score},
setvar:tx.%{rule.id}-WEB_ATTACK/SQL_INJECTION-
%{matched_var_name}=%{tx.0}"
```
Challenges

Use Case Definition

Baseline Learning

Source and Session Identification

Bypass Mitigation

Flexibility
SIEM CORRELATIONS TO THE RESCUE
ModSecurity

Has all the tools
Collections (request, session, user)
Time Windows
LUA scripting
IP and Geo operations

However
No UI
Lacks performance optimization
Check for Multiple Stages attacks and context

Detect slow rate and over time attacks

Respond! And Extend
Connecting to the Application

Real Time Analyzer

Detect and Protect from application layer attacks

App. Security Monitor

Monitor applications for attacks, users and sessions

Fortify Runtime

Syslog Connector

Protected Application

ArcSight

Application Protection Specific Content
For Further Questions contact:

Ofer Shezaf
ofr@hp.com

Feedback Form

Thank You