Making Application Threat Intelligence Practical

PRESENTED BY:
Preston Hogue, Sr Dir F5 Labs and Security Marketing
The business
The reason people use the Internet
The gateway to DATA
765
Average # of Apps in use per enterprise

8 min before its scanned
If vulnerable, you could be PWND in <2 hrs

1/3 Mission critical
Identities are the Keys to Applications

The majority of breaches start with application or identity attack.

Identity attacks surpassed application attacks to be the leading cause of breaches in 2018.

~ongoing analysis pending publication
The majority of breaches start with application or identity attacks.
Application Attacks
Injection → PHP & SQL

- Login: 1%
- Affiliates: 1%
- Admin: 2%
- Betablock: 2%
- Cart: 3%
- Comments: 4%
- Exchweb: 6%
- SQL: 56%
- PHP: 58%
Vulnerabilities are Released Faster Than Organizations Can Patch

Average Days Between Vulnerability Releases

- **Critical**
  - 2014: 1.7
  - 2015: 1.4
  - 2016: 0.9
  - 2017: 0.8
  - 2018: 0.6

- **High**
  - 2014: 0.5
  - 2015: 0.6
  - 2016: 0.5
  - 2017: 0.4
  - 2018: 0.3

9-12 hours

- **Vuln released**
- **Applicable?**
- **Test**
- **Apply & Retest**
- **Firewall what you can’t fix**
- **Continuous improvement**
Growing Popularity of API Attacks

Attack
1. Mobile Apps
2. Direct APIs

Basic Security Fails
1. Authentication
2. Injection
3. Permissions

2019
- Oct 2018 – Github: “Events” API leaked projects and logs
- Oct 2018 – Quoine: crypto-exchange breach via API
- Sep 2018 – British Airways: Magecart API attack 380k records
- Sep 2018 – Facebook: Dev API leaked 50 mill accts
- Sep 2018 – Apple MDM: API brute-forced, registering rouge devices
- Aug 2018 – SalesForce: API vuln exposes contact data and prospects
- Aug 2018 – T-Mobile: 2 Mill customer records exposed through API
- July 2018 – Venmo: Public API -> 200 million payment transactions
- Apr 2018 – RSA Conference App: Data leaked through API
- Mar 2018 – Binance: Phished target accounts -> created fake API trading accounts -> fraud transactions
- Mar 2018 – Google: API attack impacted 438 apps and 500k records
- Jan 2018 – Tinder: HTTPS API data leakage vuln

2018
- Aug 2017 – Instagram: API vuln allowed access to user contact info
- Feb 2017 – WordPress: REST API Vuln
- Mar 2015 – Tinder: API to Facebook cred spoof

2011
- Sep 2011 – Westfield: “find my car app”
Access Attacks

- **3%** Brute Force
- **5%** Access Misconfiguration
- **12%** Unknown
- **13%** Credential Stuffing
- **17%** Compromised Email
- **53%** Phishing (Social Engineering Credential Theft)
Phishing & Fraud Is A Year Round Sport

Peaks Oct $\rightarrow$ Jan
Social Media
- Interests / interest groups
- Friends, Family and relationship information
- Style of speaking
- Writing style
- Work history
- Education
- Comments on links
- Important life event dates
- Places visited
- Favorite sites, movies, TV shows, books, quotes
- Photographs
- Hacked “Private” account data

People Search Engines
- Facebook information
- Email address (which leads to possible usernames)
- Education, income / salary range
- Phone numbers
- Age / Age range
- Race
- Home address
- Middle name, maiden name, spouse and family names

Company Research
- Who works there
- Tech infrastructure
- Types of endpoints (PC/Mac/OS)
- SEC filings
- Lawsuit filings
- Aggregator search tools for corporations
  - Individuals & department names
  - business partners & affiliates
  - IP space
- WHOIS info
- Email addresses and format

Mis configurations
- Server names
- Private network addresses
- Email addresses
- Usernames
- DNS servers
- Self-signed certs
- Email headers
- Web servers
- Web cookies
- Web applications
APT’s and/or Nation-states That Begin Attacks With Phishing
Phishing emails are 3 times more likely to have a malicious link than a malicious attachment.

Email sent from North Korean ATP in Sony compromise.

Email sent from North Korean APT related to Bangladesh Bank heist.

Malicious Web Link vs Attachment
Encryption is an Attacker Disguise

93% of phishing domains use HTTPS to appear more legitimate.
Majority of Malware Hides in Encryption

70% of all Internet traffic is encrypted

68% of malware phones home over port 443
Fraud Starts With Phishing

Clients are phished → malware installed

Banking Trojans → Fraud Trojans

Fraud targets = any site with a login page
Keurig Attacks!

Various dynamic / private source ports 49152 - 65535

RFC2324: Hyper Text Coffee Pot Control Protocol
2017 DDoS Attacks by Industry

- Hosting / Colo: 31%
- Financial Service: 17%
- Tech Company: 12%
- Telecom / ISP: 11%
- Online Gaming: 9%
- Domain Registrar: 3%
- Business Services: 2%
- Government: 1%
- Education: 1%
- Entertainment: 1%
- Retail: 1%
- Automotive: 0%
- Engineering: 0%

2018 DDoS Attacks by Industry

- Online Gaming: 31%
- Financial Service: 23%
- Hosting / Colo: 22%
- Domain Registrar: 7%
- Tech Company: 5%
- Telecom / ISP: 4%
- Education: 3%
- Entertainment: 2%
- Business Services: 2%
- Retail: 2%
- Aerospace: 1%
- Government: 0%
- Aerospace: 0%
- Engineering: 0%
Application DDoS Attacks (F5 SIRT vs SOC)

Application targeted DDoS attacks are a large portion of the attack types that get escalated to our SIRT for assistance.
Oct 2016: Cellular Gateway Discovered

- Investigating airport incident in Europe + BASHLITE on a DVR digital signage solution (same timeframe as Dyn DNS DDoS attack).
- Service and host managed by 3rd party
- 39 active threat actors
- Numerous log entries show incoming attacks
  - Mirai, shellshock, brute force
- Sierra Wireless device

Note: System owner sent drives to us for forensic analysis and authorized scanning of their network.
Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEnet manager password and are reachable from the public internet. The attached technical bulletin provides information about Mirai along with instructions on how to protect your Sierra Wireless gateway and its local area network.

Based on currently available information, once the malware is running on the gateway it deletes itself and resides only in memory. The malware will then proceed to scan for vulnerable devices and report its findings back to a command and control server. The command and control server may also instruct the malware to participate in a Distributed Denial of Service (DDoS) attack on specified targets.
“Exploiting” the Vulnerability

WAN IP
166.139.19.193

PUBLIC GPS COORDINATES
40° 49′ 51.5″ N
47° 26′ 03.5″ W

NO DEPENDENCY on any vulnerability within the hardware or software.

DEFAULT PASSWORD

Bruteforce attack(s) are unnecessary.
Fleet / Vehicle Tracking

GPS Data Logging (TAIP)

TRACCAR – Open Source Fleet Software
SierraWireless.com Case Studies

St John Ambulance, Western Australia
California Highway Patrol, California
Ventura County Fire Department, California
South Bay Regional Public Communications Authority (SBRPCA), California
West Metro Fire Protection District, Colorado
Westminster Police Department, Colorado
Danish National Police, Denmark
Acadian Ambulance Service, Louisiana & Texas
East Baton Rouge Parish Emergency Medical Services (EMS), Louisiana
Mississippi Highway Safety Patrol
Gem Ambulance, New Jersey
City of Charlotte, North Carolina
Dickinson Police Department (DPD), Texas
Fairfax’s Urban Search and Rescue Team, Virginia
South Wales Police, Wales
City of Yakima, Washington
Seattle Fire Department, Washington
Check Your Cellular Gateways!

- **SIERRA WIRELESS LS300**
  - Weak Authentication

- **SIERRA WIRELESS GX450**
  - Weak Authentication

- **SIERRA WIRELESS ES440**
  - Weak Authentication

- **MOXA ONCELL G3xxx**
  - No Authentication

- **DIGI TRANSPORT WR44**
  - Weak Authentication

- **CradlePoint**
  - Hard coded tech support back door

*DISCLOSED 10/16/2018*
Your personal safety is at risk!

Privacy? Gone.
Avoiding a breach is cheaper than dealing with one.

<table>
<thead>
<tr>
<th>Cost of Breach in Millions of $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leakage of Confidential or Sensitive Information</td>
</tr>
<tr>
<td>Tampering / Unauthorized Modifications to Apps</td>
</tr>
<tr>
<td>Hack Resulting in Failure to Access Data and/or Apps</td>
</tr>
<tr>
<td>Leakage of PII About Customers, Consumers or Employees</td>
</tr>
</tbody>
</table>

*may be underestimated / not include litigation and class action lawsuit fines
Understand Your Environment

Prevent Downtime

CISO’s #1 Mission

Visibility

Everyone’s #1 Challenge
Reduce Your Attack Surface

2

Sub domains hosting other versions of the main application site

Server-side features such as search

Web service methods

Cookies/state tracking mechanisms

APIs

Data entry forms

Administrative and monitoring stubs and tools

Events of the application—triggered server-side code

Shells, Perl/PHP

Backend connections through the server (injection)

Data/active content pools—the data that populates and drives pages

Admin interfaces

Apps/files linked to the app

HTTP headers and cookies

Helper apps on client (java, flash)

Dynamic web page generators

Web pages and directories

Search

Server-side connections through the server (injection)

Data/active content pools— the data that populates and drives pages
Every 9 hrs

CRITICAL
vulnerability is released
Does it apply to you?
Has a patch been released?
Did you test it?
Did you apply it?

VULNERABILITIES
in <24 hrs

Attackers are weaponizing

ATTACKED!

When Apps Touch The Big Bad Internet
Vulnerability Management is Hard

Continuous security scanning
Team review
Remediate
Retest
Firewall what you can’t fix
Continuous improvement
<table>
<thead>
<tr>
<th><strong>Username</strong></th>
<th><strong>Password</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>user</td>
<td>user</td>
</tr>
<tr>
<td>test</td>
<td>test</td>
</tr>
<tr>
<td>ubuntu</td>
<td>ubuntu</td>
</tr>
<tr>
<td>ubnt</td>
<td>ubnt</td>
</tr>
<tr>
<td>support</td>
<td>support</td>
</tr>
<tr>
<td>oracle</td>
<td>oracle</td>
</tr>
<tr>
<td>pi</td>
<td>raspberry</td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
</tr>
<tr>
<td>postgres</td>
<td>postgres</td>
</tr>
<tr>
<td>ftpuser</td>
<td>asteriskftp</td>
</tr>
<tr>
<td>usuario</td>
<td>usuario</td>
</tr>
<tr>
<td>nagios</td>
<td>nagios</td>
</tr>
<tr>
<td>1234</td>
<td>1234</td>
</tr>
<tr>
<td>ftp</td>
<td>ftp</td>
</tr>
<tr>
<td>operator</td>
<td>operator</td>
</tr>
<tr>
<td>git</td>
<td>git</td>
</tr>
<tr>
<td>hadoop</td>
<td>hadoop</td>
</tr>
<tr>
<td>ts3</td>
<td>ts3</td>
</tr>
<tr>
<td>teamspeak</td>
<td>teamspeak</td>
</tr>
<tr>
<td>mysql</td>
<td>mysql</td>
</tr>
<tr>
<td>tomcat</td>
<td>tomcat</td>
</tr>
<tr>
<td>service</td>
<td>service</td>
</tr>
<tr>
<td>butter</td>
<td>Xuelp123</td>
</tr>
<tr>
<td>ts</td>
<td>ts</td>
</tr>
<tr>
<td>bot</td>
<td>bot</td>
</tr>
<tr>
<td>deploy</td>
<td>deploy</td>
</tr>
<tr>
<td>monitor</td>
<td>monitor</td>
</tr>
<tr>
<td>administrator</td>
<td>administrator</td>
</tr>
<tr>
<td>bin</td>
<td>bin</td>
</tr>
<tr>
<td>default</td>
<td>default</td>
</tr>
<tr>
<td>nopass</td>
<td>nopass</td>
</tr>
<tr>
<td>manager</td>
<td>manager</td>
</tr>
<tr>
<td>teamspeak3</td>
<td>teamspeak3</td>
</tr>
<tr>
<td>nobody</td>
<td>nobody</td>
</tr>
<tr>
<td>csigoserver</td>
<td>csigoserver</td>
</tr>
<tr>
<td>test2</td>
<td>test2</td>
</tr>
<tr>
<td>demo</td>
<td>demo</td>
</tr>
<tr>
<td>0</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>bot</td>
<td>bot</td>
</tr>
<tr>
<td>deploy</td>
<td>deploy</td>
</tr>
<tr>
<td>monitor</td>
<td>monitor</td>
</tr>
<tr>
<td>administrator</td>
<td>administrator</td>
</tr>
<tr>
<td>bin</td>
<td>bin</td>
</tr>
<tr>
<td>default</td>
<td>default</td>
</tr>
<tr>
<td>nopass</td>
<td>nopass</td>
</tr>
<tr>
<td>manager</td>
<td>manager</td>
</tr>
<tr>
<td>teamspeak3</td>
<td>teamspeak3</td>
</tr>
<tr>
<td>nobody</td>
<td>nobody</td>
</tr>
<tr>
<td>csigoserver</td>
<td>csigoserver</td>
</tr>
<tr>
<td>test2</td>
<td>test2</td>
</tr>
<tr>
<td>demo</td>
<td>demo</td>
</tr>
<tr>
<td>0</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>teamspeak3</td>
<td>teamspeak3</td>
</tr>
<tr>
<td>nobody</td>
<td>nobody</td>
</tr>
<tr>
<td>csigoserver</td>
<td>csigoserver</td>
</tr>
<tr>
<td>test2</td>
<td>test2</td>
</tr>
<tr>
<td>demo</td>
<td>demo</td>
</tr>
<tr>
<td>0</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>weblogic</td>
<td>weblogic</td>
</tr>
<tr>
<td>redhat</td>
<td>redhat</td>
</tr>
<tr>
<td>developer</td>
<td>developer</td>
</tr>
<tr>
<td>public</td>
<td>public</td>
</tr>
<tr>
<td>student</td>
<td>student</td>
</tr>
<tr>
<td>webmaster</td>
<td>webmaster</td>
</tr>
<tr>
<td>osmc</td>
<td>osmc</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>server</td>
<td>server</td>
</tr>
<tr>
<td>supervisor</td>
<td>supervisor</td>
</tr>
<tr>
<td>22</td>
<td>backup</td>
</tr>
<tr>
<td>hdfs</td>
<td>hdfs</td>
</tr>
<tr>
<td>linux</td>
<td>linux</td>
</tr>
<tr>
<td>postmaster</td>
<td>postmaster</td>
</tr>
<tr>
<td>cserver</td>
<td>cserver</td>
</tr>
<tr>
<td>prueba</td>
<td>prueba</td>
</tr>
<tr>
<td>matt</td>
<td>matt</td>
</tr>
<tr>
<td>vyatta</td>
<td>vyatta</td>
</tr>
<tr>
<td>hduser</td>
<td>hduser</td>
</tr>
<tr>
<td>nexus</td>
<td>nexus</td>
</tr>
<tr>
<td>ethos</td>
<td>ethos</td>
</tr>
<tr>
<td>live</td>
<td>live</td>
</tr>
<tr>
<td>Admin</td>
<td>Admin</td>
</tr>
<tr>
<td>mc</td>
<td>mc</td>
</tr>
<tr>
<td>telnet</td>
<td>telnet</td>
</tr>
<tr>
<td>top100</td>
<td>admin</td>
</tr>
<tr>
<td>creds</td>
<td>used</td>
</tr>
<tr>
<td>ssh</td>
<td>brute</td>
</tr>
<tr>
<td>force</td>
<td>attacks</td>
</tr>
</tbody>
</table>

**Top 100 Admin Creds Used in SSH Brute Force Attacks**
3

Prioritize Defenses Based on Attacks

Focus OpEx & CapEx spend
Training Reduces Phishing Success!

Phishing success without training: 33%

Phishing success with training: 13%
Implement a Culture of Curiosity

71% of phishing impersonates 10 organizations