Advances in Modern Attack Bots

PRESENTED BY:
David Warburton, Snr Threat Research Evangelist
F5 Labs
Who Am I?

David Warburton

- Senior Threat Research Evangelist
  F5 Labs
- Royal Holloway
  MSc Information Security (Distinction)
- AppSec, Identity & Auth,
  Cryptography & PKI

@warburtron
What are bots?

Advanced Bot Techniques

Detecting and mitigating Bots
- Crawler
- DOS Tool
- E-Mail collector
- Exploit tool
- Headless browser
- HTTP library
- Network Scanner
- RSS Reader
- Search bot
- Search engine
- Service agent
- Site monitor
- Social media agent
- Spam bot
- Spyware
- Vulnerability scanner
- Web downplaner
- Web spider
- Webserver stress tool
- Chat bot
- Search crawler
- Task automation
- Sniper bots
- Scanners
- Scrapers
- DDoS
- Credential stuffing
- Cryptomining

Good
- Performance/scale
- Automate a process

Bad
- Abuse functionality
- Prevent access
- Commit fraud
- Earn some $$$
Bot Breakdown

- Humans: 48.2%
- Good Bots: 22.9%
- Bad Bots: 28.9%
- Commercial Crawlers: 2.9%
- Search Engine Bots: 6.6%
- Monitoring Bots: 1.2%
- Impersonators: 24.3%
- Scrapers: 1.7%
- Spammers: 0.3%
- Scrapers: 2.6%

Web app attacks started with botnets

Source: GlobalDots Bot Report

Source: Verizon
### Bots by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Bad Bots</th>
<th>Good Bots</th>
<th>Human</th>
<th>% of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Travel (no Airlines)</td>
<td>4.50%</td>
<td>3.46%</td>
<td>92.04%</td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td>12.44%</td>
<td>37.21%</td>
<td></td>
<td>50.35%</td>
</tr>
<tr>
<td>Insurance</td>
<td>12.88%</td>
<td>18.65%</td>
<td></td>
<td>68.47%</td>
</tr>
<tr>
<td>Adult Entertainment</td>
<td>17.57%</td>
<td>0.47%</td>
<td></td>
<td>81.95%</td>
</tr>
<tr>
<td>Travel (incl. Airlines)</td>
<td>19.24%</td>
<td>2.51%</td>
<td></td>
<td>78.25%</td>
</tr>
<tr>
<td>Ecommerce</td>
<td>21.45%</td>
<td>16.49%</td>
<td></td>
<td>62.05%</td>
</tr>
<tr>
<td>Tickets</td>
<td>22.97%</td>
<td>7.82%</td>
<td></td>
<td>69.21%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>24.37%</td>
<td>57.58%</td>
<td></td>
<td>18.04%</td>
</tr>
<tr>
<td>Financial</td>
<td>24.66%</td>
<td>4.35%</td>
<td></td>
<td>70.99%</td>
</tr>
<tr>
<td>Airlines</td>
<td>43.90%</td>
<td>0.93%</td>
<td></td>
<td>55.18%</td>
</tr>
<tr>
<td>Gambling</td>
<td>53.08%</td>
<td>0.09%</td>
<td></td>
<td>46.80%</td>
</tr>
</tbody>
</table>

Source: GlobalDots Bad Bot Report 2018
Good Bots

![Chat interface with support messages]

- Nice. Also, can I use my Revolut card in India?
  - For sure. Your RevolutCard works in INR and over 120 currencies; check them out here: https://goo.gl/kglSIC
- What’s your exchange rate today for GBP to INR?
  - Our GBP to INR rate is 84.8071. That’s the live market exchange rate.
- Wow, I love Revolut!

![Diagram with robots.txt file]

```
User-agent: *
Disallow: /template/
Disallow: /secret/
```
Bad Bots – Top 20 OWASP Automated Threats

DoS / Resource Hoarding
- OAT-015 Denial of Service
- OAT-005 Scalping
- OAT-021 Denial of Inventory
- OAT-013 Sniping
- OAT-006 Expediting

Account Takeover
- OAT-007 Credential Cracking
- OAT-008 Credential Stuffing
- OAT-019 Account Creation
- OAT-020 Account Aggregation

Content Theft
- OAT-011 Scraping

Payment Card Data
- OAT-010 Card Cracking
- OAT-001 Carding
- OAT-012 Cashing Out

Other Attacks
- OAT-003 Ad Fraud
- OAT-009 CAPTCHA Defeat
- OAT-016 Skewing
- OAT-017 Spamming
- OAT-002 Token Cracking

Vulnerability Scanning
- OAT-014 Vulnerability Scanning
- OAT-004 Fingerprinting
- OAT-018 Footprinting
OAT-014 Scanning
Top 10 Attacked Ports Globally

2018
- HTTPS: 443
- MS SMB: 445
- SSH: 22
- Alt HTTPS?, ICS?:...
- Port 11684
- SIP: 5060
- HTTP: 80
- Port 51413
- Port 23810
- Telnet: 23

Q1 2019
- MS SMB: 445
- SIP: 5060
- Alt HTTPS?, ICS?:...
- SSH: 22
- HTTP: 80
- Alt SSH?, ICS?: 2222
- MySQL: 3306
- Telnet: 23
- Port 3128

SOURCE: F5 Labs & Baffin Bay Networks
OAT-011 Scraping

Apps

Browser extensions
OAT-011 Scraping-as-a-Service

Developer tools
Ideal for: developers, data scientists, data teams looking to execute web scraping projects.

PROJECT BUDGET  TOTAL BIDS
$250 - $750 USD  31

PROJECT DESCRIPTION:
i need a bot that will scrape odds on various sporting events from a number of bookie websites. some of these have real-time XML feeds which can be used, others, the actual odds need to be scraped. the odds are then to be stored into a SQL database for analysis. provisions need to be made to ensure that the pages that are being scraped are not done too regularly in order to avoid IP being blocked. i can provide guidance on this area. some formatting needs to be done between some sites, as different bookies have different ways of representing data.

i would like the application ideally written in either C# or .net (c sharp).

there will be a further phase of this project which will involve automating login to the bookie sites. is to award this project to whoever successfully completes this phase, so when bidding please bid if you can complete this role.

Web Scraping Bots
This project was awarded to ASYanush for $400 USD.
Copping, Scalping and Sniping
OAT-005, OAT-013, OAT-021
OAT-008 Credential Stuffing

Credentials from Previous Breaches

- Healthcare Data
- Credit Card Data
- Financial Data
- Passport Data
- Intellectual Property
Choose Your Bot:

Sentry MBA

Detection:

- Selenium
- Phantom
- No JavaScript
- Known Bot
- Not Real Browser
- Not Human
- Human

Mitigation:

- JavaScript Challenge
- TCP Reset
- Captcha
- Blocking Page
- No Mitigation

Connected (encrypted) to win-4mv/Netbooks
OAT-019 New Account Creation Attacks

Personal Data
Previous Breaches

Healthcare Site
E-Commerce Site
Finance Site
Services Site
Other Sites
OAT-019 New Account Creation Attacks
(FSI 2017)

Volume per Transaction Type

- Payments
- Account logins
- New account creations

Attack rate per Transaction Type

- Payments: 6.00%
- Account logins: 0.00%
- New account creations: 2.00%

Source: threatmetrix.com
8.4B DEVICES
Gartner

2017

1T DEVICES
SoftBank

2035

*Excludes smartphones, tablets, and computers
Shifting from primarily DDoS to multi-purpose...
Thingbots

Affected Devices

- CCTV
- DVRs
- SOHO routers
- IOS
- WAPs
- Set-Top Boxes
- Media Center
- ICS
- Android
- IP Cameras
- Wireless Chipsets
- NVR Surveillance
- VoIP Devices
- Cable Modems
- Busybox Platforms
- Smart TVs

84% Discovered since Mirai

6Bots
Death
Anarchy
Torii
Yasaku
Thanos

13Bots
SORA
OWARI
UPnPProxy
OMNI
RoamingMantis
Wicked
VPNFilter
DaddyL33t
Sakur

5Bots
Vermelho
MIzI
IZIH9
APEP
SEFA
Yowai

1Bot
Psyb0t

2Bots
Hydra

3Bots
Moon

4Bots
CCTV
DVRs
WAPs
Set-Top Boxes
Media Center
Ics
Android
IP Cameras
Wireless Chipsets
NVR Surveillance
VoIP Devices
Cable Modems
Busybox Platforms
Smart TVs
Mirai
(SOHO Routers, DVRs, IP Cameras - Oct 2018)

- 20,000 devices in less than 24 hours
- Peak of over 600,000 devices
- Conducted over 15,000 attacks as of early 2017
- Has spun-off at least 10 variants since source code went public
  - ‘Wicked’ installs rentable bots
- Effective
  - Efficient internet-wide scanning
  - Simple cross-platform architecture
  - Default credentials
How “Things” Are Compromised

Service Attacked To Infect IoT Device

- TCP
- Telnet
- HNAP
- IEC 101, 104, OPC
- TR-064, TR 069
- SOAP
- UPnP
- HTTP
- CVE Specific

Broader scope of attack methods + CVEs
F5 Labs discovers cellular gateway vulns
F5 Labs discovers cellular gateway vulns
“Exploiting” the Vulnerability

NO DEPENDENCY on any vulnerability within the hardware or software.

DEFAULT PASSWORD *****

Bruteforce attack(s) are unnecessary.

WAN IP 166.139.19.193

PUBLIC GPS COORDINATES 40° 49’ 51.5” N
47° 26’ 03.5” W
<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>root</td>
<td>ts</td>
<td>ts</td>
<td>manager</td>
<td>manager123</td>
<td>csparse3</td>
<td>nobody</td>
<td>test2</td>
<td>no</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
<td>bot</td>
<td>bot</td>
<td>nobody</td>
<td>nobody</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>user</td>
<td>user</td>
<td>deploy</td>
<td>deploy</td>
<td>csgoserver</td>
<td>csgoserver</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>test</td>
<td>test</td>
<td>monitor</td>
<td>monitor</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>ubuntu</td>
<td>ubuntu</td>
<td>administrator</td>
<td>administrator</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>ubnt</td>
<td>ubnt</td>
<td>bin</td>
<td>bin</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>support</td>
<td>support</td>
<td>default</td>
<td>default</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>oracle</td>
<td>oracle</td>
<td>adm</td>
<td>adm</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>pi</td>
<td>raspberry</td>
<td>vagrant</td>
<td>vagrant</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
<td>anonymous</td>
<td>any@</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>postgres</td>
<td>postgres</td>
<td>uucp</td>
<td>uucp</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>ftpuser</td>
<td>asteriskftp</td>
<td>jenkins</td>
<td>jenkins</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>usuario</td>
<td>usuario</td>
<td>apache</td>
<td>apache</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>nagios</td>
<td>nagios</td>
<td>sshd</td>
<td>sshd</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>1234</td>
<td>1234</td>
<td>P1cSmSpIp</td>
<td>P1cSmSpIp</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>ftp</td>
<td>ftp</td>
<td>cisco</td>
<td>cisco</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>operator</td>
<td>operator</td>
<td>sinusbot</td>
<td>sinusbot</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>git</td>
<td>git</td>
<td>user1</td>
<td>user1</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>hadoop</td>
<td>hadoop</td>
<td>backup</td>
<td>backup</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>ts3</td>
<td>ts3</td>
<td>Management</td>
<td>Management</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>teamspeak</td>
<td>teamspeak</td>
<td>steam</td>
<td>steam</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>mysql</td>
<td>mysql</td>
<td>mother</td>
<td>mother</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>tomcat</td>
<td>tomcat</td>
<td>dev</td>
<td>dev</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>service</td>
<td>service</td>
<td>zabbix</td>
<td>zabbix</td>
<td>test2</td>
<td>test2</td>
<td>test2</td>
<td>demo</td>
<td>test2</td>
<td>demo</td>
</tr>
<tr>
<td>butter</td>
<td>xuelp123</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Top 100 Admin Creds Used in SSH Brute Force Attacks

H1 2019

Source: F5 Labs
## Mirai Attack Types

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Attacks</th>
<th>Targets</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP flood</td>
<td>2,736</td>
<td>1,035</td>
<td>A</td>
</tr>
<tr>
<td>UDP-PLAIN flood</td>
<td>2,542</td>
<td>1,278</td>
<td>V</td>
</tr>
<tr>
<td>UDP flood</td>
<td>2,440</td>
<td>1,479</td>
<td>V</td>
</tr>
<tr>
<td>ACK flood</td>
<td>2,173</td>
<td>875</td>
<td>S</td>
</tr>
<tr>
<td>SYN flood</td>
<td>1,935</td>
<td>764</td>
<td>S</td>
</tr>
<tr>
<td>GRE-IP flood</td>
<td>994</td>
<td>587</td>
<td>A</td>
</tr>
<tr>
<td>ACK-STOMP flood</td>
<td>830</td>
<td>359</td>
<td>S</td>
</tr>
<tr>
<td>VSE flood</td>
<td>809</td>
<td>550</td>
<td>A</td>
</tr>
<tr>
<td>DNS flood</td>
<td>417</td>
<td>173</td>
<td>A</td>
</tr>
<tr>
<td>GRE-ETH flood</td>
<td>318</td>
<td>210</td>
<td>A</td>
</tr>
</tbody>
</table>
Application targeted DDoS attacks are a large portion of the attack types that get escalated to our SIRT for assistance.
Detecting bots

- IP block list
- User-agent & reverse DNS checks
- Insertion of HTML elements
- Javascript challenge
- CAPTCHA challenge
- Fingerprinting
- Human interaction
- Behaviour based / server stress
## IPs Attacking UK
(last 90 days as of 3/1/2019)

### Top 20 targeted ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>SIP</td>
</tr>
<tr>
<td>2222</td>
<td>SSH &amp; Rockwell</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>445</td>
<td>SMB</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>1433</td>
<td>MS SQL</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
</tr>
<tr>
<td>8291</td>
<td>MikroTik</td>
</tr>
<tr>
<td>7547</td>
<td>TR069</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
</tr>
<tr>
<td>3389</td>
<td>RDP</td>
</tr>
<tr>
<td>1723</td>
<td>PPTP</td>
</tr>
<tr>
<td>5061</td>
<td>Secure SIP</td>
</tr>
<tr>
<td>61137</td>
<td>HTTPS</td>
</tr>
<tr>
<td>4433</td>
<td>HTTPS</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>12555</td>
<td>HTTPS</td>
</tr>
<tr>
<td>8545</td>
<td>JSON</td>
</tr>
<tr>
<td>139</td>
<td>NetBios</td>
</tr>
</tbody>
</table>
Shifting Sources

Thanks to proxies & IoT devices

Previously unseen IP addresses: 100%

Previously unseen networks (ASN): 80%
User-agent

- 1,080,598 user-agents
- 3,999 of which are bots
- Fake GoogleBot: 13,037 IP’s in June 2019 alone
  - e.g. 38.124.xxx.xx
- MikroTik device - lots of known vulns
- Combat with reverse DNS lookups
JavaScript Based Bot Detection

LEGITIMATE BROWSER VERIFICATION

WAF responds with injected JS:
Request is not passed to the server

No challenge response from bots
Bots are dropped

Valid response is sent to the server

WAF verifies response authenticity
Cookie is signed, time stamped, and fingerprinted
Headless Browsers

- Command line and scriptable execution of browsers
- Chrome without the chrome!
- Able to render HTML and execute JavaScript & AJAX
- Often Selenium based

---

**Headless Browser** | **Website** | **Rendering Engine** | **JavaScript Engine** | **Common Browsers** | **Other Notes**
--- | --- | --- | --- | --- | ---
Sahi | [http://sahi.co.in/](http://sahi.co.in/) | Any | Any | Any | [http://sahi.co.in/w/configuring-sahi-with-xvfb](http://sahi.co.in/w/configuring-sahi-with-xvfb)
Selenium

```python
from selenium import webdriver
from selenium.common.exceptions import TimeoutException

browser = webdriver.Firefox()
browser.get("http://www.facebook.com")

username = browser.find_element_by_id("email")
password = browser.find_element_by_id("password")
submit = browser.find_element_by_id("submit")

username.send_keys("me")
password.send_keys("mykewlpass")

submit.click()

wait = WebDriverWait( browser, 5 )

try:
    page_loaded = wait.until_not(
        lambda browser: browser.current_url == login_page
    )

except TimeoutException:
    self.fail( "Loading timeout expired" )

self.assertEqual(
    browser.current_url,
    correct_page,
    msg = "Successful Login"
)
```
Scriptable Browser as-a-Service

- Detect headless browsers via extensions and browser flags

Splash
Lightweight, scriptable browser as a service

Splash is a lightweight, scriptable headless browser with an HTTP API. It is used to:
- Properly render web pages that use JavaScript
- Interact with them
- Get detailed information about requests/responses initiated by a web page
- Apply Adblock Plus filters
- Take screenshots of the crawled websites as they are seen in a browser

Pricing
We offer hosted Splash instances in 3 sizes:

<table>
<thead>
<tr>
<th></th>
<th>SMALL</th>
<th>MEDIUM</th>
<th>LARGE</th>
<th>ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRICE</td>
<td>$25/month</td>
<td>$50/month</td>
<td>$100/month</td>
<td>Custom</td>
</tr>
<tr>
<td>CPU</td>
<td>1x</td>
<td>2x</td>
<td>4x</td>
<td>Custom</td>
</tr>
<tr>
<td>RAM</td>
<td>1.25GB</td>
<td>2.5GB</td>
<td>5GB</td>
<td>Custom</td>
</tr>
<tr>
<td>PRIORITY SUPPORT</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
</tbody>
</table>
CAPTCHA

Type the two words:

morning overlooks

Select all squares with traffic lights
If there are none, click skip
CAPTCHA Solvers – Browser Extensions

Rumola

AntiCaptcha

- Detect CAPTCHA extensions based on HTML insertion
Bot detects that a CAPTCHA is existing on the page
- Bot saves CAPTCHA into an image file
- Bot uploads the saved image file to the solver servers
- The solver will respond with a CAPTCHA ID
- Bot polls the solver API using the CAPTCHA ID it received until the status of the CAPTCHA id is changed to solved
- Bot sends solution to the scraped website and continues attack process
Simulated Mouse Events

Fake mouse movements can lack cursor positioning.
Detect GET flood attacks against Heavy URIs

Identify non-human surfing patterns

Fingerprint to identify beyond IP address

Operating system
Geolocation
Browser
  • Screen size and colour depth
  • Plugin details
  • Time zone
  • HTTP_ACCEPT headers
  • Language
  • System fonts
  • Touch support
  • Extensions
What is Required for Accurate Bot Detection?

Server should not receive traffic
In a shocking finding, scientists discovered a herd of unicorns living in a remote, previously unexplored valley, in the Andes Mountains. Even more surprising to the researchers was the fact that the unicorns spoke perfect English.

The scientist named the population, after their distinctive horn, Ovid’s Unicorn. These four-horned, silver-white unicorns were previously unknown to science.

Now, after almost two centuries, the mystery of what sparked this odd phenomenon is finally solved.

Dr. Jorge Pérez, an evolutionary biologist from the University of La Paz, and several companions, were exploring the Andes Mountains when they found a small valley, with no other animals or humans. Pérez noticed that the valley had what appeared to be a natural fountain, surrounded by two peaks of rock and silver snow.
A growing system of teams gathering application threat data.
A global network of experienced security incident handlers

24/7 availability

When you are under attack, we are there for you

Always-available for emergency security issues
Read more about these and other threats

Stay up-to-date
Sign up for F5 Labs

https://interact.f5.com/AppProtectLibrary

F5labs.com