Get Your SaaS In Gear

PRESENTED BY:
Paul Simmons, Solutions Engineer, F5
Agenda

• Introduction
• IaaS, PaaS & SaaS
• Current Application Hosting Models
• Application Services
  • Authentication
  • Security
  • Availability
• Application Architectures
• Conclusion
IT Progression Over Time

- Mainframes
- Self Hosted, Discrete Servers
- Datacenter Consolidation & virtualization
  - IaaS
- Cloud, Containerization & Automation
  - PaaS
- SaaS
**IaaS, PaaS, SaaS**

- **IaaS** - Infrastructure as a service is a service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. Typically, IaaS provides hardware, storage, servers and data center space or network components; it may also include software. (VMWare)

- **PaaS** - Platform as a service is a cloud computing model in which a third-party provider delivers hardware and software tools, usually those needed for application development to users over the internet. A PaaS provider hosts the hardware and software on its own infrastructure. (OpenShift, K8S)

- **SaaS** - a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers. (O365, ServiceNow, SAP, Salesforce, ADP)
SaaS Providers

SaaS Applications that Power Modern Businesses
Cloud-based software is disrupting the way businesses operate and services, with more efficient and effective applications designed to be easier to use.

f5
Application Hosting Models
Datacenter Application Hosting
Cloud Application Hosting

https://github.com/f5devcentral/f5-azure-saca

- 3 Tier Design
- Includes WAF
- Includes B&I with Inspection Zone
- Fully Automated Deployment
- Supports multiple Mission Owners
SaaS Application Hosting

- Cloud Computing SRG Requirements for SaaS (5.10.3.1):
  - WAF
  - Reverse Web Proxy
  - Network Requirements on SaaS Provider
  - FIPS 140-2 Compliant Key Management
  - FIPS 140-2 Encryption for Data at Rest and in Transit
  - CAC/PIV Authentication
Application Services
Authentication

- CAC/PIV/ALT Token
- Kerberos
- Federation
- SAML
- ADFS
- Oauth
- Etc.
Client Cert Auth Options

- C3D in LTM
- CCA -> CCA

- C3D in APM
- CCA -> CCA
- Federated Auth -> CCA
- Username & Password -> CCA*

- Federated CAC Auth without refactoring Apps
Single Sign On

- Federated Authentication / Token Brokering
# Single Sign On Portal

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eTIME</td>
<td>Time and Attendance</td>
</tr>
<tr>
<td>GlobalView Payroll</td>
<td>Employee Self-Service</td>
</tr>
<tr>
<td>Bugzilla</td>
<td>FS PTG defect tracking system.</td>
</tr>
<tr>
<td>Concur</td>
<td>FS travel and expenses managing application.</td>
</tr>
<tr>
<td>FS Policy Portal</td>
<td>ConvergePoint is FS's Policy Management Portal. Click to view policies.</td>
</tr>
<tr>
<td>Finder</td>
<td>Corporate Maps</td>
</tr>
<tr>
<td>GlobeSmart</td>
<td>Enhance your cultural intelligence and improve your global business interactions.</td>
</tr>
<tr>
<td>LearnFS</td>
<td>Your hub for learning at FS.</td>
</tr>
<tr>
<td>Linkedin Learning</td>
<td>Access over 13,000+ expert-led video courses to build your business, creative and technical skills.</td>
</tr>
<tr>
<td>Office 365</td>
<td>Office 365 Email</td>
</tr>
<tr>
<td>Outlook</td>
<td>Office 365 Email</td>
</tr>
<tr>
<td>Oracle EBS</td>
<td>E-Business Suite</td>
</tr>
<tr>
<td>Salesforce</td>
<td>FS CRM Solution</td>
</tr>
<tr>
<td>NAVEX</td>
<td>FS HR Training</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>FS.service-now.com</td>
</tr>
<tr>
<td>Tableau</td>
<td>BI Data Visualization</td>
</tr>
<tr>
<td>Workday</td>
<td>FS HRIS Solution</td>
</tr>
<tr>
<td>Zoom</td>
<td>Enterprise Audio &amp; Video Conferencing.</td>
</tr>
<tr>
<td>Tableau</td>
<td>FS Networks Interactive data visualization dashboards.</td>
</tr>
<tr>
<td>Workday</td>
<td>FS HR global workforce managing tool.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Enterprise Audio &amp; Video Conferencing.</td>
</tr>
</tbody>
</table>

### Other Resources

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS 4261 Console</td>
<td>SALES - NA-FED</td>
</tr>
<tr>
<td>BitLocker</td>
<td>Get a BitLocker Recovery Key to regain access to Windows.</td>
</tr>
<tr>
<td>Business Integrity Hotline</td>
<td>File a report on violations of FS policies or standards.</td>
</tr>
<tr>
<td>CA PPM</td>
<td>Project &amp; Portfolio Management for IT and PTG</td>
</tr>
<tr>
<td>Email Quarantine</td>
<td>quarantine.fsn.net.com</td>
</tr>
</tbody>
</table>


Security

- L3/4 Firewall
- IDS/IPS
- Inspection/Visibility/PCAP
- RWP
- FIPS
- Advanced WAF…
Advanced WAF

- L7 FW
- OWASP Top 10
- SQL Injections, XSS, XSRF
- Credential Stuffing (Shape)
- Anti Fraud
- Data Leakage Prevention
- Bi-Direction Protection
- SSN, EDIPI, Credit Card info
- Threat Campaigns…
AWAF – Threat Campaigns

[Image of a network security application interface showing a threat campaign against a Tomcat administrator password guessing - MSIE 10.0 campaign. The request details include GET /manager/html HTTP/1.1, Accept: text/html, application/xhtml+xml, /**, User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Host: 15.200.18.226:80 Authorization: **********. The response is N/A as no response details are available because the request was blocked.]
AWAF – Threat Campaigns

GET /struts2-rest-showcase/orders.xhtml HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %s

Request actual size: 1951 bytes.
AWAF – Threat Campaigns

This campaign aims to spread malware by abusing the Apache Struts 2 Jakarta Multipart Parser vulnerability (CVE-2017-5638) to download and install malware (crypto mining) software by creating jobs. The jobs instruct the compromised machine to download and then execute the spearhead script which would download and deploy the mined-crypto mining software. An examination of the deployed configuration files showed that the threat actor deploys the malware to the "CryptNight" cryptocurrency. CryptNight is a proof-of-work algorithm. It is designed to be suitable for end-user PC CPUs, but currently no special purpose devices for mining are available. Therefore, CryptNight can only be CPU-mined for the time being.

CryptNight was originally implemented in the CryptoNote codebase. More information about CryptNight can be found in the bitcoin wiki. It was changed in Bitcoin to CryptNight.

**Target:** Servers with the Apache Struts 2 framework on Linux

**Payload Tactics:** Download the spearhead script and set a delayed task (cron) to download and install the full malware package.

**Payload Analysis:** The threat actor abuses the vulnerability (CVE-2017-5638) to deploy mined-crypt mining software.

**Catastrophic Damage:** Machines with the malware deployed will suffer from poor performance due to high resource consumption.

**Delivered Malware:**
- **Type:** shell script
- **Family:** Cryptocurrency Miner (mined-crypt)
- **Target System:** Linux
- **Programming Language:** C
- **Malware Analysis:** Downloads the configuration and the malware.
DDOS Prevention

- L3/4
- L7
- Bot Protection
- Geolocation
- IP Intelligence

<table>
<thead>
<tr>
<th></th>
<th>Volumetric Attacks</th>
<th>Protocol Attacks</th>
<th>Application Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is it?</td>
<td>Attacks that use massive amount of traffic saturating the bandwidth of the target.</td>
<td>Attacks that render a target in-accessible by exploiting a weakness in the Layer 3 and Layer 4 protocol stack.</td>
<td>Attacks that exploit a weakness in the Layer 7 protocol stack. The most sophisticated of attacks and most challenging to identify/mitigate.</td>
</tr>
<tr>
<td>How does it cripple the target?</td>
<td>The sheer quantity of traffic generated by the attack can completely block access to the end-resource (a website or a service). The magnitude of the attack is commonly measured in bits or packets per second.</td>
<td>Protocol attacks consume all the processing capacity of the attacked-target or intermediate critical resources like a firewall causing service disruption.</td>
<td>Application attacks establish a connection with the target and then exhaust the server resources by monopolizing processes and transactions.</td>
</tr>
<tr>
<td>Examples</td>
<td>NTP Amplification, DNS Amplification, UDP Flood, TCP Flood</td>
<td>Syn Flood, Ping of Death</td>
<td>HTTP Flood, Attack on DNS Services</td>
</tr>
</tbody>
</table>
Availability & Performance

- Load Balancing
- Global Server Load Balancing - GSLB
- SSL/TLS Offloading (Centralized FIPS Key MGMT)
- WAN & LAN Traffic Optimization
Application Architectures
Office 365

- How do we maximize the investment in O365?
- SSL/TLS Termination
- CAC Auth
- ADFS Web Application Proxy (WAP)
- ADFS Server Farms
- URI Rewrites
- Kerberos Constrained Delegation
- Token Broker / Traffic Direction
- SSO
Using a centralized trusted source of user identity – such as IDaaS, leveraging single sign-on (SSO), and federating identity across **ALL** apps – even those not supporting modern authentication (SAML, OAuth, OIDC) – simplifies user access to **ANY** app.
SAML IDP for SaaS

- BIG-IP can be deployed in both IDP and SP initiated SAML Configurations.

- This is by far the most common SaaS use case.

- BIG-IP can perform CAC Auth in front of either scenario

Cisco UC CAC Enablement and SSO

BIG-IP as the IDP for Cisco Unified Communications Applications

Can be IDP and ADP Proxy

Enabled CAC and SSO for MGMT and Application Access

Configure 2 Factor

Solutions for non-CAC holders

Easy to setup

Enabled CAC and SSO for MGMT and Application Access

Free Options Available
https://duo.com/pricing/duo-free

https://duo.com/docs/f5bigip
More information

• Configuration guide for 215 SaaS Applications:
  • https://github.com/f5devcentral/f5-bigip-agc-config-guides/tree/master/saml-saas-applications/docs

• 4:22 video on configuring the BIG-IP as IDP for Service now:
  • https://www.youtube.com/watch?v=0SRv3ROIYB8
Collocate with CAP/VDSS Services

GSLB

Enterprise VDSS

Navy User
Remote User
Mobile User

Enterprise App Services
SSO Portal, C3D, SAML IDP
IPI, DDOS, TLS Term,
L3/4 FW, AWAF, Threat
Campaigns, IPS, Visibility

IDaaS

On Prem App Services
SSO Portal, C3D, SAML IDP
+ Security

Navy Datacenter
Navy SaaS Apps
Navy Cloud Apps
<table>
<thead>
<tr>
<th>Agency</th>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Force</td>
<td>Eddie Augustine</td>
<td><a href="mailto:e.augustine@f5.com">e.augustine@f5.com</a></td>
<td>301-717-4131</td>
</tr>
<tr>
<td>Air Force</td>
<td>Dustin Purkey</td>
<td><a href="mailto:D.Purkey@F5.com">D.Purkey@F5.com</a></td>
<td>714-501-4815</td>
</tr>
<tr>
<td>Air Force</td>
<td>Arnulfo Hernandez</td>
<td><a href="mailto:A.Hernandez@f5.com">A.Hernandez@f5.com</a></td>
<td>202-360-1984</td>
</tr>
<tr>
<td>Air Force</td>
<td>Paul Deakin</td>
<td><a href="mailto:p.deakin@f5.com">p.deakin@f5.com</a></td>
<td>949-395-0051</td>
</tr>
<tr>
<td>DISA</td>
<td>David Thomas</td>
<td><a href="mailto:d.thomas@f5.com">d.thomas@f5.com</a></td>
<td>703-930-9623</td>
</tr>
<tr>
<td>DISA</td>
<td>Thomas Ries</td>
<td><a href="mailto:T.Ries@f5.com">T.Ries@f5.com</a></td>
<td>703-850-4654</td>
</tr>
<tr>
<td>DISA</td>
<td>Anthony Graber</td>
<td><a href="mailto:anthony.graber@f5.com">anthony.graber@f5.com</a></td>
<td>443-987-6487</td>
</tr>
<tr>
<td>Navy Marine Corps</td>
<td>John Manning</td>
<td><a href="mailto:j.manning@f5.com">j.manning@f5.com</a></td>
<td>703-898-4135</td>
</tr>
<tr>
<td>Army</td>
<td>Archie Newell</td>
<td><a href="mailto:a.newell@f5.com">a.newell@f5.com</a></td>
<td>858-922-2654</td>
</tr>
<tr>
<td>Navy Marine Corps</td>
<td>Paul Simmons</td>
<td><a href="mailto:p.simmons@f5.com">p.simmons@f5.com</a></td>
<td>843-300-7392</td>
</tr>
<tr>
<td>Navy Marine Corps</td>
<td>Jimmy Jennings</td>
<td><a href="mailto:j.jennings@f5.com">j.jennings@f5.com</a></td>
<td>951-334-8558</td>
</tr>
<tr>
<td>Pentagon Defense Agencies</td>
<td>Mark Oldknow</td>
<td><a href="mailto:m.oldknow@f5.com">m.oldknow@f5.com</a></td>
<td>512-410-9462</td>
</tr>
<tr>
<td>Pentagon Defense Agencies</td>
<td>August Weinerstein</td>
<td><a href="mailto:a.winterstein@f5.com">a.winterstein@f5.com</a></td>
<td>301-660-9644</td>
</tr>
<tr>
<td>Army</td>
<td>Brig Lambert</td>
<td><a href="mailto:b.Lambert@f5.com">b.Lambert@f5.com</a></td>
<td>801-319-1221</td>
</tr>
<tr>
<td>Army</td>
<td>Todd Favakeh</td>
<td><a href="mailto:t.favakeh@f5.com">t.favakeh@f5.com</a></td>
<td>847-334-5610</td>
</tr>
<tr>
<td>Army</td>
<td>Shaun Simmons</td>
<td><a href="mailto:s.simmons@f5.com">s.simmons@f5.com</a></td>
<td>412-329-8366</td>
</tr>
<tr>
<td>Army</td>
<td>Michael Slavinsky</td>
<td><a href="mailto:M.Slavinsky@f5.com">M.Slavinsky@f5.com</a></td>
<td>206-637-2056</td>
</tr>
</tbody>
</table>
Thank You
# F5 DoD Virtual User Group (DoDVUG) Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>F5 DoDVUG Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 9th</td>
<td>F5 DoD Virtual User Group #1</td>
<td>F5 Access Policy Manager with remote access, network tunneling, and CAC/PIV Authentication.</td>
</tr>
<tr>
<td>April 23rd</td>
<td>F5 DoD Virtual User Group #2</td>
<td>Get Your SaaS in Gear Enterprise Application Strategy</td>
</tr>
<tr>
<td>May 7th</td>
<td>F5 DoD Virtual User Group #3</td>
<td>Ghastly Wealth Compliance using F5 ASM</td>
</tr>
<tr>
<td>May 21st</td>
<td>F5 DoD Virtual User Group #4</td>
<td>Automation/Orchestration - F5 A/O Toolchain</td>
</tr>
<tr>
<td>June 4th</td>
<td>F5 DoD Virtual User Group #5</td>
<td>SCCA / SACA</td>
</tr>
<tr>
<td>June 18th</td>
<td>F5 DoD Virtual User Group #6</td>
<td>SSLO Orchestrator</td>
</tr>
</tbody>
</table>