

F5 Security Executive Briefing

July 13, 2020





F5 Strategic Direction

DELIVERING CODE TO CUSTOMER

Customer challenges

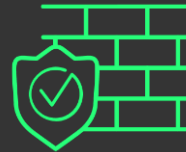
INFRASTRUCTURE LOCK-IN



Limits ability to move apps to new environments

87% of customers are adopting multi-cloud

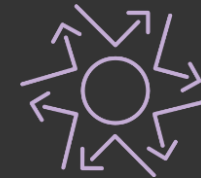
COMPLEX COMPLIANCE & POLICY REQUIREMENTS



Reduces speed to market and impacts customer experience

86% of all cyber-threats target applications and app identities*

TOOL SPRAWL



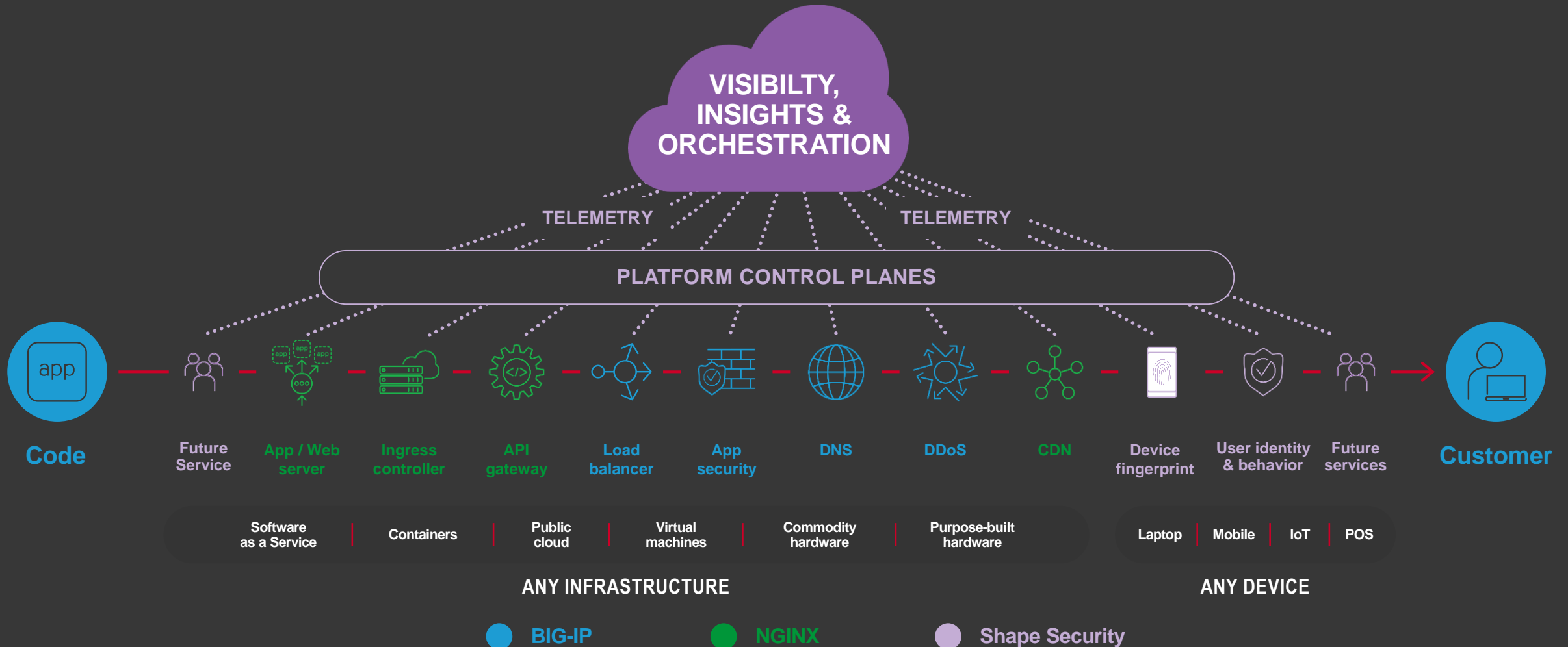
Increases operational complexity and cost

85% of new app workload instances are container based

100% of customers lack visibility

F5 Secure App Delivery Vision

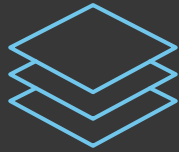
Expand services, deliver insights via telemetry and analytics



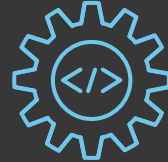
Technology principles to guide our design



**APPLICATION-
CENTRIC**



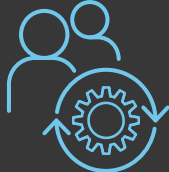
**PLATFORM
INDEPENDENT**



**OPEN SOURCE
AT OUR CORE**



**INTEGRATED
SECURITY**



**ANALYTICS BUILT-IN
AND AI ENABLED**



API FIRST



**MODULAR
AND REUSABLE**

CVE-2020-5902



CVE-2020-5902 – What is it?

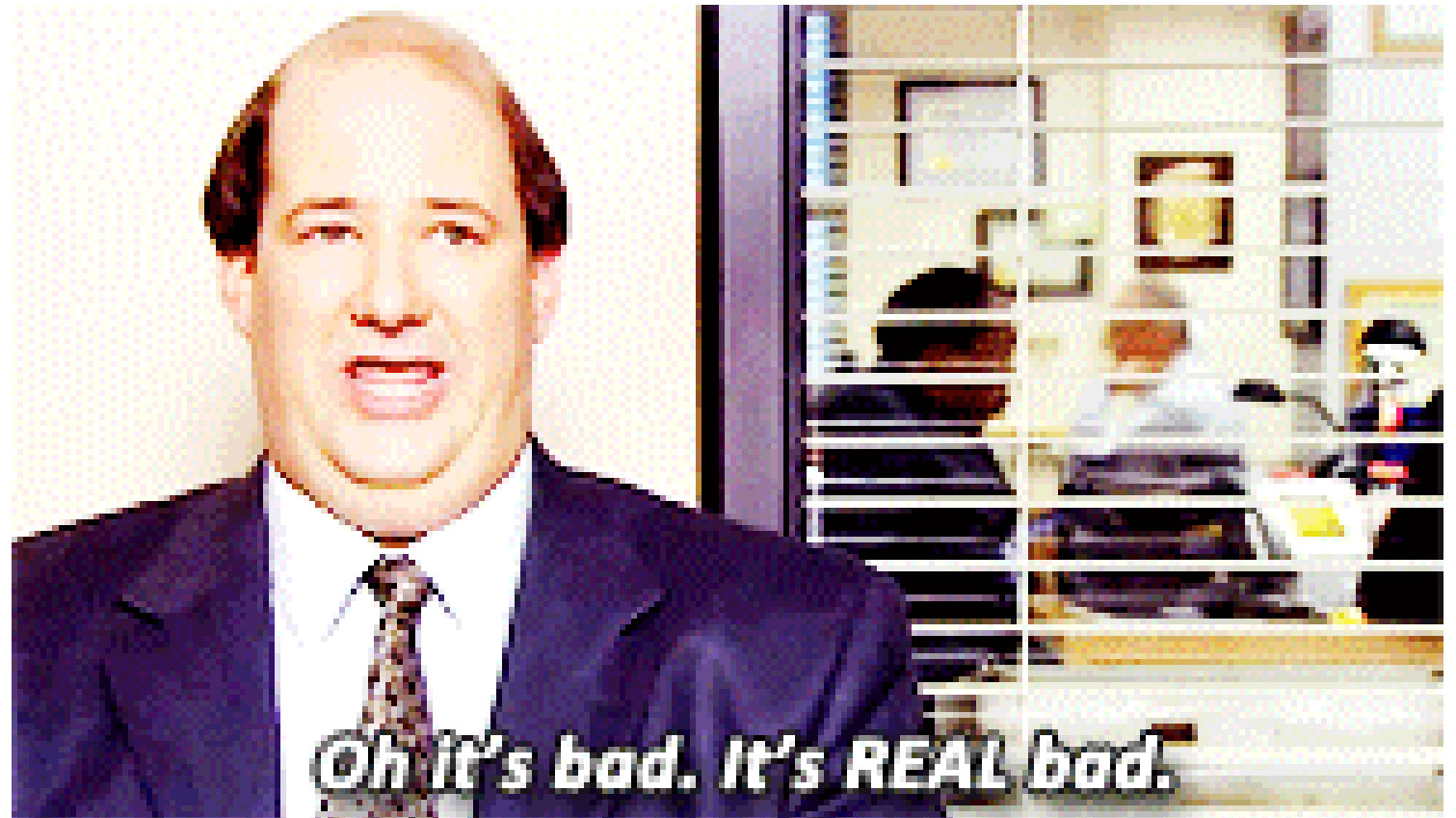
WHAT IS CVE-2020-5902

Level 10 Vulnerability in the
Apache Management Plane

Easily exploitable when there
is access to Management

Hard to track if you have
been exploited

BIG-IP Management Plane is
compromiseable on 11.x
through 15.x



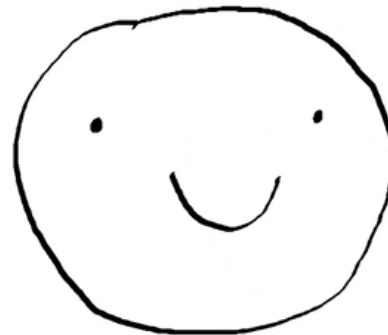
CVE-2020-5902: Can we stop it?

YES... WE HAVE THE TECHNOLOGY

Our SIRT has updated
mitigation steps

First mitigation was
compromised unfortunately

IT'S SOME
GOOD
NEWS!



Mia Page

Constantly updating:

K52145254: TMUI RCE

vulnerability CVE-2020-5902

CVE-2020-5902: Recommendations

NOTE: AS OF JULY 9, 2020 SUBJECT TO CHANGE

Restrict access to Management IPs (SelfIPs and Management IPs)

Know that Management includes API, iControl and Command Line as well as GUI

Patch the httpd service with the latest suggested changes

Upgrade to a version which has been fixed as soon as possible

```
include 'FileETag MTime Size
<LocationMatch ">
Redirect 404 /
</LocationMatch>
<LocationMatch "hsqldb">
Redirect 404 /
</LocationMatch>
'
```

CVE-2020-5902

Good DevCentral Lightboard explains
this in detail

<https://youtu.be/xbtp0gZCxEQ>

There is a live panel on DevCentral
Today on July 9

https://youtu.be/PVsyh_JseI4



Threat Update

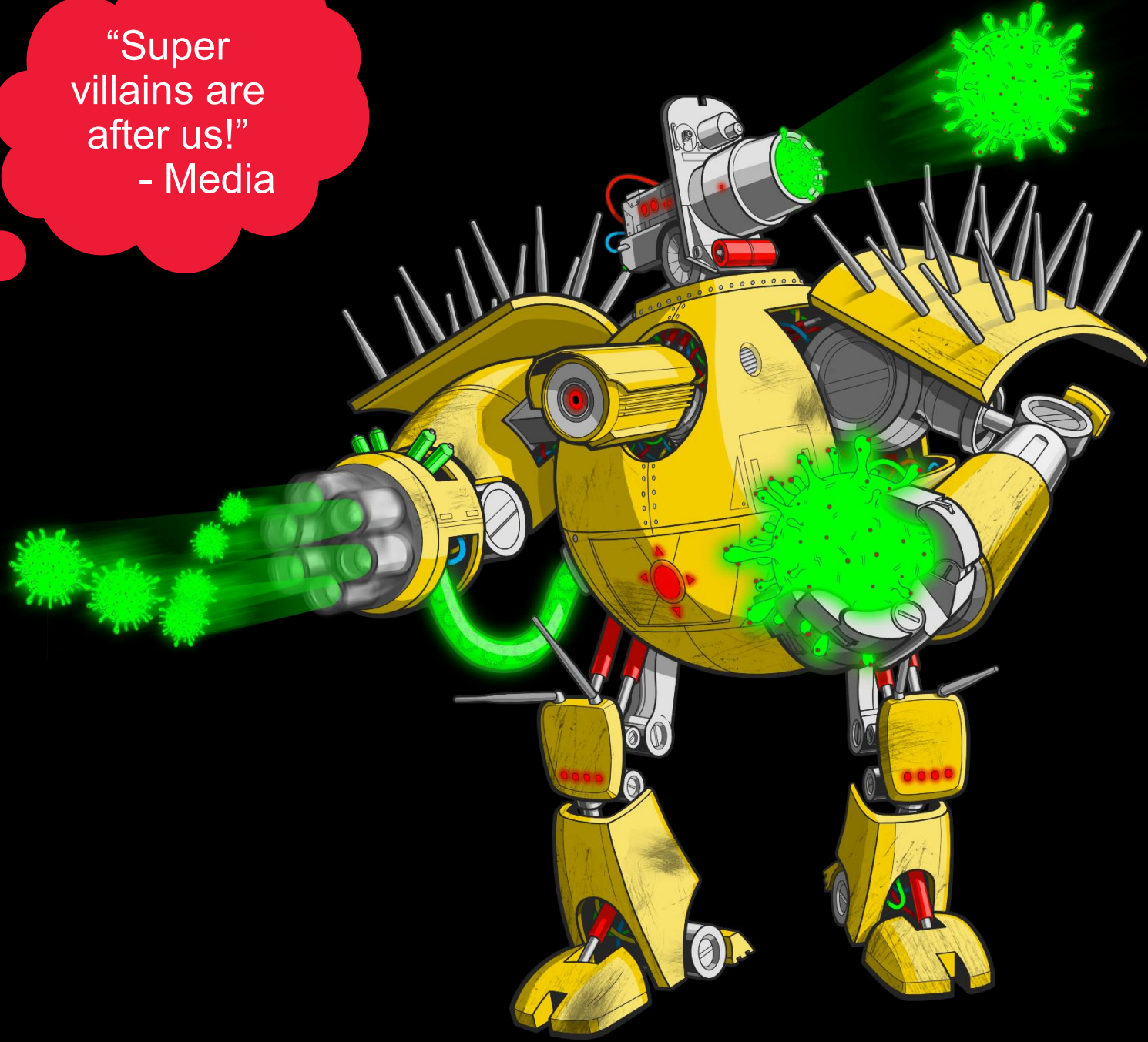
BARELY HANGING ON IN TODAY'S CRAZY WORLD!



Covid-19 ATTACKS!

- Pandemic paralysis
- Reality: The struggle is real for everyone
- Shifting into new normal

“Super
villains are
after us!”
- Media





COVID Attacks



Phishing,
Spam

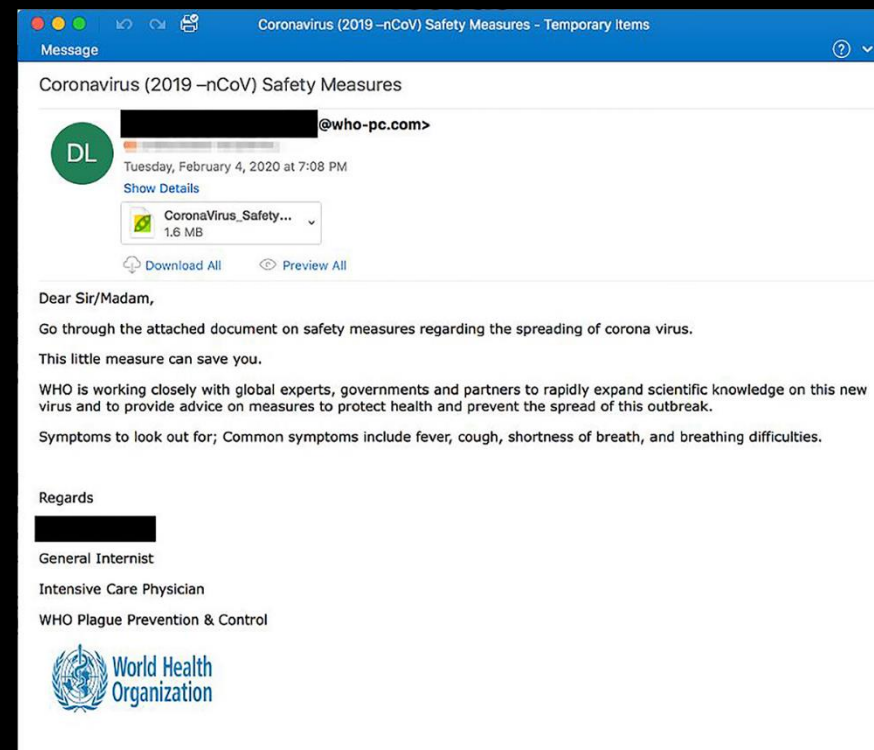
Email and access
based attacks

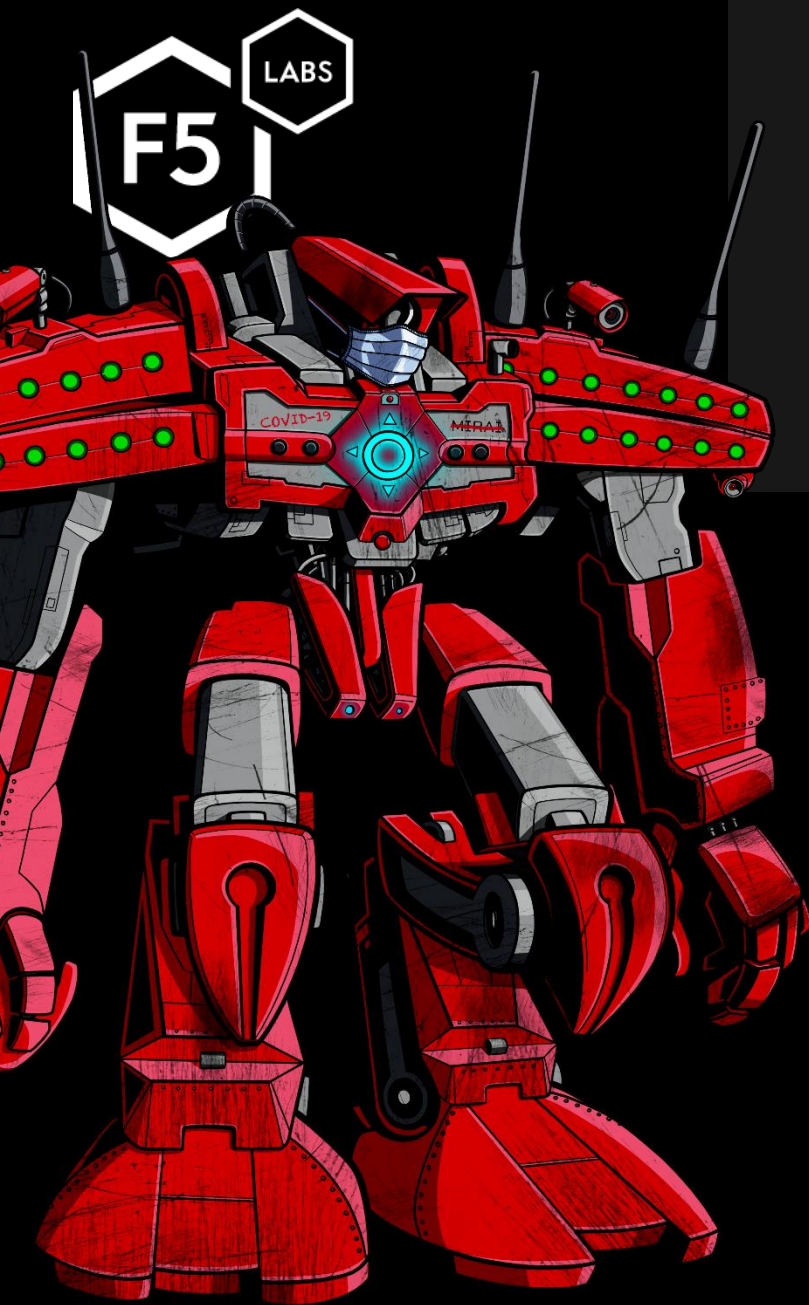
Brute force
Cred stuffing
Business logic

- VPNs, RDP
- Web logins & mail
- Account fraud

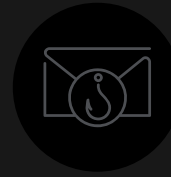
Phishing Impersonating

- WHO
- Public Health Offices (CDC)
- Revenue Agencies
- Human Rights offices
- Charities
- Unicef
- WSJ
- FedEx






COVID Attacks



Email and
access
based attacks



Targeting
consumers
and specific
industries

 **TLP:WHITE**
Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020
PIN Number
20200521-003

Please contact the FBI with any questions related to this Private Industry Notification at either your local Cyber Task Force or FBI CyWatch.
www.fbi.gov/contact-us/field
E-mail:
cywatch@fbi.gov
Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Cyber Criminals Take Advantage of COVID-19 Pandemic to Target Teleworking Employees through Fake Termination Phishing Emails and Meeting Invites

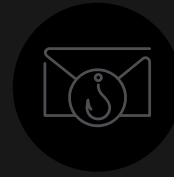
Summary
In response to the recent increase in teleworking during the COVID-19 pandemic, cyber criminals are targeting teleworking employees with fraudulent termination phishing emails and VTC meeting invites, citing COVID-19 as the reason. Employees who are alarmed by the message may not scrutinize the spoofed email address that looks similar to their company's legitimate one. The emails entice victims to click on malicious links purporting to provide more information or online conferences pertaining to the victim's termination or severance packages. Companies should alert their employees to look for emails coming from Human Resources or management with spoofed email domains.

Targeting

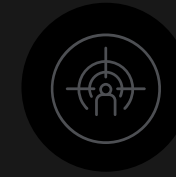
- Consumers / Employees
- Medical Supply Chain, Pharma, Manufacturing
- Government & Military
- Specific VPNs & SOHO routers
- WhatsApp, TeamSpeak
- Languages: English, Italian, Ukrainian, Korean, Chinese



COVID Attacks



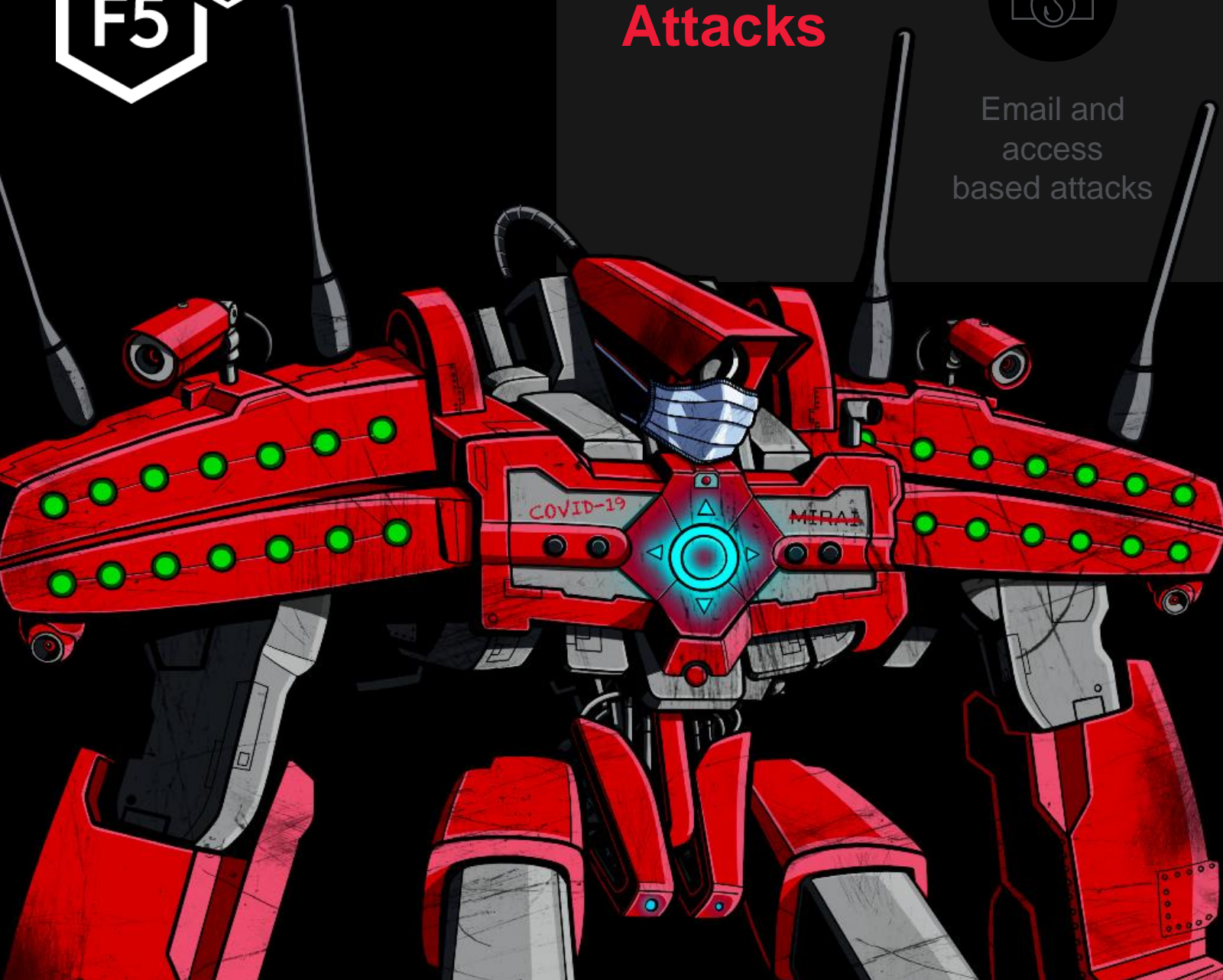
Email and
access
based attacks



Targeting
consumers
and specific
industries



Recycled /
reskinned malware
& ransomware



Malware Families

Ransomware

- **Coronavirus**
- REvil
- Ryuk
- Maze
- Silence

Banking Trojans

- Emotet
- Trickbot
- IoT Botnets
- Oski
- **COVID**

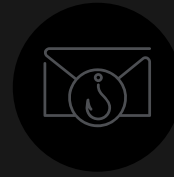
RATs

- Babyshark
- LokiBot
- Nanobot
- HawkEye
- Remcos
- GuLoader
- Koadic
- Ostap
- Kpot

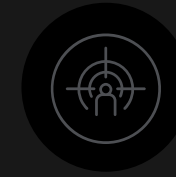
Existed prior to COVID / **Old malware, new name**



COVID Attacks



Email and access based attacks



Targeting consumers and specific industries



Stolen data available for use with new COVID opportunities



Compromised SSNs

86% of US population BEFORE Equifax

Compromised Credit Cards

Compromised Credentials

1 Trillion Records in Cred Stuffing DBs



COVID Attacks



Email and
access
based
attacks



Targeting
consumers
and specific
industries



Recycled /
reskinned malware
& ransomware



Espionage

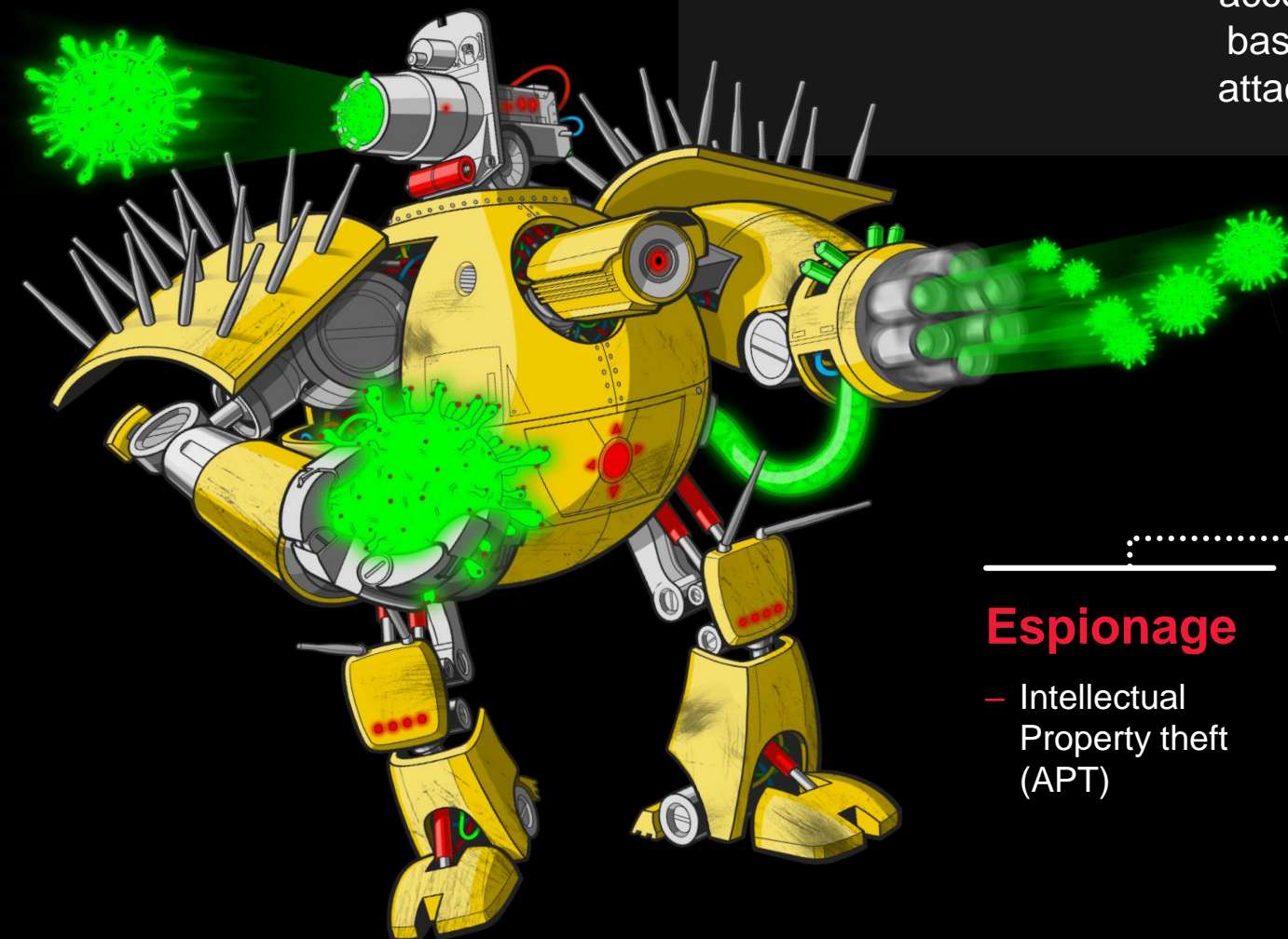
- Intellectual Property theft (APT)

Cybercrime

- Fraud
- Ransom / Extortion
- Cred Stuffing
- PII theft

Hacktivism

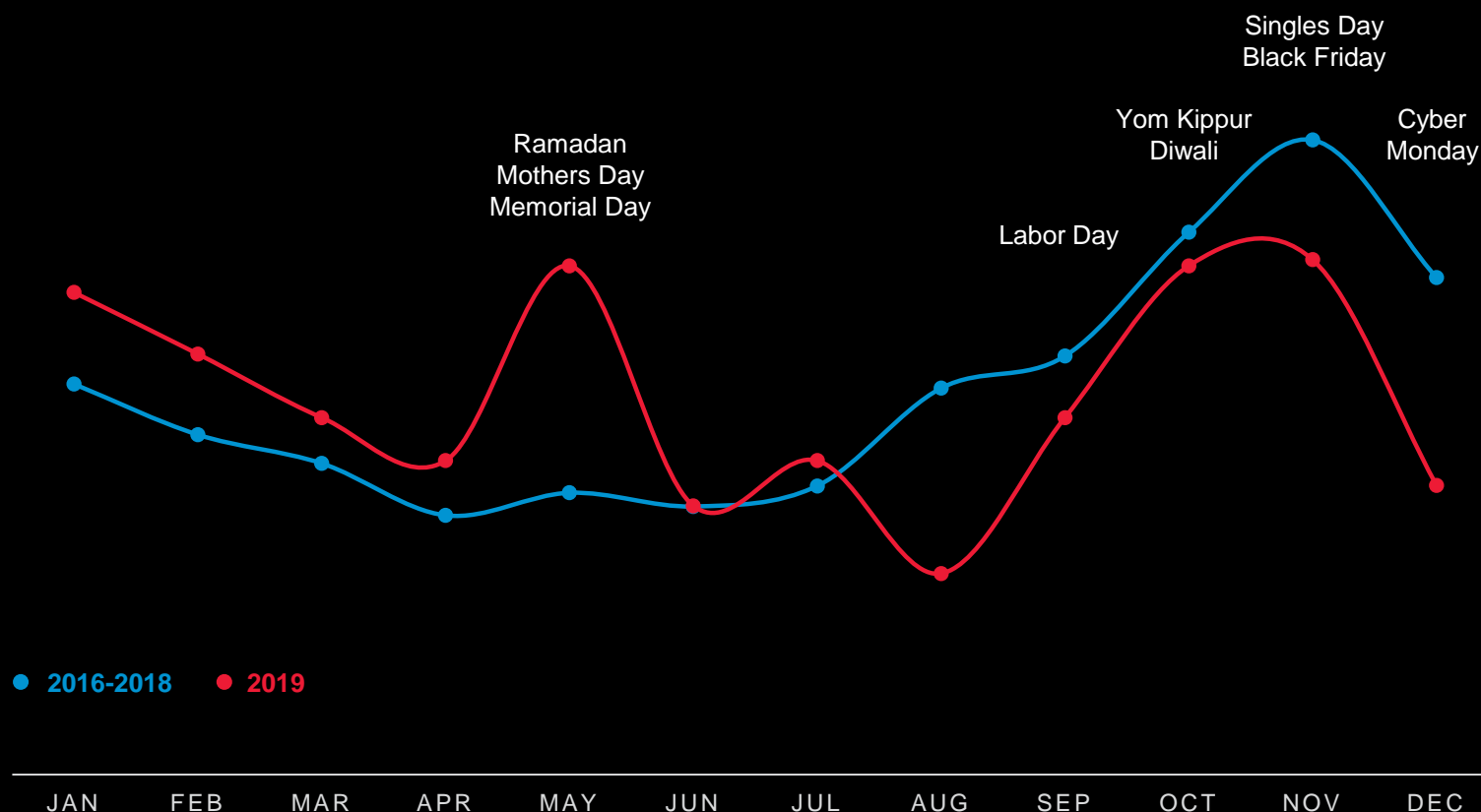
- Disclosing controversial approaches / plans





Phishing and Fraud Attacks

(WebSafe detections 2016 – 2018 compared to 2019)

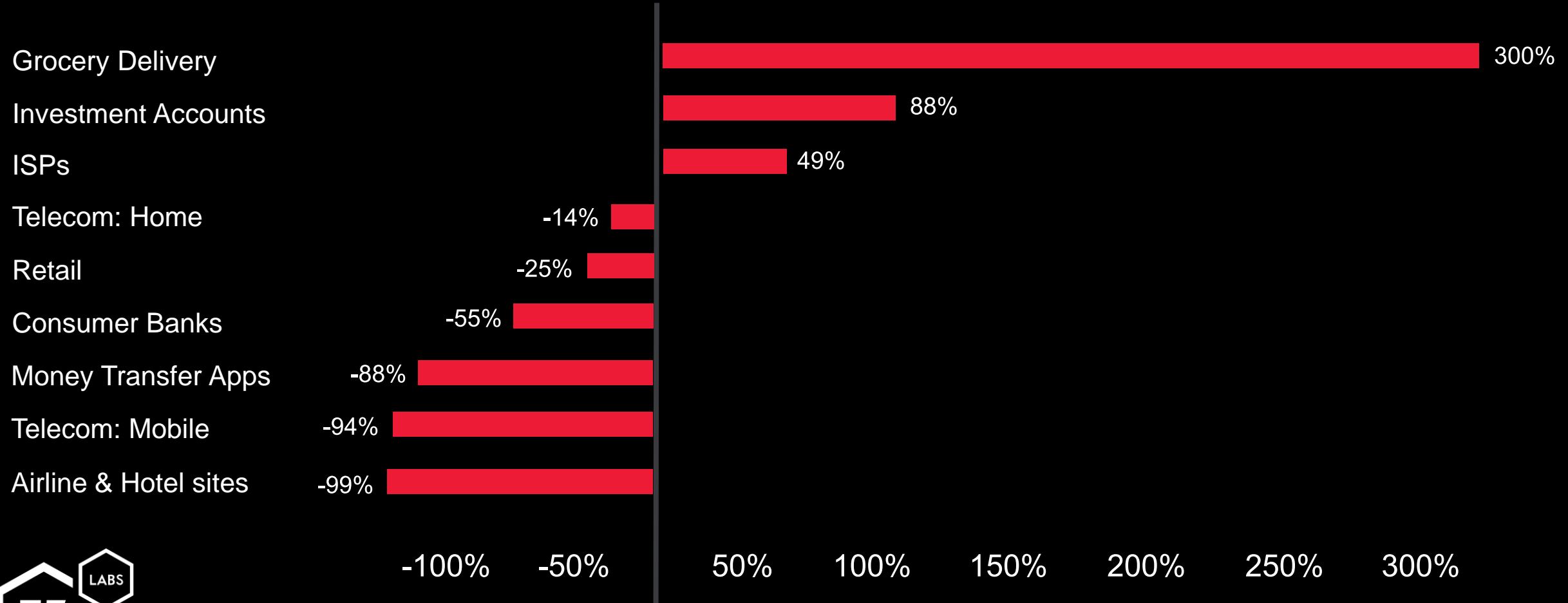


SH-PE

Part of F5

Attacking is a Business

Automated attacks shifting to COVID economic impact
(Average Daily Volumes Jan 1 → March 6th, compared to March 7th and 31st)

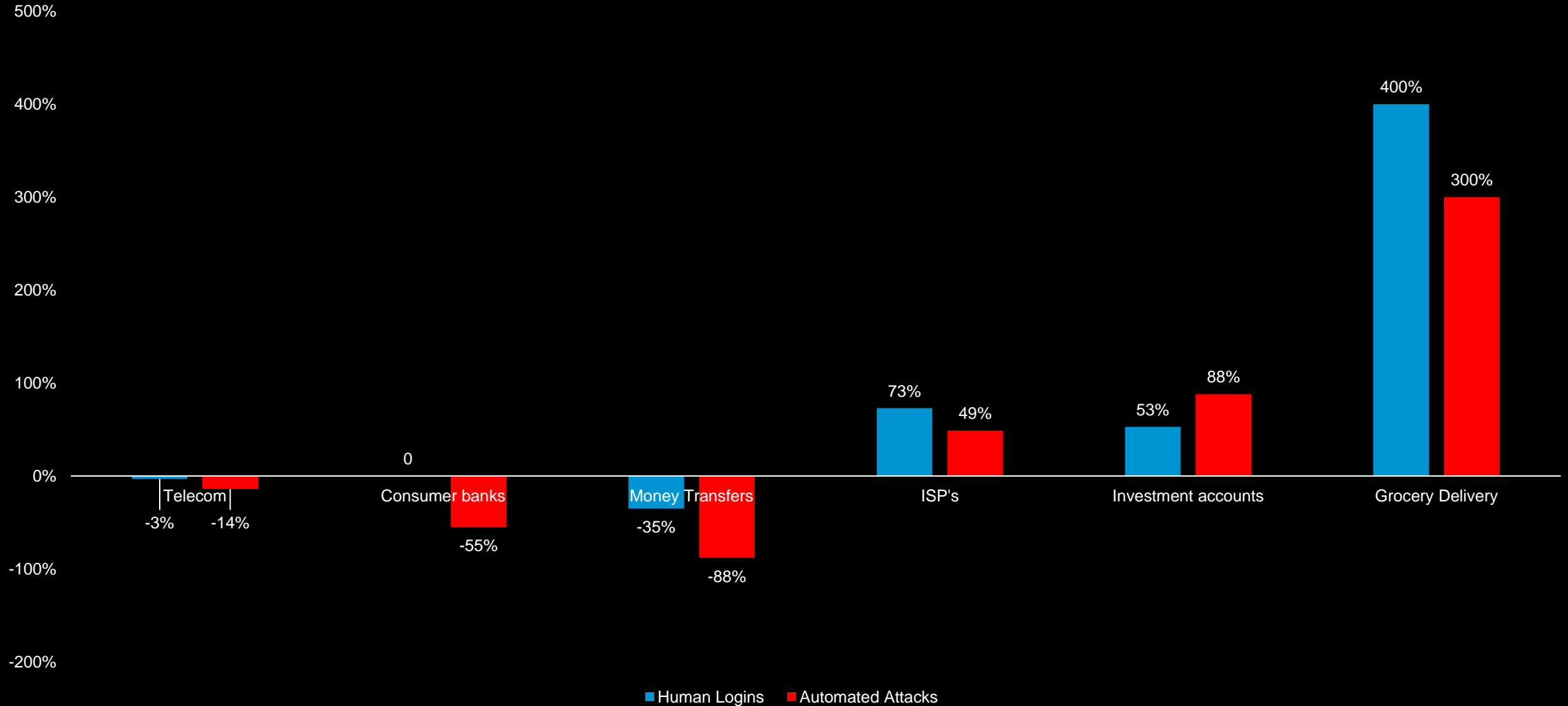


SH=PE

Part of F5

Attacking is a Business

Automated attacks shifting to COVID economic impact
(Average Daily Volumes Jan 1 → March 6th, compared to March 7th and 31st)



SH-PE

Part of F5

Attacking is a Business

Automated attacks shifting to COVID economic impact
(Average Daily Volumes Jan 1 → March 6th, compared to March 7th and 31st)

Travel Industry

Flight & hotel
bookings

Scraping
attempts

Credential
stuffing →
account
takeover

-75%

-65%

-40%





Architecture Changes Driven by Pandemic Response



Attacks go after easy targets



Rapid increase of remote access

Rapid expansion of unplanned remote access can introduce over privileged risks

Increased risk of pivoting attacks

Working “offline” drives more local PII storage and remote management security hurdles

Allowing BYOD authentication to corp network



MFA is being disabled

At a time when phishing campaigns are targeting consumers using corporate resources at home.



RDP (port 3389) exposure publicly up 41%

Publicly discoverable RDP hosts (in Shodan) are up 45% since Jan.

Exposing highly targeted ports publicly attracts brute force, cred stuffing and DoS attacks.

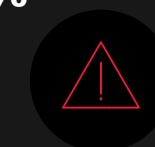


VPN (IKE & PPTP) exposure publicly up 33%

Lack of posture assessments with BYOD

Can't secure internet connection of remote assets when split tunneling.

Exposing login to internet attracts brute force, cred stuffing and DoS attacks.



Rapid expansion of remote access while decreasing security controls



It's not about you... It's how you look.

If Shodan can find
you...

US

AWS
Google Cloud
Azure

China

Tencent
China Telecom

Terminal Servers?
Shifted workloads to the
cloud?

Shodan search results for port:3389. The interface shows a search bar with 'port:3389' and a search button. Below the search bar, there are tabs for 'Exploits', 'Maps', 'Images', 'Like 97', 'Download Results', and 'Create Report'. The main content area displays 'TOTAL RESULTS: 4,415,992' and a world map showing the distribution of results by country. A table lists the top countries and their respective result counts:

Country	Count
United States	1,326,569
China	1,228,366
Germany	166,417
Netherlands	106,755
Brazil	103,162

Below the table, there are sections for 'TOP ORGANIZATIONS' and 'TOP OPERATING SYSTEMS'. The 'TOP ORGANIZATIONS' section lists:

Organization	Count
Tencent cloud computing	605,774
Amazon.com	361,990
Google Cloud	330,935
Microsoft Azure	312,576
China Telecom	179,454

The 'TOP OPERATING SYSTEMS' section lists:

Operating System	Count
Windows 10 or Server 12	10,360
Windows 7 or 8	4,061
Windows Server 2008	2,833
Windows 10	2,273
Windows Server 2003	864

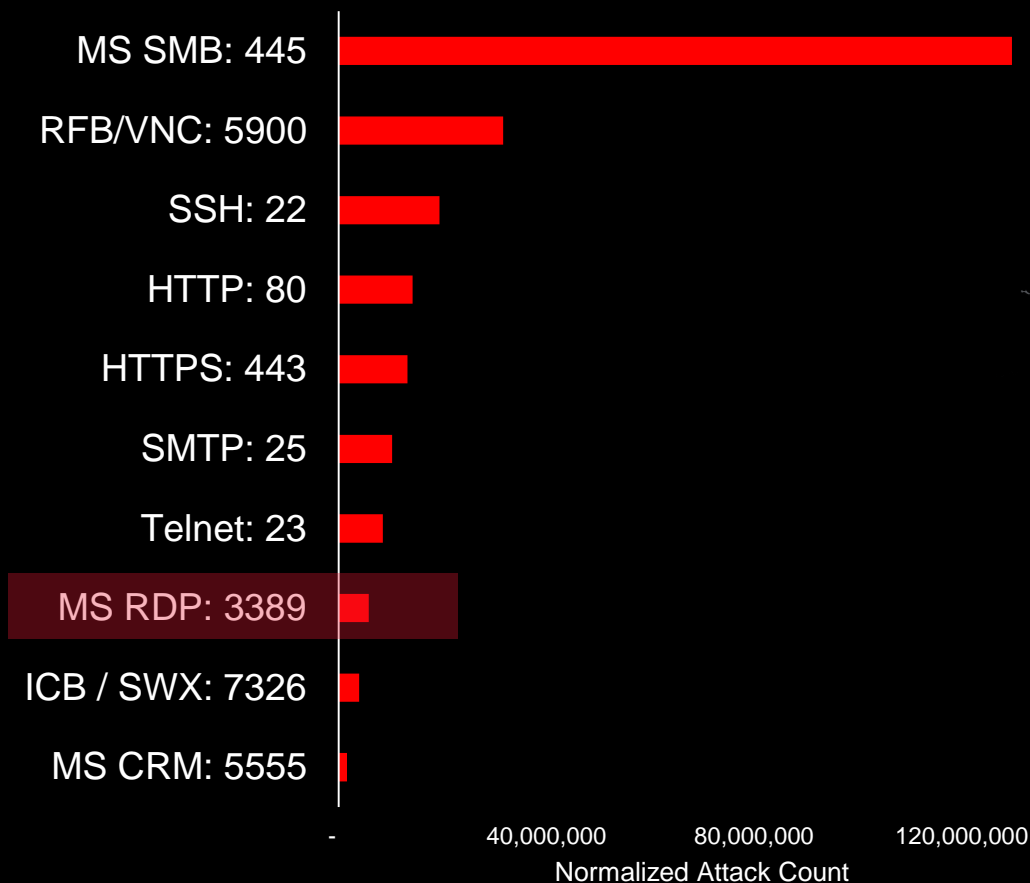
The detailed view of the IP address 61.174.255.251 shows it is located in JINHUA, ZHEJIANG Province, P.R.China. A login page overlay is visible on the right side of the screen, featuring a user icon, a login form with fields for '用户名' (Username) and '密码' (Password), and a '安全登录' (Secure Login) button.



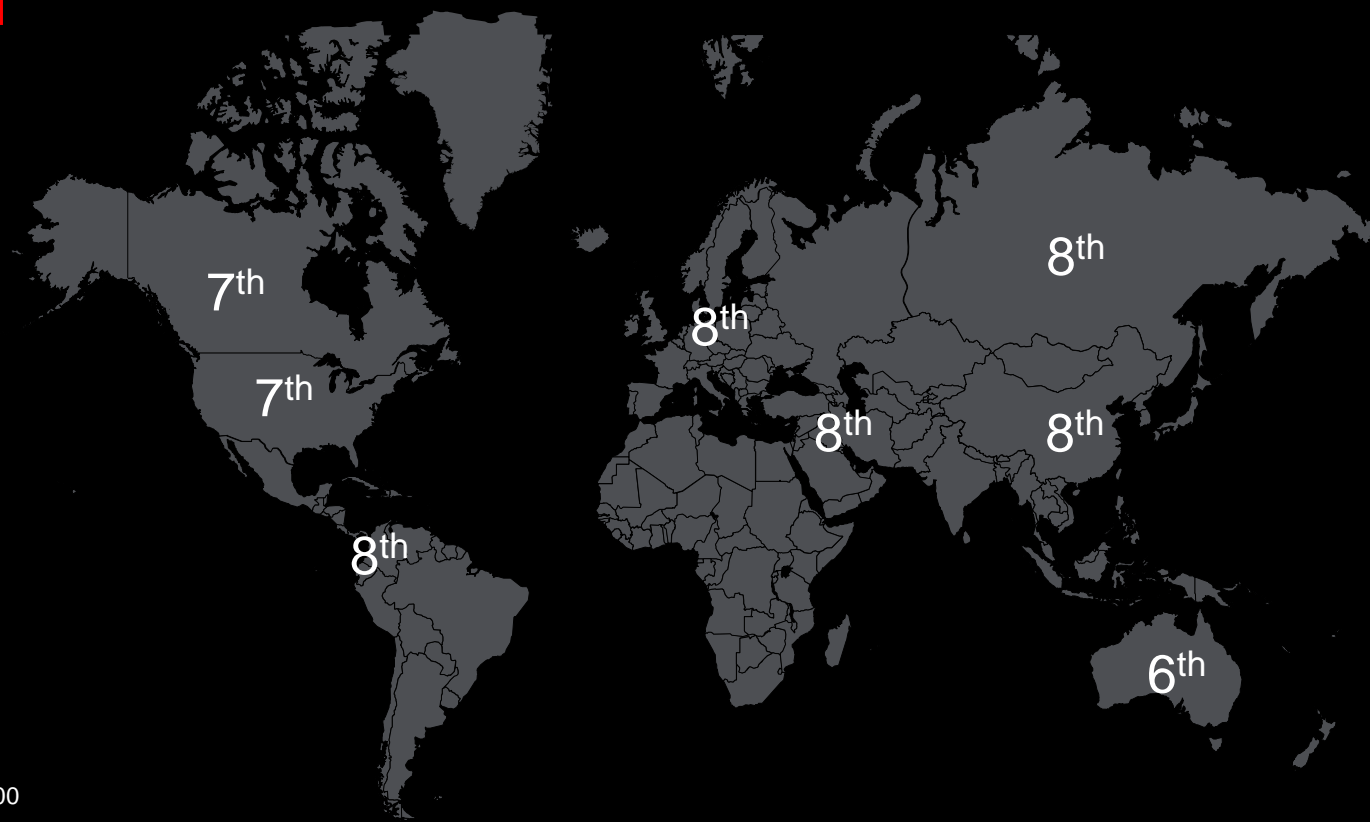
RDP is a Top Target Globally

(Q4 2019)

Global Top Targeted Ports



Top 10 position of RDP port targeting across global regions





Architecture Changes Driven by Pandemic Response



Attackers go after easy targets



Rapid increase of remote access

Review access privileges and true up to business need (and compliance reqs)

Monitor privileged user groups

Keep up with endpoint patching!!!

Limit BYOD devices to web mail only vs full VPN



RDP (port 3389) exposure publicly up 41%

Firewall off insecure and highly targeted services

Deploy an SSL VPN and a remote tech support app instead of enabling RDP.



VPN (IKE & PPTP) exposure publicly up 33%

Ensure posture assessments are conducted upon VPN auth

Remove split tunneling when remote access decreases

Enable decryption to inspect encrypted traffic for malware



MFA is being disabled

Enable MFA in a timely manor prioritized by privileged users and access to critical data

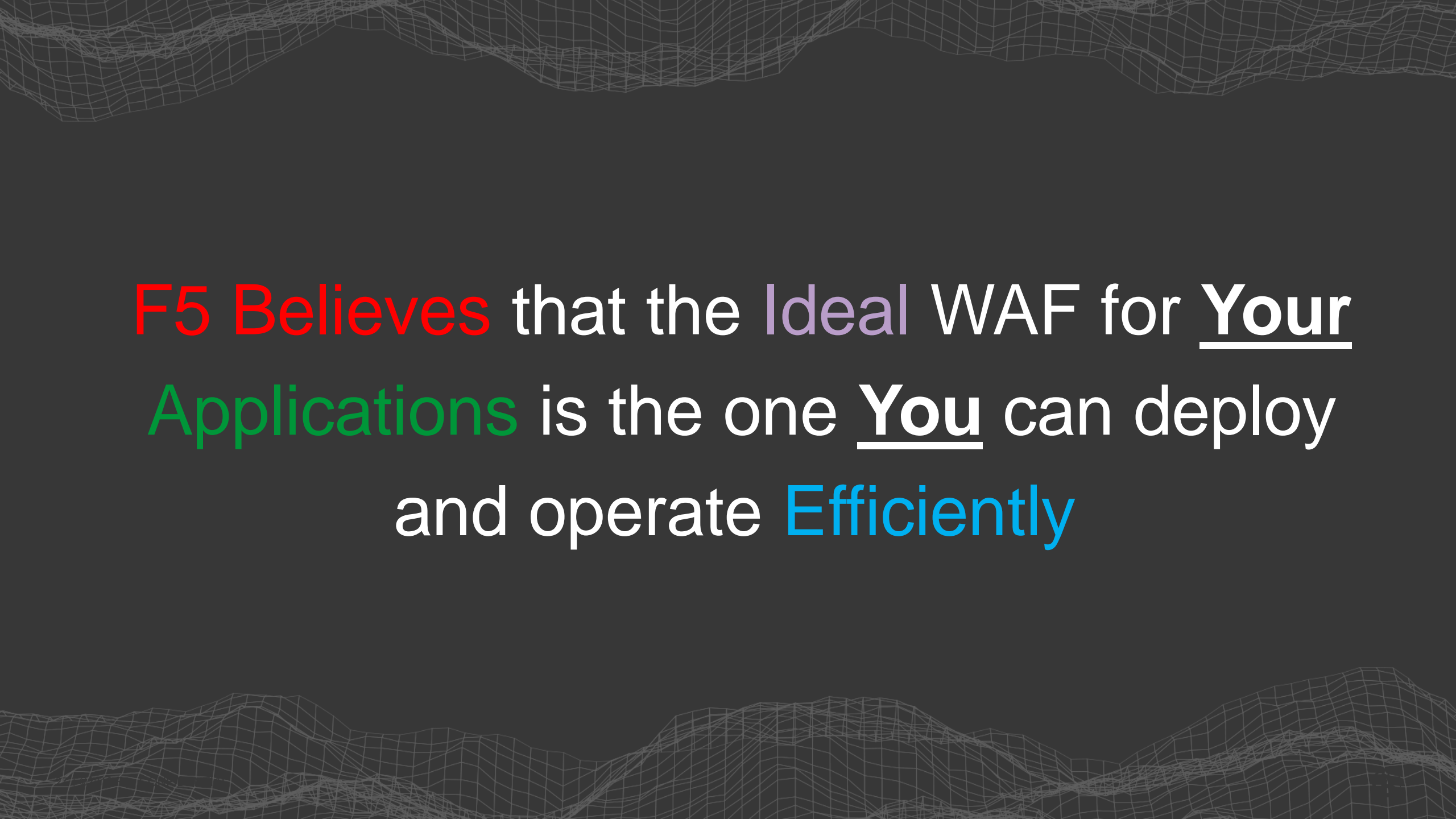
Rapid expansion of remote access access while decreasing security controls





Web Application Firewall

MISSION CRITICAL PROTECTION ACROSS THE FULL
APPLICATION FOOTPRINT

A dark gray background with a white wireframe grid pattern that forms a wavy, mountain-like landscape across the top and bottom of the image.

F5 Believes that the Ideal WAF for Your
Applications is the one You can deploy
and operate Efficiently

Driving WAF Solutions that Address Modern Challenges

- **Compliance** PCI, FIPS, HIPPA, OFAC, NIST....
- **Complicated** Driven by AI/ML and F5 Threat Intelligence.
- **Cloud** Fully automated, in every cloud.
- **Cumbersome** From carrier-grade, to cloud, to container.

Driving WAF Solutions that Address Modern Challenges

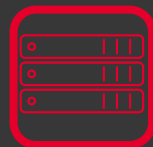
- **Compliance** PCI, FIPS, HIPPA, OFAC, NIST....
- **Complicated** Driven by AI/ML and F5 Threat Intelligence.
- **Cloud** Fully automated, in every cloud.
- **Cumbersome** From carrier-grade, to cloud, to container.

F5 WAF Platforms

F5 Silverline
Managed WAF Service

Essential App Protect
Cloud Based WAF SaaS

F5 Advanced WAF
Best in Class Protection
Hardware and Virtual Edition



+

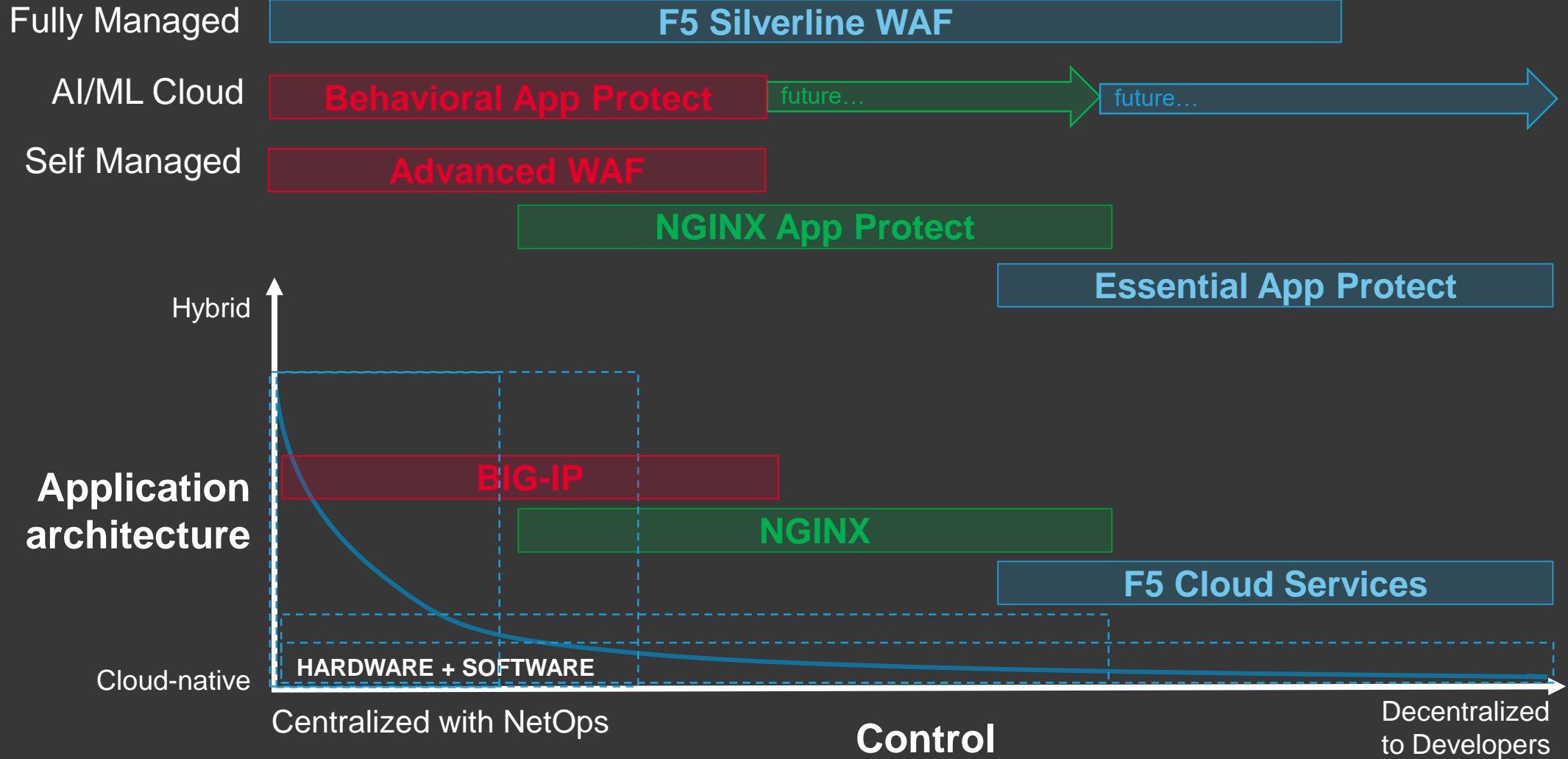


NGINX App Protect
F5 WAF on NGINX *in beta

F5 Intelligent Threat Services



Protecting All Applications: WAF





F5 Advanced WAF

**BEST IN CLASS PROTECTION FOR WEB APPLICATIONS ON
THE BIG-IP PLATFORM**

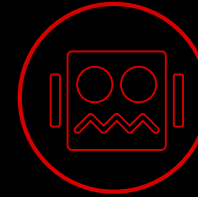
Traditional WAF vendors have been slow to offer protections against Non-OWASP Top 10 attacks



OWASP Top 10



OWASP Top 10



Malicious Bots



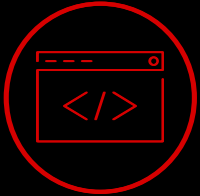
SSL/TLS Inspection



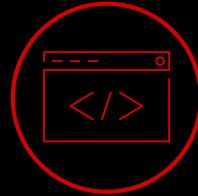
SSL/TLS Inspection



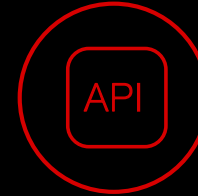
Credential Attacks



Scripting



Scripting



API Attacks

Attacks are evolving and becoming more sophisticated

Automated attacks
increasing in frequency
and sophistication

77% of web attacks start
from botnets

Hackers are targeting
credentials and sensitive
data

3 Billion Credentials were
reported stolen in 2016

App-layer DoS evades
signature-based security
solutions

App-layer DDoS has
increased by 43%

Advanced WAF Delivers New Solutions

- **Bot Protection**

- Key Capabilities: Unified Anti-Bot, Anti-Bot Mobile SDK, Bot Signatures
- Key Business Problems: See the OWAT Top 20.
- Key Components: Advanced WAF, Anti-Bot SDK, BIG-IQ

- **Credential Protection**

- Key Capabilities: Anti-Bot Tech, Device-ID/Centralized Device-ID, Datasafe {client-side credential theft protection}
- Key Business Problems: Brute Force, Targeted Credential Theft
- Key Components: Advanced WAF
- Optional Consideration: Access Policy Manager {enable MFA, federation, etc}

Advanced WAF Delivers New Solutions

- **L7 DDoS Protection**
- Key Capabilities: Auto-Thresholding, L7 Behavioral DDoS Protection, Bad Actor Shunning, Silverline Signaling
- Key Business Problems: Encrypted L7 DDoS Attacks, “Low and Slow” DDoS Attacks, L7 DDoS Protection for Public Cloud Deployments
- **API Protection:**
- Key Capabilities: Advanced Guided Configuration, Reporting, Federation and AAA, JSON/XML fluency, microservices support, bot mitigation, rate-limits and quotas.
- Key Business Problems: API protection, protect sites with co-mingled “web” apps and endpoints, Auth transformation.

But What about “Good OI’ WAF”?

- **Advanced WAF makes the WAF more capable and easier to manage:**
- Bot Protections reduce the threat surface, allowing the administrator to focus on real threat actors.
- Unified Bot Profile makes it easier to apply just Bot mitigation to an application.
- Threat Campaigns provide an accelerated path to high fidelity and high relevance WAF protections for known, active campaigns from the most dangerous global Threat Actors.
- API protection and microservices support provide real-world protections for “apps” and API/Mobile App endpoints—which are often hosted within the same site/fqdn as a traditional web app.

The background is a dark gray grid of circular icons. Each icon contains a white symbol related to technology and security, such as a lightbulb, a fingerprint, a padlock, a right-pointing arrow, a lightning bolt, a Wi-Fi signal, and an atom. The icons are arranged in a repeating pattern across the entire background.

ADVANCED WAF CAPABILITIES

Threat Campaigns

An Advanced WAF will protect against known attack campaigns by threat actors:

- Dynamically updated database of CURRENT known threats
- Context around the attack:
- X exploit by Y threat actor to deliver Z payload
- “Apache struts exploit used by Chinese threat actor to deliver crypto-mining software.”
- Near zero false positives

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential Protection

6 Device-based Protection

6 API Protection

Threat Campaigns

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based DoS Protection

4 Credential Stuffing Protection



5 Client-side Credential Protection




6 Device-based Protection

6 API Protection

Security » Application Security : Threat Campaigns

Threat Campaigns

test   Learning Mode: Automatic Auto-Apply: Real-Time Changes not applied Apply Policy

Q   Name A to Z 

Policy Threat Campaigns

<input type="checkbox"/> Advertisement spam bot - no-cache	Enforced
Comments Spam	
<input type="checkbox"/> Advertisement spam bot - Trident	Enforced
Comments Spam	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - 211720811	Enforced
Malware Spreading - Generic	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - awsnfdp	Enforced
Command Execution Reconnaissance	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - crontab	Enforced
Malware Spreading - Crypto Currency Miner	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - ddos.ctlers.info	Enforced
Malware Spreading - DDoS	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - echo Aman4Wo...	Enforced
Command Execution Reconnaissance	
<input checked="" type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - echo kiss	Enforced
Malware Spreading - DDoS	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - echo Struts2045	Enforced
Command Execution Reconnaissance	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - gbK Bill Gates	Enforced
Malware Spreading - DDoS	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - gift	Enforced
Command Execution Reconnaissance	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - index.action wh...	Enforced
Command Execution Reconnaissance	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - kaK2m2c@	Enforced
Backdoor User	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - Little Snitch	Enforced
Malware Spreading	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - nMaskCustom...	Enforced
Command Execution Reconnaissance	
<input type="checkbox"/> Apache Struts2 Jakarta Multipart Parser - ozo	Enforced
Malware Spreading - Multiple	

Update

Enforcement State

Enforced Disabled

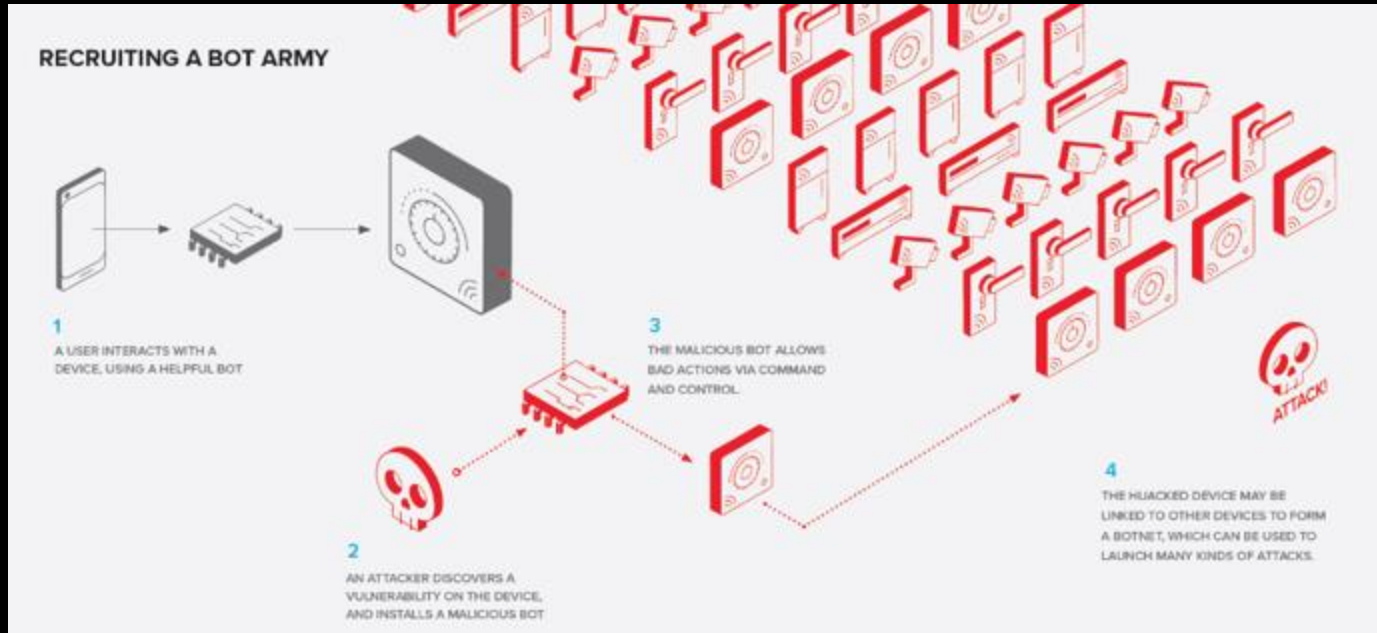
Threat Campaign Details

Name	Apache Struts2 Jakarta Multipart Parser - echo kiss	Risk	High
Intent	Malware Spreading - DDoS	First Observed	2017-03-12
Attack Type	Other Application Attacks	Last Updated	2018-04-01
Description	A campaign exploiting Apache Struts 2 based servers running on Linux systems vulnerable to Jakarta Multipart Parser vulnerability (CVE-2017-5638). The campaign is based on the popular tool which sends two sequential requests, usually within a single minute. First request instructs the server to reply with the string "kiss" as a reconnaissance step and then conducting the attack, by sending a command to stop firewall on popular Linux versions and download and run the malware. Threat actor sends POST requests to /mainAction.action URL which contain 4 URLs in the body as an uploaded file content parameter, named "tmp.txt". The deployed malware belongs to the XorBot Linux malware family which is main purpose to launch DDoS attacks. This malware family usually reports to C&C servers in China and mostly focused in attacking Chinese targets.		
Target	Servers based on Struts 2 framework on Linux		
Collateral Damage	Infected machines will be used to conduct DDoS attacks against various targets and execute attackers arbitrary tasks.		
Delivered Malware			
Type	DDoS		
Family	XorBot		
Target System	Unix/Linux		
Programming Language	C		

Reference	CVE-2017-5638
-----------	---------------

Total Entries: 65

Automation is the Single Biggest Threat



Half of Internet traffic
comes from bots

30% is malicious

web attacks

77% of web app attacks
were the targets of botnet
activity

account takeover

Total account takeover
losses reached \$2.3B in
2016

Vulnerability Scanning
Web Scraping
Denial of Service

FIGHTING THE BOT BATTLE ON MANY FRONTS



Simple bots



Impersonating Bots



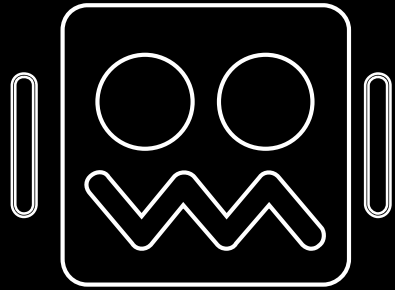
Bots with cookies / JS support



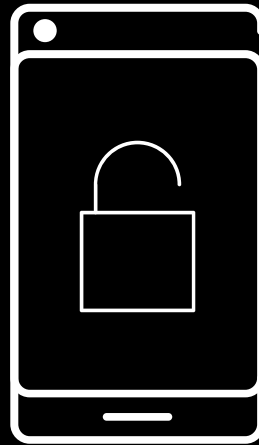
Bots that simulate browsers



Security for Mobile Applications



target of the same
automated attacks



lack mature
security capabilities



needs mobile
specific security

Advanced Bot Protections

An Advanced WAF will protect against sophisticated bots and automated browsers:

- Validation of browser capabilities
- Allow, Block, Drop, Rate limit
- Granular control of mitigations
- “Order of Operations” is significant
- Remove all the “noise” from your WAF logs
- Anti-bot Mobile SDK
- Validate requests from mobile clients/apps
- Simple integration thru AppDome

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

Advanced Bot Protections

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

Bot Profile Configuration

General Settings

Mitigation Settings

Microservice Protection

Browser Verification

Mobile Applications

Signature Enforcement

Whitelist

Mitigation Settings

Trusted Bot	Alarm
Untrusted Bot	Alarm
Suspicious Browser	CAPTCHA
Malicious Bot	<div>None Alarm CAPTCHA ✓ Rate Limit Block TCP Reset</div>
Unknown	for 30 transactions per second

Strict Mitigation Enforcement Cases

DoS Attack Mitigation Mode	Enabled	Disabled	?
API Access for Browsers and Mobile Applications	Enabled	Disabled	?

Mitigation Settings Exceptions

+ Add Exceptions

iMacros Extension Suspicious Browser Extensions (Suspicious Browser)	Alarm	Cancel
Selenium WebDriver Browser Automation (Malicious Bot)	CAPTCHA	Cancel
YiioBot Search Engine (Trusted Bot)	Rate Limit for 5 transactions per second	Cancel

Advanced Bot Protections

1 Threat Campaign Protection

2 Advanced Bot Protection

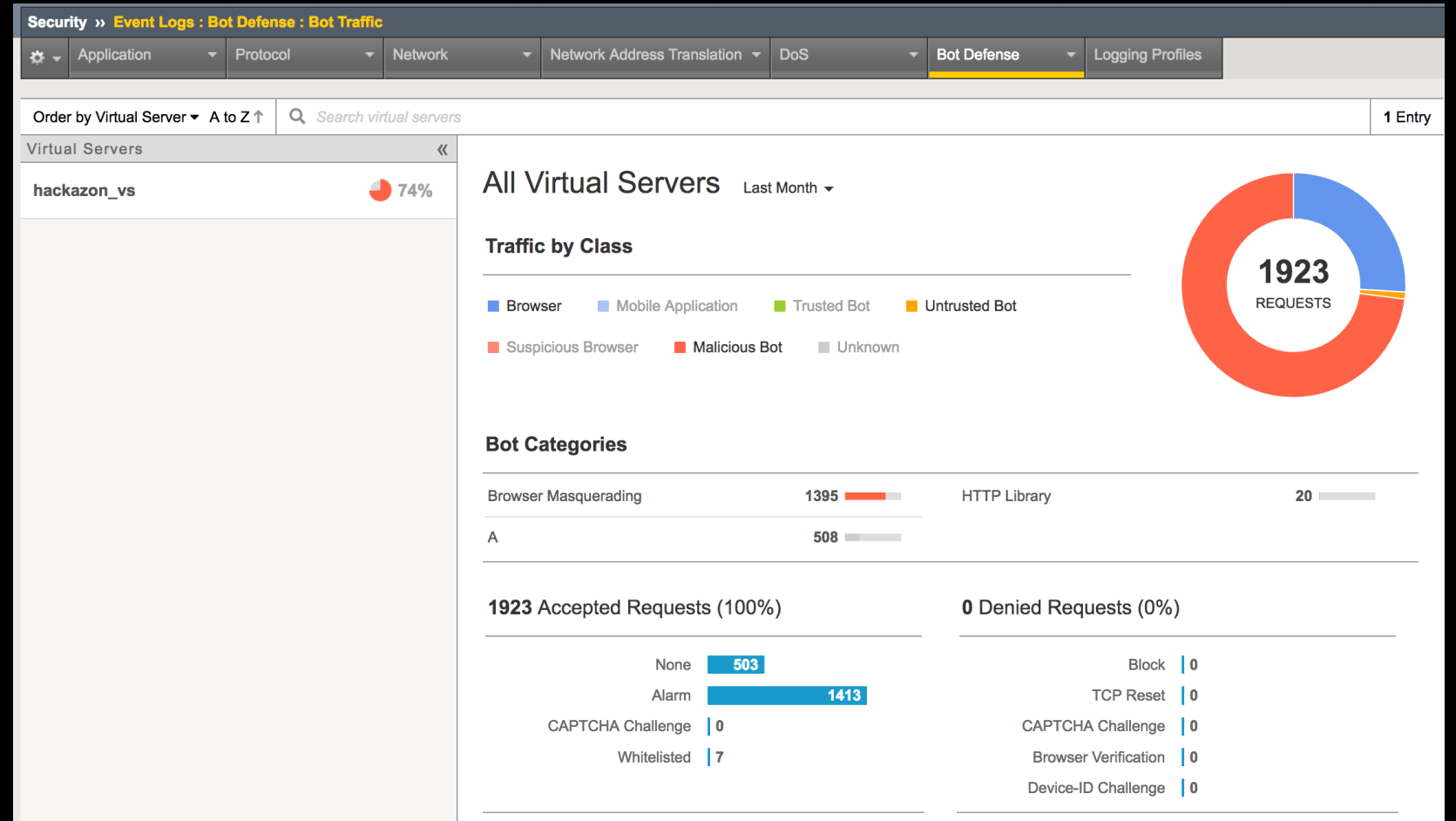
3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

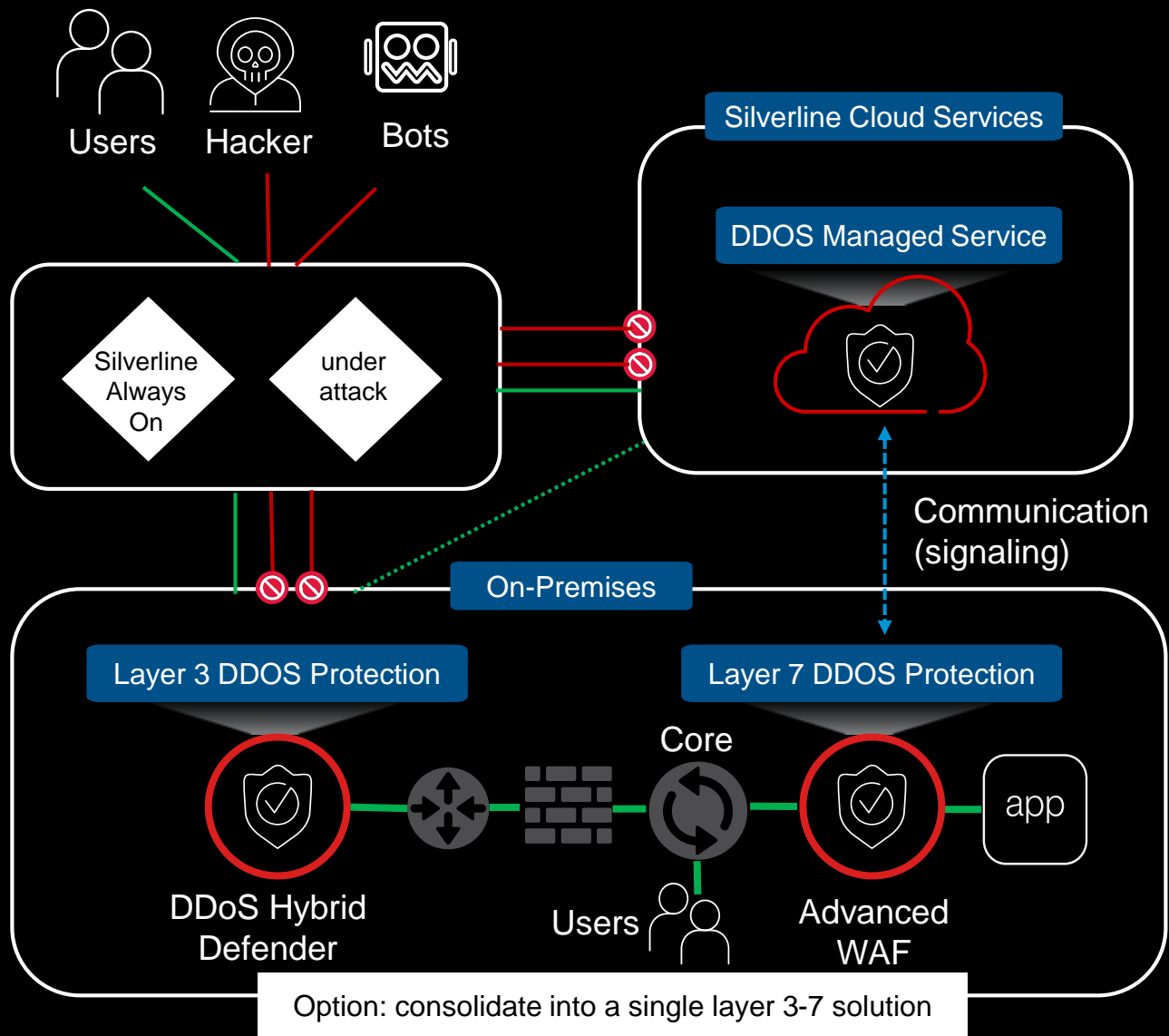
5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection



Use Case - DDoS Attacks



Problem:

- DDOS attacks are growing, but your resources are not
- DDoS mitigation time is slow due to manual initiation and difficult policy tuning

Solution:

- Always-on protection with on-premises hardware
- Mitigate with layered defense strategy and cloud services
- F5 SOC monitoring with portal
- Protect against all attacks with granular control
- Eliminate time-consuming manual tuning with machine learning

Benefits:

- On-premise hardware acts immediately and automatically to mitigate attacks.
- Silverline cloud services minimizes the risk of larger attacks crippling your site or applications

L7 & Behavioral DoS Protection

An Advanced WAF will protect against Layer 7 attacks against web applications:

- "Low-and-slow" attacks (SlowLoris, Slow POST)
- Resource-intensive URLs
- Behavioral0based detection and mitigation
- Profile traffic during "peace-time"
- Headers, URI, query string, parameters, user-agent, more...
- Watch application health/stress
- Identify anomalies and create dynamic signature based on behavior of requests causing stress

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

L7 & Behavioral DoS Protection

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential Protection

6 Device-based Protection

6 API Protection

L7 Behavioral DoS Signature

Dynamic

							Creation Info				Threshold EPS			
<input checked="" type="checkbox"/>	Name	Family	Deployment State	Approval State	Shareability	Attack Status	Creation Time	Context	Profile	Attack ID	Detection	Mitigation	Dropped EPS	Current EPS
<input type="checkbox"/>	HTTPSig14578913620402084120434809167	HTTP	Mitigate	Unapproved	Not-shareable	➔	Mon Mar 19, 11:34:51 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0
<input type="checkbox"/>	HTTPSig3979798321798008414434809167	HTTP	Mitigate	Unapproved	Not-shareable	➔	Mon Mar 19, 11:32:37 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0
<input type="checkbox"/>	HTTPSig5578984904294979364434809167	HTTP	Mitigate	Unapproved	Not-shareable	➔	Mon Mar 19, 11:32:37 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0

HTTPSig5578984904294979364434809167

Alias
/Common/HTTPSig5578984904294979364434809167

Creation Time
Mon Mar 19, 11:32:37 2018 -0400

Last Modified
Mon Mar 19, 11:32:37 2018 -0400

Description

Predicates String

(http.x_forwarded_for_header_exists eq true) and (http.accept_encoding_header_exists eq true) and (http.user_agent_header_exists eq true) and (http.pragma_header_exists eq true) and (http.host_header_exists eq true) and (http.uri_len between 0-15) and (http.accept_contains application) and (http.accept_header_exists eq true) and (http.uri_parameters eq no-query) and (http.headers_count eq 8) and (http.referer_header_exists eq true) and (http.request.method eq GET) and (http.cache_control_header_exists eq true) and (http.cache_control hashes-to 14) and (http.referer hashes-like http://www.coolmike.com/yippie.html) and (http.uri_file hashes-like /wishlist)

Most Recent Attacks

Attack ID	Context	Profile	Attack Time	Accuracy	Detection Threshold EPS	Mitigation Threshold EPS	Current EPS
434809168	Hackazon_BaDOS_protected	Hackazon_BaDOS	Mon Mar 19, 11:43:43 2018 -0400	100%	0	0	0

Password-Stealing Malware Remains Key Tool for Cybercriminals



McAfee Labs Threats Report
June 2017

This report was researched and written by:

Christiaan Beek
Diwakar Dinkar
Yashashree Gund
German Lancioni
Niamb Minihane

SC Magazine US > News > CloudFanta campaign suspected of stealing 26K email credentials



CloudFanta campaign suspected of stealing 26K email credentials



Netskope researchers spotted a variant of malware campaign dubbed “CloudFanta” which may have been used to steal 26,000 email credentials including addresses, usernames, and passwords.



Researchers said the malware is unique because it uses cloud services to d infects users executables)

Schneier on Security

[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Talks](#) [Academic](#) [About Me](#)

Content

[Blog](#) >

Executive Summary

Key Topics

Malware evasion tec

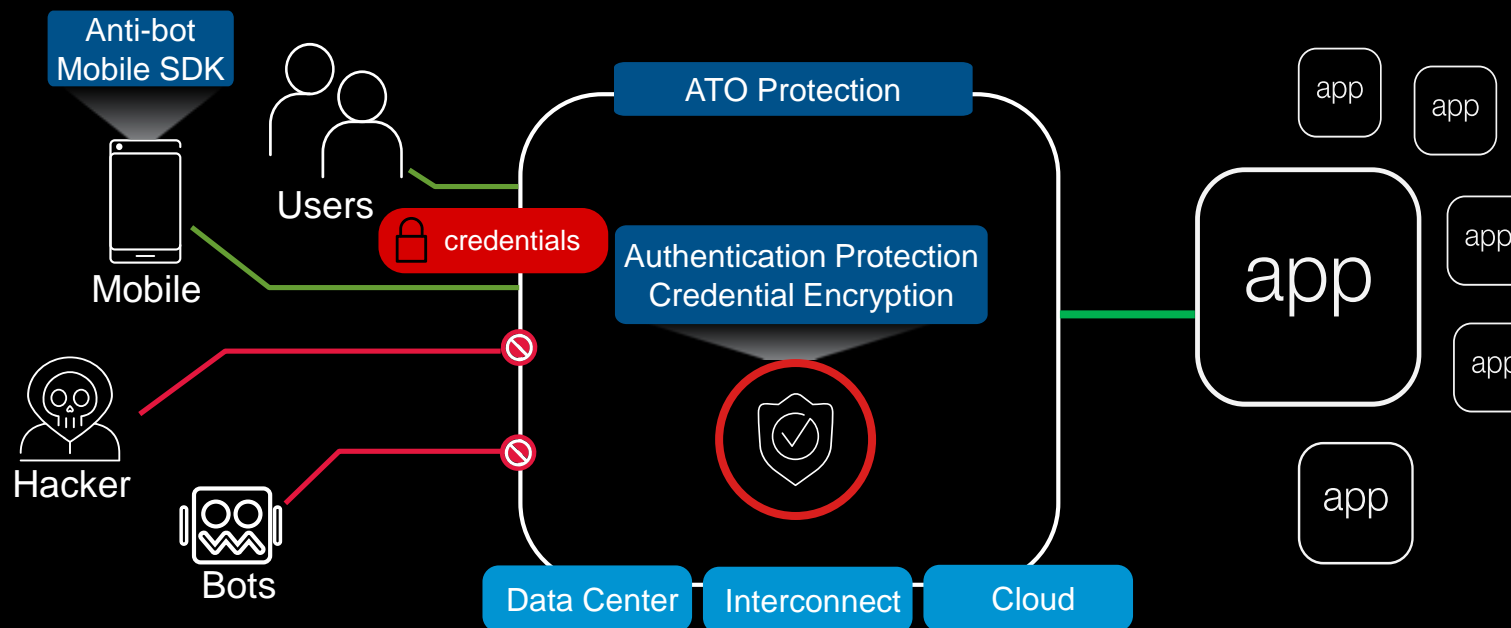
Hiding in plain sight: of steganography

The growing danger

Credential Stealing as an Attack Vector

Traditional computer security concerns itself with vulnerabilities. We employ antivirus software to detect malware that exploits vulnerabilities. We have automatic patching systems to fix vulnerabilities. We debate whether the FBI should be permitted to introduce vulnerabilities in our software so it can get access to systems with a warrant. This is all important, but what's missing is a recognition that software vulnerabilities aren't the most common attack vector: credential stealing is.

Use Case - Account Takeover



Problem:

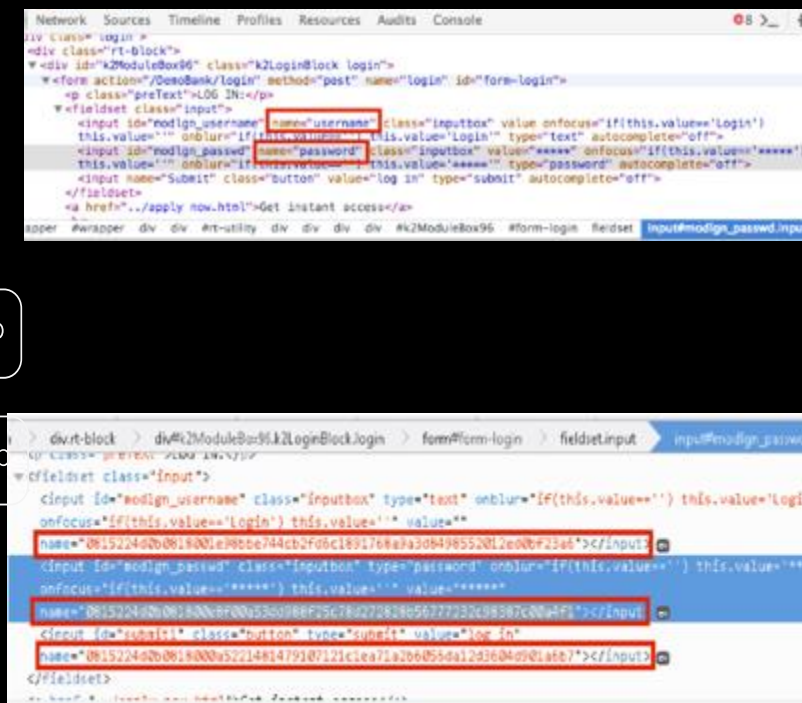
- Criminals are performing account takeover by stealing account credential via malware

Solution:

- App-level credential encryption
- Anti-bot mobile SDK
- Credential Stuffing protection
- Brute force protection

Benefits:

- Prevent the use of dumped credential databases (credential stuffing)
- Prevent the theft of user credentials (credential harvesting)
- Protect mobile apps - Identify and pass only the desired mobile applications.



Credential Stuffing Protection

An Advanced WAF will protect against attempts to authenticate using known leaked/stolen credentials:

- Dynamically updated database of known stolen credentials
- Detection and mitigation for "low-and-slow" login attacks
- Detection and mitigation for JS-challenge and CAPTCHA-challenge bypass
- Cloud-based subscription service {available 2H19}.

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

Credential Stuffing Protection

1 Threat Campaign Protection

2 Advanced Bot Protection



3 L7 & Behavior-based DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential Protection

6 Device-based Protection

6 API Protection

Brute Force Protection Configuration	
Login Page	[HTTP] /user/login
IP Address Whitelist 	IP Address Whitelist is empty
Source-based Brute Force Protection	
Detection Period	2 Minutes
Maximum Prevention Duration	2 Minutes
Username	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 3 failed login attempts Action: <input type="text" value="Alarm and CAPTCHA"/>
Device ID	Trigger: <input checked="" type="radio"/> Never <input type="radio"/> After 3 failed login attempts Action: <input type="text" value="Alarm and CAPTCHA"/>
IP Address	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 20 failed login attempts Action: <input type="text" value="Alarm and Honeypot Page"/>
Client Side Integrity Bypass Mitigation	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 3 successful challenges with failed logins from IP Address / Device ID / Username Action: <input type="text" value="Alarm and CAPTCHA"/>
CAPTCHA Bypass Mitigation	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 5 successful challenges with failed logins from IP Address / Device ID Action: <input type="text" value="Alarm and Drop"/>
Note: Default Honeypot page will be used for the "Honeypot Page" enforcement action. Failed Login Honeypot Response may be customized in the Response Pages 	
Distributed Brute Force Protection	
Detection Period	15 Minutes
Maximum Prevention Duration	60 Minutes
Detect Distributed Attack	<input type="radio"/> Never <input checked="" type="radio"/> After 100 failed login attempts
Detect Credential Stuffing	<input checked="" type="radio"/> Never <input type="radio"/> After 100 login attempts that match known leaked credentials dictionary
Mitigation	<input type="text" value="Alarm and CAPTCHA"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/> <input type="button" value="Restore Defaults"/>	

Credential Stuffing Protection

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

Security » Event Logs : Application : Brute Force Attacks														
⚙		Application		Protocol		Network		DoS		Bot Defense		Logging Profiles		
Q		⬆️ Attack Start Time		Newest		↓		Total Entries: 4						
Distributed Attack				Ongoing										
322		[HTTP] /user/login		13:12:26 2017-10-30										
Distributed Attack				Ended			Attack Summary							
10706		[HTTP] /user/login		12:41:11 2017-10-30			Mitigated IP Addresses		Mitigated Device IDs		Mitigated Usernames		Known Leaked Credentials	
Distributed Attack				Ended			100 out of 128 Mitigated IP Addresses							
10100		[HTTP] /user/login		12:36:04 2017-10-30										
Distributed Attack				Ended										
650		[HTTP] /user/login		12:30:55 2017-10-30										

Client-side Credential Protection

An Advanced WAF will protect against credential theft at the client browser:

- Man-in-the-browser malware
- Steals credentials:
- POST grabbers
- Injected JS – even before credentials are submitted

- DataSafe protects credentials in client browser
- Field obfuscation
- Real-time encryption of password (other fields)
- JS keylogger protection

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

Device-based Protection

An Advanced WAF will identify individual devices and detect and mitigate malicious devices:

- Injected JS fingerprints device
- DeviceID used to correlate requests from the same device, regardless of proxies used and/or other attempts to evade detection
- Cloud-based Security Analytics for Global protection. {Early Access}

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential Protection

6 Device-based Protection

6 API Protection

API Protection

In coordination with Access Policy Manager, Advanced WAF provides robust protections for modern APIs:

- Advanced Guided Configuration for ease of deployment.
- API Reporting Dashboard with rich analytics.
- Federation, SSO and Auth Transformation.
- API fluency: JSON, XML, WebSockets.
- Microservices support, traffic steering, Bot mitigation and flexible rate-limiting and quota enforcement.

1 Threat Campaign Protection

2 Advanced Bot Protection

3 L7 & Behavior-based
DoS Protection

4 Credential Stuffing Protection

5 Client-side Credential
Protection

6 Device-based Protection

6 API Protection

API Protection Updates + Dashboard

Customer Challenges

- Customers need to protect their APIs and have confidence and visibility in that respect; they need to know what risks they are facing and what kinds of attempts are being made against them.

F5 Solution

- New configuration pane dedicated to APIs to simplify the creation and management of API security policies
- New API dashboard provides details on API protection including the following information:
 - API health and performance
 - APIs processed based on user/group/device criteria
 - WAF statistics per API / endpoint, includes DoS and Bot Defense
 - Most common API source accessed
 - API groups usage (statistics)
 - API Profile - AVR data - used / blocked / Rate limited

Security > Application Security : Security Policies : Policies List

★ Policies List Policy Groups Policies Summary Policy Diff

Create Policy Cancel

On this screen you can configure policy settings for new policies and review policy settings for existing policies. Once a policy is configured, some settings on this page will have a link for editing the setting.

Basic Advanced

Policy Name *

Partition: Common

Description

Policy Type Security Parent ?

Policy Template API Security

OpenAPI (Swagger) File Upload File

