F5 Fraud Protection Service Uncovered

Alfredo Vistola

Sr. Security Solution Architect

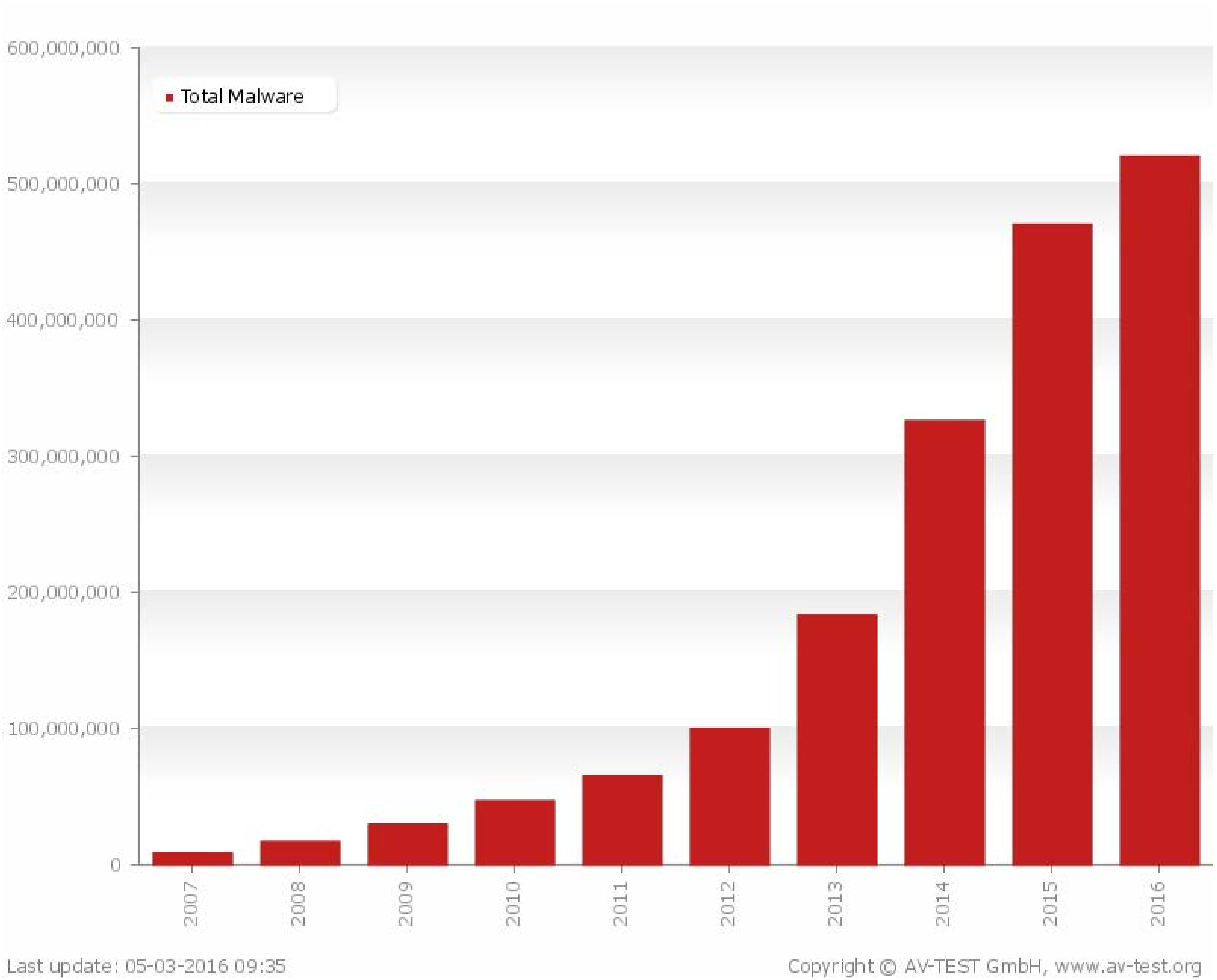
Agenda

Current situation

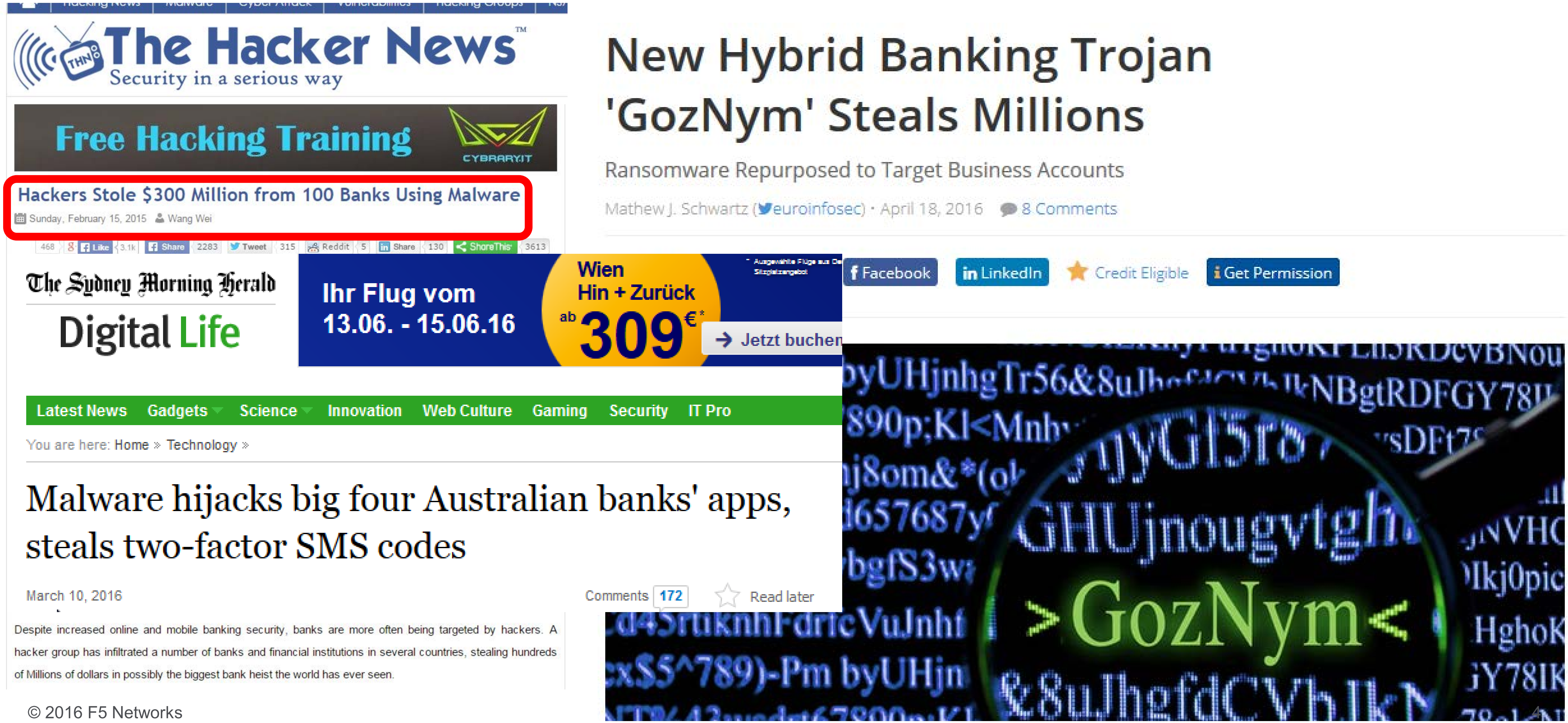
Trojan examples

WebSafe and MobileSafe explained

Total Malware Growth



Malware Attacks - From The News



The Hacker News™
Security in a serious way

Hackers Stole $300 Million from 100 Banks Using Malware

Sunday, February 15, 2015 · Wang Wei

Despite increased online and mobile banking security, banks are more often being targeted by hackers. A hacker group has infiltrated a number of banks and financial institutions in several countries, stealing hundreds of Millions of dollars in possibly the biggest bank heist the world has ever seen.

The Sydney Morning Herald
Digital Life

You are here: Home » Technology »

Malware hijacks big four Australian banks' apps, steals two-factor SMS codes

March 10, 2016

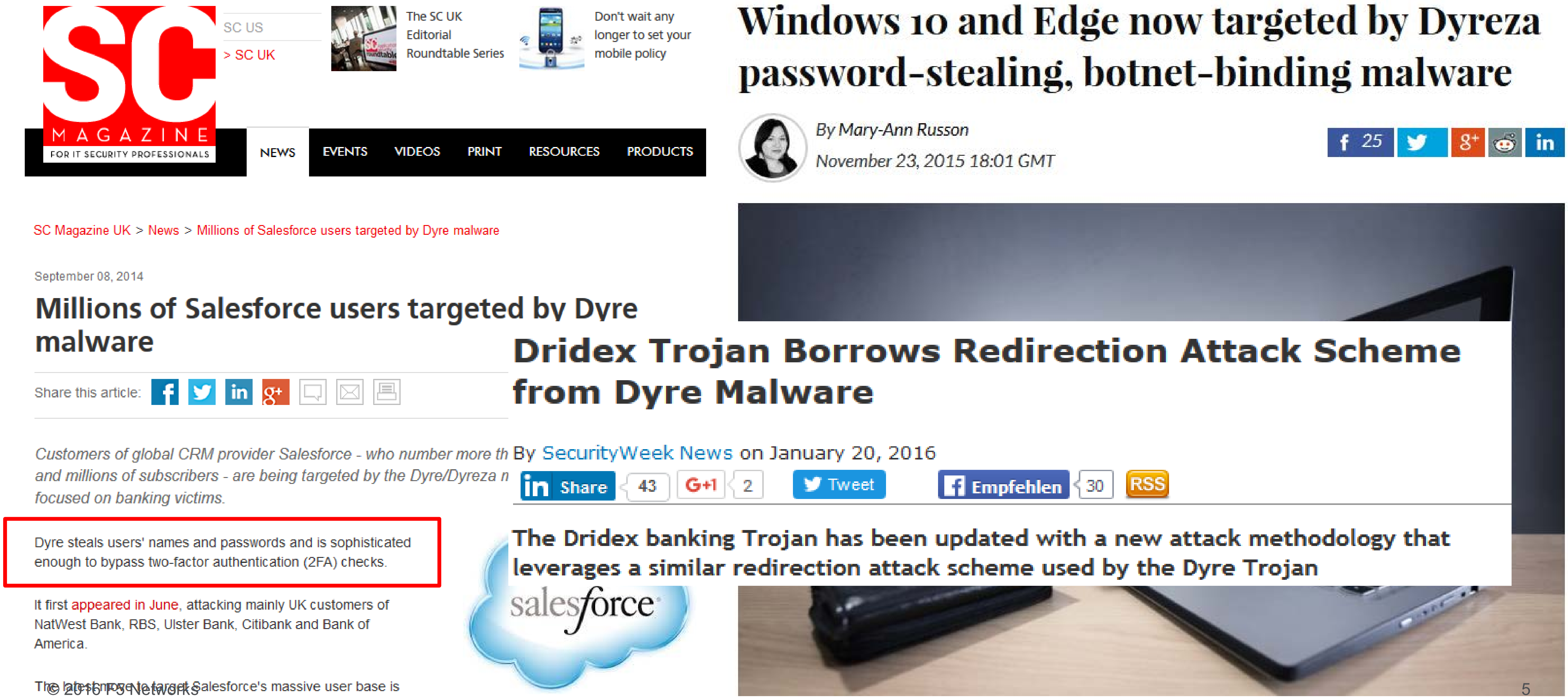
Comments 172 · Read later

New Hybrid Banking Trojan 'GozNym' Steals Millions

Ransomware Repurposed to Target Business Accounts

Mathew J. Schwartz (euroinfosec) · April 18, 2016 · 8 Comments

Malware Target Various Industries



SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
SC US
> SC UK
The SC UK Editorial Roundtable Series
Don't wait any longer to set your mobile policy
NEWS
EVENTS
VIDEOS
PRINT
RESOURCES
PRODUCTS

SC Magazine UK > News > Millions of Salesforce users targeted by Dyre malware

September 08, 2014

Millions of Salesforce users targeted by Dyre malware

Customers of global CRM provider Salesforce - who number more th and millions of subscribers - are being targeted by the Dyre/Dyreza n focused on banking victims.

Dyre steals users' names and passwords and is sophisticated enough to bypass two-factor authentication (2FA) checks.

It first appeared in June, attacking mainly UK customers of NatWest Bank, RBS, Ulster Bank, Citibank and Bank of America.

The latest move to target Salesforce's massive user base is

Windows 10 and Edge now targeted by Dyreza password-stealing, botnet-binding malware

By Mary-Ann Russon
November 23, 2015 18:01 GMT

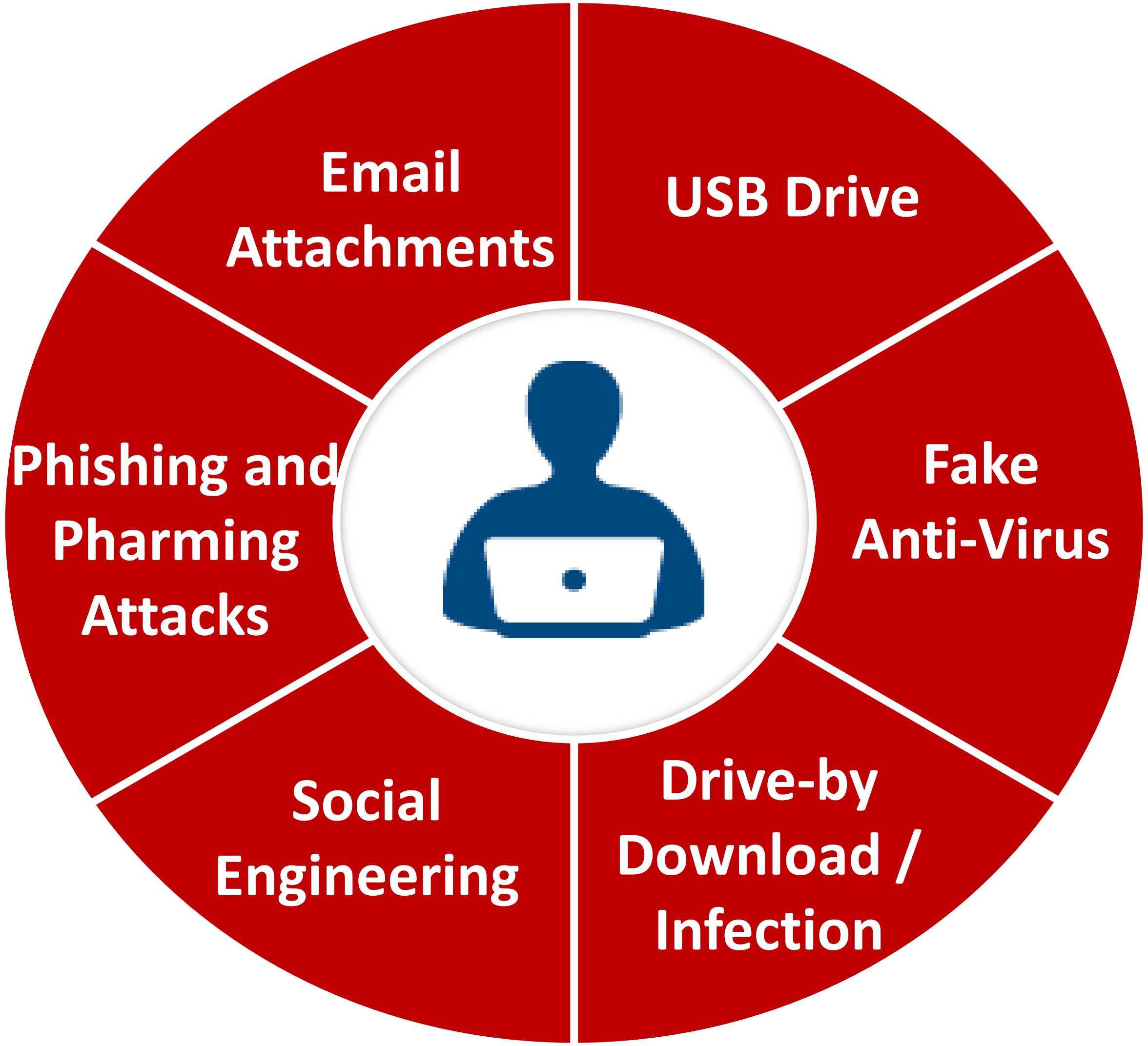
Dridex Trojan Borrows Redirection Attack Scheme from Dyre Malware

By SecurityWeek News on January 20, 2016

The Dridex banking Trojan has been updated with a new attack methodology that leverages a similar redirection attack scheme used by the Dyre Trojan

ATTACK VECTORS

How Trojans Infect Devices



Email Attachments

USB Drive

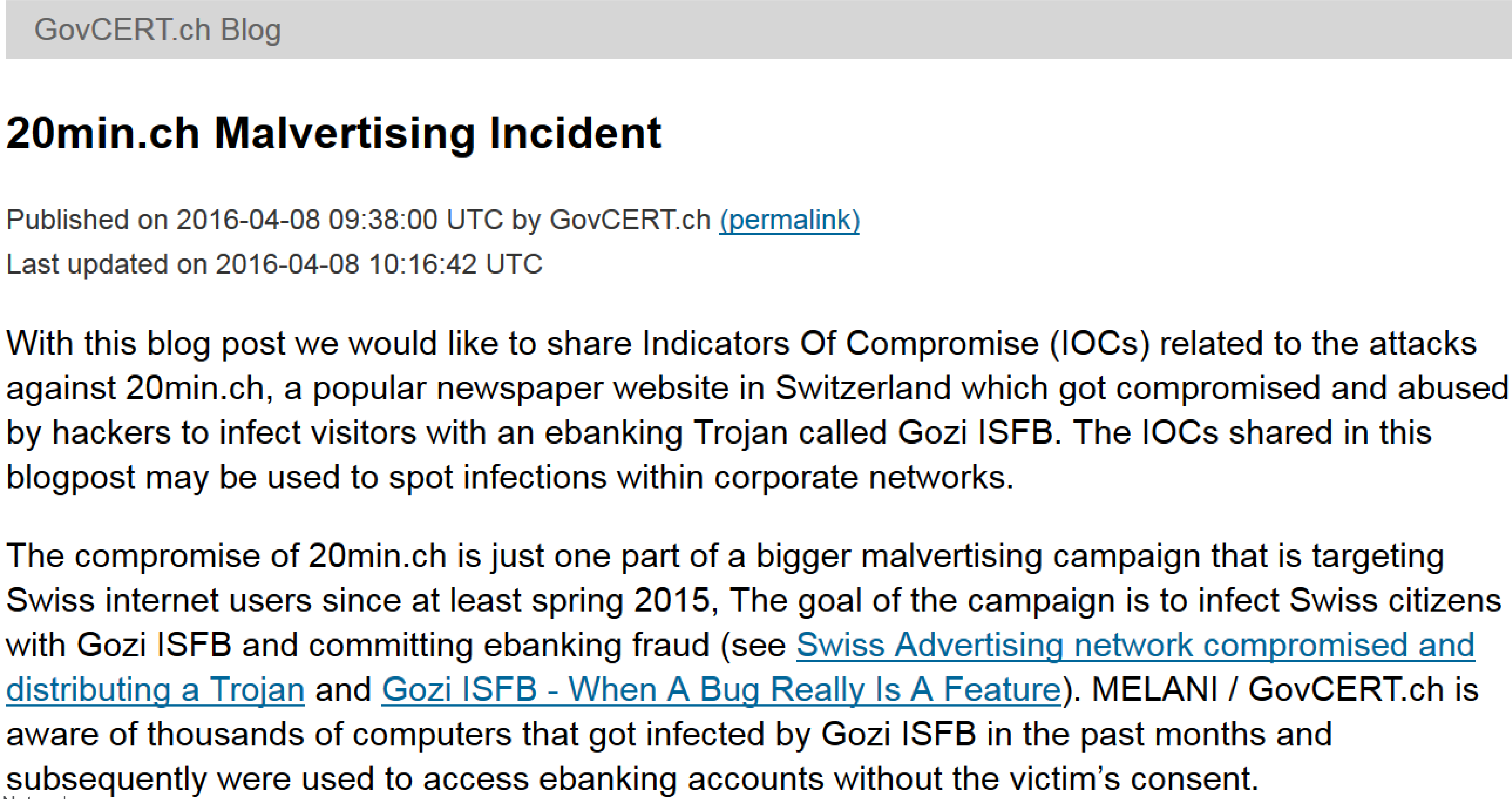
Fake Anti-Virus

Drive-by Download / Infection

Social Engineering

Phishing and Pharming Attacks

Newspaper Website Involuntary Spreads Ebanking Trojan



GovCERT.ch Blog

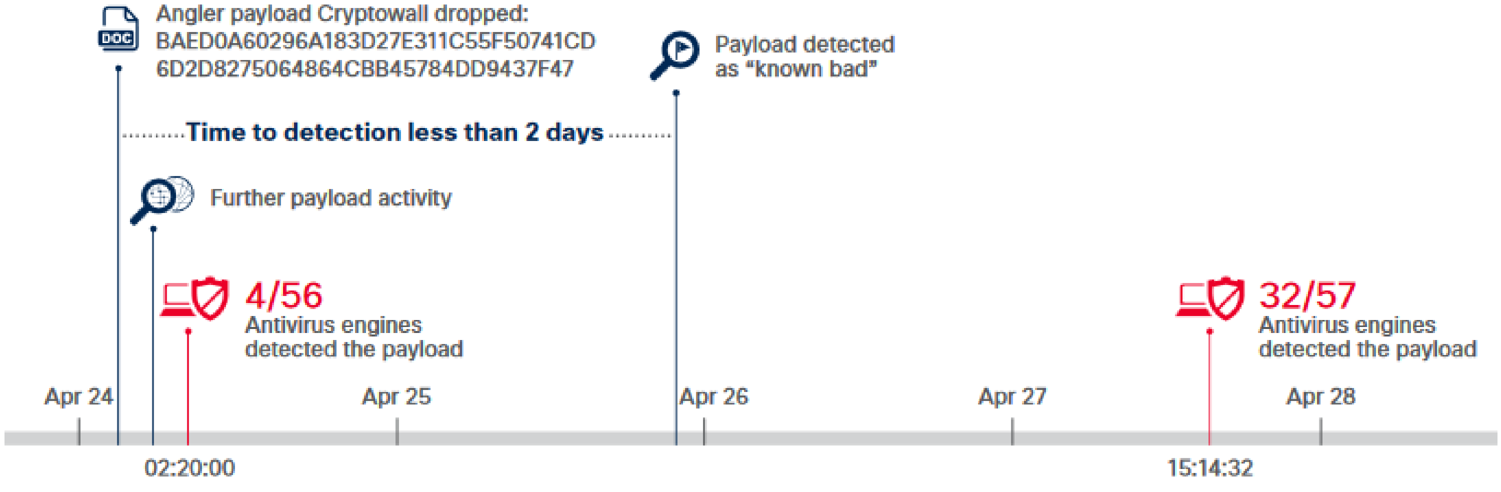
20min.ch Malvertising Incident

Published on 2016-04-08 09:38:00 UTC by GovCERT.ch (permalink)
Last updated on 2016-04-08 10:16:42 UTC

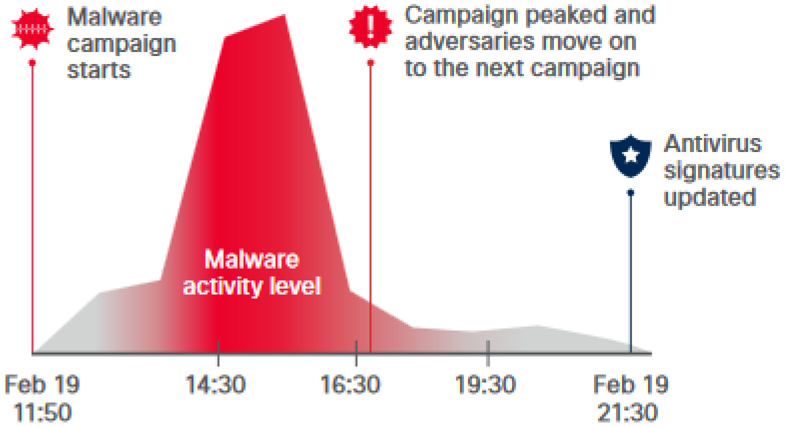
With this blog post we would like to share Indicators Of Compromise (IOCs) related to the attacks against 20min.ch, a popular newspaper website in Switzerland which got compromised and abused by hackers to infect visitors with an ebanking Trojan called Gozi ISFB. The IOCs shared in this blogpost may be used to spot infections within corporate networks.

The compromise of 20min.ch is just one part of a bigger malvertising campaign that is targeting Swiss internet users since at least spring 2015, The goal of the campaign is to infect Swiss citizens with Gozi ISFB and committing ebanking fraud (see Swiss Advertising network compromised and distributing a Trojan and Gozi ISFB - When A Bug Really Is A Feature). MELANI / GovCERT.ch is aware of thousands of computers that got infected by Gozi ISFB in the past months and subsequently were used to access ebanking accounts without the victim’s consent.

Time to detect Trojans by Antivirus Engines



Source: Cisco Security Research

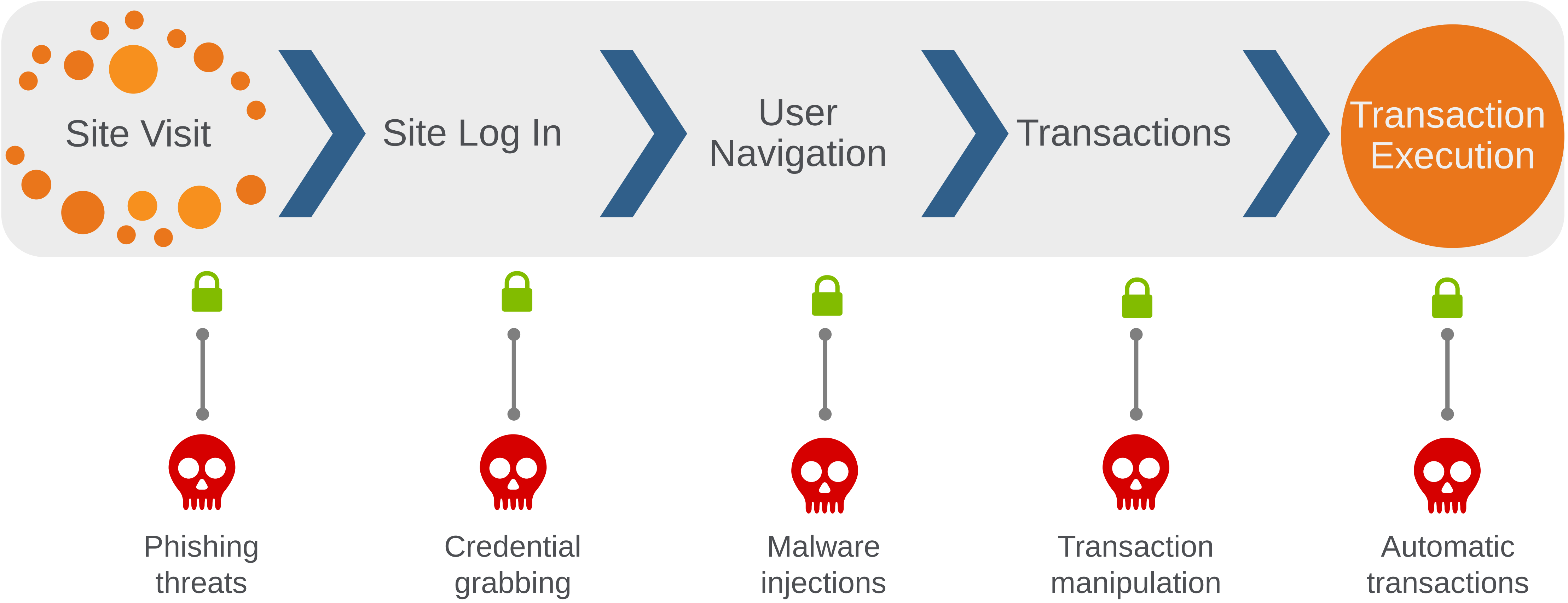


Source: Cisco Security Research

Trojans are able to stop the automatic signature update or trigger just once

Attack Vectors

Web application transaction flow



Site Visit

Site Log In

User Navigation

Transactions

Transaction Execution

Phishing threats

Credential grabbing

Malware injections

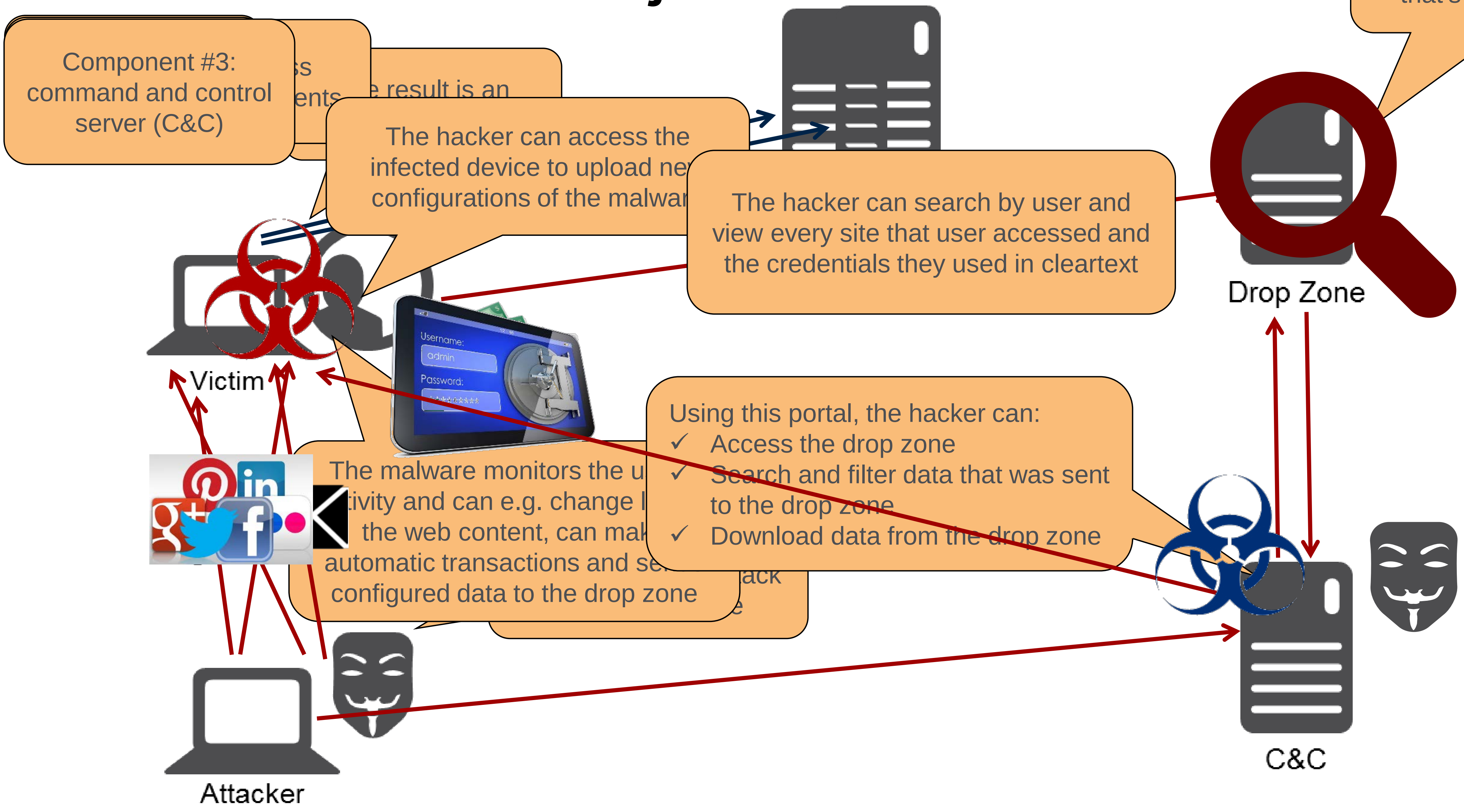
Transaction manipulation

Automatic transactions

Ensure defense against these threats

Browser-Based Trojan Malware Process

Quite often the drop zone is a legitimate web server that's been high jacked



Component #3: command and control server (C&C)

ss
ents

e result is an

The hacker can access the infected device to upload ne configurations of the malwar

The hacker can search by user and view every site that user accessed and the credentials they used in cleartext

Using this portal, the hacker can:

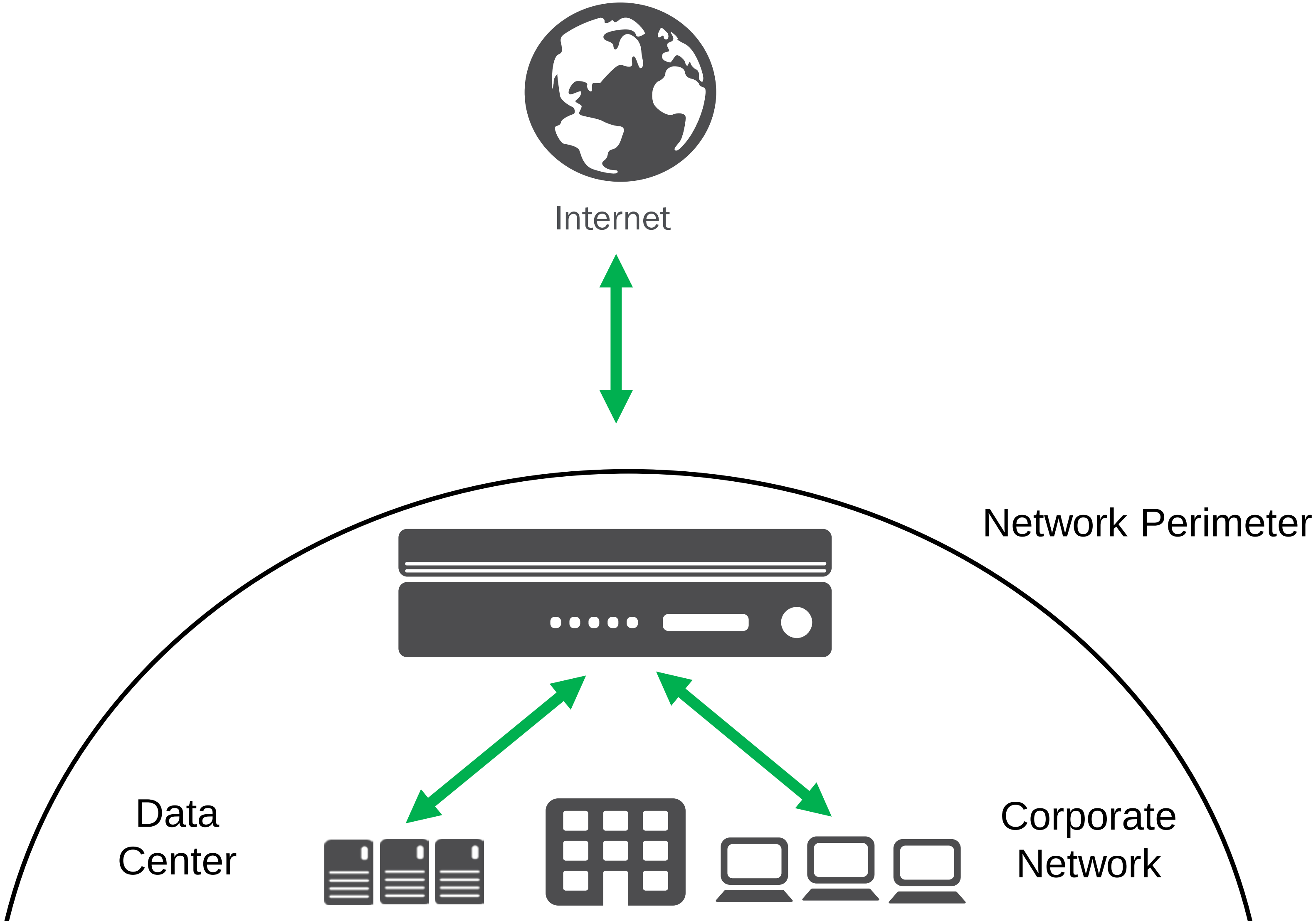
- ✓ Access the drop zone
- ✓ Search and filter data that was sent to the drop zone
- ✓ Download data from the drop zone

The malware monitors the u tivity and can e.g. change l the web content, can mak automatic transactions and se configured data to the drop zone

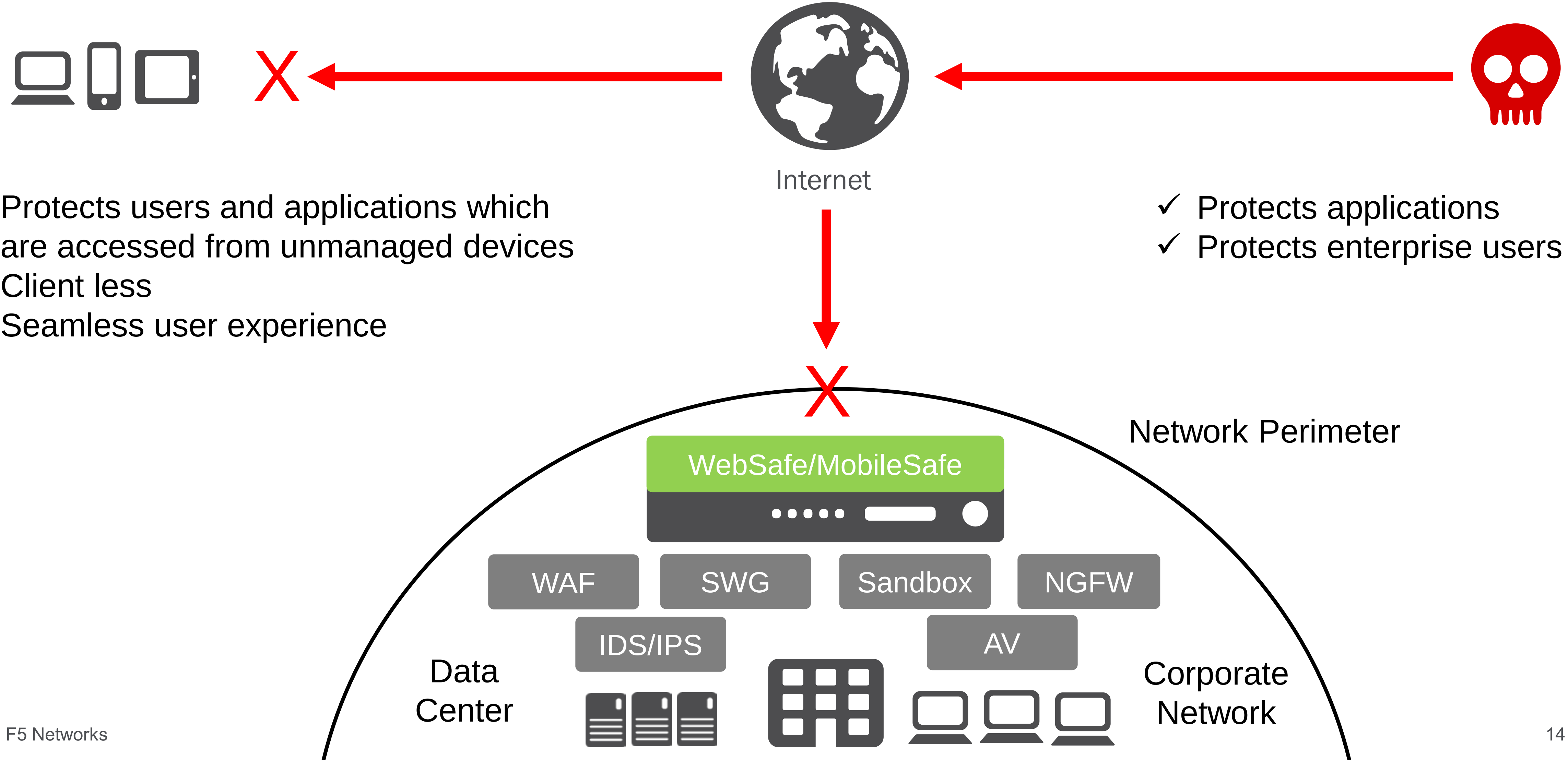
ack
e

MITIGATION WITH THE F5 CLIENTLESS WEBSAFE AND MOBILESAFE SOLUTION

F5 Fraud Protection Versus Traditional Malware Solutions



F5 Fraud Protection Versus Traditional Malware Solutions

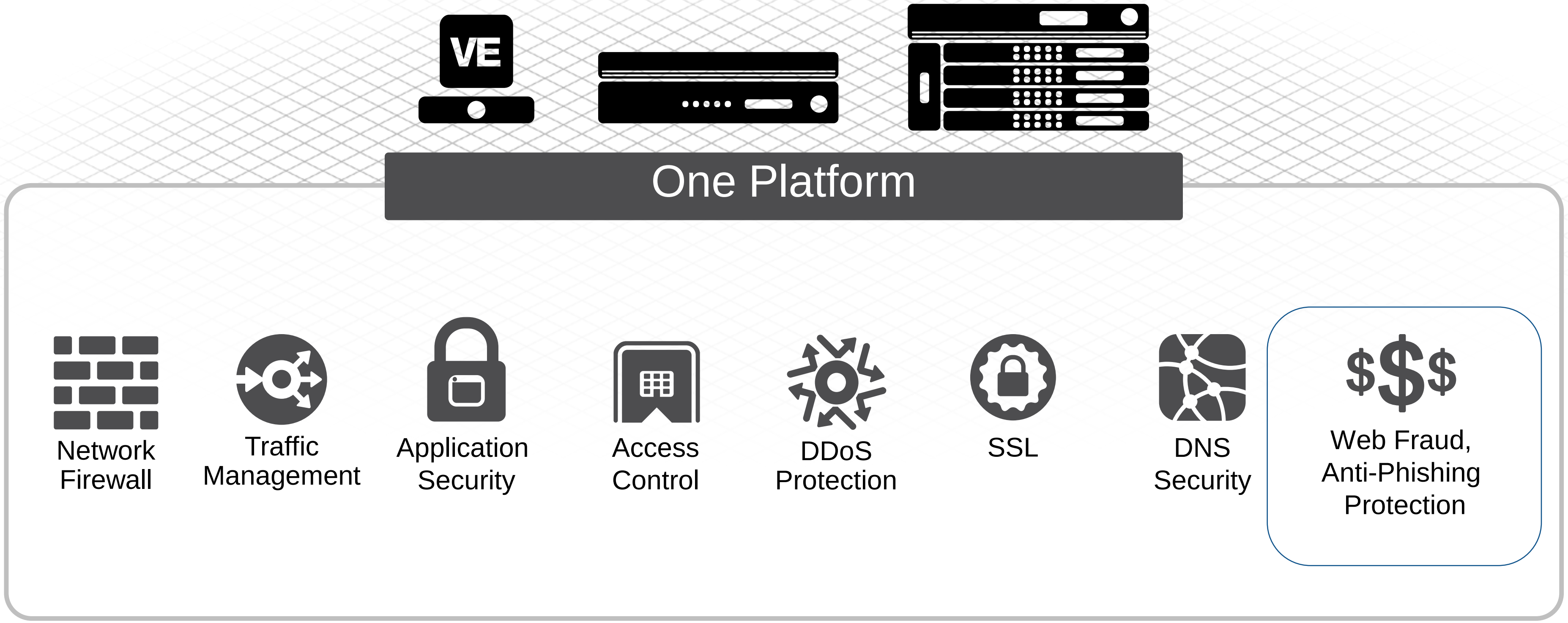


- ✓ Protects users and applications which are accessed from unmanaged devices
- ✓ Client less
- ✓ Seamless user experience

- ✓ Protects applications
- ✓ Protects enterprise users

Application Delivery Security Solution

Bringing deep application fluency to security



One Platform

Network Firewall

Traffic Management

Application Security

Access Control

DDoS Protection

SSL

DNS Security

Web Fraud, Anti-Phishing Protection

ICSA labs CERTIFIED IPSEC

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

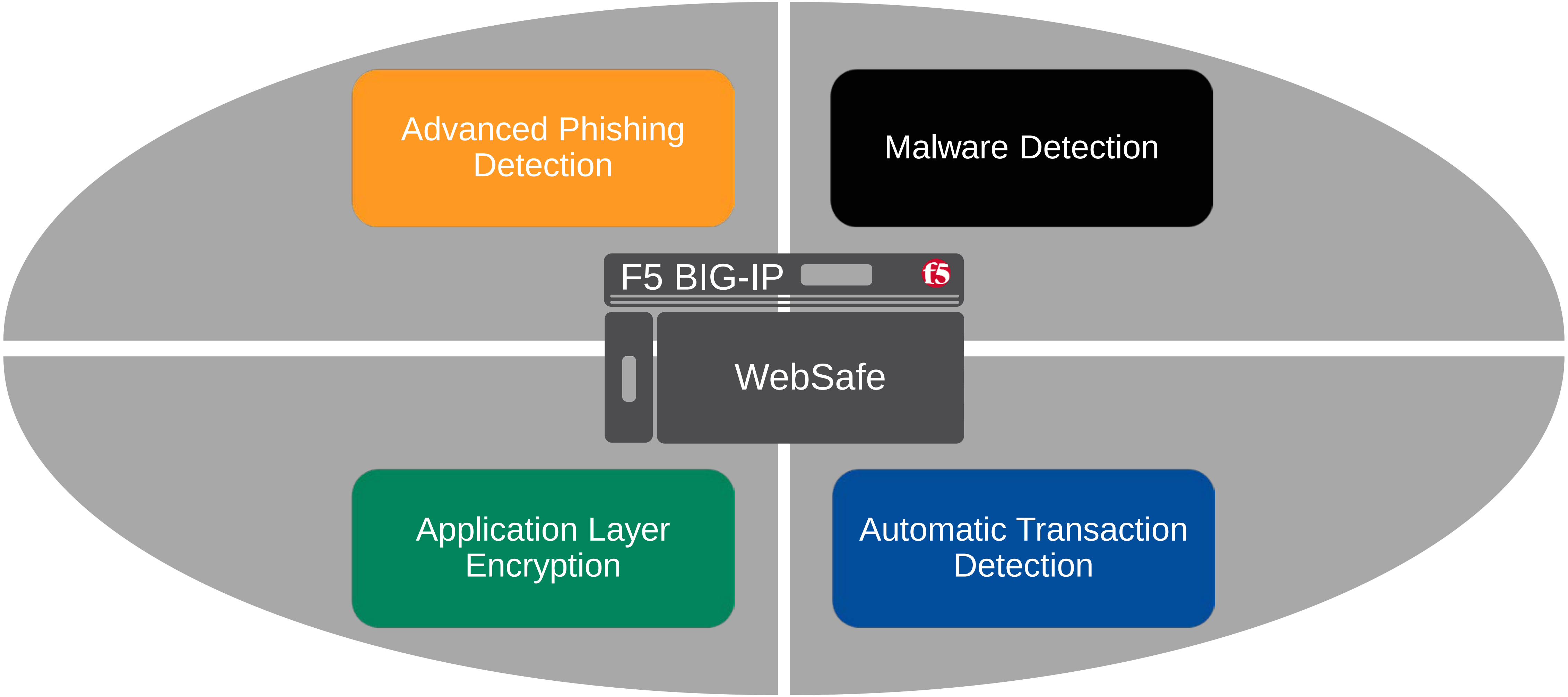
Common Criteria
EAL2+
EAL4+ (in process)

NSS LABS
DC FW (in process)
WAF (in process)
DDoS (pending)

WEBSAFE

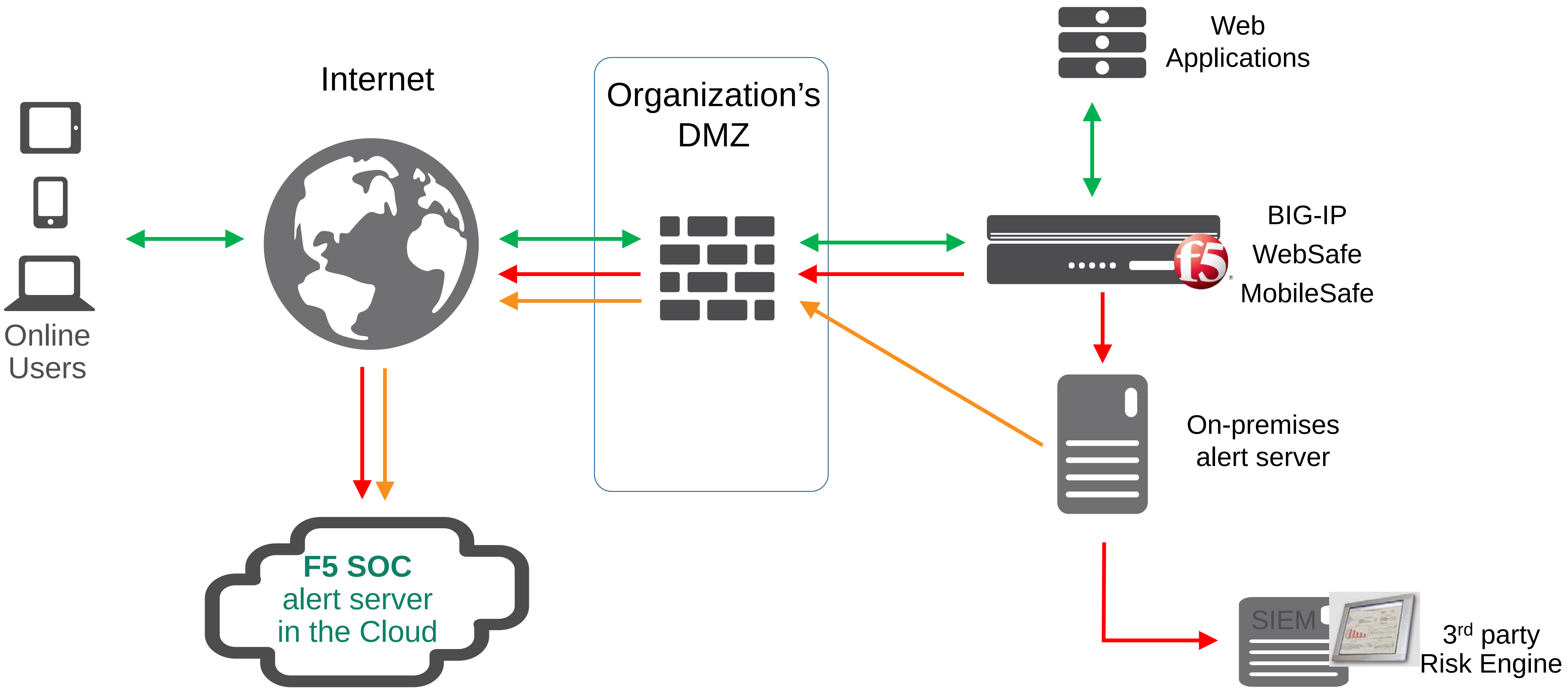
F5’s Web Fraud Protection Services

Extends application security to the client-side

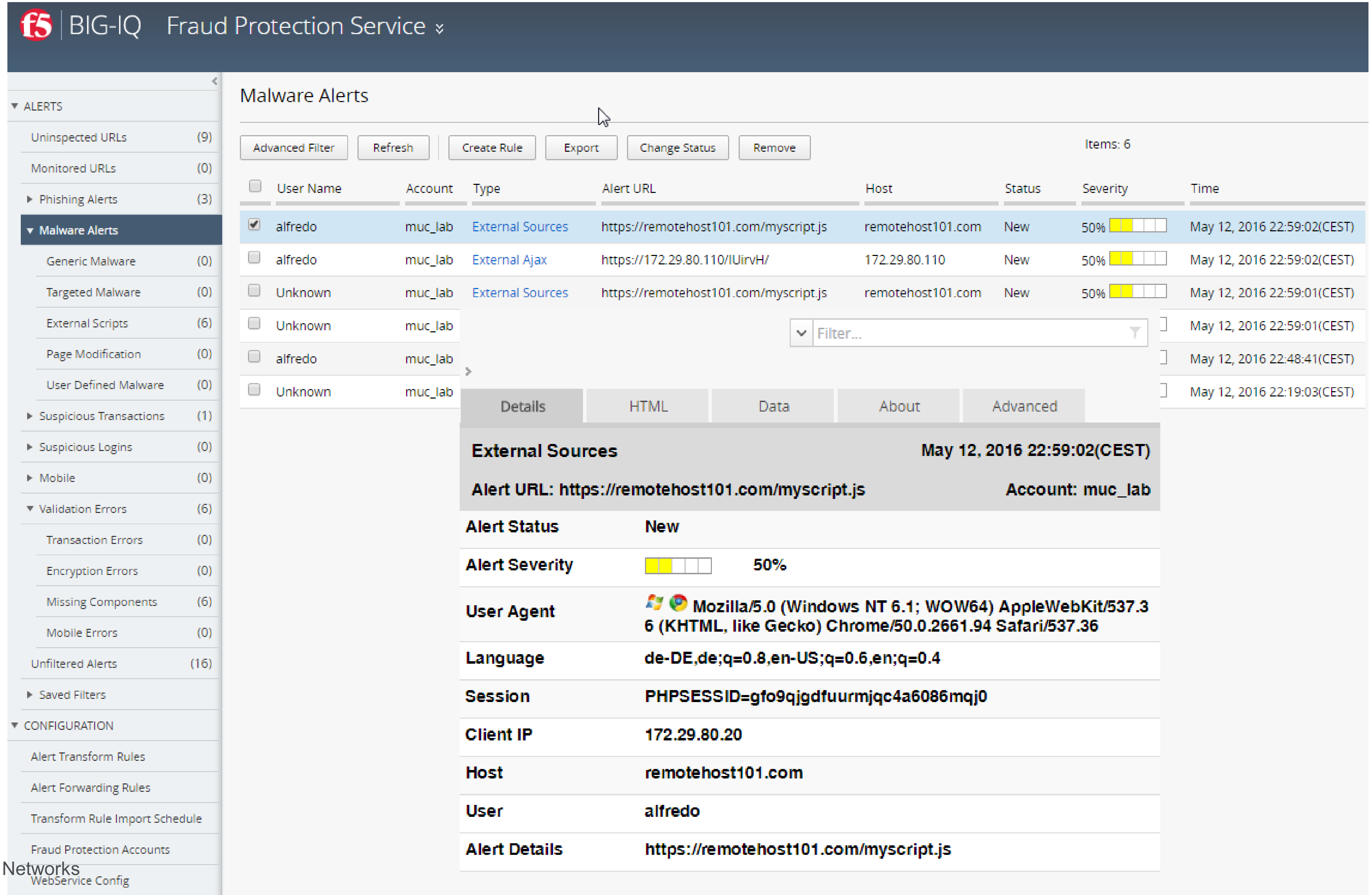


Advanced Phishing Detection
Malware Detection
F5 BIG-IP
f5
WebSafe
Application Layer Encryption
Automatic Transaction Detection

Web Fraud Protection Implementation Options



Real-Time Alerts Dashboard



▼ ALERTS

Uninspected URLs	(9)
Monitored URLs	(0)
▸ Phishing Alerts	(3)
▾ Malware Alerts	
Generic Malware	(0)
Targeted Malware	(0)
External Scripts	(6)
Page Modification	(0)
User Defined Malware	(0)
▸ Suspicious Transactions	(1)
▸ Suspicious Logins	(0)
▸ Mobile	(0)
▾ Validation Errors	(6)
Transaction Errors	(0)
Encryption Errors	(0)
Missing Components	(6)
Mobile Errors	(0)
Unfiltered Alerts	(16)
▸ Saved Filters	

▼ CONFIGURATION

Alert Transform Rules
Alert Forwarding Rules
Transform Rule Import Schedule
Fraud Protection Accounts
WebService Config

Malware Alerts

Items: 6

□	User Name	Account	Type	Alert URL	Host	Status	Severity	Time
☑	alfredo	muc_lab	External Sources	https://remotehost101.com/myscript.js	remotehost101.com	New	50%	May 12, 2016 22:59:02(CEST)
□	alfredo	muc_lab	External Ajax	https://172.29.80.110/IUirvH/	172.29.80.110	New	50%	May 12, 2016 22:59:02(CEST)
□	Unknown	muc_lab	External Sources	https://remotehost101.com/myscript.js	remotehost101.com	New	50%	May 12, 2016 22:59:01(CEST)
□	Unknown	muc_lab						May 12, 2016 22:59:01(CEST)
□	alfredo	muc_lab						May 12, 2016 22:48:41(CEST)
□	Unknown	muc_lab						May 12, 2016 22:19:03(CEST)

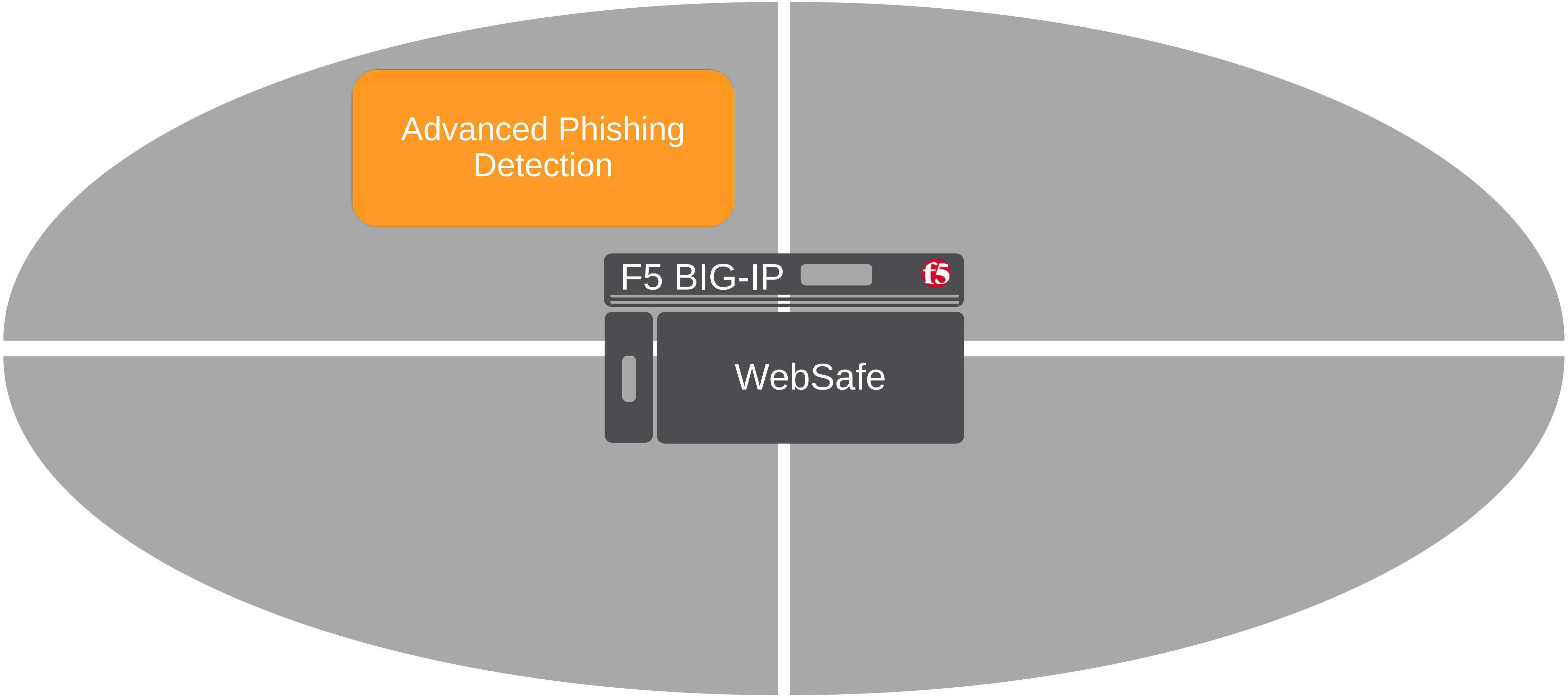
External Sources May 12, 2016 22:59:02(CEST)

Alert URL: https://remotehost101.com/myscript.js **Account: muc_lab**

Alert Status	New
Alert Severity	50%
User Agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36
Language	de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4
Session	PHPSESSID=gfo9qjgdfuurmjqc4a6086mqj0
Client IP	172.29.80.20
Host	remotehost101.com
User	alfredo
Alert Details	https://remotehost101.com/myscript.js

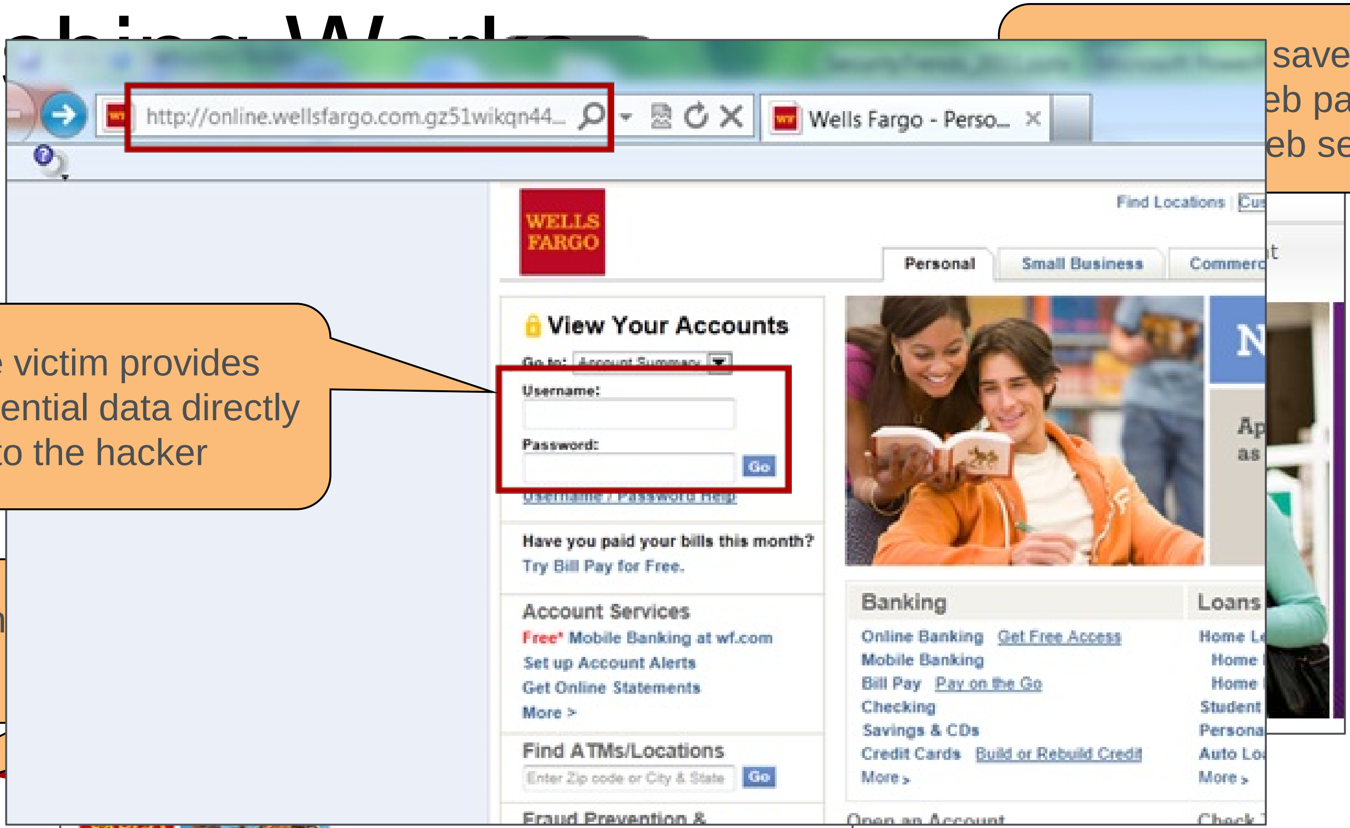
F5's Web Fraud Protection Services

Extends application security to the client-side



How Phi

saves a
eb pages
eb server



View Your Accounts

Go to: Account Summary

Username:

Password:

Have you paid your bills this month?
Try Bill Pay for Free.

Account Services
Free* Mobile Banking at wf.com
Set up Account Alerts
Get Online Statements
More >

Find ATMs/Locations
Enter Zip code or City & State Go

Fraud Prevention &

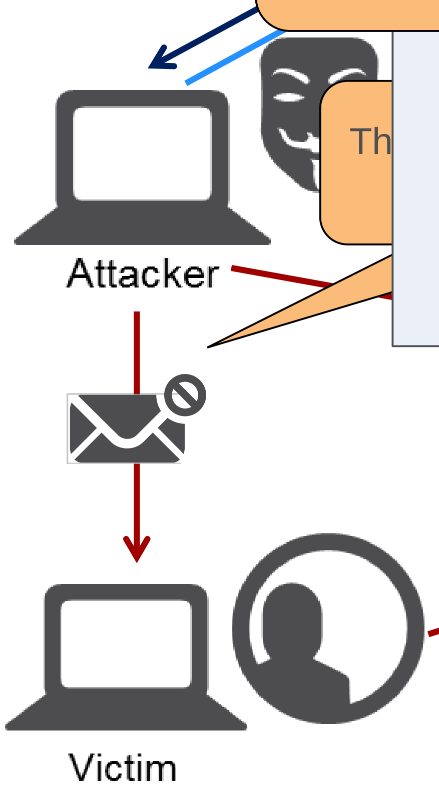
Banking
Online Banking Get Free Access
Mobile Banking
Bill Pay Pay on the Go
Checking
Savings & CDs
Credit Cards Build or Rebuild Credit
More >

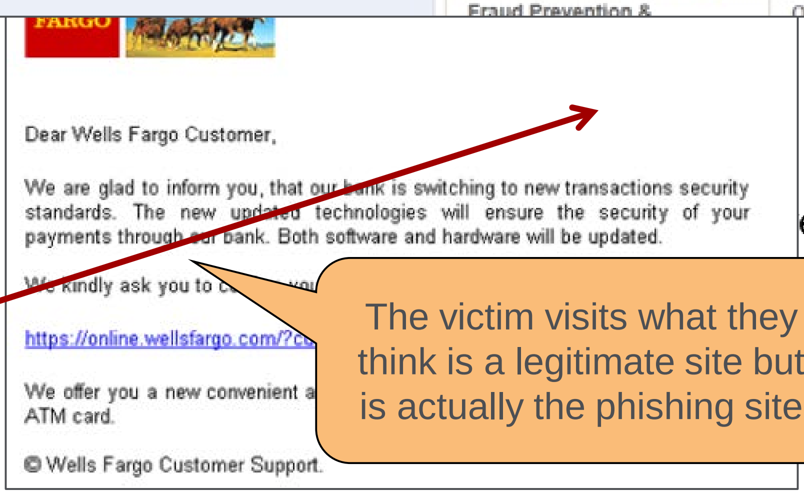
Open an Account

Loans
Home L
Home
Home
Student
Persona
Auto Lo
More >

Check

The victim provides confidential data directly to the hacker





Dear Wells Fargo Customer,

We are glad to inform you, that our bank is switching to new transactions security standards. The new updated technologies will ensure the security of your payments through our bank. Both software and hardware will be updated.

We kindly ask you to c you

https://online.wellsfargo.com/?c

We offer you a new convenient a ATM card.

© Wells Fargo Customer Support.

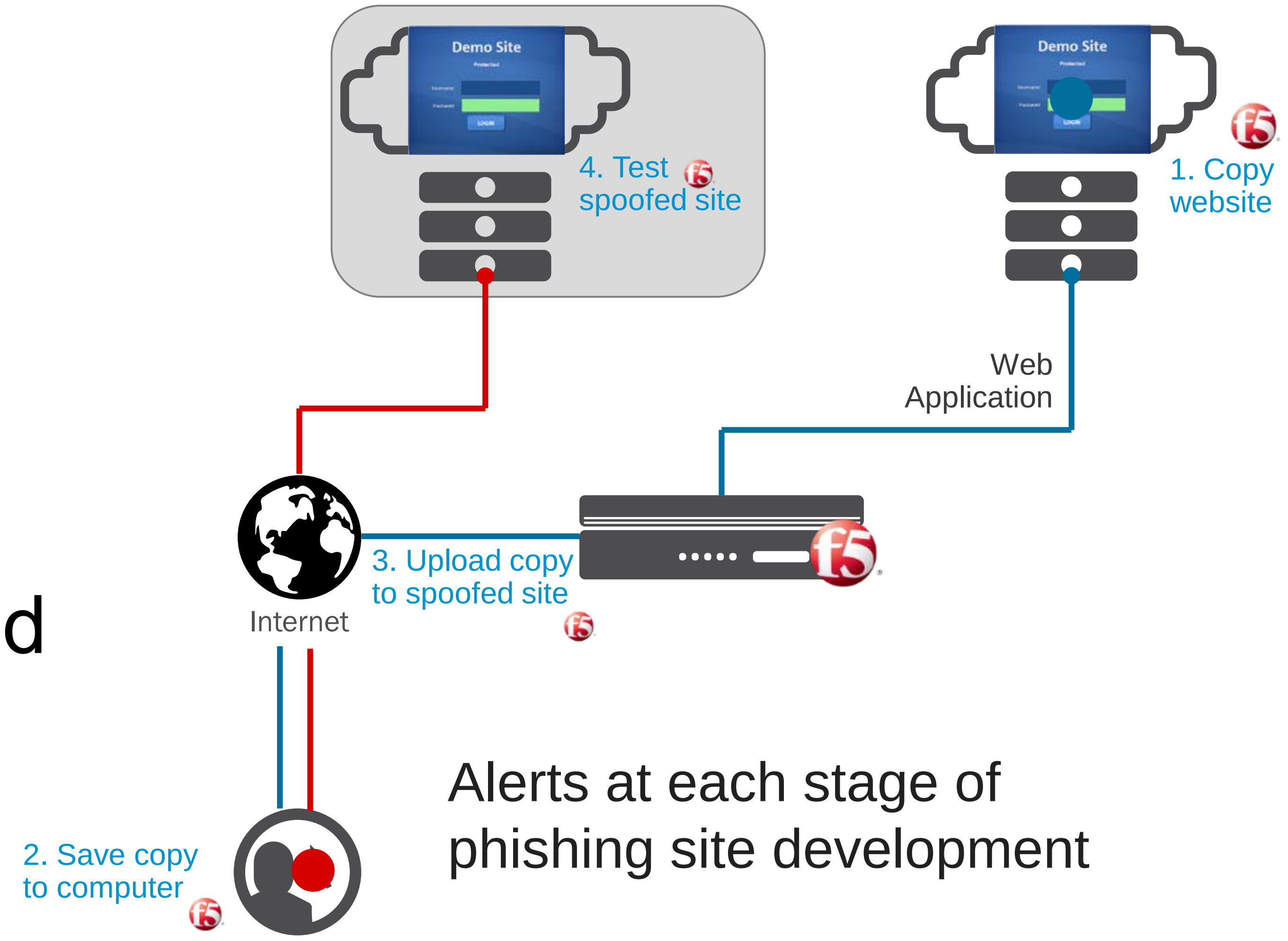
er

The victim visits what they think is a legitimate site but is actually the phishing site

Advanced Phishing Attack Detection and Prevention

Identifies phishing threats early-on and stops attacks before emails are sent

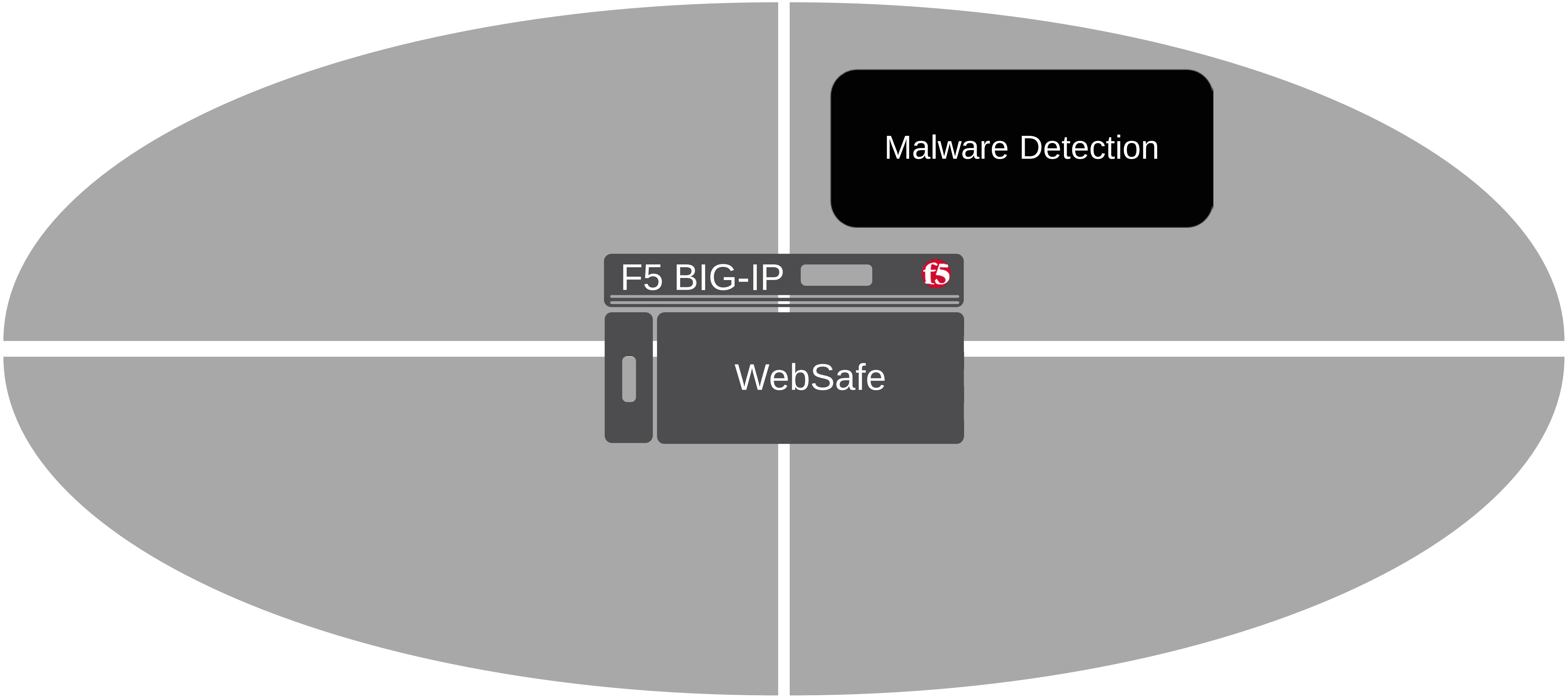
- Alerts of site copying to different server
- Alerts upon login and testing of phishing site
- Enable detection and rapid shutdown of copied content



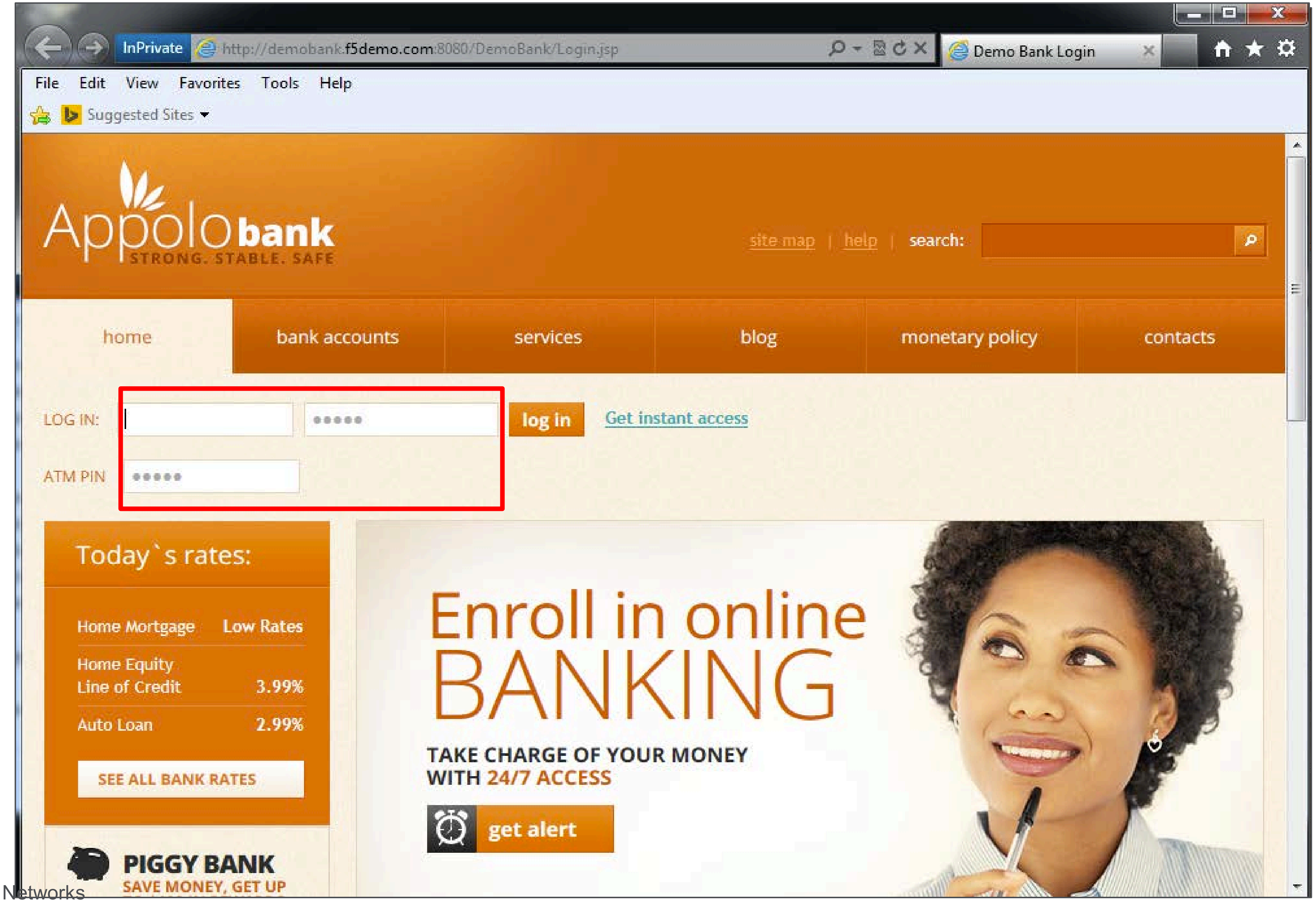
Alerts at each stage of phishing site development

F5’s Web Fraud Protection Services

Extends application security to the client-side



Web Injection Example

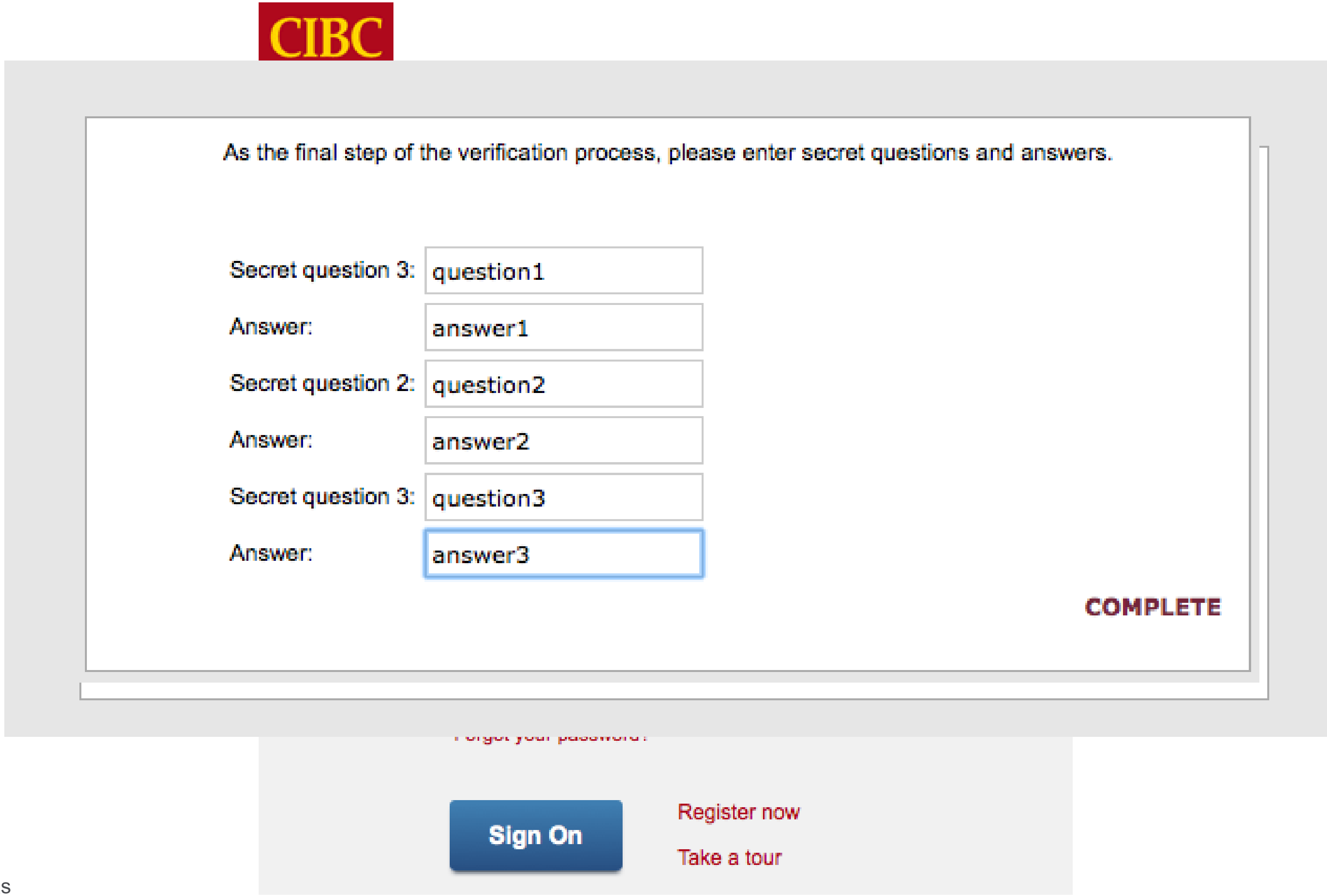


Home Mortgage	Low Rates
Home Equity Line of Credit	3.99%
Auto Loan	2.99%

Enroll in online
BANKING

TAKE CHARGE OF YOUR MONEY
WITH 24/7 ACCESS

Web Injection Example



As the final step of the verification process, please enter secret questions and answers.

Secret question 3:	question1
Answer:	answer1
Secret question 2:	question2
Answer:	answer2
Secret question 3:	question3
Answer:	answer3

Clientless Generic and Targeted Malware Detection

Summary

Analyzes browser for traces of common malware (i.e., Zeus, Citadel, Carberp, Hesperbot, Dyre, Cridex, Dridex, …)

Detects client side code injection and browser redressing

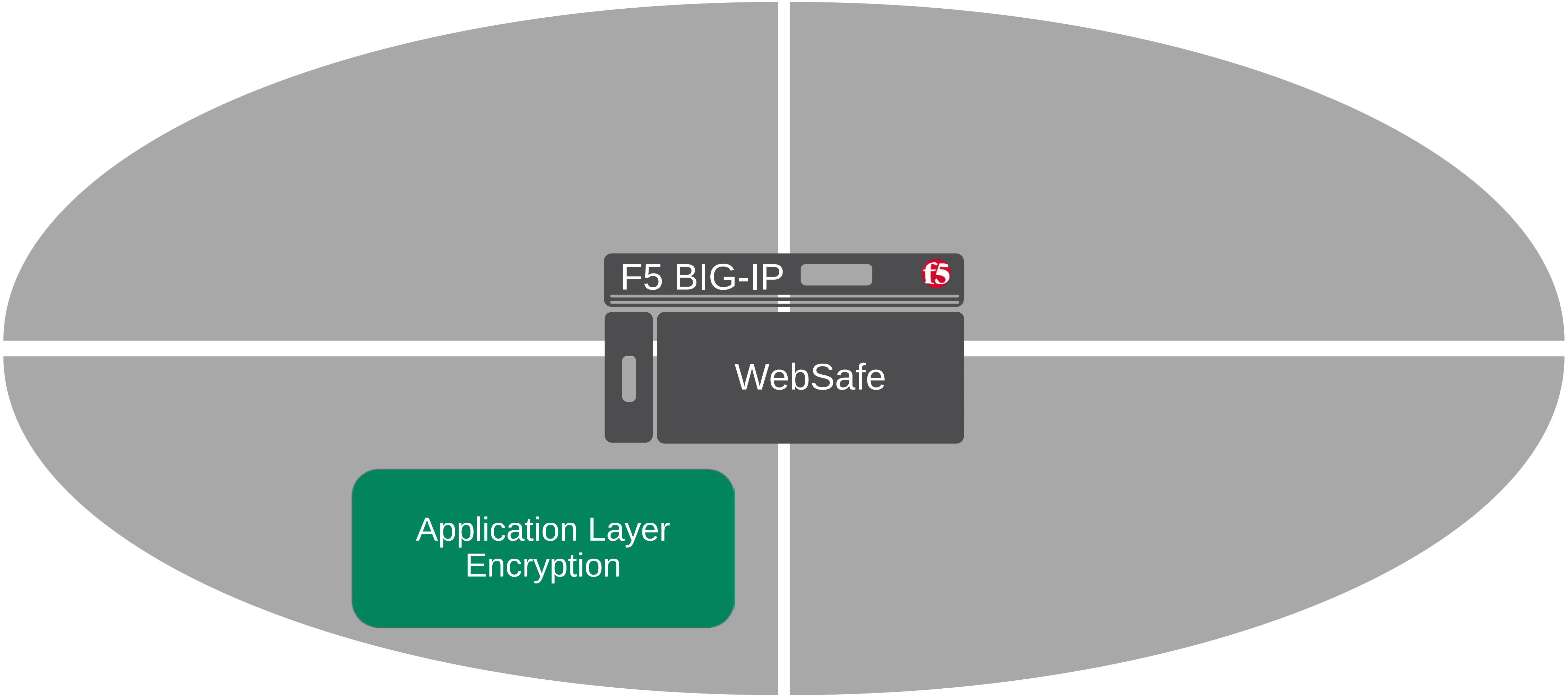
Performs checks on domain and other components

Identifies the presence of Remote Access Trojans

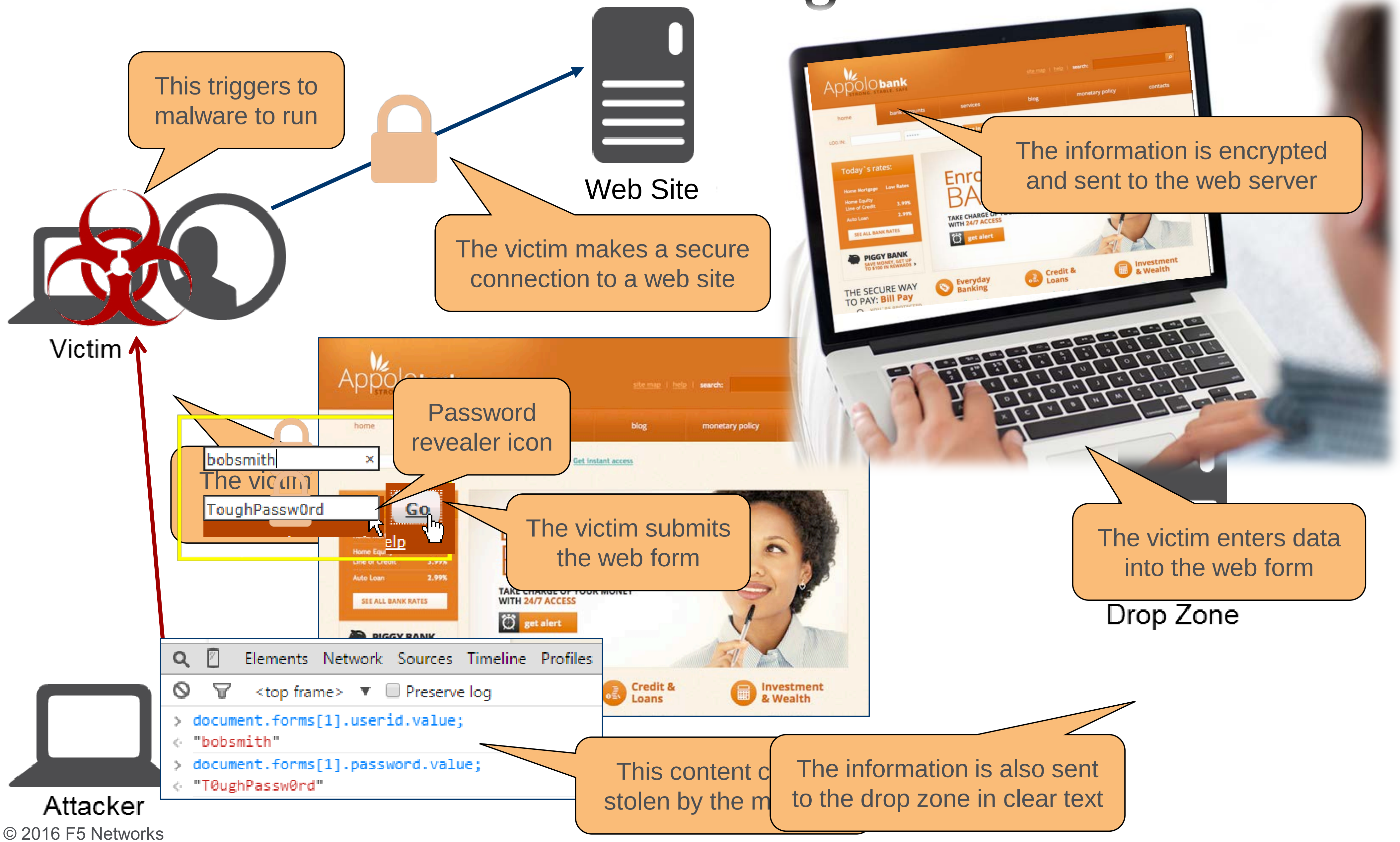
Determines if a computer is being remotely controlled

F5’s Web Fraud Protection Services

Extends application security to the client-side



Credential /Form Grabbing



This triggers to malware to run

The victim makes a secure connection to a web site

Web Site

Victim

The information is encrypted and sent to the web server

The victim enters data into the web form

Drop Zone

bobsmith

The victim

ToughPassw0rd

Password revealer icon

The victim submits the web form

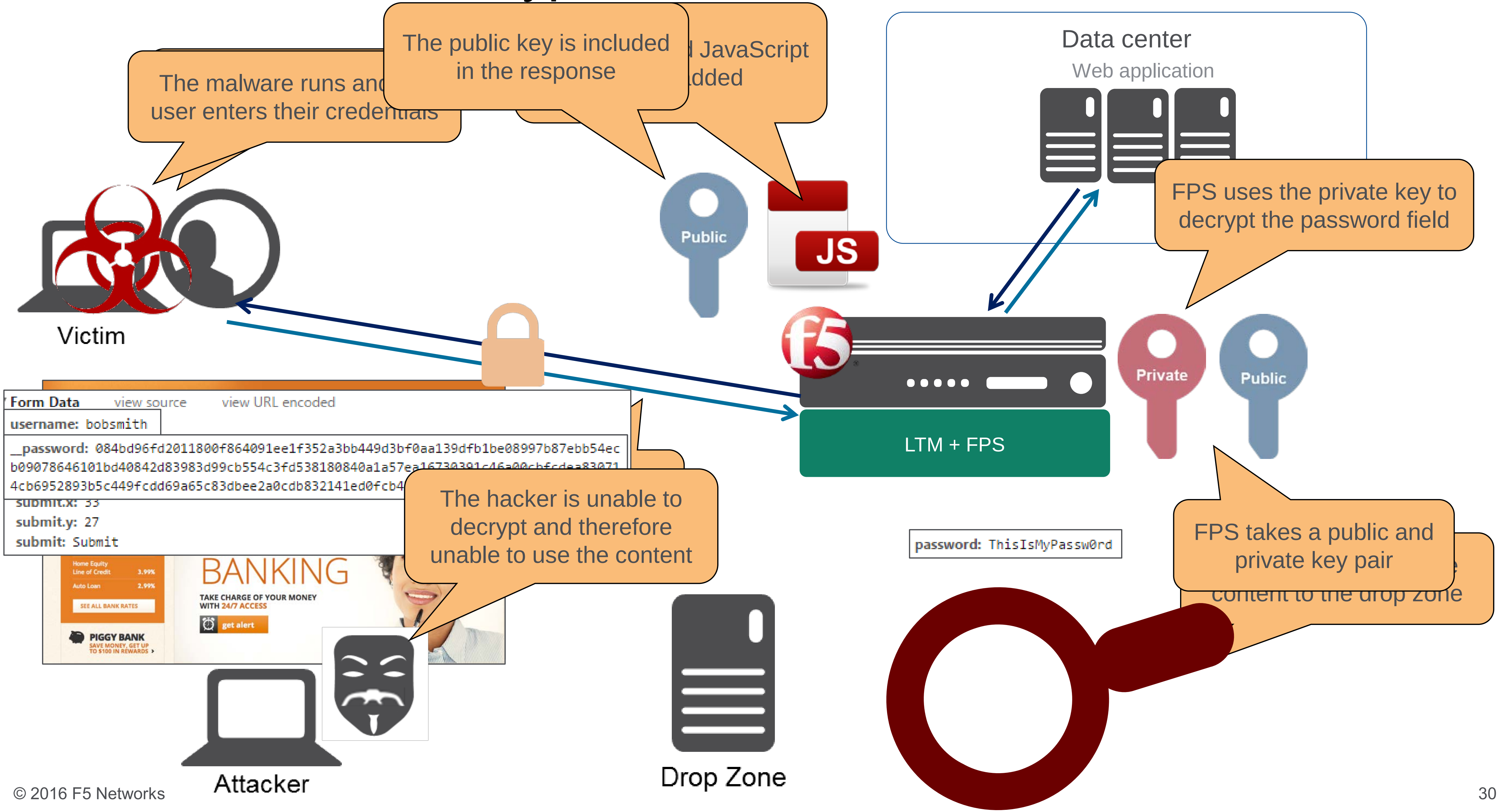
```
> document.forms[1].userid.value;
< "bobsmith"
> document.forms[1].password.value;
< "T0ughPassw0rd"
```

This content c
stolen by the m

The information is also sent to the drop zone in clear text

Attacker

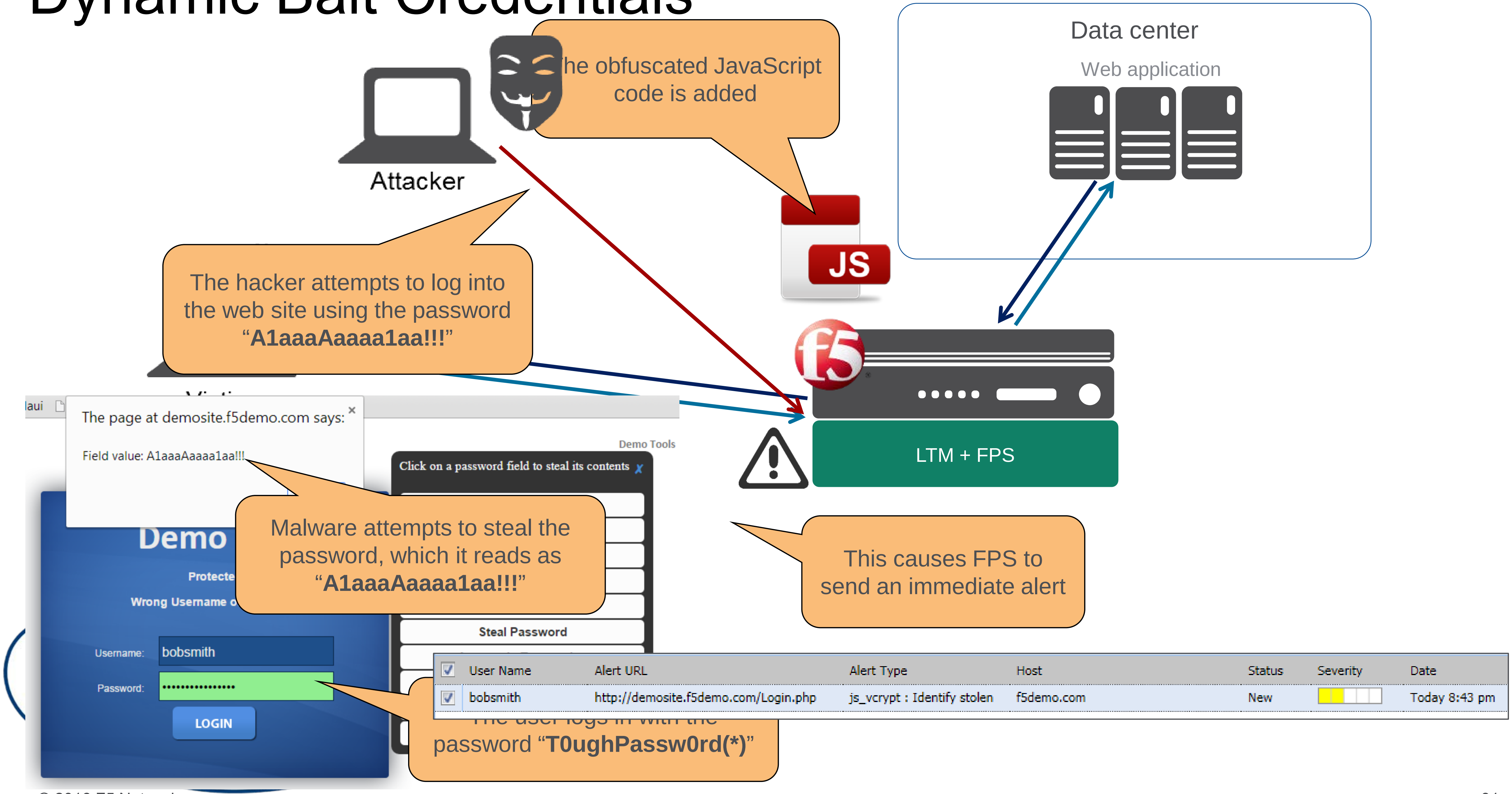
How FPS Uses Encryption to Protect Confidential Data



```
Form Data    view source    view URL encoded
username: bobsmith
_password: 084bd96fd2011800f864091ee1f352a3bb449d3bf0aa139dfb1be08997b87ebb54ec
b09078646101bd40842d83983d99cb554c3fd538180840a1a57ea16730391c46a00cbfcdea83071
4cb6952893b5c449fcdd69a65c83dbee2a0cdb832141ed0fcb4
submit.x: 33
submit.y: 27
submit: Submit
```

```
password: ThisIsMyPassw0rd
```

Dynamic Bait Credentials



The obfuscated JavaScript code is added

The hacker attempts to log into the web site using the password “**A1aaaAaaaa1aa!!!**”

The page at demosite.f5demo.com says: ×

Field value: A1aaaAaaaa1aa!!!

Click on a password field to steal its contents ✗

Wrong Username o

Username: bobsmith

Password: ••••••••••••••••

Malware attempts to steal the password, which it reads as “**A1aaaAaaaa1aa!!!**”

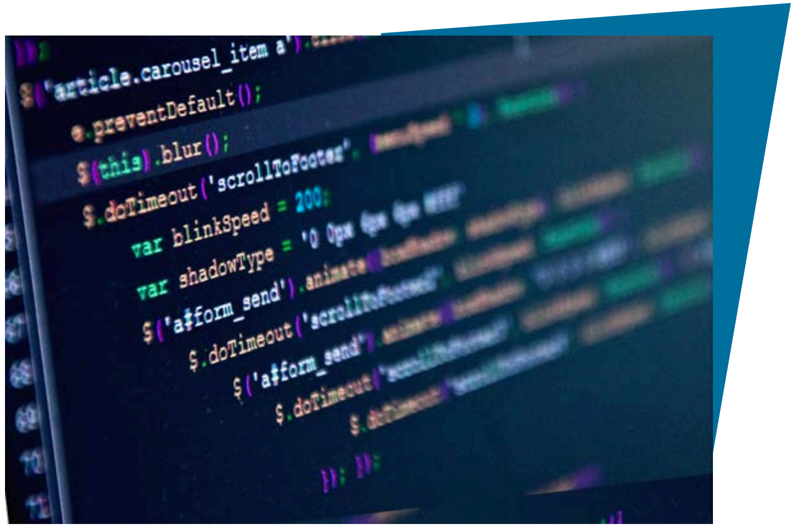
This causes FPS to send an immediate alert

The user logs in with the password “**T0ughPassw0rd(*)**”

☑	User Name	Alert URL	Alert Type	Host	Status	Severity	Date
☑	bobsmith	http://demosite.f5demo.com/Login.php	js_vcrypt : Identify stolen	f5demo.com	New	🟨🟨□□□	Today 8:43 pm

HTML Field Obfuscation (HFO)

Obscures visibility and slows down attackers



```
$('article.carousel_item a').
    e.preventDefault();
    $(this).blur();
    $.doTimeout('scrollToFooter',
        var blinkSpeed = 200;
        var shadowType = '0 0px
        $('a#form_send').animate
            $.doTimeout('scroll
                $('a#form_send').
                    $.doTimeout(
                        $.
                }); });
```

Uses advanced HFO techniques to go beyond encrypting field values on the client

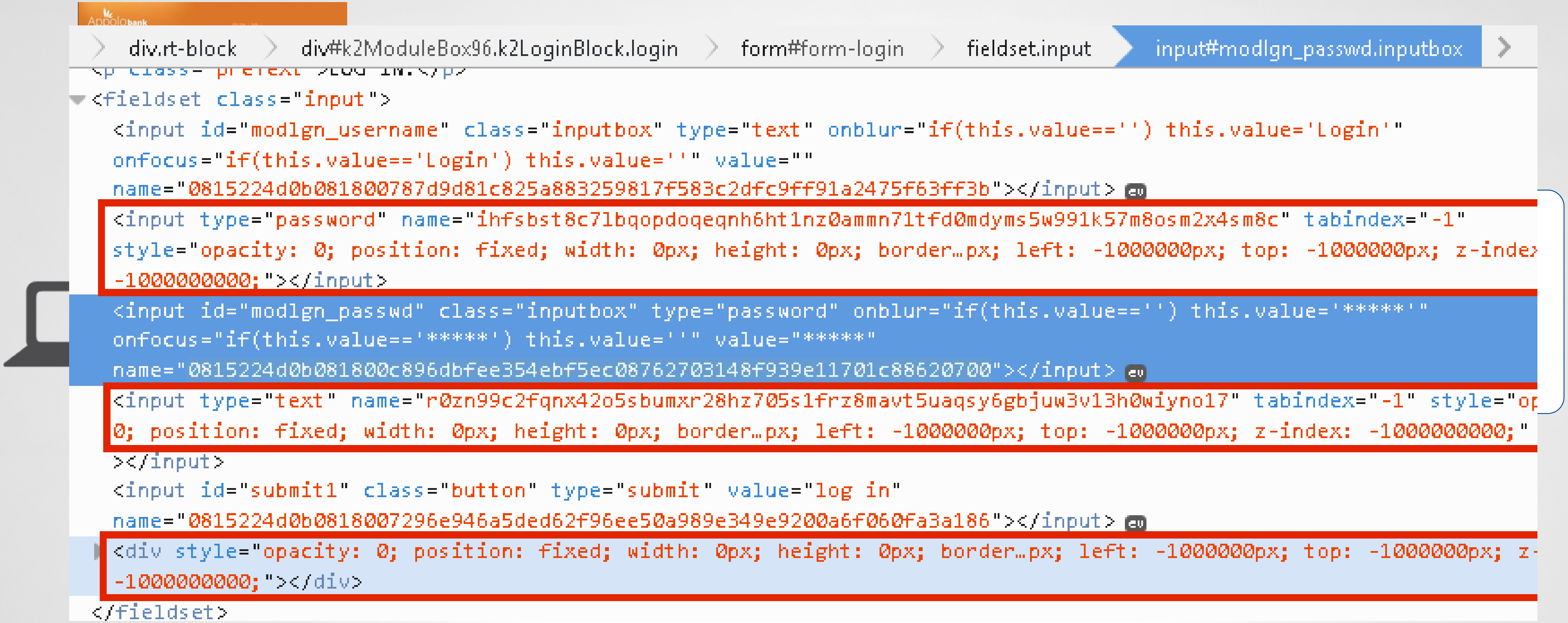
Protects against malicious scripts that seek out specific form elements

Dynamically changes field names on a frequent interval

Adds fake form fields to further confuse attackers

How HFO Works – With Decoy Fields

How HFO Works – Field Name Obfuscation


Appolobank
div.rt-block
div#k2ModuleBox96.k2LoginBlock.login
form#form-login
fieldset.input
input#modlgn_passwd.inputbox

```
<p class="pretext">LOG IN:</p>
<fieldset class="input">
  <input id="modlgn_username" class="inputbox" type="text" onblur="if(this.value=='') this.value='Login'"
  onfocus="if(this.value=='Login') this.value=''" value=""
  name="0815224d0b081800787d9d81c825a883259817f583c2dfc9ff91a2475f63ff3b"></input> ev
  <input type="password" name="ihfsbst8c7lbqopdoqeqnh6ht1nz0ammn71tfd0mdyms5w991k57m8osm2x4sm8c" tabindex="-1"
  style="opacity: 0; position: fixed; width: 0px; height: 0px; border…px; left: -1000000px; top: -1000000px; z-inde
  -1000000000;"></input>
  <input id="modlgn_passwd" class="inputbox" type="password" onblur="if(this.value=='') this.value='*****'"
  onfocus="if(this.value=='*****') this.value=''" value="*****"
  name="0815224d0b081800c896dbfee354ebf5ec08762703148f939e11701c88620700"></input> ev
  <input type="text" name="r0zn99c2fqnx42o5sbumxr28hz705s1frz8mavt5uaqsy6gbjuw3v13h0wiyno17" tabindex="-1" style="op
  0; position: fixed; width: 0px; height: 0px; border…px; left: -1000000px; top: -1000000px; z-index: -1000000000;"
  ></input>
  <input id="submit1" class="button" type="submit" value="log in"
  name="0815224d0b0818007296e946a5ded62f96ee50a989e349e9200a6f060fa3a186"></input> ev
  <div style="opacity: 0; position: fixed; width: 0px; height: 0px; border…px; left: -1000000px; top: -1000000px; z-
  -1000000000;"></div>
</fieldset>
```

Application-Layer Protection

Secures valuable data submitted on forms

Encryption as you type

The sensitive information is encrypted in real time on the client with a public key

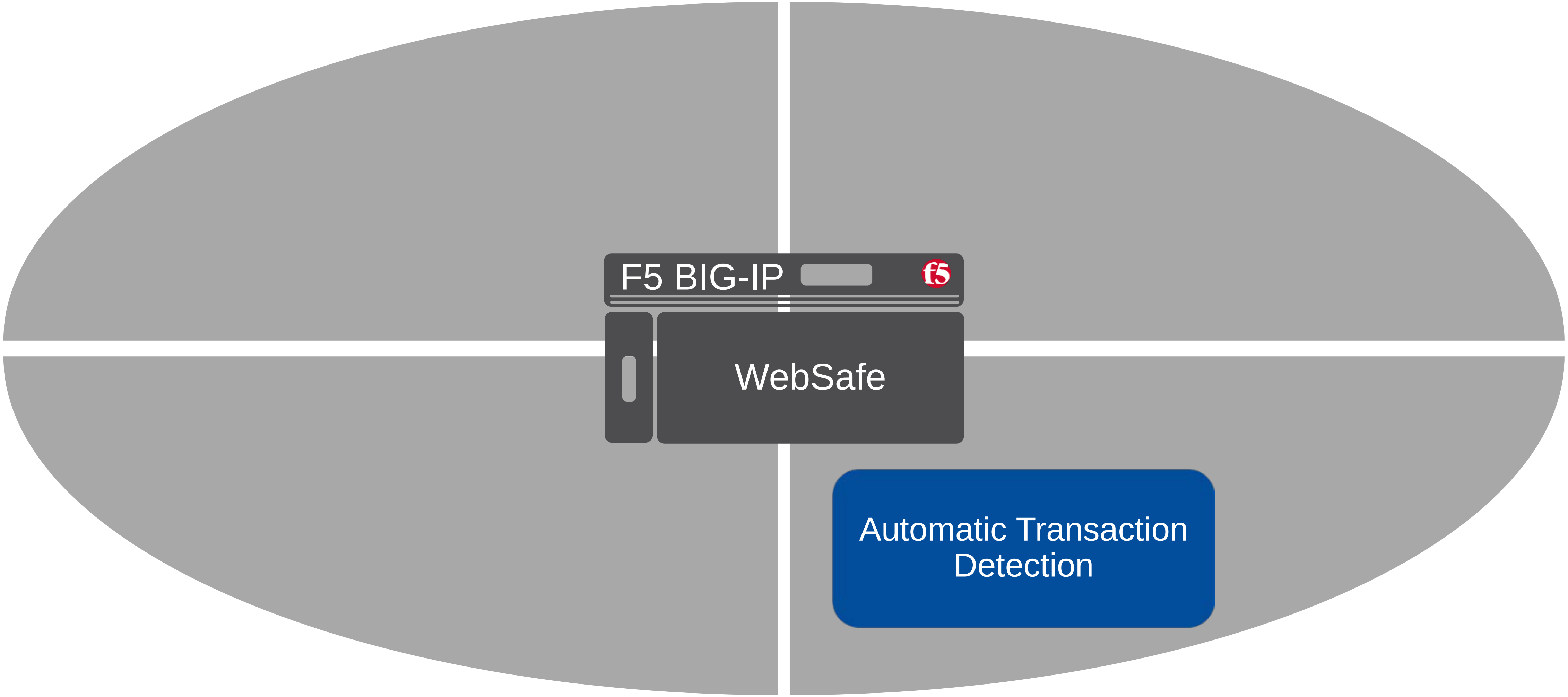
Decrypted in hardware on the BIG-IP by using the private key

Intercepted information rendered useless to attackers

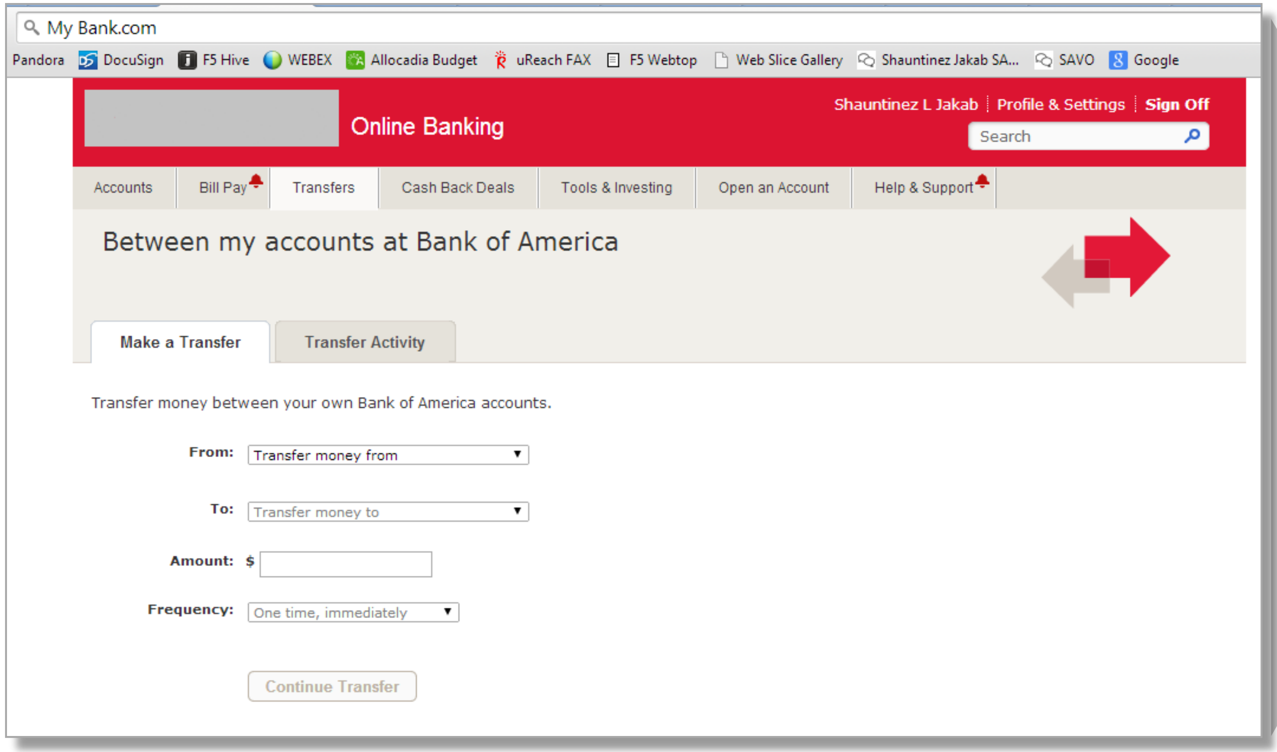
Form fields can be obscured to slow down or impede hacker visibility

F5’s Web Fraud Protection Services

Extends application security to the client-side



Automatic Transaction Detection



Between my accounts at Bank of America

Transfer money between your own Bank of America accounts.

From: Transfer money from

To: Transfer money to

Amount: $

Frequency: One time, immediately

- Gather client details related to the transaction
- Run a series of checks to identify suspicious activity
- Assign risk score to transaction
- Send alert based on score

Uniquely analyzes user interaction with the browser

Detects automatic transaction

Ensure integrity of transaction data

Trigger alerts upon detecting non-human behavior

MobileSafe

MobileSafe

Extends protection to mobile mobile applications

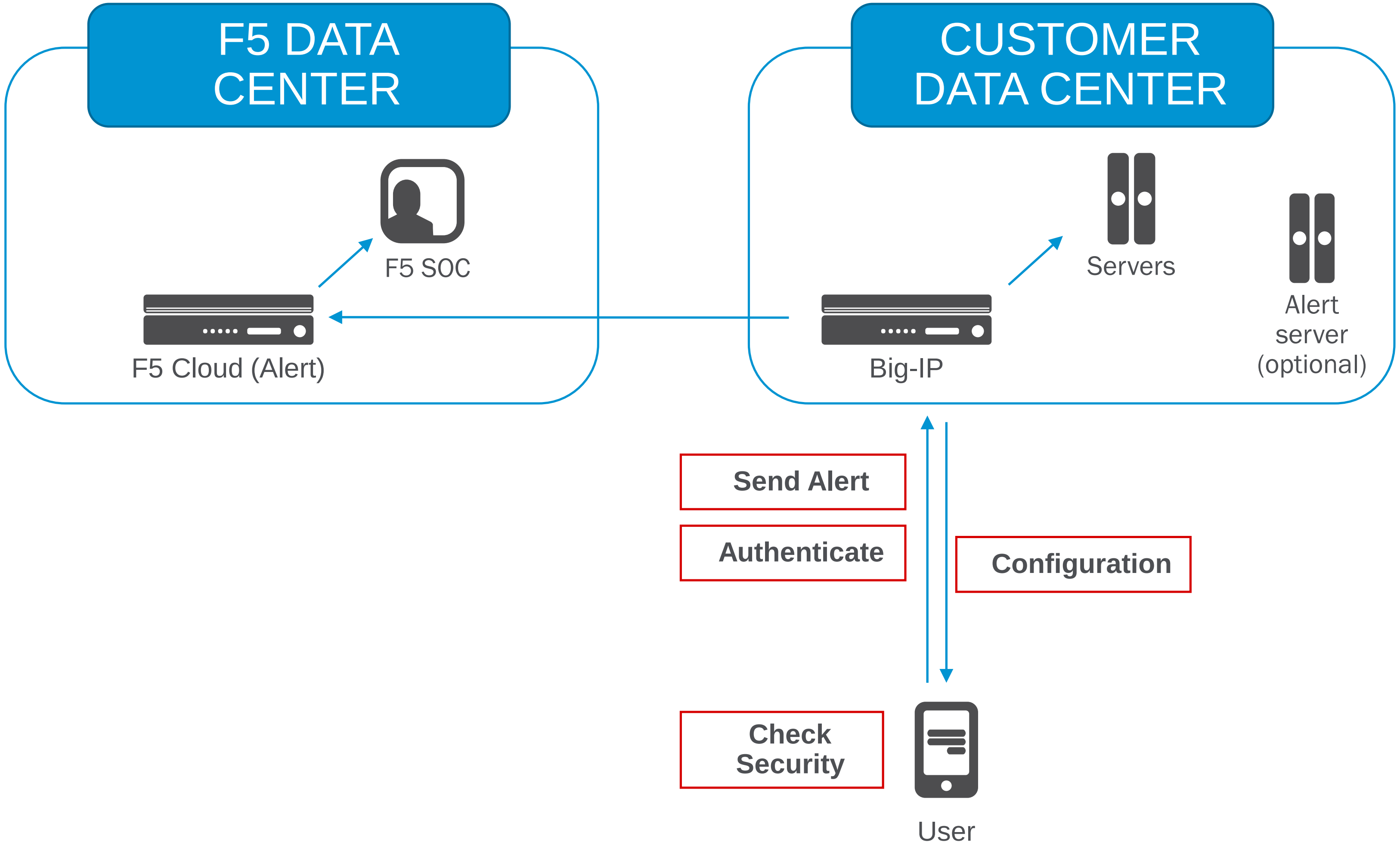
MobileSafe is a service based on BIG-IP, SDK and the F5 SOC to secure mobile applications

The SDK is deployed by the institutions within their mobile applications and used to check the security of the app and the device running it

Configuration and security settings are loaded from BIG-IP

WebSafe and MobileSafe share the same Dashboard

MobileSafe Workflow



MobileSafe Security Features 1/2

DNS spoofing detection

The target domain is checked against a pre-loaded list of known IPs

Certificate forging detection

The target certificate is compared against a pre-loaded certificate

Jailbreak/Rooting detection

Detection of a jailbreak and rooted device

Unpatched/unsecure OS detection

Identify unpatched versions with known vulnerabilities

Application repackaging detection

Integrity check to detect repackaging

MobileSafe Security Features 2/2

Malware detection using a variety of techniques

Signature based detection
Behavior based detection
Scan running processes
Scan app registry and folders
Scan dynamic libraries
SMS grabber detection
Focus Stealing detection

Application Level encryption

Protect sensitive data

Key logging protection

F5 SECURITY OPERATION CENTER (SOC)

Augment Resources with the F5 Security Operations Center

Fraud analysis that extends a customer's security team

Real-time alerts activated by phone, SMS, and email

SOCs in the US and EMEA

SOC services complimentary for fraud protection customers

Optional website take-down for phishing sites

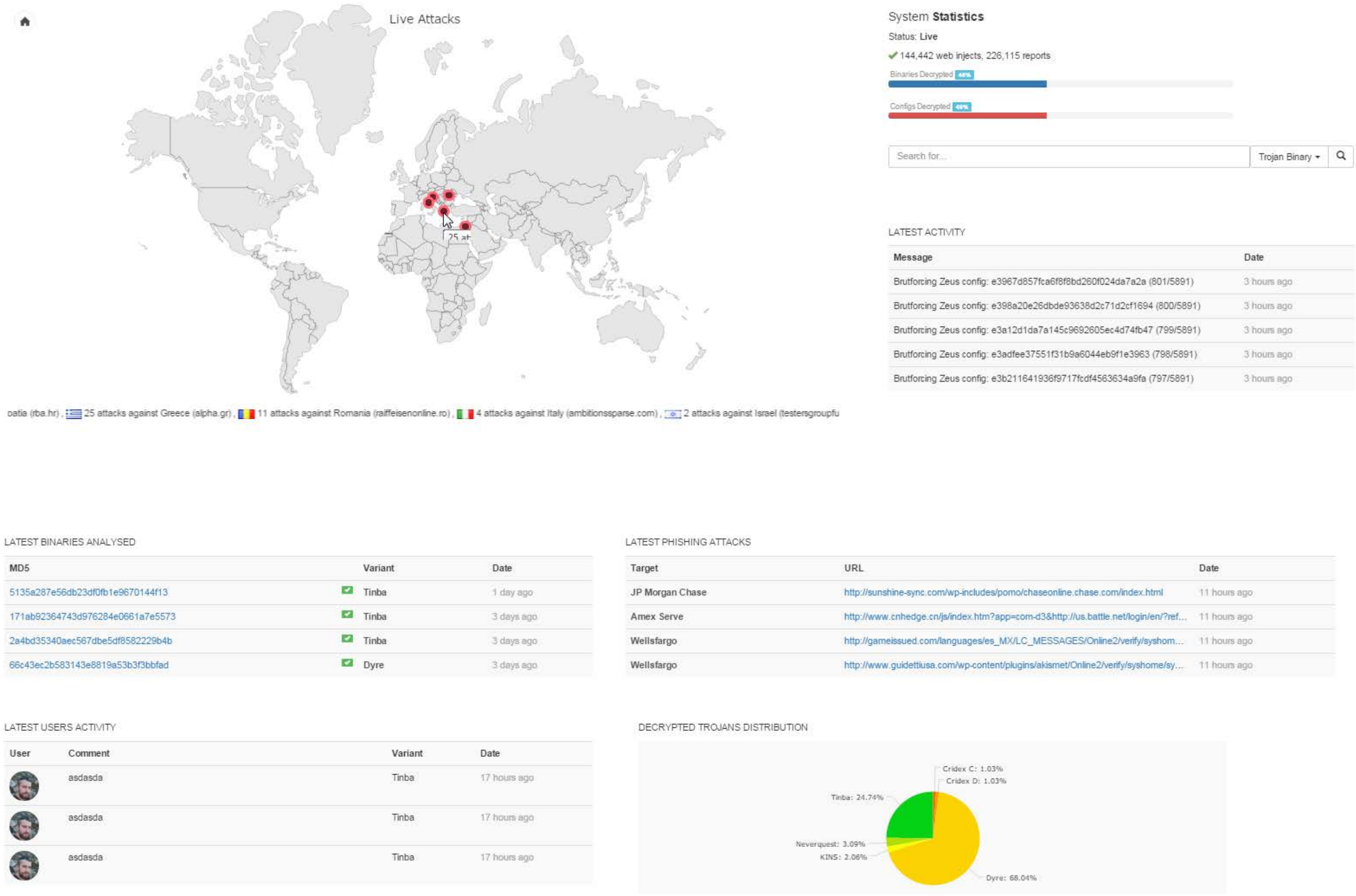
Filtering alerts by severity and ignoring false positives

Detailed incident reports

Continuous web fraud deployment validation

Researching and investigating new global fraud technologies

F5 Threat Monitor



oatia (rba.hr) , 25 attacks against Greece (alpha.gr) , 11 attacks against Romania (raiffeisenonline.ro) , 4 attacks against Italy (ambitionssparse.com) , 2 attacks against Israel (testersgroupfu

System **Statistics**

Status: **Live**

✓ 144,442 web injects, 226,115 reports

Binaries Decrypted 46%

Configs Decrypted 46%

LATEST ACTIVITY

Message	Date
Brutforcing Zeus config: e3967d857fca6f8f8bd260f024da7a2a (801/5891)	3 hours ago
Brutforcing Zeus config: e398a20e26dbde93638d2c71d2cf1694 (800/5891)	3 hours ago
Brutforcing Zeus config: e3a12d1da7a145c9692605ec4d74fb47 (799/5891)	3 hours ago
Brutforcing Zeus config: e3adfee37551f31b9a6044eb9f1e3963 (798/5891)	3 hours ago
Brutforcing Zeus config: e3b211641936f9717fcdf4563634a9fa (797/5891)	3 hours ago

LATEST BINARIES ANALYSED

MD5		Variant	Date
5135a287e56db23df0fb1e9670144f13	✓	Tinba	1 day ago
171ab92364743d976284e0661a7e5573	✓	Tinba	3 days ago
2a4bd35340aec567dbe5df8582229b4b	✓	Tinba	3 days ago
66c43ec2b583143e8819a53b3f3bbfad	✓	Dyre	3 days ago

LATEST PHISHING ATTACKS

Target	URL	Date
JP Morgan Chase	http://sunshine-sync.com/wp-includes/pomo/chaseonline.chase.com/index.html	11 hours ago
Amex Serve	http://www.cnhedge.cn/js/index.htm?app=com-d3&http://us.battle.net/login/en/?ref...	11 hours ago
Wellsfargo	http://gameissued.com/languages/es_MX/LC_MESSAGES/Online2/verify/syshom...	11 hours ago
Wellsfargo	http://www.guidettiusa.com/wp-content/plugins/akismet/Online2/verify/syshome/sy...	11 hours ago

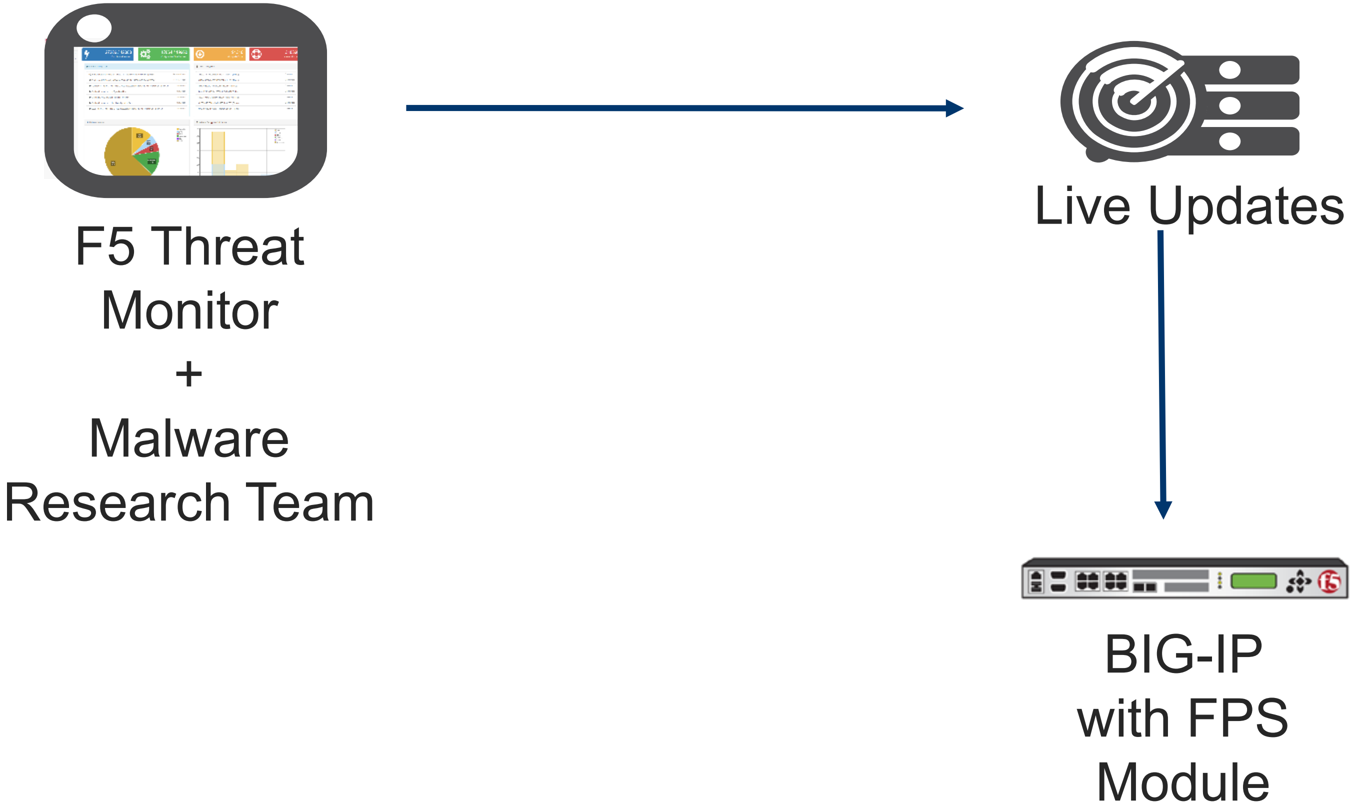
LATEST USERS ACTIVITY

User	Comment	Variant	Date
	asdasda	Tinba	17 hours ago
	asdasda	Tinba	17 hours ago
	asdasda	Tinba	17 hours ago

DECRYPTED TROJANS DISTRIBUTION

A cloud service analyzing thousands of malware samples every day

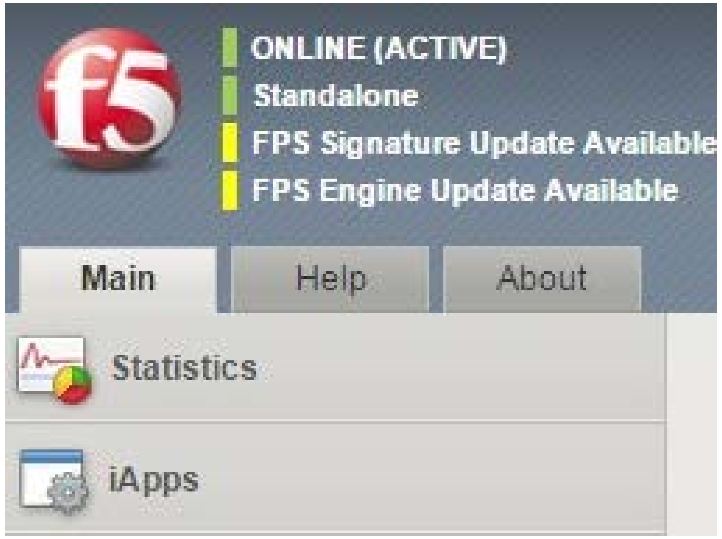
Live Update in v12



F5 Threat Monitor
+
Malware Research Team

Live Updates

BIG-IP
with FPS
Module



ONLINE (ACTIVE)
Standalone
FPS Signature Update Available
FPS Engine Update Available

Signatures for detecting new threats get deployed quickly

F5's Web Fraud Protection Service Solutions

Prevent Fraud

Targeted malware, MITB, zero-days, MITM, phishing, automated transactions…

Protect Online User

Clientless solution, enabling 100% coverage

On All Devices

Desktop, tablets & mobile devices

Full Transparency

No software or user involvement required

In Real Time

Alerts and customizable rules

If I can be of further assistance please contact me:
a.vistola@f5.com

SOLUTIONS FOR AN APPLICATION WORLD