Protecting Your Customers and Online Businesses Against Modern Malware Threats

Alfredo Vistola

Sr. Security Solution Architect

Agenda

Statistics

Trojan examples

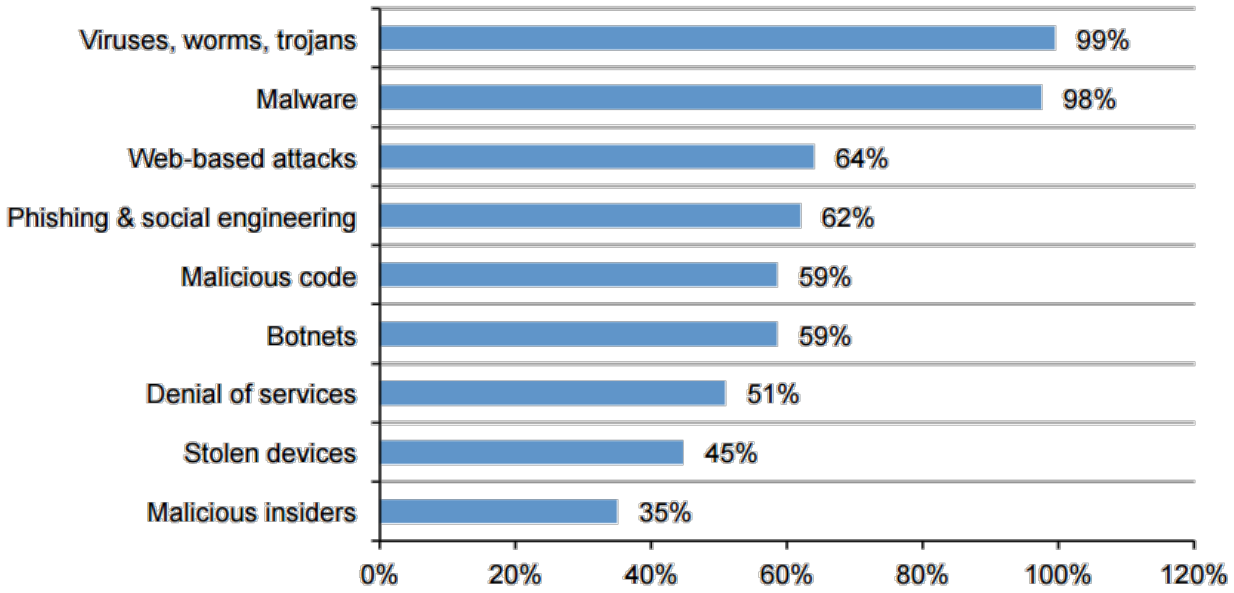
Attack vectors

Mitigation with WebSafe and MobileSafe

Cost of Cyber Crime Global, Ponemon Report

Types of Cyber Attacks experienced

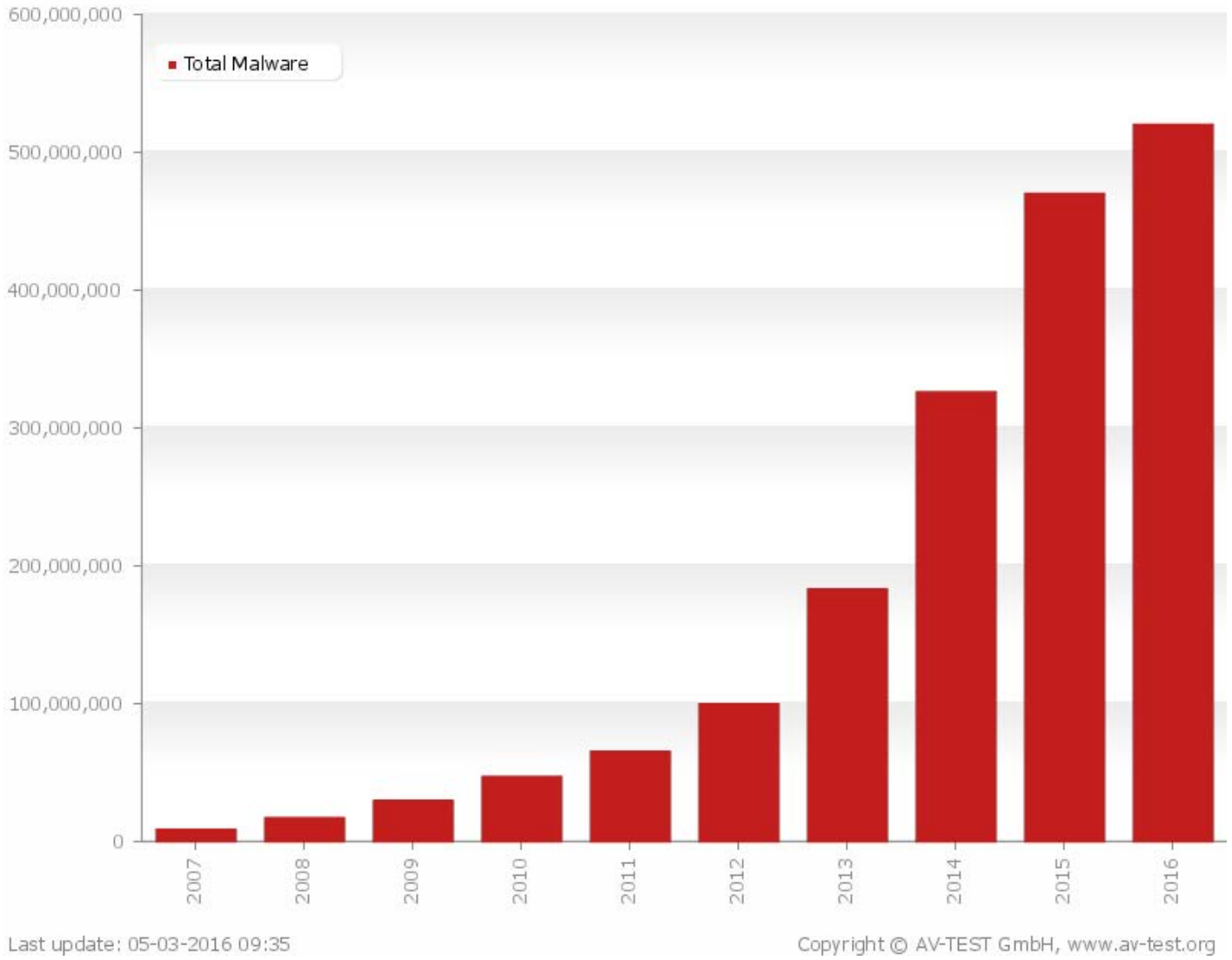
Figure 9. Types of cyber attacks experienced by 252 benchmarked companies
Consolidated view, n = 252 separate companies



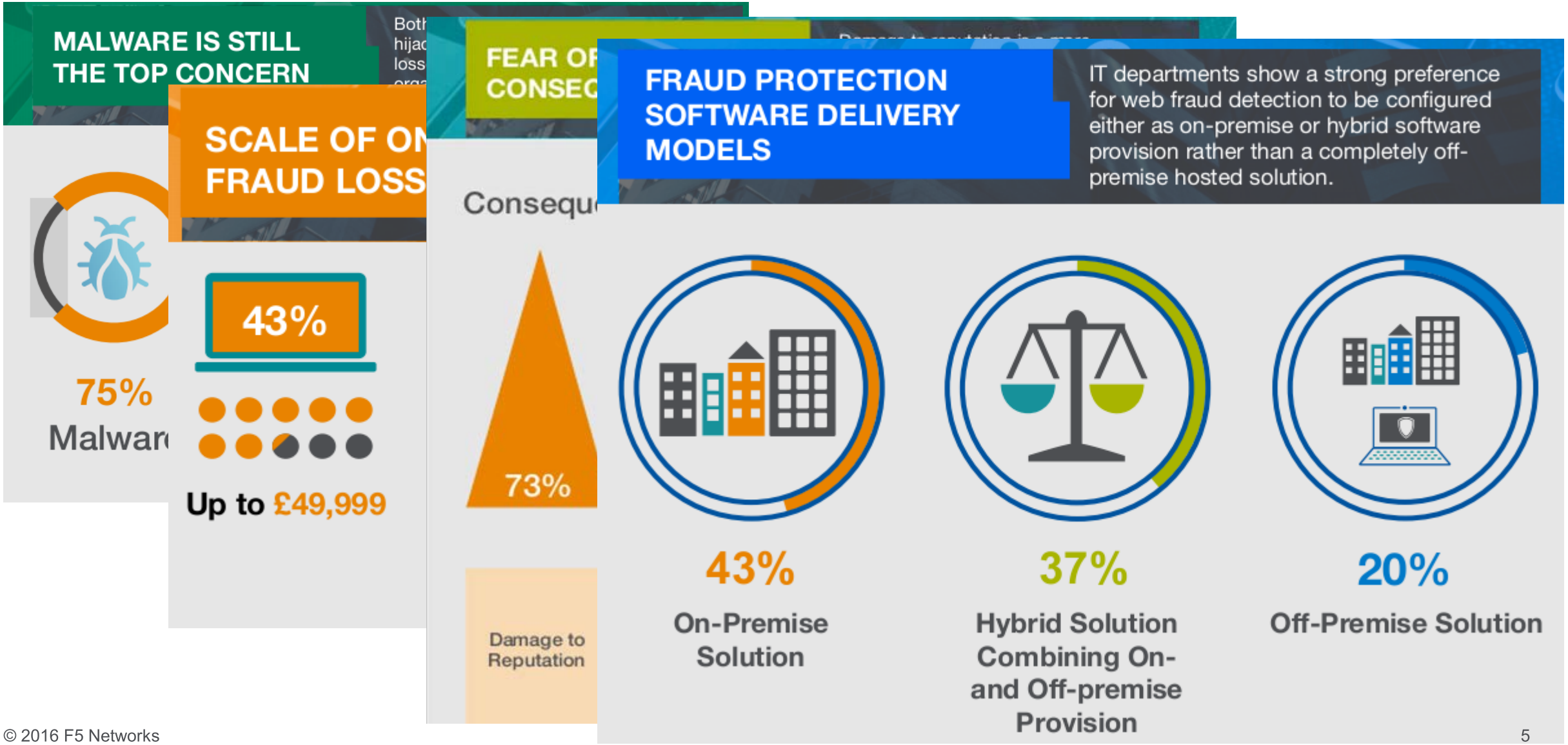
Source: Cost of Cyber Crime, Ponemon Institute Oct. 2015

The mean annualized cost for 252 benchmarked organizations is $7.7 million per year, with a range from $0.31 million to $65 million

Total Malware Growth



Malware Threat Landscape – Growth and Targets



70 percent of CxOs think rogue individuals make up the largest threat to their organizations. The reality is that 80 percent of cyberattacks are driven by highly organized crime rings in which data, tools and expertise are widely shared according to an United Nations report

https://www-03.ibm.com/press/uk/en/pressrelease/49137.wss
UNODC Comprehensive Study on Cybercrime 2013

Cyber‘s most wanted by the FBI

https://www.fbi.gov/wanted/cyber

Malware Attacks - From The News

The Hacker News™
Security in a serious way

Free Hacking Training
CYBRARY.IT

Hackers Stole $300 Million from 100 Banks Using Malware
Sunday, February 15, 2015 Wang Wei

New Hybrid Banking Trojan 'GozNym' Steals Millions

Ransomware Repurposed to Target Business Accounts

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

Facebook LinkedIn Credit Eligible Get Permission

The Sydney Morning Herald
Digital Life

Ihr Flug vom 13.06. - 15.06.16
Wien Hin + Zurück ab 309€*
Jetzt buchen

Latest News Gadgets Science Innovation Web Culture Gaming Security IT Pro

You are here: Home » Technology »

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

March 10, 2016 Comments 172 Read later

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.

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

Share this article:

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 Dyre 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

f 25

Dridex Trojan Borrows Redirection Attack Scheme from Dyre Malware

By SecurityWeek News on January 20, 2016

Share 43 | G+1 2 | Tweet | Empfehlen 30 | RSS

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

salesforce

New Variants

New Dridex Variants Achieve High Infection Rate Using Poisoned Docs

By SecurityWeek News on November 25, 2015

Share 43 G+1 5 Tweet Empfehlen 13 RSS

The infamous Dridex banking Trojan recently surfaced again in spam campaign runs that have managed to achieve a high infection rate, security companies ESET and Trend Micro warn.

New Variant of Tinba Banking Trojan Targets European Users

By Eduard Kovacs on June 09, 2015

Share 48 G+1 4 Tweet Empfehlen 17 RSS

A new and improved version of Tinba, a banking malware been spotted in attacks targeting the customers of Europe

Tinba, also known as Tinybanker and Zusy, was first spotted Similar to other banking Trojans, Tinba uses man-in-the-brov injects to collect valuable information from victims.

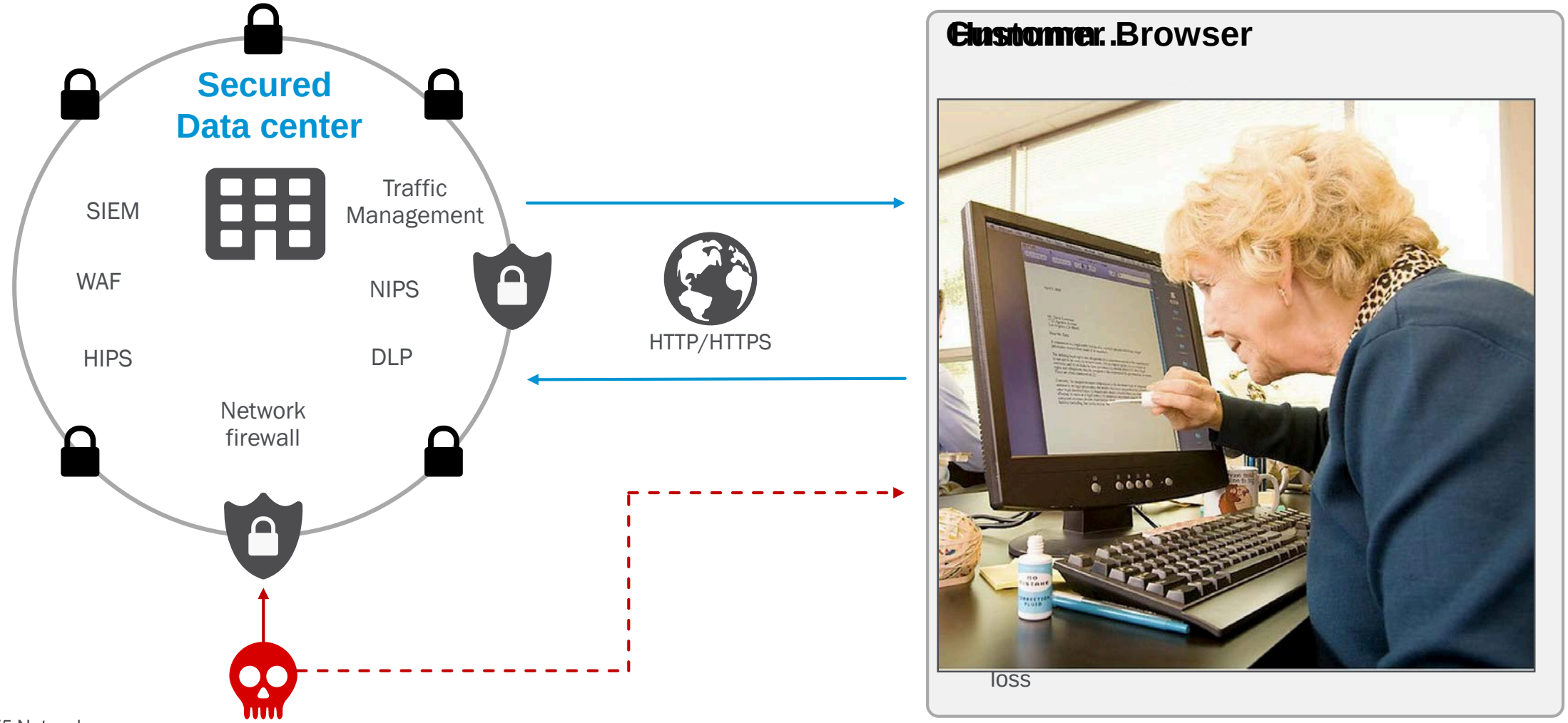
Tinba Number Five Takes Aim at Asia-Pacific Finance

BY DOUGLAS BONDERUD • JANUARY 19, 2016

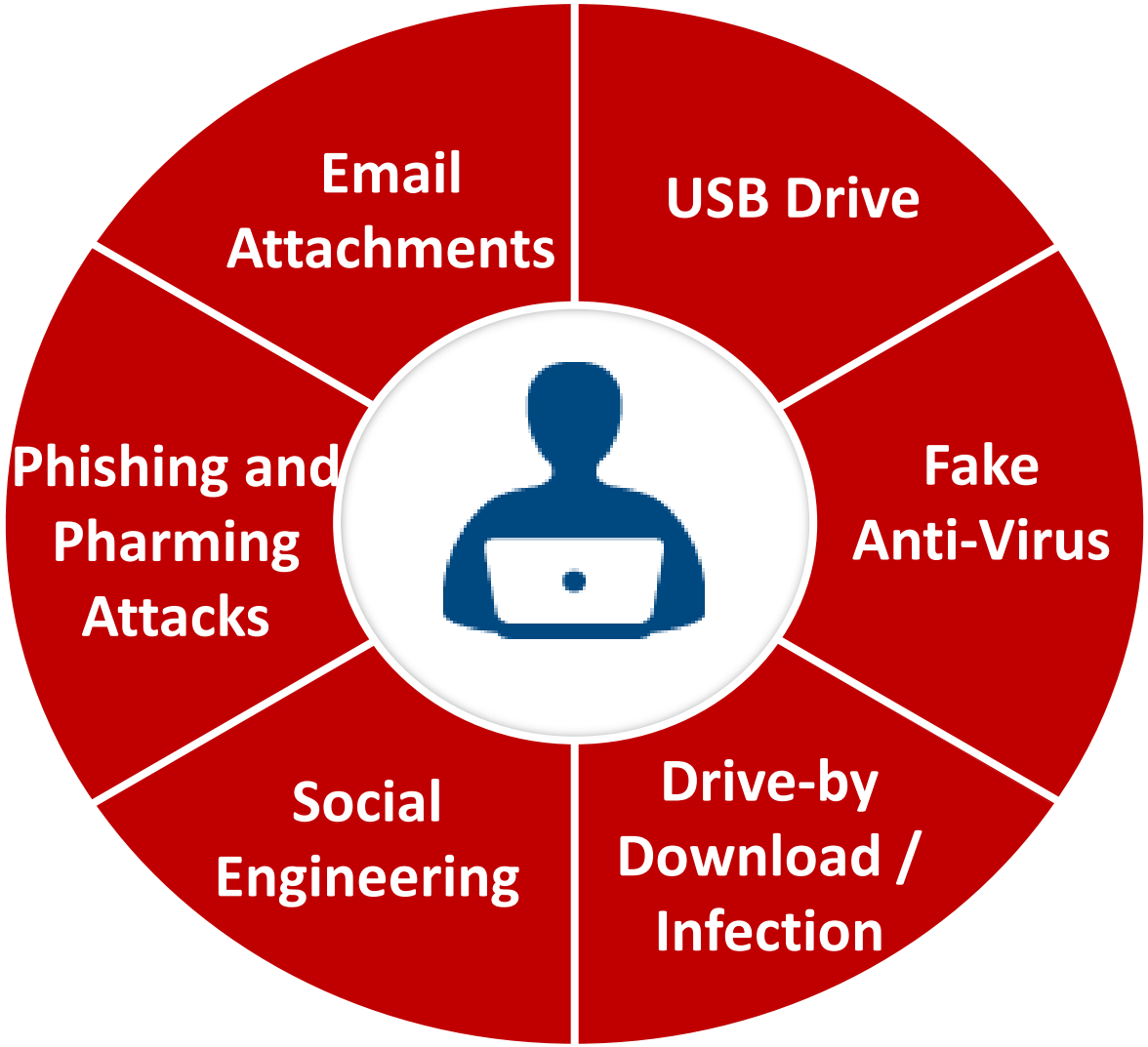
ATTACK VECTORS

Browser is the Weakest Link

End point risks to “Data In Use”



How Trojans Infect Devices



Newspaper Website Involuntary Spreads Ebanking Trojan

GovCERT.ch Blog

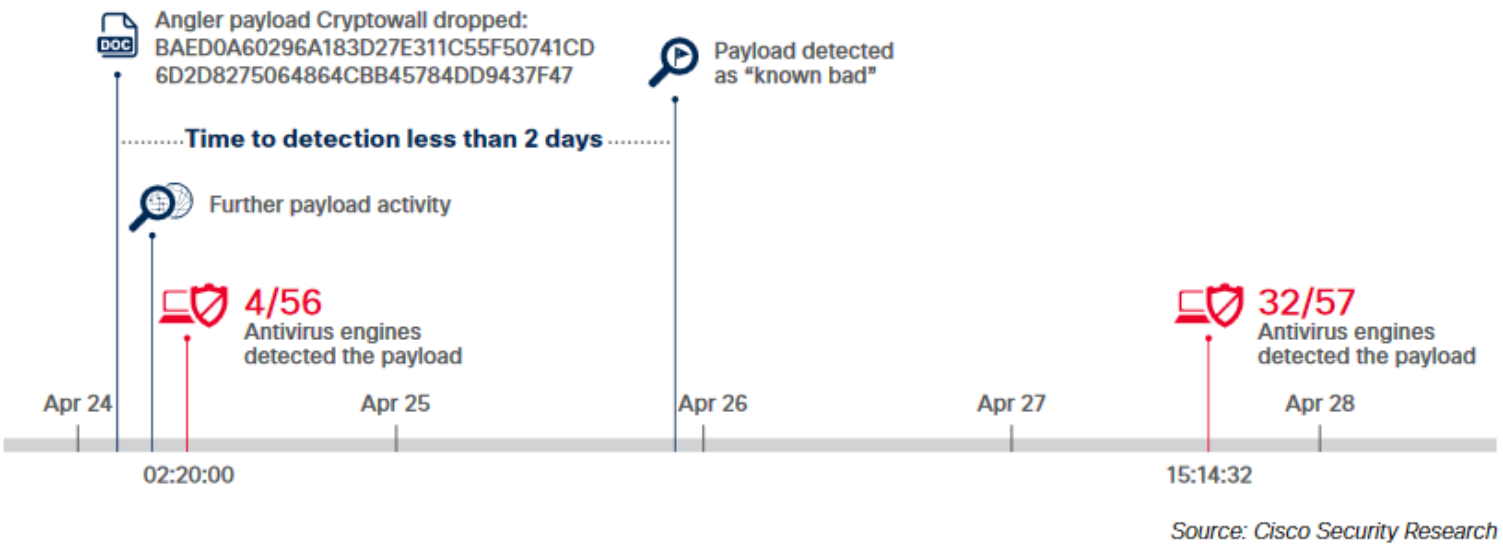
20min.ch Malvertising Incident

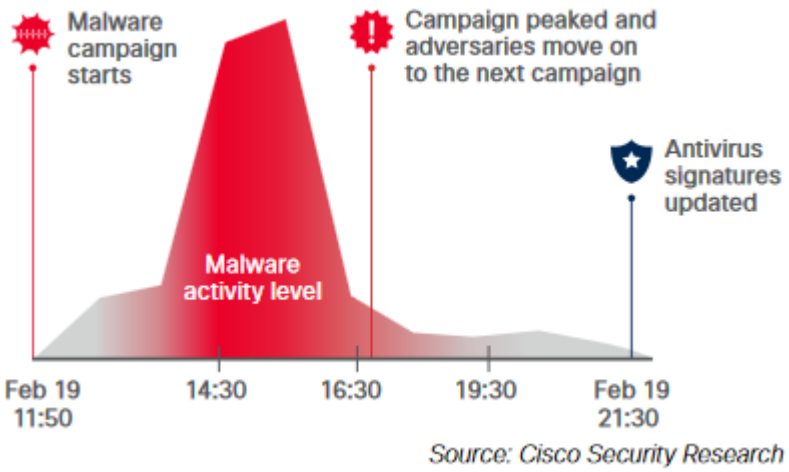
Published on 2016-04-08 09:38:00 UTC by GovCERT.ch (permalink)
Last updated on 2016-04-08 10:16:42 UTC

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

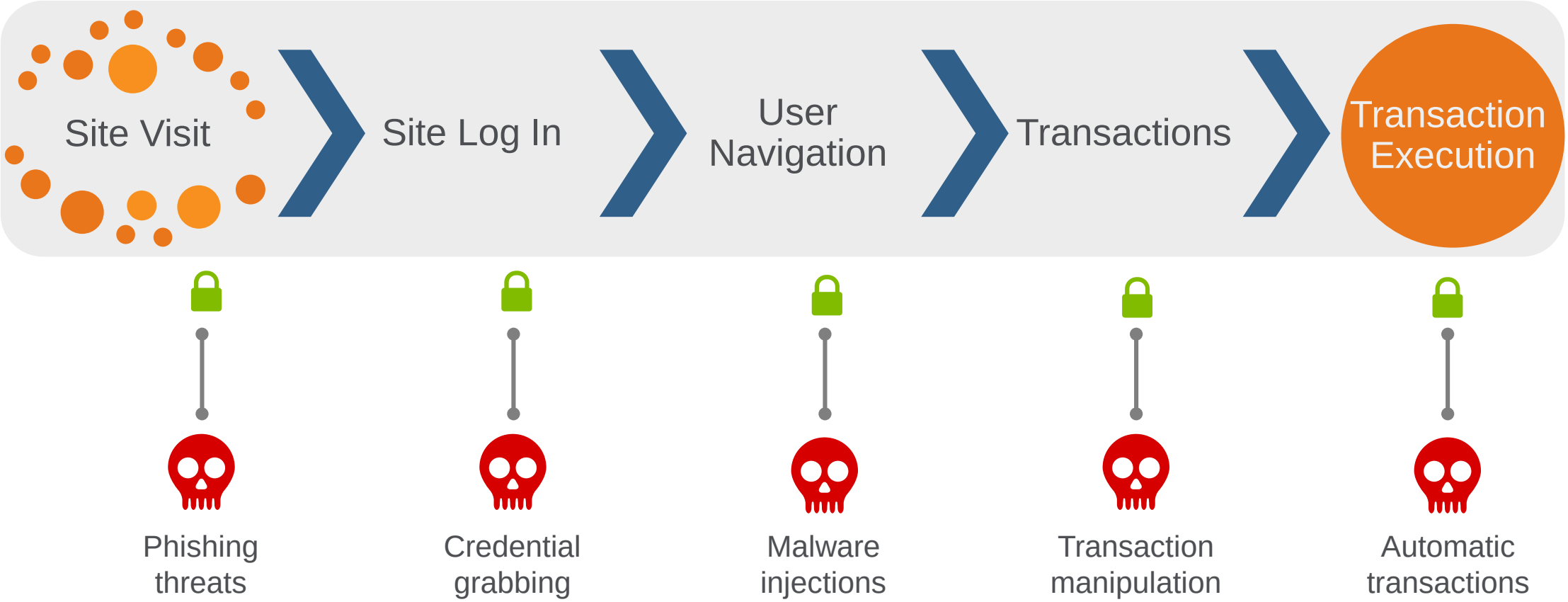




Trojans are able to stop the automatic signature update or trigger just once

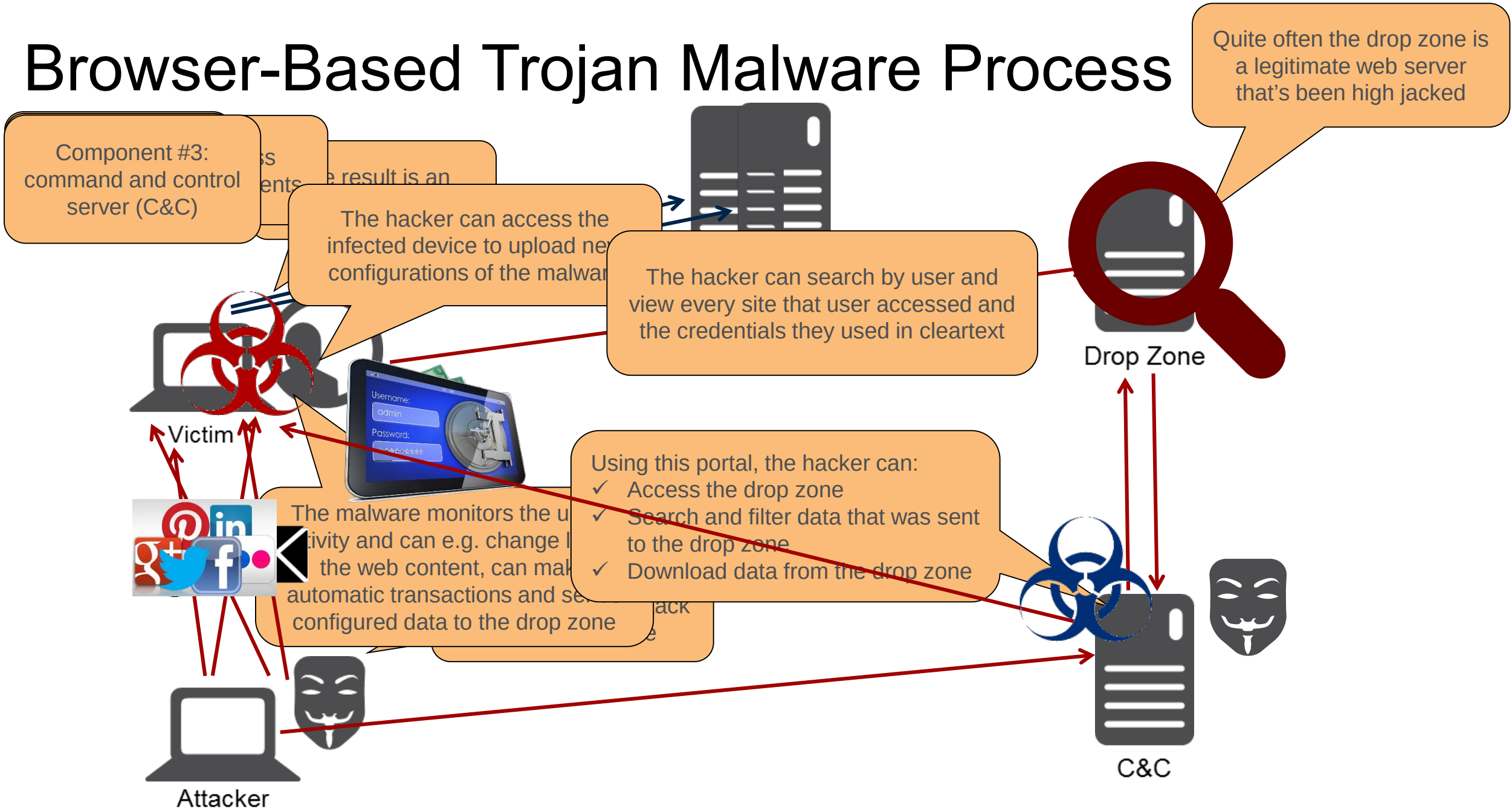
Attack Vectors

Web application transaction flow



Ensure defense against these threats

Browser-Based Trojan Malware Process



Why Should You Care About Identity Theft?

…because your customers and employees are targeted

Server side and client side credential stealing attacks

Database access (SQL Injection,...)

Phishing

Brute Force

Malware

...

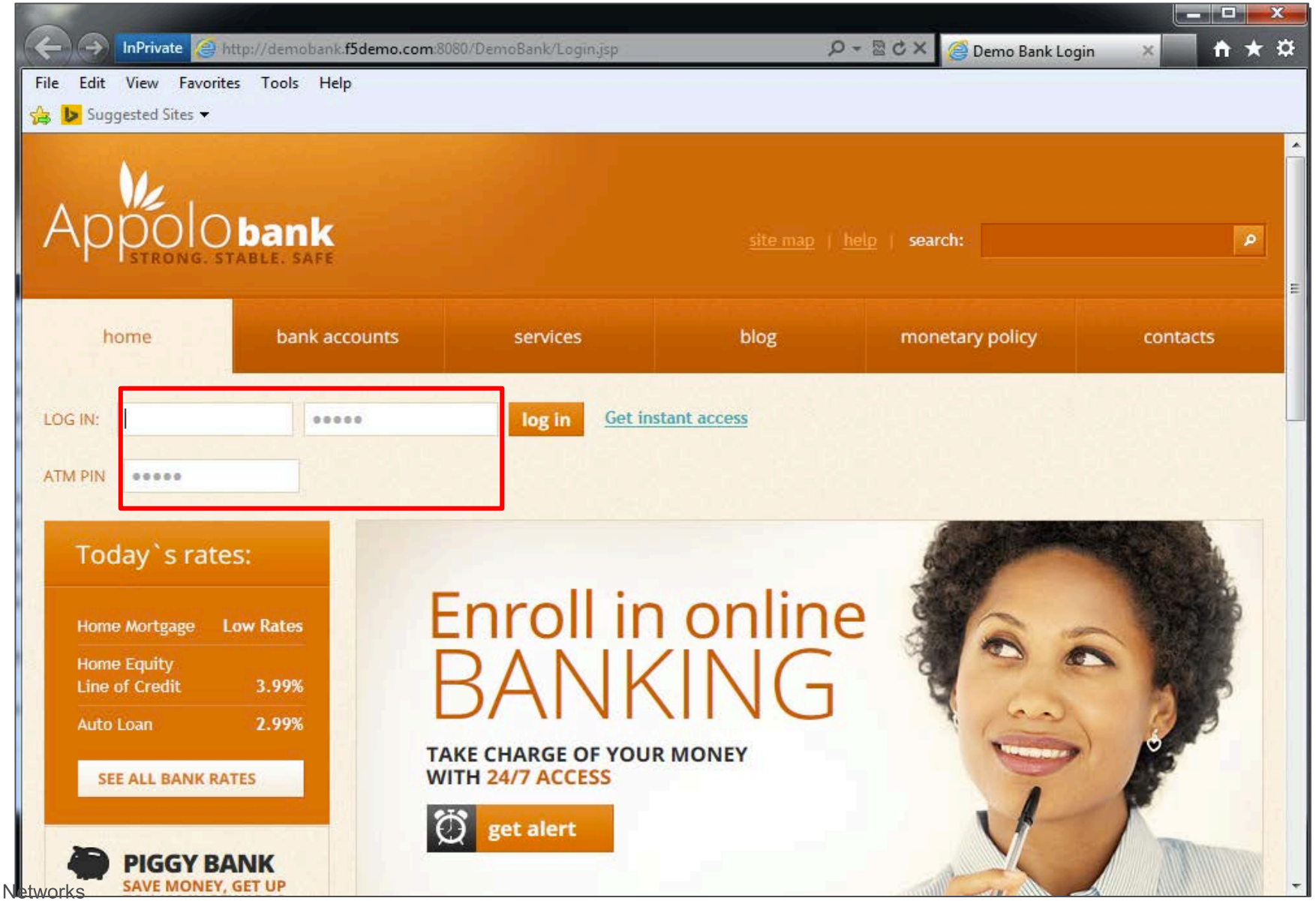
Gartner Blog Network

Avivah Litan

A member of the Gartner Blog Network

"Over the past couple of months, Gartner clients have been telling us about the significant rise in automated attacks, whereby hackers use bot armies to run through user credentials at various consumer service websites"

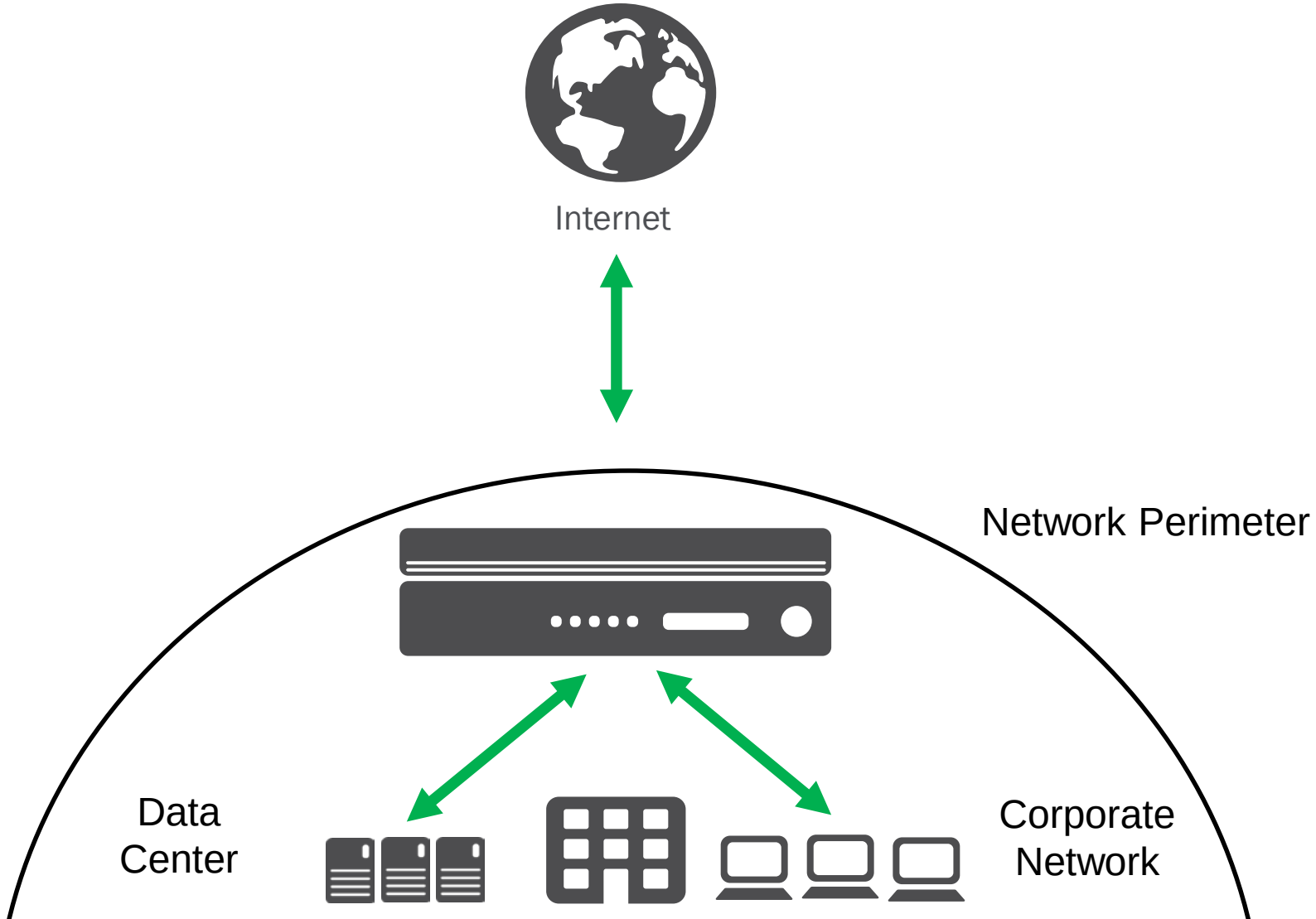
Web Injection Example



Web Injection Example

MITIGATION WITH THE F5 CLIENTLESS WEBSAFE AND MOBILESAFE SOLUTION

F5 Fraud Protection Versus Traditional Malware Solutions



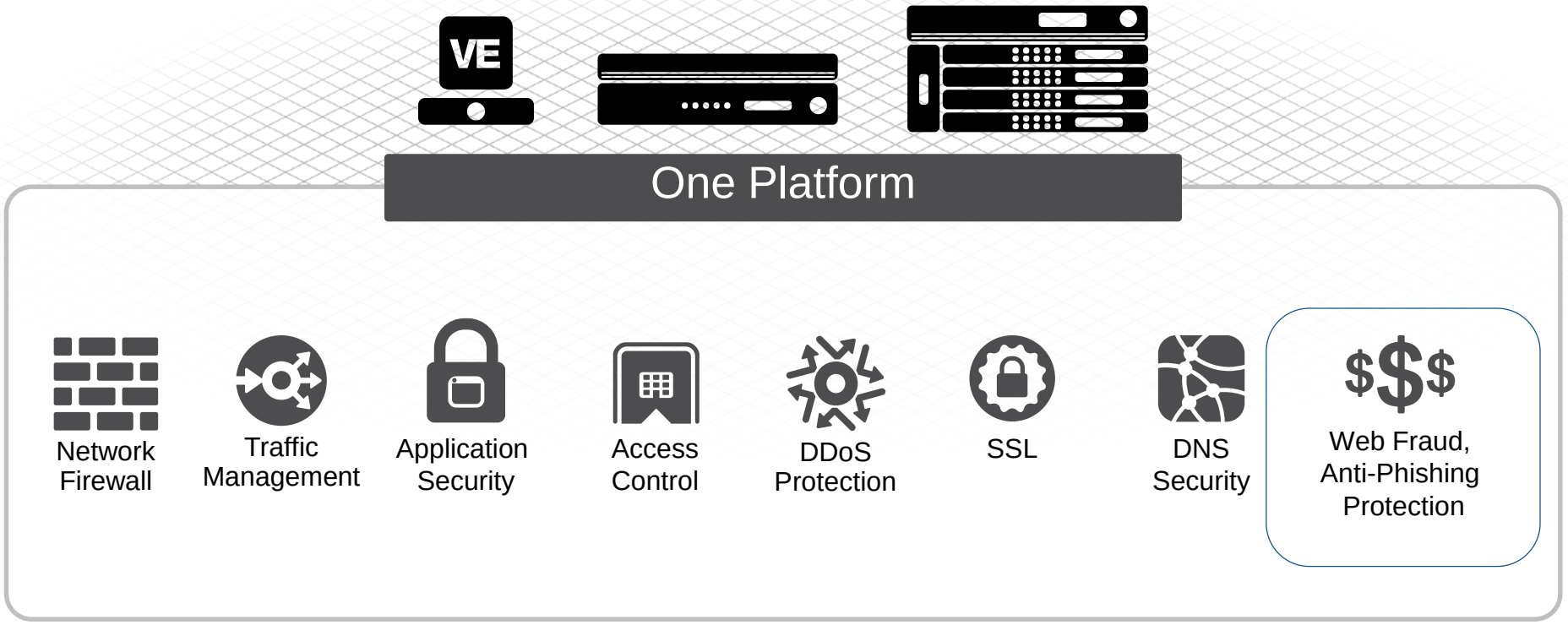
F5 Fraud Protection Versus Traditional Malware Solutions

- ✓ 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



ICSA labs CERTIFIED IPSEC

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

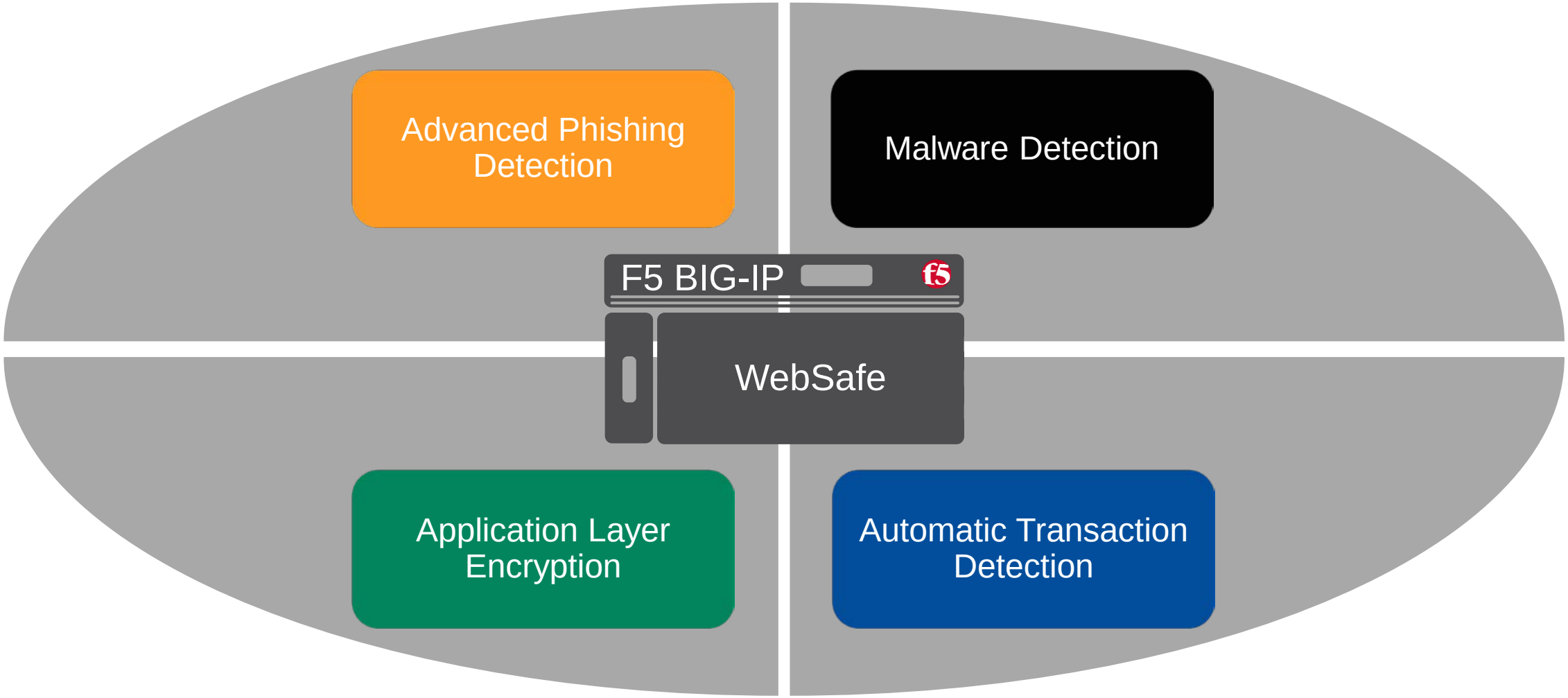
Common Criteria
EAL2+
EAL4+ (in process)

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

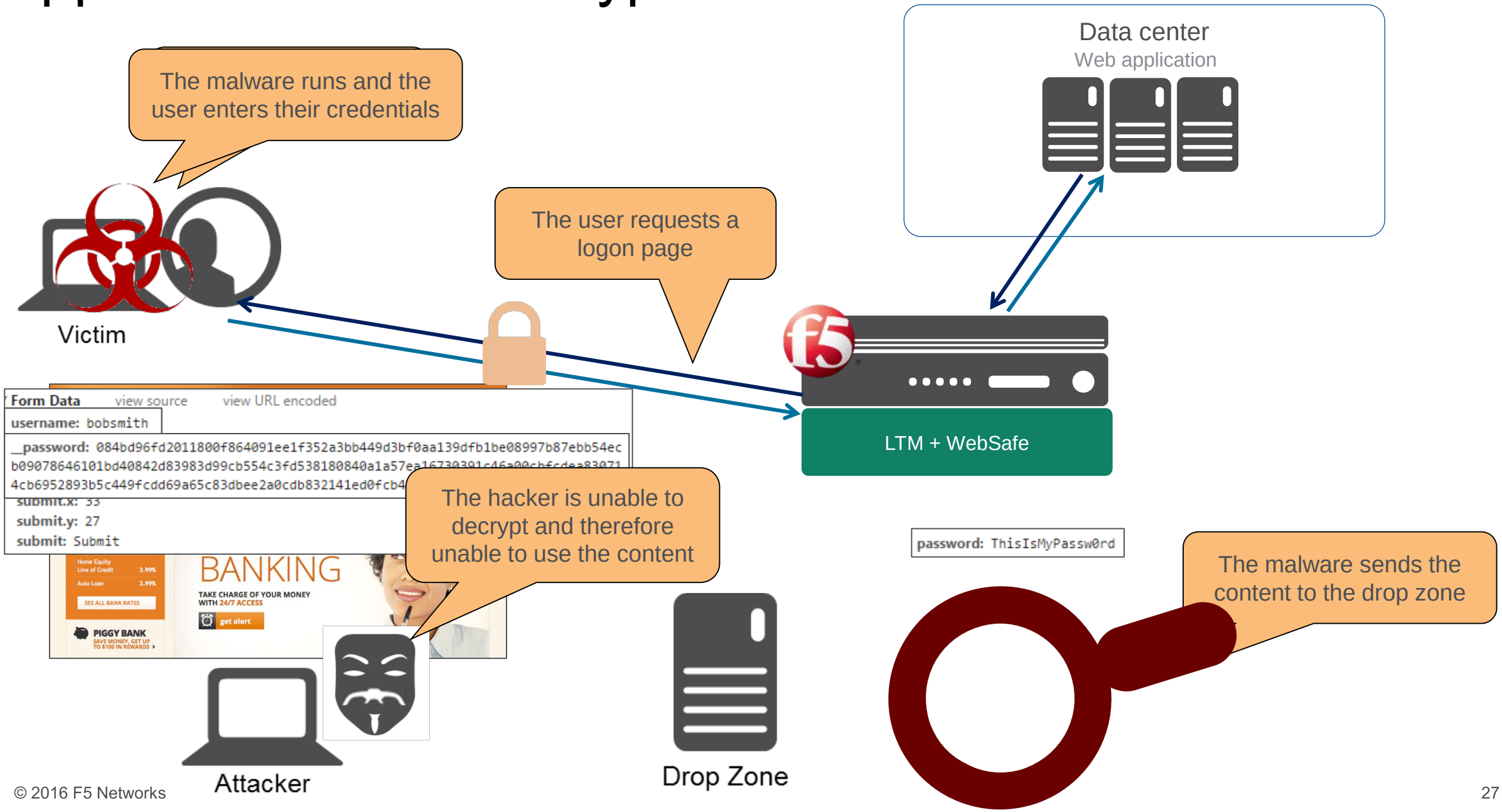
WEBSAFE

F5's Web Fraud Protection Services

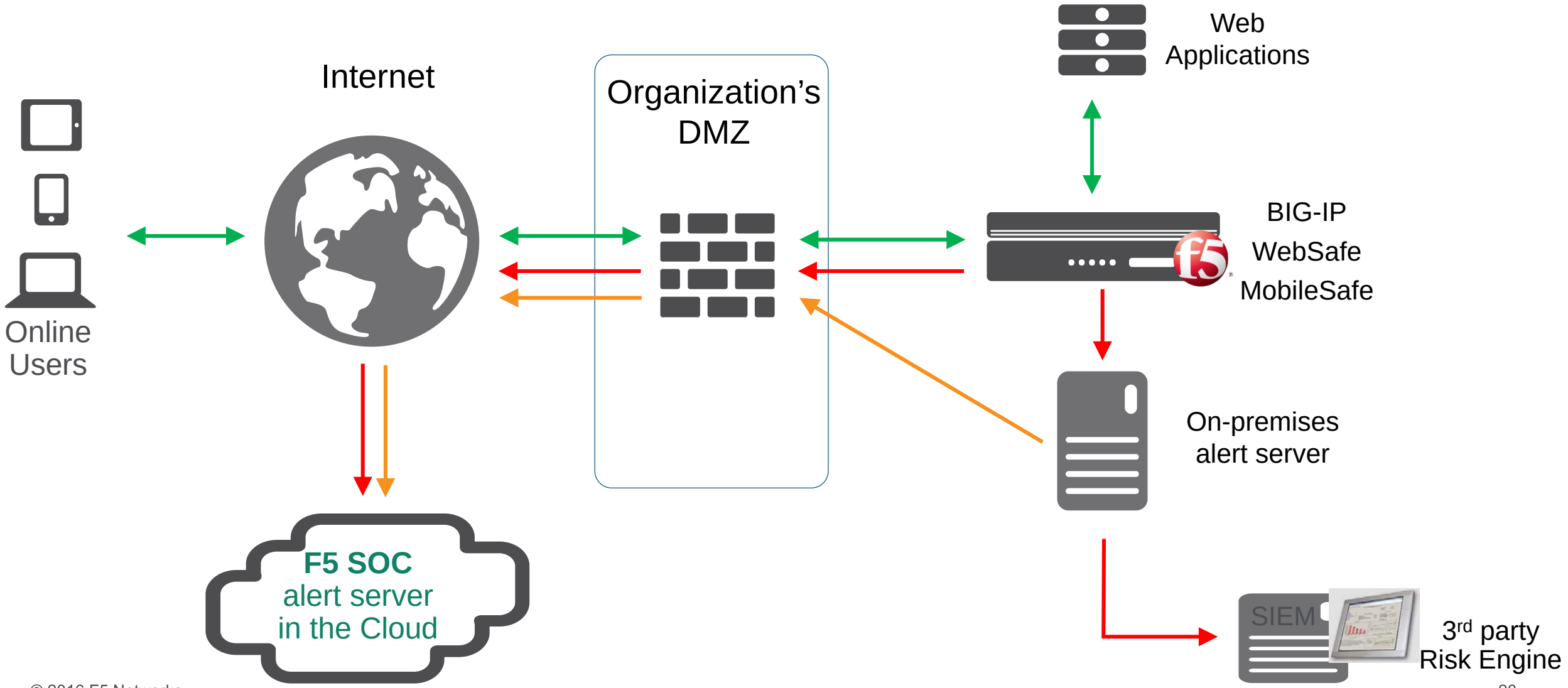
Extends application security to the client-side



Application Level Encryption to Protect Confidential Data



Web Fraud Protection Implementation Options



Real-Time Alerts Dashboard

BIG-IQ Fraud Protection Service

- 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

Advanced Filter | Refresh | Create Rule | Export | Change Status | Remove

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/lUirvH/	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)

Filter...

Details | HTML | Data | About | Advanced

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

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 Security Features

Detection Modules

Certificate forging detection

DNS Spoofing detection

Jailbreak/Rooting detection

Malware detection

Unpatched/Unsecure OS detection

Repackaging detection

Other Features

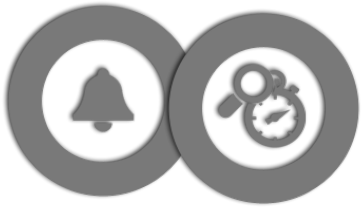
App Level Encryption

Key Logging Protection

F5 SECURITY OPERATION CENTER (SOC)

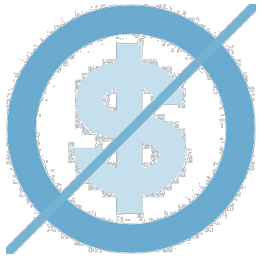
Augment Resources with the F5 Security Operations Center

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

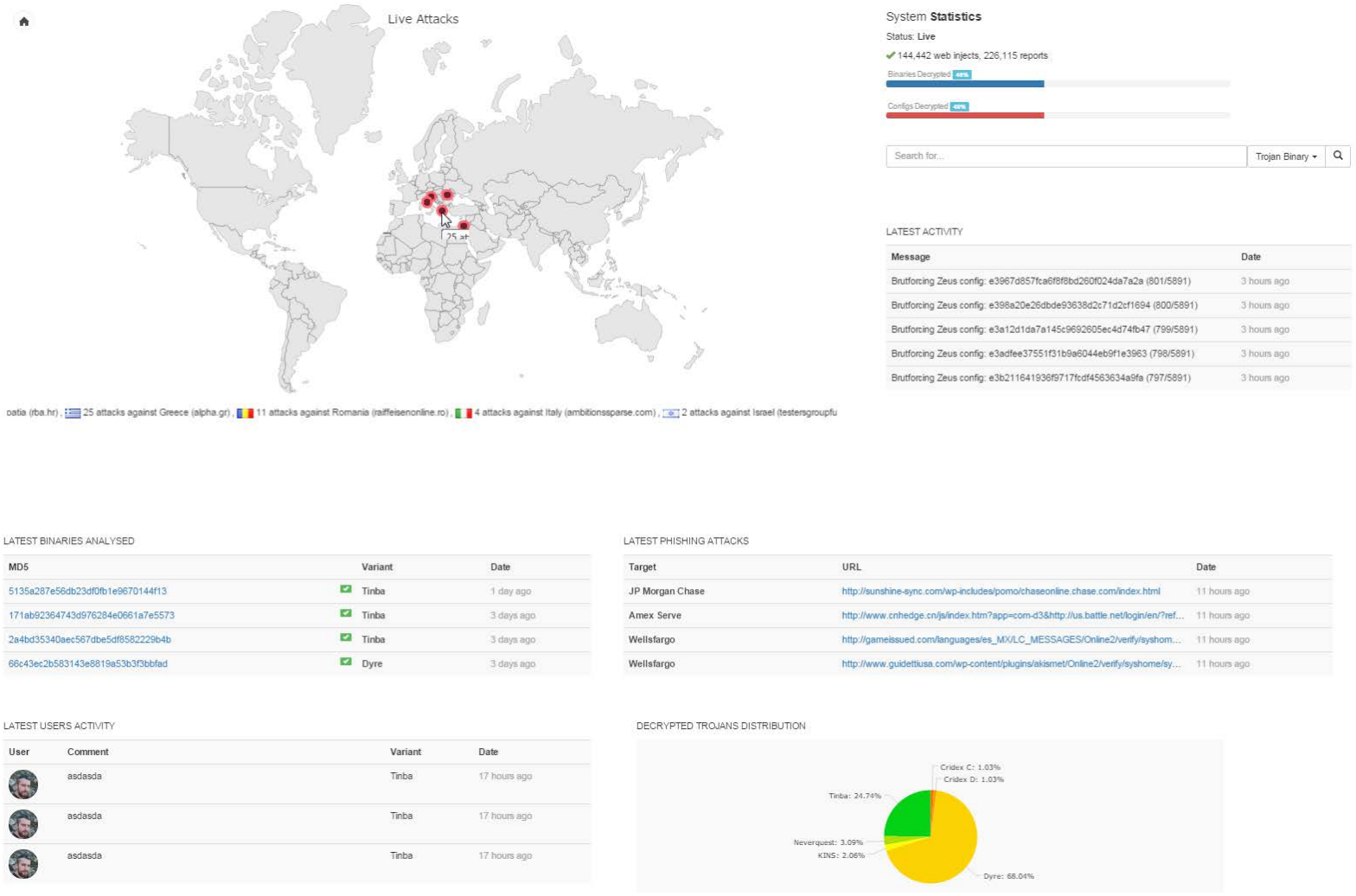
Filtering alerts by severity and ignoring false positives

Detailed incident reports

Continuous web fraud deployment validation

Researching and investigating new global fraud technologies

F5 Threat Monitor



A cloud service analyzing thousands of malware samples every day

Live Update

F5 Threat Monitor
+
Malware Research Team

Live Updates

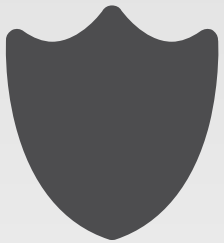
BIG-IP with FPS Module

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…

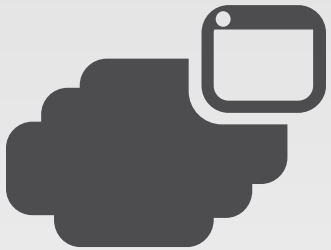


Protect Online User

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

Banking, Financial Services and Insurance

How do you currently protect your online services against fraud?

Does your current solution requires client side installation?

What do you use to mitigate credential theft?

Does your current solution provides browser visibility, to see fraud activities on the user side?

How are you effectively meeting ECB/EBA/FFIEC recommendation/compliance?

Enterprises

How do you protect internet facing applications or corporate applications which are accessed remotely or via SSL VPN

Secure credentials

Malware detection on unmanaged devices

Phishing detection

Remember that Trojans are sophisticated enough to bypass SSL and two-factor authentication checks

SOLUTIONS FOR AN APPLICATION WORLD