SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Evolution of eBanking frauds

Radovan Gibala

F5 Networks

Agenda

- **Facts & details**
- **Phishing attacks – Easy & common**
- **Malware attacks**
- In the media
- Once upon a time…
- Malware attacks today
- **Mitigation**
- **Summary**
- **Q&A**

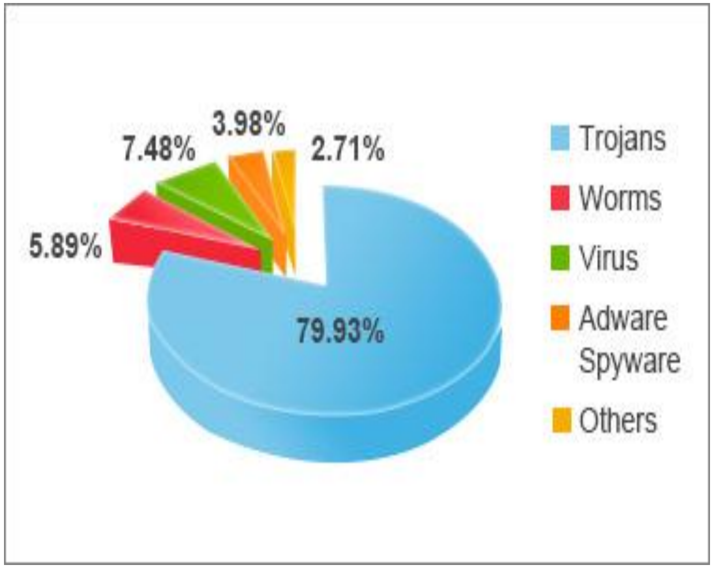
Threats Landscape

Malware Statistics

- "In 2012, more than 40 million Windows systems were infected with malware" – Microsoft (from Five Habits Of Highly Successful Malware: http://www.darkreading.com/advanced-threats/five-habits-of-highly-successful-malware/240154057)
- Researchers found that, of four common antivirus scanners, the best only detected 25% of real-world malware, and combined, the scanners only caught 40 percent of malicious downloads. - Google (from Five Habits Of Highly Successful Malware: http://www.darkreading.com/advanced-threats/five-habits-of-highly-successful-malware/240154057)

Malware attacks are getting more sophisticated and intelligent

- Cross-device and cross-channel attacks.
- Polymorphic signatures continue to leave antiviruses lagging behind. This is the new norm.
- Malware bypassing traditional sandboxing methods by including time delays and activation only after a triggered event.



PandaLabs Q1 Report
http://press.pandasecurity.com/usa/news/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/

Understanding Malware: What exactly is it?

- Malware comes in many forms:
  - Trojans – "A Trojan horse, or Trojan, is a **non-self-replicating type of malware which gains privileged access to the operating system** while appearing to perform a desirable function but instead drops a malicious payload, often including a backdoor allowing unauthorized access to the target's computer."
  - Worms – "A computer worm is a **standalone malware computer program that replicates itself in order to spread to other computers**. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, **it does not need to attach itself to an existing program**. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer."
  - Viruses – "A computer virus is a type of malware that, when executed, **replicates by inserting copies of itself (possibly modified) into other computer programs**, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected"."
  - Spyware / Adware – "Spyware is software that **aids in gathering information about a person or organization without their knowledge and that may send such information to another entity** without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."

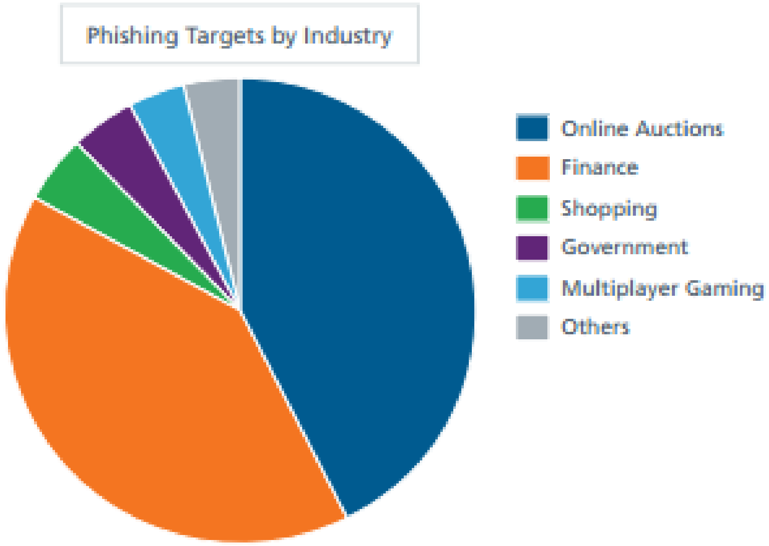
Malware Violates the Principles of:

- Consent: We may not even know it is being installed
- Honesty: We thought it would do one thing, but it actually does something different
- Privacy: PII is captured and shared
- Non-Intrusiveness: Often slows down or crashes system. In general, it interferes.
- Harmlessness: Malware often hurts us financially, socially, etc.

Malware Threat Landscape – Phishing by Number of Attacks

Phishing Attacks by Industry:

- Finance, Government, Shopping, Online Auctions, and Multiplayer Games.



McAfee Threats Report: First Quarter 2013
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf

United States
Amazon
Blizzard Entertainment
eBay
Internal Revenue Service
J.P. Morgan Chase
PayPal
Wells Fargo

United Kingdom
Barclays
HM Revenue & Customs
HSBC
Lloyds TSB
Natwest
Royal Bank of Scotland

Brazil
Banco Bradesco
Banco do Brasil
Banco Itau

Italy
Intesa Sanpaolo
Posteitaliane
UniCredit

Australia
ANZ (Australia and New Zealand Banking Group)
Westpac Bank

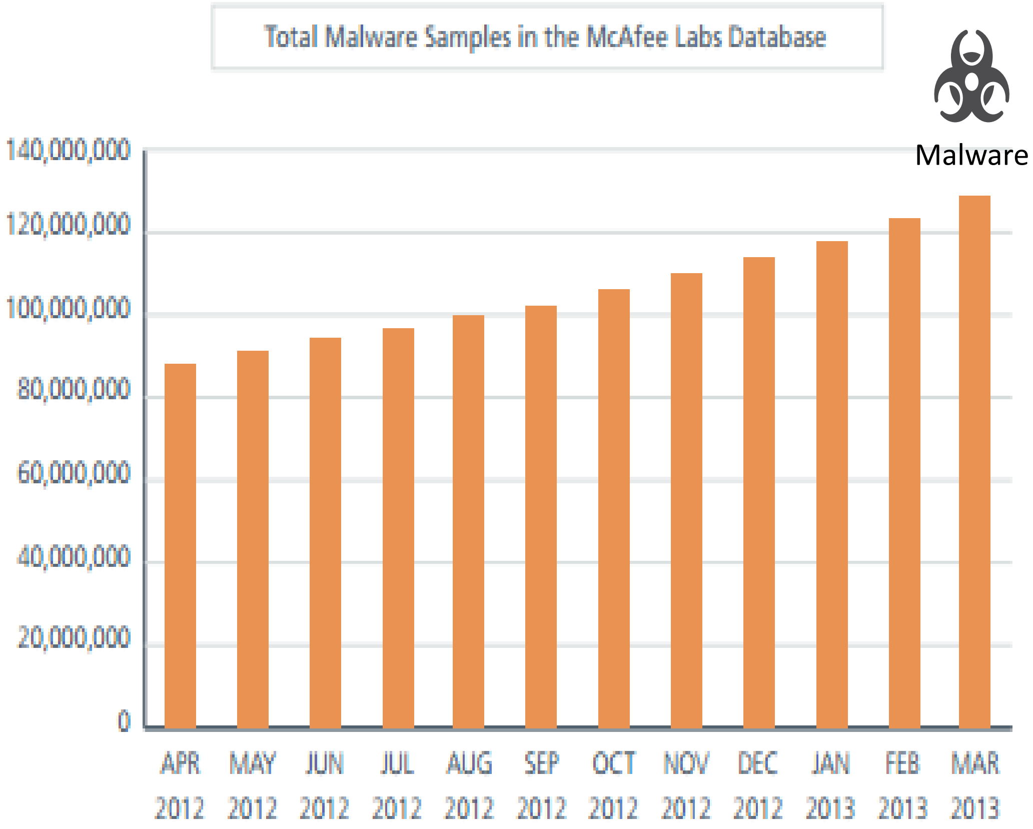
Malware Threat Landscape – Growth and Targets

25 % Of real-world malware is caught by anti-virus

50 % Of malware code is logic to bypass defenses

79 % Existing malware strains are Trojans

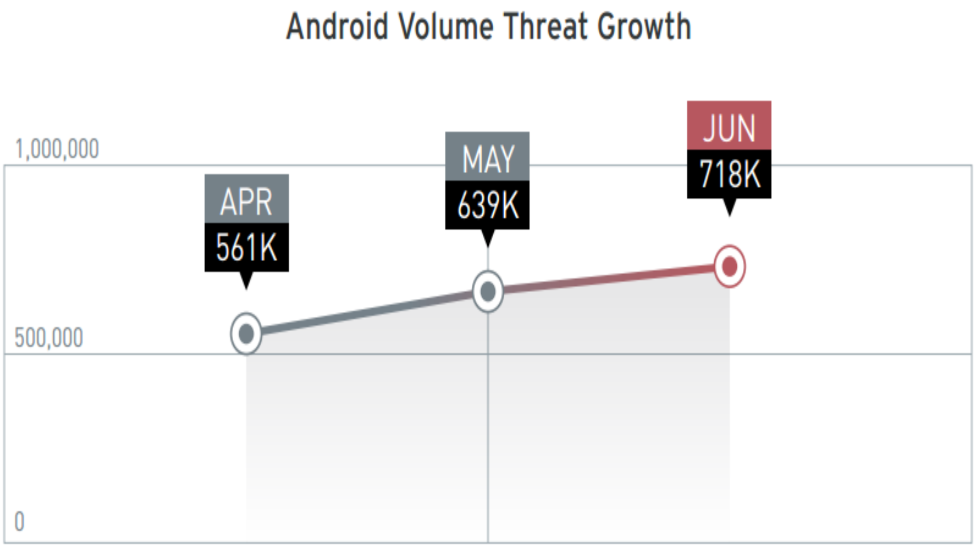
82 % Of Institutions learned about fraud incidents from their customers



Total Malware Samples in the McAfee Labs Database

Mobile Malware

- 99% of newly discovered mobile malware attacks Android devices – Kapersky Security Bulletin 2012 (http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012#1)
- Common Attacks Include:
  - Key Logging
  - SMS Grabbing
  - DNS Hijacking
- Perkele examples:
  - http://krebsonsecurity.com/wp-content/uploads/2013/08/Versafe-SOC-Mobile-attacks-summary-1.pdf
  - http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/



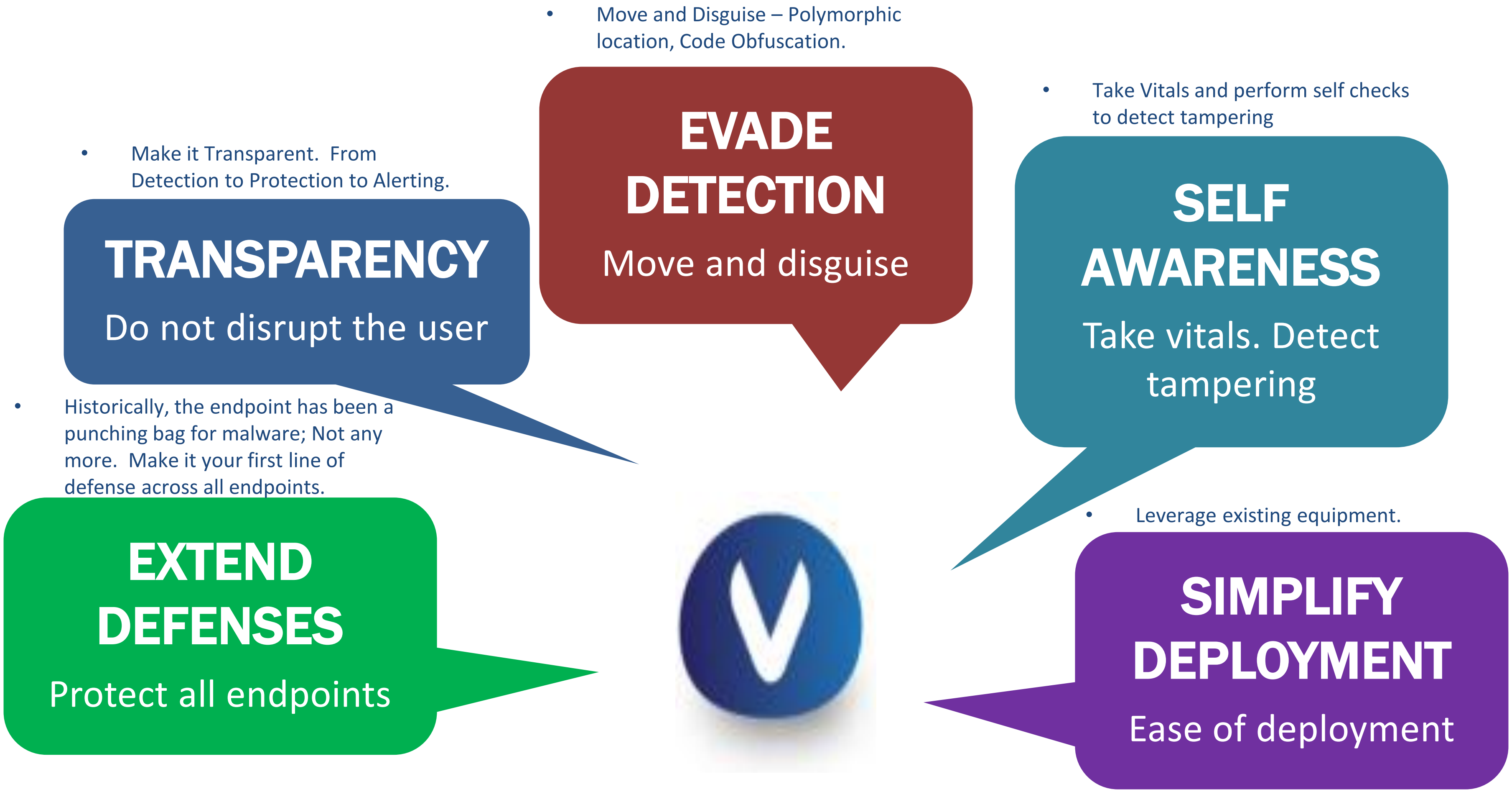
Android malware growth in the first six months of 2013. Source: Trend Micro
http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/

Familiarizing yourself with malware

Read the following:

- OWASP Anti-Malware Knowledge Base
  - Specifically "Appendix B: Banking Malware Families (Active in 2012)"
- Zeus Tracker
  - Specifically the Statistics page
- Threat Modeling of Banking Malware
  - Overview from 2011 of banking malware threats
  - Review slides 32-53 only.

Approach



- Make it Transparent. From Detection to Protection to Alerting.

TRANSPARENCY

Do not disrupt the user

- Move and Disguise – Polymorphic location, Code Obfuscation.

EVADE DETECTION

Move and disguise

- Take Vitals and perform self checks to detect tampering

SELF AWARENESS

Take vitals. Detect tampering

- Historically, the endpoint has been a punching bag for malware; Not any more. Make it your first line of defense across all endpoints.

EXTEND DEFENSES

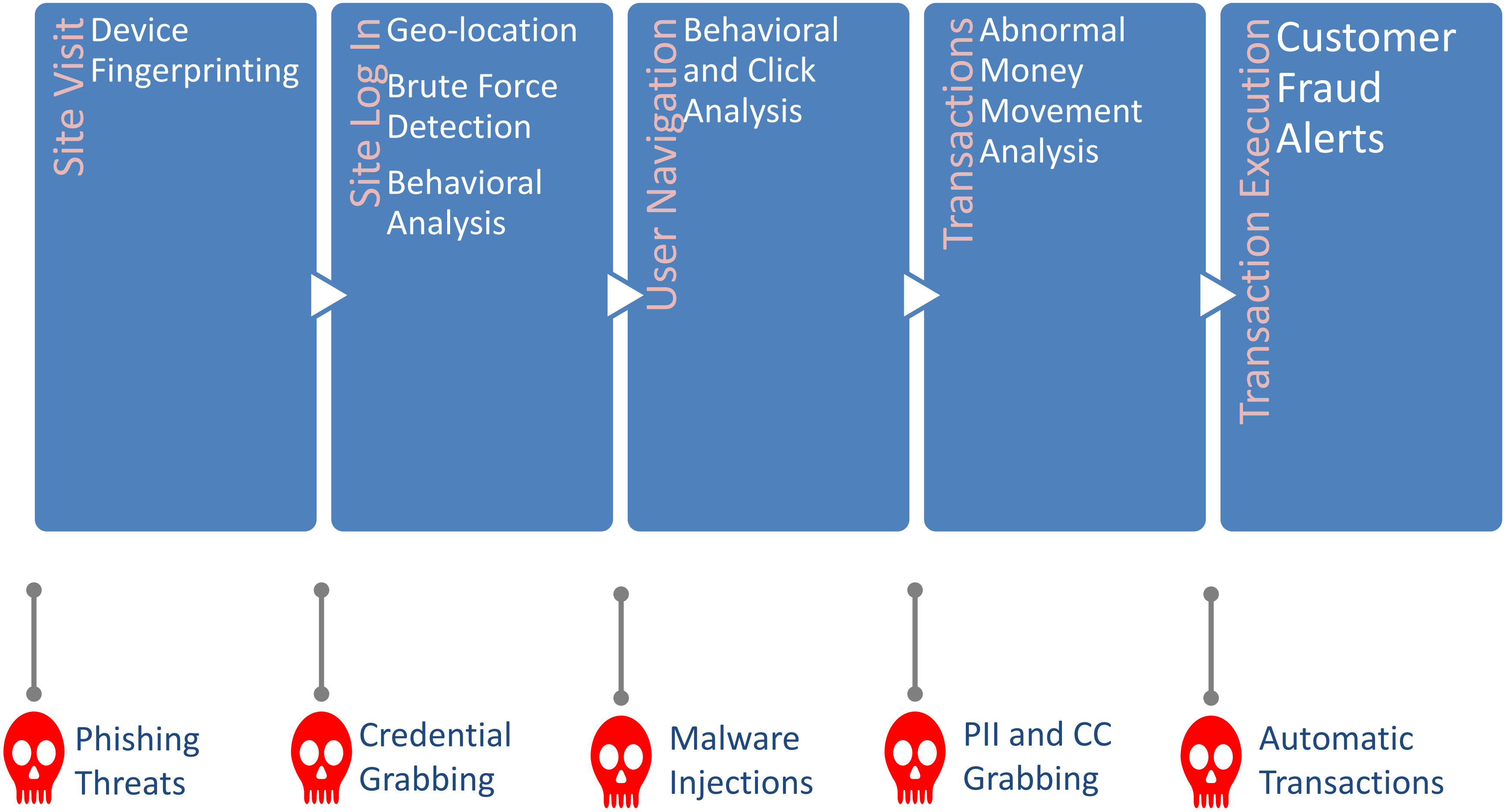
Protect all endpoints

- Leverage existing equipment.

SIMPLIFY DEPLOYMENT

Ease of deployment

What Do Our Customers Need ?



Site Visit
- Device Fingerprinting

Site Log In
- Geo-location
- Brute Force Detection
- Behavioral Analysis

User Navigation
- Behavioral and Click Analysis

Transactions
- Abnormal Money Movement Analysis

Transaction Execution
- Customer Fraud Alerts

Phishing Threats

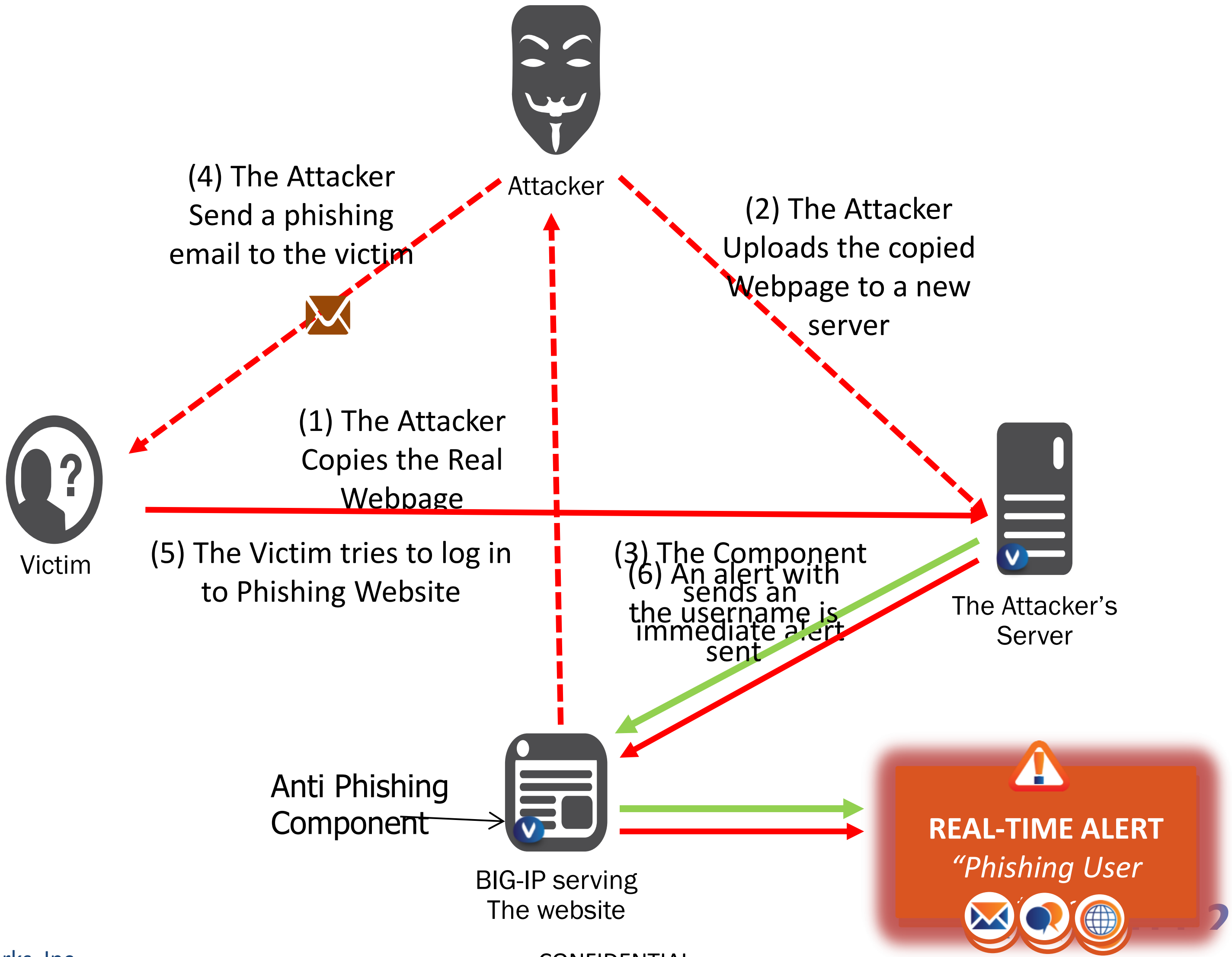
Credential Grabbing

Malware Injections

PII and CC Grabbing

Automatic Transactions

Phishing Detection – How does it work?



Attacker

(4) The Attacker Send a phishing email to the victim

(2) The Attacker Uploads the copied Webpage to a new server

Victim

(1) The Attacker Copies the Real Webpage

The Attacker's Server

(5) The Victim tries to log in to Phishing Website

(3) The Component sends an immediate alert

(6) An alert with the username is sent

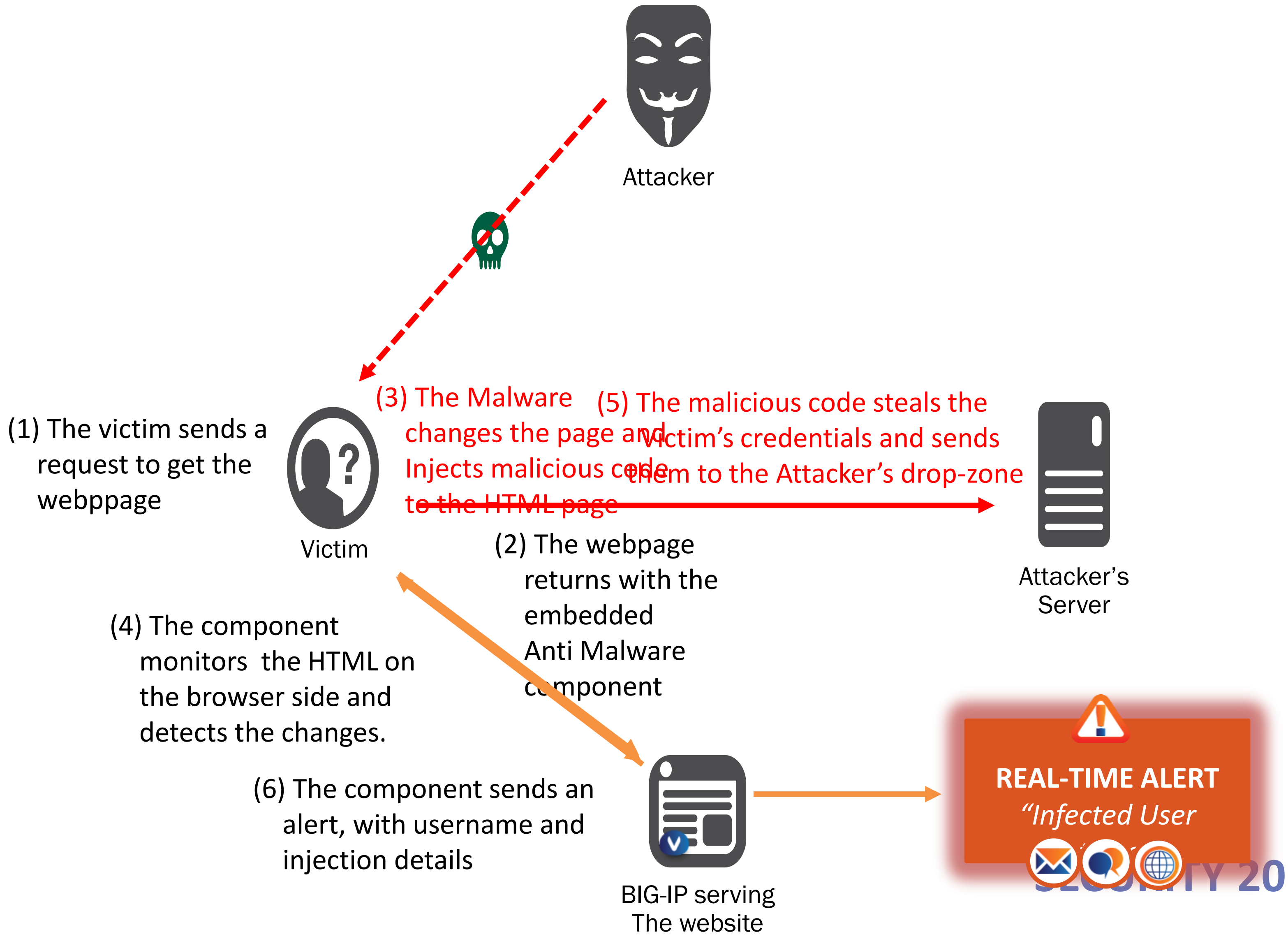
Anti Phishing Component

BIG-IP serving The website

REAL-TIME ALERT

"Phishing User

Malware Detection – How does it work?



(1) The victim sends a request to get the webppage

(2) The webpage returns with the embedded Anti Malware component

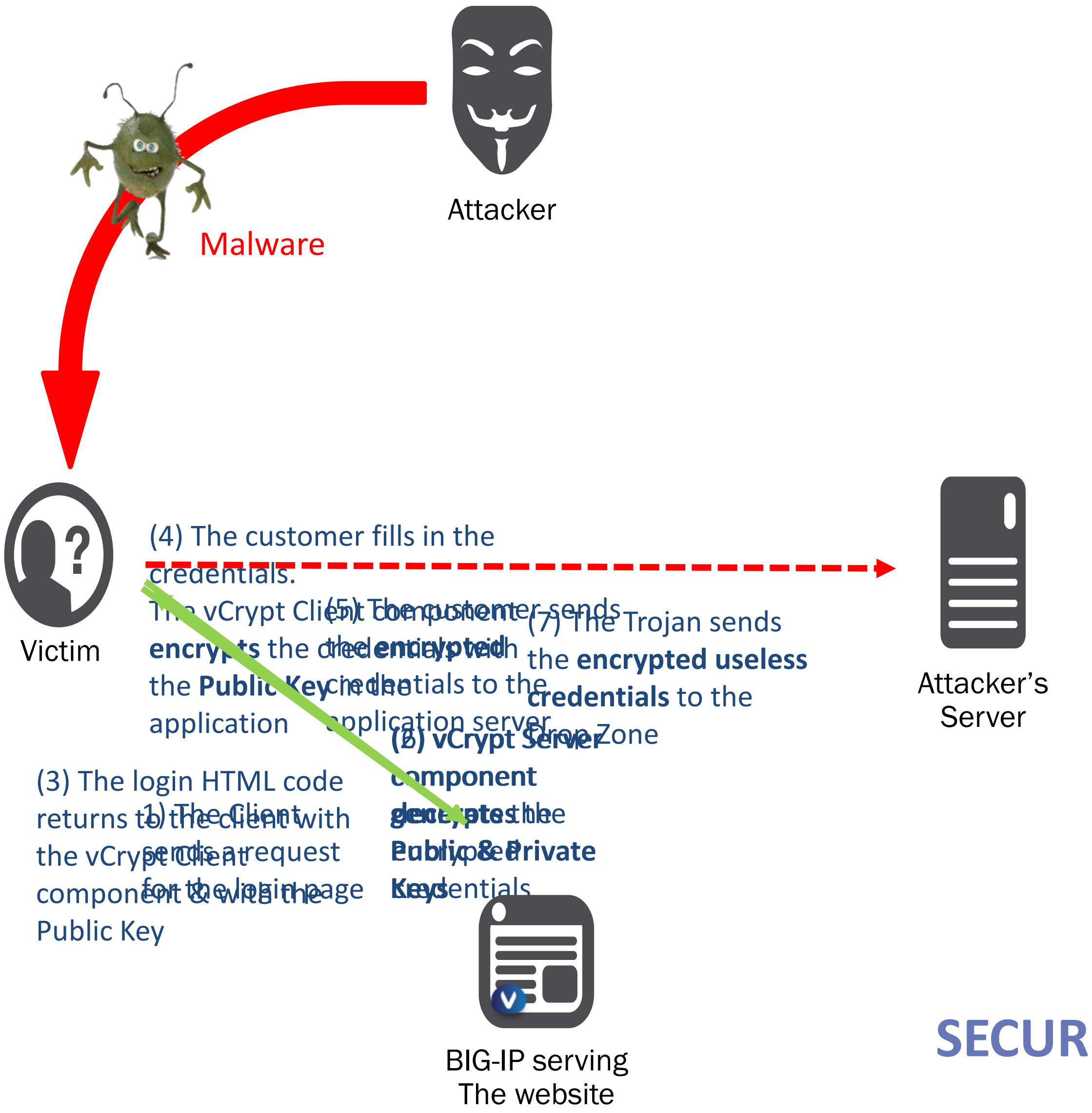
(3) The Malware changes the page and Injects malicious code to the HTML page

(4) The component monitors the HTML on the browser side and detects the changes.

(5) The malicious code steals the victim’s credentials and sends them to the Attacker’s drop-zone

(6) The component sends an alert, with username and injection details

Application Layer Encryption



(4) The customer fills in the credentials. The vCrypt Client component **encrypts** the credentials with the **Public Key** in the application

(5) The customer sends the **encrypted** credentials to the application server

(7) The Trojan sends the **encrypted useless credentials** to the Drop Zone

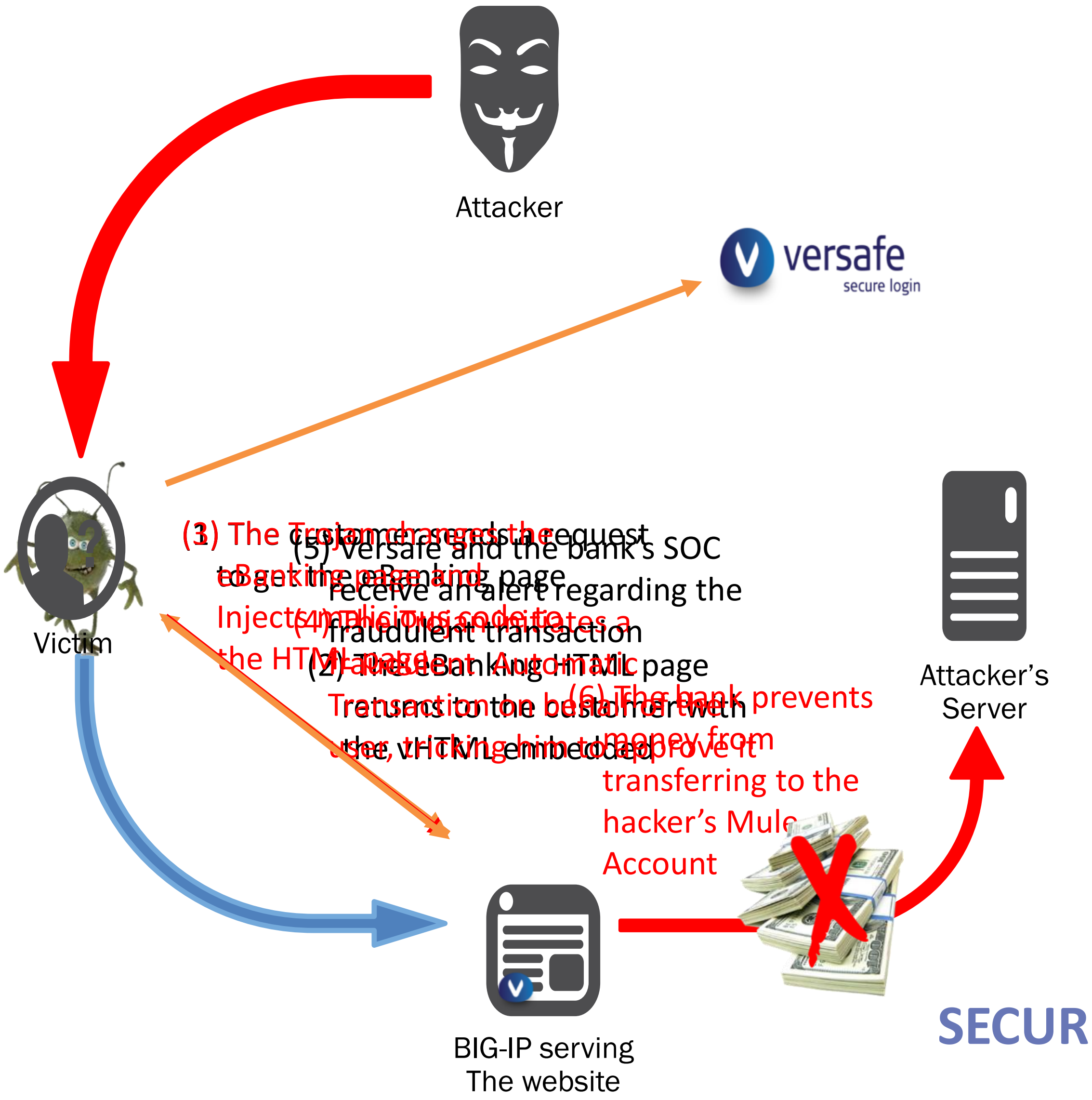
(2) vCrypt Server component generates the **Public & Private Keys**

(6) vCrypt Server component decrypts the credentials

(3) The login HTML code returns to the client with the vCrypt Client component & with the Public Key

1) The Client sends a request for the login page

Transaction Integrity – How does it work?



(1) customer sends a request to get the eBanking page

(2) The eBanking HTML page returns to the customer with the vHTML embedded

(3) The Trojan changes the eBanking page and Injects malicious code to the HTML page

(4) The Trojan initiates a Fraudulent Automatic Transaction on behalf of the user, tricking him to approve it

(5) Versafe and the bank's SOC receive an alert regarding the fraudulent transaction

(6) The bank prevents money from transferring to the hacker's Mule Account

SOC Overview

- What does the SOC do?
  - Malware Investigation / Threat Analysis
  - Review and handling of real-time alerts
  - Dropzone / C&C analysis
  - Incident Report write-ups
  - Takedown services
  - Component QA checks
  - Support (will likely transition to F5 support post integration)

"With the Versafe solution, the results were immediate. Soon after deployment, we mitigated a malware-infected device attempting to conduct a fraudulent transaction.”

Děkujeme za pozornost.

Radovan Gibala
F5 Networks
r.gibala@f5.com