Automating Online Banking Fraud via Automatic Transfer Systems

What is an ATS?

An automatic transfer system (ATS) is often an unknown part of the *WebInject* files that ZeuS or SpyEye malware variants commonly use. ATS code is often incorporated into simple or very complex JavaScript code embedded in *WebInject* files.

How does an ATS differ from a *WebInject* file?

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. ATSs are often just parts of *WebInject* files. These are, however, more damaging in that they no longer require user intervention via inputting information into pop-ups to steal money from victims' bank accounts, for instance.

Why should users take time out to know what ATSs are?

Various active ATSs currently found in the wild are being used by cybercriminals to conduct automated online financial fraud. They steal money from victims' bank accounts every time users log in or conduct transactions online. They do this without having to ask victims to key in personal credentials that banks require to approve transactions like bank transfers. We have seen evidence of ATSs that break two-factor authentication security methods as well.

How do cybercriminals make money out of ATSs?

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 Trend Micro 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.

What can users do to protect themselves from ATS attacks?

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).

What can banks and other financial institutions do to protect their customers from ATS attacks?

Financial institutions should review the research paper and analyze the attack method to determine if their existing security practices can protect their customers from this threat.