

JANUS versus ZEUS

Clash of the Titans in the Digital Age

Shane Lett
FrontOne Limited
shane.lett@frontone.com

Overview:

This paper has been written to give the reader a high level overview of the functionality of the JANUS product suite including 3AKEY developed by FrontOne Internet Security, using the well known Zeus Trojan as a reference case.

© FrontOne Limited. 2007-2010.

Important Notice: This document is provided for private viewing only. It is not intended for reproduction or public distribution. For permission to publish or electronic distribution of this article, please contact FrontOne Limited. Email: info@FrontOne.com

Contents

Clash of the Titans in the Digital Age	1
Overview:	1
JANUS versus ZEUS	1
Introduction: Comparison to Greek Mythology	3
Overview of the Zeus Trojan	3
Distribution	3
Availability.....	3
How does Zeus work?	4
Man In the Browser Attack by Zeus	4
Identity Theft Attack	4
Scenario: Identity Theft attack via Zeus	4
What if the bank uses "strong" two factor authentication?	5
Next steps, covering his tracks	5
The JANUS Data Sentry Solution	5
3AKEY - JANUS is Granted a Sword!	6
What is 3AKEY?.....	7
What if 3AKEY is Stolen?	7
Transactions under duress	7
Protection from Targeted Attacks.....	8
Protection from the Zeus VNC Module.....	8
Introducing 3AKEY+	8
Conclusion	9
About FrontOne	10
Acknowledgements.....	10
About the Author	10
References.....	10

Introduction: Comparison to Greek Mythology

ZEUS: Possibly the best known of all the Greek gods, Zeus has been popularised in everything from action comics and video games through to new release movies. Originally known as the "God of War" Zeus has widely been considered as the most powerful of all the Greek gods of ancient mythology.

JANUS: A somewhat more obscure character appeared in Greek mythology as Janus, the "God of Gates and Keys". At first glance it would seem Janus could be no match for a god of war such as Zeus, however according to ancient belief, only Janus as the gate keeper has the ability to protect other gods and mortals alike in times of war and distress, by offering a safe haven and other necessities. Even Zeus had to go to Janus for the keys to leave the spirit realm and enter the world of men.

Overview of the Zeus Trojan

Appropriately named, the Zeus Trojan (also known as WSNPOEM, Gohax, Zbot, Kneber and others) has proven itself indeed as a "God of War" in its persistent and successful attacks against corporate and private personal computers and perhaps more notably, banking and financial organisations.

Although Zeus is by no means a new phenomenon in the dark world of Malware, it has been continuously updated, modified and improved since its first discovery in 2008 and it is still one of the most widely used Trojans in successful attacks against financial organisations and their customers. This is evidenced by its distribution, with some estimates stating that 160,000,000 PC's may be infected in the US alone. Due to secrecy in the banking sector, statistics are scarce regarding actual financial losses but it could safely be assumed, based on the infection rates, that losses attributed to Zeus likely number into the hundreds of millions of dollars worldwide.

Distribution

Zeus is spread in a number of ways but mainly by downloads from poisoned websites and Phishing schemes commonly using emails with links or attachments that contain the Zeus Trojan executable. These distribution techniques are covered in greater detail, later in this document.

Availability

The Zeus tool-kit can be found online using an internet search and subsequently purchased and downloaded for as little as £700 for the most basic version while the full list of features will set the purchaser back up to £12,000.

Hackers boldly offer additional add-ons that provide more advanced functionality and even offer pre-made configuration files (which are usually encrypted) for targeting specific online banking sites. Some hacking communities offer technical support and interestingly the Zeus

tool-kit includes copy protection similar to that used by mainstream products such as Microsoft Office, i.e. computer profile footprint and security keys.

How does Zeus work?

The attacker purchases and installs the Zeus toolkit on their computer in the same way as a typical software package would be installed. They then use the tool kit to generate a Zeus Trojan that is uploaded to an innocent website or a phony website setup by the attacker or rented from other hackers. This is often referred to as bullet proof hosting. Alternatively the executable is sent out as an email attachment, imbedded in a PDF file, or via a link to direct an unsuspecting user to install an innocuous file that actually contains the Zeus Trojan. Once a user runs and installs the Trojan from any source, the attacker receives a notification that a computer has been successfully infected (referred to by hackers as "owned"). Now, for the hacker, the fun starts. For the poor computer user, this is their worst nightmare.

Leveraging the Zeus tool kit, the criminal has a range of attack options at their disposal. We will discuss two of the most commonly used attacks to demonstrate the JANUS solution; Man In The Browser (MitB) Attack and Identity Theft Attack.

Man In the Browser Attack by Zeus

MitB attacks by Zeus may take several forms and MitB attacks are often defined differently by various parties. Some independent definitions for your consideration can be found in the references section of this paper, [\[1\]](#) however regardless of the exact definition, most experts agree that the only way to mitigate MitB attack is by including Transaction Verification in the overall security strategy.

Identity Theft Attack

Identity Theft may be better named "credential theft" as a person's true identity is probably the one thing that can never be stolen. However in an Identity Theft attack, the criminal has gathered enough information about the customer that they can successfully impersonate them to the banking system, such that they can illegally withdraw money from the customers account. The Zeus Trojan provides ample ammunition to conduct Identity Theft attacks by gathering information about the user from the PC itself, for example from saved internet files and by extracting OTP/Passcode/Password information from the user using web injection techniques to create false web pages or by adding additional web fields.

To help explain this, please consider the following imaginary scenario:

Scenario: Identity Theft attack via Zeus

A user is surfing the net looking for some free software. They come across a website featuring a product and proceed to download it. Little do they know that the download contains a "piggy back" file, the Zeus Trojan. The user runs the download and inadvertently installs the Trojan also. The only noticeable change to the user is that now their Windows Firewall appears as disabled (assuming it was previously running) but the user is not concerned and assumes it will come right when they next reboot. The hacker is now notified

via their Zeus toolkit that they have another infected computer at their disposal. Using the search capabilities of the Zeus toolkit they run a search for familiar files (such as history and cookies) on the user's computer to indicate which websites they frequently visit. After discovering the user regularly accesses EXAMPLEBANK.COM the attacker updates the Zeus Configuration file to look for this URL*. When the user next accesses this URL their User ID and password are captured by the Zeus key logger and sent back to the attacker, who then accesses the online bank and steals the money, normally doing so via an unsuspecting intermediary known as a "money mule".

*Alternatively in some cases this step is bypassed altogether by pre-configuring a long list of target websites in the Configuration file, the browser event may trigger a Zeus attack based on any matching URL.

What if the bank uses "strong" two factor authentication?

In an attempt to stop Trojans, many banks now deploy two factor authentication solutions, however this presents no problem to the Zeus Trojan. If the bank uses a two factor authentication solution such as a CAP reader or OTP/Passcode/Password generator token etc, the hacker can use a screen injection technique to harvest the second factor PIN or Pass code. Using the Zeus tool-kit they inject an additional field into the online banking page asking the user to input their two factor OTP/Passcode/Password. Because this bogus field makes up part of the legitimate page displayed to the user it appears valid (SSL Certificates and the "green browser bar" function as normal) and the user inputs their OTP "as usual". This is sent to the hacker using an IM client (typically Jabber) along with the other credentials and they now have all the information they need to transfer funds from the customer's account. Even if the OTP/Passcode/password contains a timeout, because the credentials are received in real time by the hacker he will typically have plenty of time to transfer the money before signing out of the system in the usual way.

Some banks have now progressed to using a MAC (Hash) generated from the CAP device, based on the transaction details to secure the transaction (transaction signing). This is a step in the right direction however it seems likely that emerging Zeus attacks could circumvent this using screen injection and Social Engineering, much as they currently do to capture the OTP/Passcode/Password.

Next steps, covering his tracks

Now that the hacker has stolen all the available funds from the user he can cover his tracks by destroying the PC. Using the "kill" or "KOS" (Kill Operating System) function built into the Zeus Trojan, the hacker runs a script that deletes important Operating System files making the computer unusable.

The JANUS Data Sentry Solution

JANUS Data Sentry is a world first, fully automated Message Verification Technology that is designed to ensure the integrity of the user's transaction from start to finish, offered in a unique Zero Footprint and Zero Knowledge solution: **i.e. no software needs to be installed**

on the end user's computer, and no personal or transactional information is stored anywhere on JANUS systems.

In a nutshell, a MitB attack may use the victim's own computer and hijack the real-time online banking session to steal money. These types of attacks are favourable to hackers because they do not need to interact directly with the remote computer, thereby helping to evade detection.* These types of MitB attacks can also be highly automated, meaning a potentially greater payout for less work. These attacks typically change fields within the legitimate session, such as the account number and transaction amount in real-time, during an internet payment or transfer. This type of exploit was perhaps first noticed on a large scale with the discovery of the "Silent Banker" Trojan in 2008 and is now available as a subset of the functionality offered by many Trojans including Zeus.

**Hackers often use a "Command and Control" server to act as a proxy between the hacker and the infected PC to protect the hacker from detection.*

JANUS Data Sentry is an effective defence against these types of automated MitB attacks. Any attempt to change the real-time information in the session will nullify the transaction by means of JANUS' patented Transaction Verification technology. In addition, an attempt to change the protected web page results in an alert to the JANUS system that can be reviewed by the Security Administrator, providing valuable information regarding Trojan attacks against the organisation. In brief, the core functionality of JANUS Data Sentry that mitigates MitB attack can be summarised as follows:

- JANUS deploys a dynamically configured client side script that is loaded with the web page, to monitor the user input throughout the entire transaction;
- Each client side script completes a data round trip originating from the JANUS server. It will send a message back to JANUS every time a user input is completed, independent of standard HTML post action (note that Trojans such as Zeus are activated upon form submit).

With a real-time Man-In-The-Middle or Man-In-The-Browser attack, the attacker modifies the data in the current transaction or initiates a new transaction after the user authentication is completed.

JANUS provides essential tools to enable Service providers to authenticate the data received from a users' browser with the JANUS server. The Server Side script is synchronized with the client side script within the same session, thus producing the same hash. If any data has been tampered with, the hash produced at the JANUS Server will be different from the one the client side script has produced earlier. - *For more detailed information on JANUS concepts, including the secure mechanism of hash creation and delivery, please see the document "JANUS Application Guide" for further information.*

3AKEY - JANUS is Granted a Sword!

In Greek Mythology, going up against Zeus without a powerful weapon is a bold call. He is, after all, the God of War! To this end, although JANUS can be deployed alongside a customer's existing authentication solution, to fully defend against the full arsenal available to

a criminal armed with the Zeus tool-kit, we need to arm JANUS with a weapon of his own. This can be done by combining JANUS Data Sentry with FrontOne's 3AKEY solution - JANUS' "Sword!"

What is 3AKEY?

3AKEY is a strong multi factor authentication solution. It is a personal authentication server, using distributed authentication technology where the user ID and password are submitted to the 3AKey for verification. 3AKEY authenticates all incoming requests for information before a dynamic digital credential is produced in return. This of course differs from most solutions that transmit the user credentials to a central server for verification, a flawed strategy that is vulnerable to interception and attack.

Also, unlike typical two factor authentication solutions which use a OTP/Passcode which can be harvested and reused easily by Zeus with its built in capabilities (for example screen or field injection techniques as discussed earlier), the 3AKEY solution requires the user to physically have the 3AKEY in their possession and connected to their registered computer in order to complete the online banking transaction or e-payment. This means that even if a hacker is able to successfully extract a portion of the user's credentials by any means; they will not be able to steal any money as they do not hold the 3AKEY. It is that simple!

3AKEY literally becomes the key to your online security, much in the way you would use a key to secure and enter your home.

What if 3AKEY is Stolen?

Because 3AKEY must be registered to the computer before it can be used (it is linked to the computer using the user's logged in account profile), theft of a 3AKEY would not benefit the attacker unless they also steal the registered computer and know the User ID and password.*

In addition, if a 3AKEY is reported stolen, an instruction can be sent to disable the key automatically when it next attempts to connect to an online system.

*Note registration to multiple computers is supported (at the Financial Organisation's discretion).

Transactions under duress

Imagine an unscrupulous criminal follows the victim home and forces them to log in and transfer funds to another account - a terrible but possible scenario. For the customer's safety, 3AKEY includes a sophisticated anti-duress function. Essentially this works by allowing the user to input their User ID as normal but to add a suffix to their usual password. The 3AKEY server understands the user has logged in under duress and alerts the Security Administrator; however the transaction appears to proceed correctly thus helping to protect the user's safety.

The user need only recall part of their prefix or anything similar as the intelligent factors included in the 3AKEY solution understand the theme of the anti-duress code rather than just a specific phrase or password combination which may be difficult to remember under such circumstances.

It must be acknowledged that these kinds of attacks are rare however sadly they have occurred, sometimes with tragic results. [2] FrontOne believes that personal safety must be treated with utmost concern and always considered in any Security Solution. For this reason much effort has been expended to include the most sophisticated anti-duress functionality available in our 3AKEY solution which we invite you to investigate further for your safety and that of your customers.

Protection from Targeted Attacks

Protection from the Zeus VNC Module

Recently an additional VNC (Virtual Network Computing) module has been made available for purchase as an add-on to the Zeus tool-kit. This module enables the attacker to remote control the customer's computer without their knowledge, thus acting as if they are the legitimate user sitting at their own PC. Such an exploit can bypass even hardware based security devices such as smart cards, which are typically deployed to customers who regularly complete high value transactions and we acknowledge that this type of committed and highly targeted attack could be successful if performed while our first generation 3AKEY is attached to the user's computer.

To return to our earlier analogy, this could be likened to somebody robbing your house while your key is in the door.

To mitigate this exploit, our second generation 3AKEY has incorporated a new user control feature.

Introducing 3AKEY+

To provide an even greater degree of security against highly targeted attacks such as those using the Zeus VNC Module, FrontOne also offer an even more advanced authentication solution, "3AKEY+".

3AKEY+ builds on the same Strong Authentication functionality as 3AKEY but adds protection from highly targeted attacks such as the VNC module, by incorporating the new **User Control** and **Trusted Display** features.

User Control and **Trusted Display** are features unique to 3AKEY+ that provide the functionality for the user to approve their transaction using a simple button located on the 3AKEY+ device. Because this action needs to be conducted manually by the user, it is impossible for a Trojan or even an attacker connected by a Remote Control session to complete this task.

For example, before proceeding with an account transfer, the Account Number is shown to the customer on the 3AKEY+ **Trusted Display** screen. The user checks it is accurate and then accepts by clicking the **User Control** button. The **Trusted Display** then displays the amount, which is in turn accepted and the transaction, now verified by the customer is

approved and processed. **User Control** is a two step process, press once for acknowledgement and again for confirmation. This is to prevent accidental acceptance of any transaction.

Because 3AKEY+ is linked to the transaction fields, any attempt to change the transaction information is clearly visible to the user.

3AKEY+ provides an unparalleled measure of control to the customer in an easy to use, cost effective and familiar form factor and an unrivalled level of protection to the Financial Organisation to defeat Phishing, Man in the Browser and Trojan attacks. Even highly targeted attacks using Remote Control Tools are defeated because the attacker is unable to process the fraudulent transaction without physical access to the 3AKEY+ device.

Due to the simplicity of the one button solution, high volume transactions are more easily supported where a CAP reader or token based solution may be cumbersome.

An alternative but functionally matched device meeting DDA recommendations will also be available for disabled customers.

Conclusion

Clearly Zeus has proved a formidable adversary for financial organisations and their customers. Equipped with the "King of Trojan Tool-kits" hackers have used Zeus to strike fear into even some of the most secure Financial Organisations - until now! Protected by JANUS and armed with 3AKEY or 3AKEY+ your organisation can take a stand against Trojans.

- **JANUS Data Sentry** - World first "Zero Footprint" / "Zero Knowledge" intelligent Transaction Verification;
- **3AKEY** - Strong Mutual Authentication;
- **3AKEY+** - Strong Mutual Authentication plus User Control and user input verification;
- **3ACARD** (coming soon!) - The features of 3AKey+ with an integrated keypad for data entry and a battery for standalone operation; 3ACard provides mutual authentication and transaction signing in both connected and disconnected applications. 3ACard is designed to cater for organisations that have the need for multi-channel support (internet, telephone and mobile banking etc) using a single security device.

About FrontOne

Although FrontOne or its representatives have been working in the security field now for many years, we are certainly the "new kid on the block" compared to the industry giants that are entrenched in the security market. We don't pretend to compete on quantity of customers or even product placement. Our approach is to listen to our customers needs and deliver using innovative solutions that work, even if this means a paradigm shift away from traditional thinking. We have developed our products to offer future proof solutions rather than stop gap measures.

We welcome your own testing of our products and your comments on this paper. Please feel free to contact the author: shane.lett@frontone.com

Contents accurate at the time of writing, details subject to change.
Information in this paper may be based on opinion.

Acknowledgements

This work would not have been possible without the help from all the team at FrontOne. We also wish to thank the anonymous reviewers.

About the Author

Shane has more than 10 years experience in the IT Industry consulting to some of the UK's largest Media Organisations, Telco's and Banks. Shane has a background in Infrastructure Security, Technical and Solutions Architecture, Server Based Computing and Virtualisation.

Shane currently works at FrontOne Limited as the Chief Technology Officer.

References

[http://en.wikipedia.org/wiki/Zeus_\(trojan_horse\)](http://en.wikipedia.org/wiki/Zeus_(trojan_horse))

http://www.owasp.org/index.php/Man-in-the-browser_attack

http://en.wikipedia.org/wiki/Man_in_the_Browser

<http://www.secureworks.com/research/threats/zeus>

<http://www.guardian.co.uk/uk/2008/jul/05/knifecrime.ukcrime>

http://news.cnet.com/2010-1071_3-5669408.html

<http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>