wontok™ SafeCentral SafeDesktop

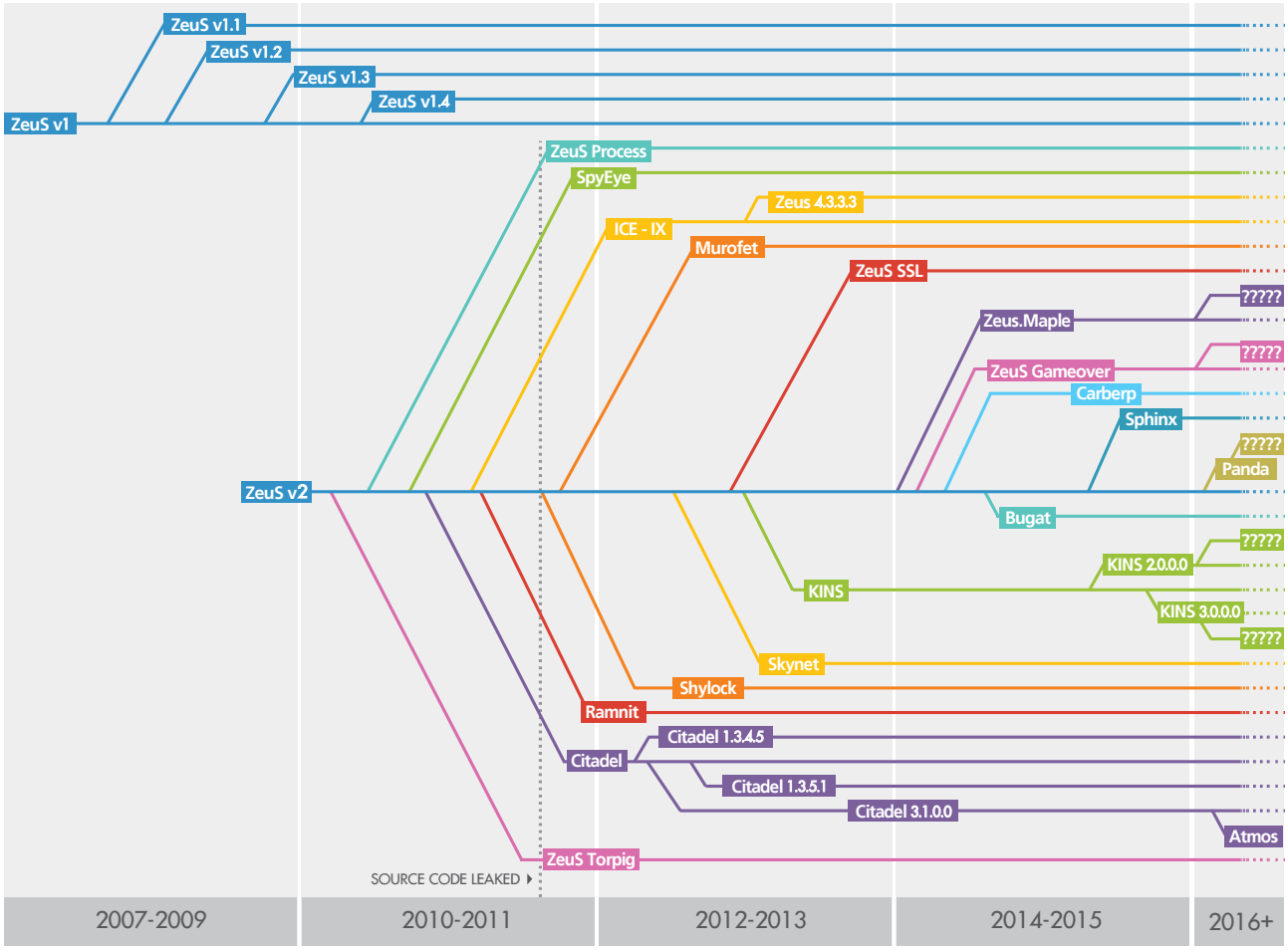
The Evolution of Financial Malware
2007-2016

Overview

The vanguard of botnet malware, and source of constant botnet innovations, has always been financial malware.

In 2007, the arrival of Zeus heralded a breakthrough for fraudsters. The trojan's ability to bypass multifactor authentication allowed criminals to hijack a fully authenticated session and then divert funds from compromised accounts. Originally these funds were sent to money mules, but in late 2013 these funds were instead diverted to compromised prepaid debit cards for immediate liquidity and higher losses by banks.

The Zeus Timeline



Zeus is a highly polymorphic malware kit capable of avoiding detection by advanced antivirus suites. Zeus and many other financial botnets are resident in the browser, and able to manipulate the HTML display of the client. They are also immune to Secure Sockets Layer (SSL) chain complexities as they work post-SSL decryption. Many of the most successful financial trojans are man-in-the-browser (MitB) technologies. MitB attacks infect web browsers, allowing malware to modify web pages and transaction content in a completely covert fashion.

Depending on how the web page modifications are carried out, the bank site may not see suspicious activity or artifacts, such as inappropriate cookies, sent back to their web server, which, if caught, would alert the bank to a modification of the HTML code.

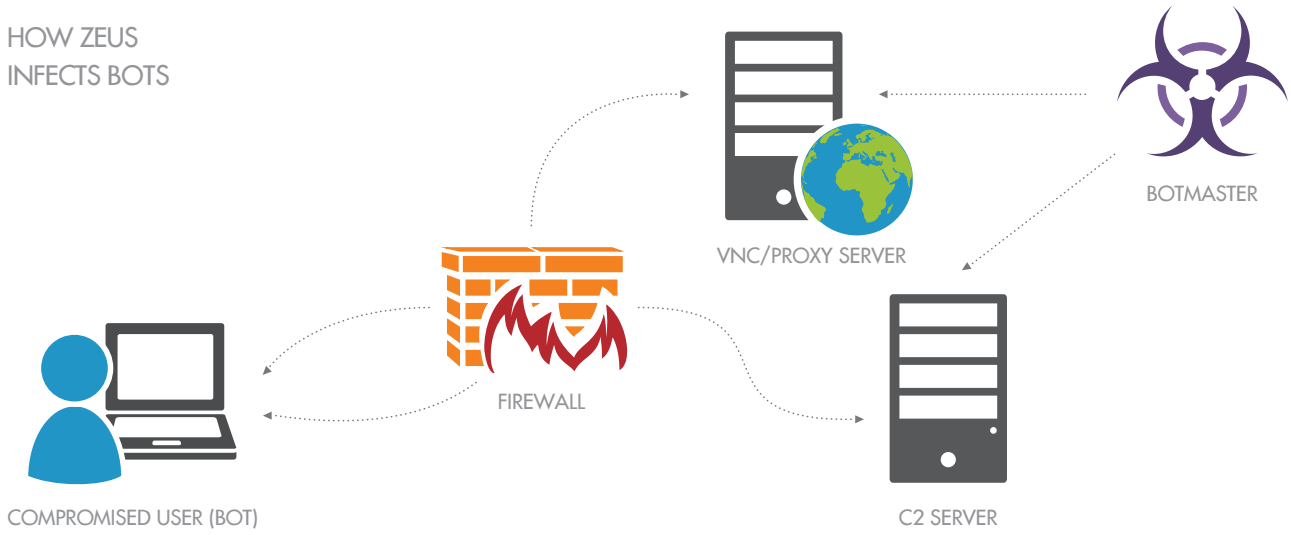
Zeus and its progeny are the primary MitB fraud tool. Currently installed on millions of PCs (now classed as "bots" themselves), Zeus has a huge following in the criminal underground. Zeus took over from a generation of primarily keylogger bank malware and provided a robust framework to which advanced functionality could be added. Zeus has since undergone many evolutions and is used as the template for other MitB.

IN 2015 ZEUS (OR ITS DERIVATIVE, CITADEL) WAS ASSOCIATED WITH UP TO 88% OF FINANCIAL MALWARE ATTACKS ON BANKS

Zeus' advanced capabilities have been used for purposes other than financial fraud, including distributed denial of service (DDoS) campaigns, spamming, and advanced data theft. *In 2015, Zeus (or its derivative, Citadel) was associated with up to 88% of financial malware attacks on banks,* while Dridex (a competing financial malware) was responsible for approximately 5% of bank attacks.

Understanding how to defeat modern financial botnets requires a thorough understanding of Zeus. This trojan is a multicomponent system comprising bots and command and control servers, and may contain backconnect proxies for Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC).

Simplified Zeus structure



Infected bots bypass firewall security by opening outgoing connections to the C2 server and the VNC/Proxy Server (backconnect). The botmaster interacts with these servers to control bot endpoints.

Zeus commonly infects users while they surf the internet or when they click a link in a malicious email. Zeus does not require the user to have administrator access in order to infect the machine. The key functions of the Zeus bot are to:

+ Compromise the PC
+ Keylog all activity unless instructed otherwise
+ Activate whenever visiting a site on the "site of interest" list (i.e., targeted banks)
+ Implement Webinjects (which manipulate the HTML on the page displayed to the user)
+ Communicate with the command and control (C2) server as required, sending logs and receiving updates

The key functions of the C2 server are to:

+ Act as the key administration panel for the botmaster
+ Update bots as required
+ Act as the central repository for all log data received from bots
+ Create and execute scripts targeted on bots
+ Provide management reports

Zeus Capabilities

Zeus has powerful keylogging abilities.

Anything typed on a Zeus-infected device is keylogged by default and is regularly uploaded to a C2 server. High-risk bank accounts, such as commercial accounts, generally use multifactor authentication for better protection. Even multifactor authentication, however, is compromised by the MitB features of Zeus. Webinjects are highly customizable JavaScript pop-ups purporting to be two-way communications with the bank that take the form of a request for additional authentication of a customer's identity. Zeus automatically copies digital certificates and can readily overcome this method of authentication.

Citadel

Citadel is a recent incarnation of Zeus, first appearing in February 2012. The owners of Citadel are actively building on to the source code of leaked Zeus (2.0.8.9) and adding new functionality.

2015 has been a banner year for cybercriminals. Their tools have greatly evolved, and new advanced malware suites are available. Hesperbot, Shylock, Beta Bot, KINS and Carberp are now being used against banks, and this trend shows no sign of abatement. Citadel's successor, Atmos, emerged in the first half of 2016.

> To learn more, read **"Financial Institutions: How to Protect Customers from Advanced Malware in 2016"**.

About Wontok

Founded in 2005 and headquartered in Sydney, Wontok has operations in Australia, Asia and the United States. Wontok has a team of security industry veterans with a proven history of bringing to market value-added security services that fill the gaps left in traditional security solutions. Wontok crafts scalable services delivery platforms and security solutions to be robust and easily deployable to keep up with the demands of business continuity. With ever shrinking margins, Wontok ensures ARPU is maintained through continually evolving value-added services.

Wontok is partner-focused and supports branded or white-label delivery of its world-class security solutions and its value-added services delivery platform. Whether you are a communications service provider, systems integrator, value added distributors, resellers, portal owners, financial institutions or enterprise; visit www.wontok.com for more information today.

Contact Information

San Francisco – USA
americas@wontok.com
+ 1 561 472 5200

Hong Kong
apac@wontok.com
+ 852 2824 8330

Sydney – Australia
anz@wontok.com
+ 61 2 8355 5270

http://linkd.in/1hZrjk1 Twitter: @SafeCentral

www.wontok.com

wontok™