The life and death of the ZeuS Trojan

blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/

Malwarebytes Labs July 21, 2021

Whether you've read up on Greek mythology or you're simply a big fan of Marvel comics, the name "Zeus" should be familiar to you. In the context of cybercrime though, ZeuS (aka the Zbot Trojan) is a once-prolific malware that could easily be described as one of a handful of information stealers ahead of its time. Collectively, this malware and its variants infected millions of systems and stole billions of dollars worldwide.

ZeuS was primarily created to be a financial or banking Trojan, otherwise known as crimeware. But, as you'll see, the extent of its information stealing ability could easily go beyond covertly pilfering financial information, making it a real threat to individuals and organizations of all sizes.

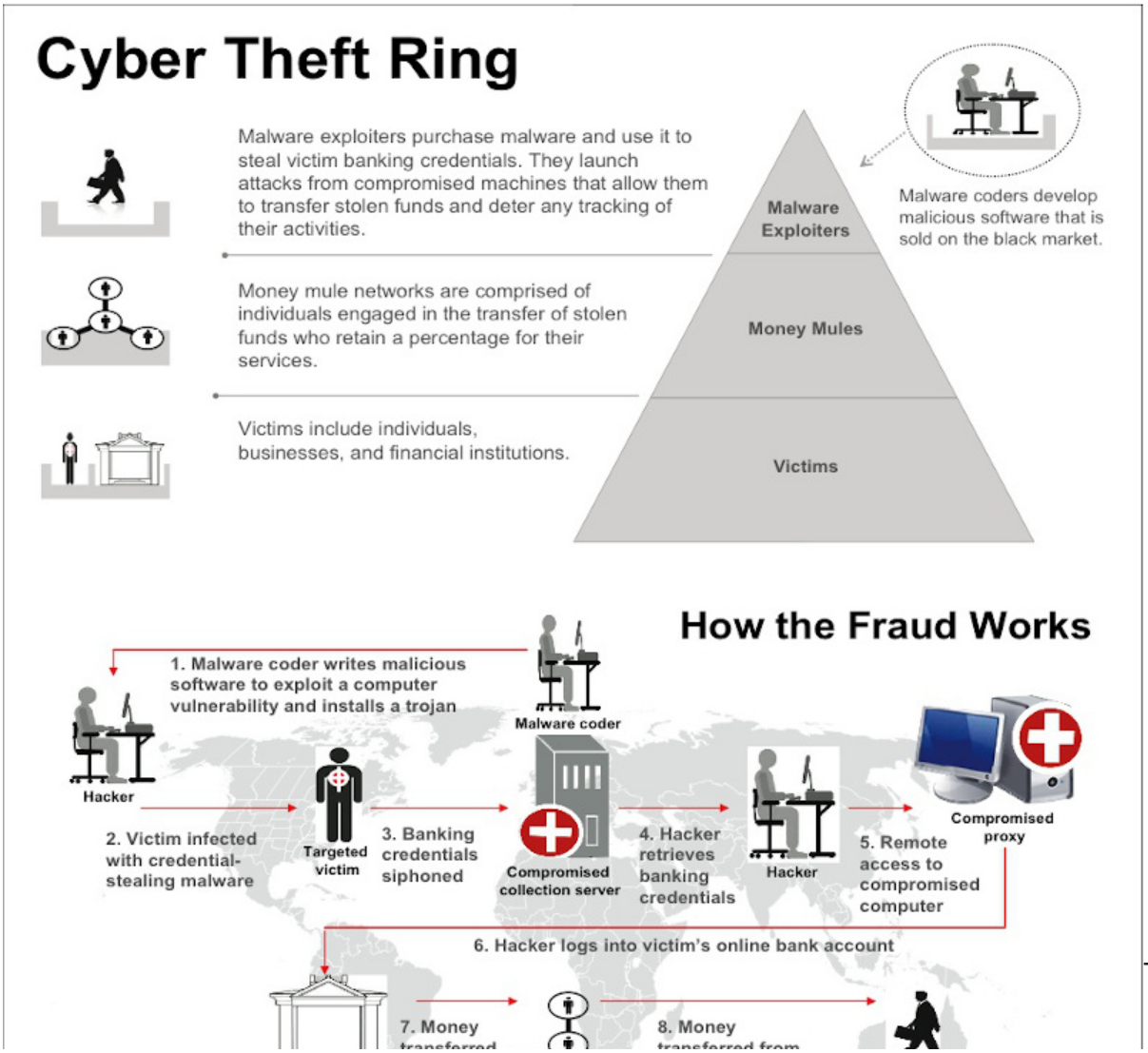
First spotted in-the-wild in 2007, the earliest known version of the ZeuS Trojan was caught stealing sensitive information from systems owned by the United States Department of Transformation. It was believed that ZeuS originated in Eastern Europe. ZeuS affiliates focused their efforts away from corporations and large banks, going after small- to medium-sized organizations, including towns and churches, according to the Federal Bureau of Investigation (FBI).

ZeuS usually arrives via phishing campaigns, spam campaigns, and drive-by downloads. However, this is easy to change and anyone motivated to conduct financial fraud can easily change who they target and how they want their ZeuS to be delivered. Victims have been infected by ZeuS variants via instant messengers (IM), messaging features in social media platforms, and even a pay-per-install (PPI) service—a way to distribute ads to users that a ZeuS user employed for their campaigns.

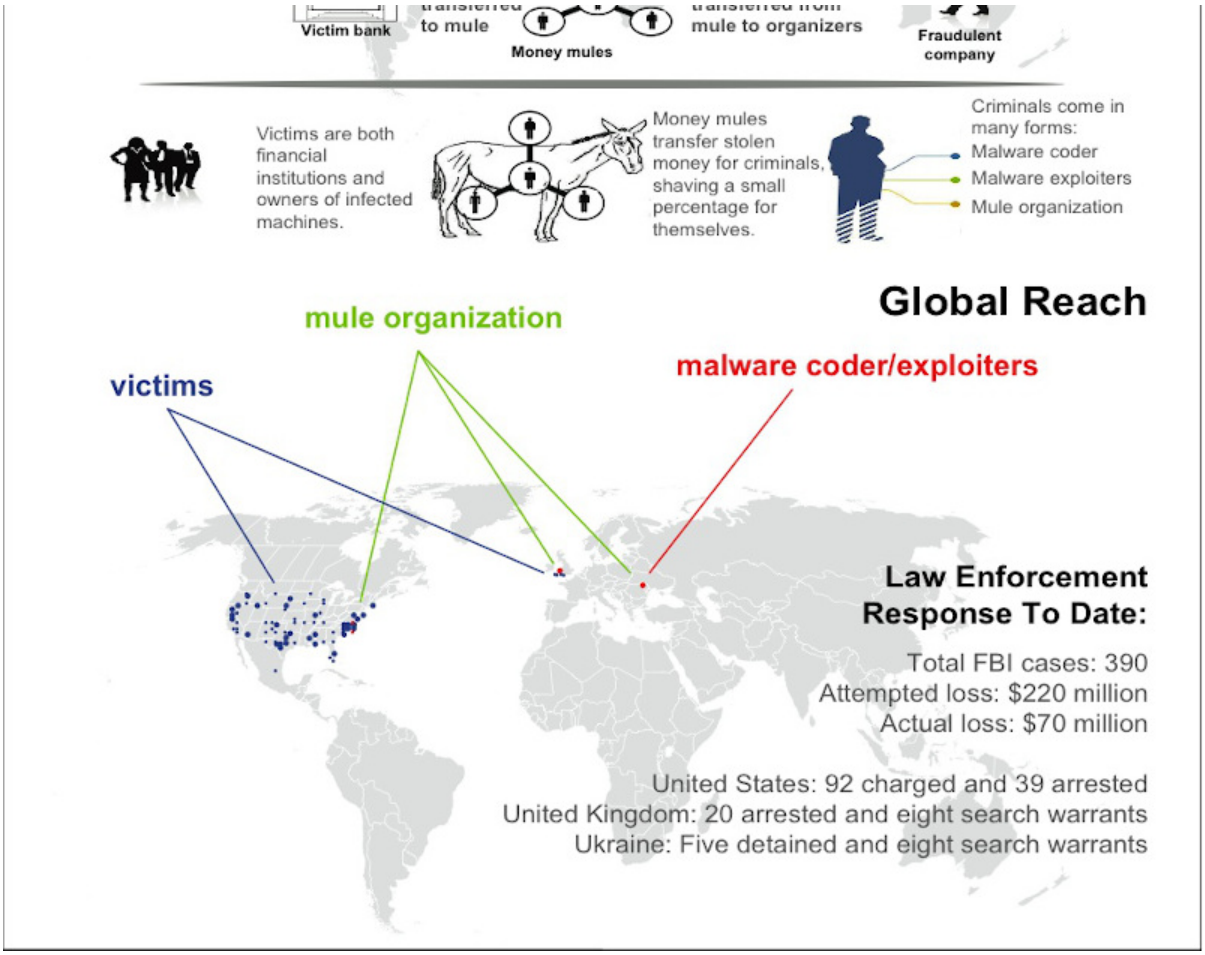
Once a machine gets infected, ZeuS immediately steals information from web browsers and Windows' protected storage (PStore), such as banking or financial information and stored account credentials, respectively. All stolen data are siphoned off via a command & control (C&C) server.

Furthermore, any system infected with ZeuS also becomes a bot in a botnet. A kind of illegal Cloud computing platform that can be rented out to other criminals. These bots were also used to remotely update the ZeuS variants residing in them.

To date, there are 545 versions of the ZeuS Trojan, according to a website called ZeuSMuseum.com.



The



FBI's illustration of a ZeuS cyber theft ring works. (Source: FBI)

How mighty is the ZeuS Trojan?

A ZeuS Trojan toolkit can be fashioned to do a number of things both for the fledgling and adept fraudster.

ZeuS lurks inside infected machines as it stealthily monitors the websites users visit. It recognizes when a user is on a banking website, for example, and then records keystrokes when the user logs into the site. Because of this, fraudsters can easily log back into that banking account using the recorded keystrokes.

Some variants of ZeuS also affect mobile devices that run Android, Symbian, and Blackberry. ZeuS is the first information stealing malware that steals Mobile Transaction Authentication Numbers (mTANs), a type of two-factor authentication (2FA) method that banks use when you want to perform transactions. An mTAN, also called SMS TAN code, is usually a 6-digit number that is unique per transaction and is sent via SMS.

ZeuS steals information in a number of ways, including: Stealing user keystrokes; collecting the text users enter into web forms; taking screenshots whenever the mouse is clicked; so-called man-in-the-browser (MiTB) attacks that add new elements to web forms asking for things like social security numbers or bank PINs.

As to what, exactly, ZeuS steals, here is non-exhaustive a list provided by the SecureWorks security researchers:

- Data submitted in HTTP forms
- Account credentials stored in the Windows Protected Storage
- Client-side X.509 public key infrastructure (PKI) certificates
- FTP and POP account credentials
- HTTP and Flash cookies

ZeuS is also capable of re-encrypting itself every time it infects a system, making each infection “unique” and therefore harder to detect.

Many researchers attribute ZeuS’s ability to stay under the radar for long periods of time as the main reason why it became the most sought-after info-stealer kit in the underground market during its time. It’s likely that ZeuS infected millions of computers, with many victims not realizing that their sensitive data had fallen into the hands of criminals and that their computer was part of a botnet.

The ZeuS developers also put a lot of effort into protecting their malware. According to SecureWorks, ZeuS 1.3.4.x, a privately sold version of the kit, is protected via a hardware-based licensing system. Also known as hardware-locked licensing, this system allows the kit to be installed on only one computer.

The “fall” of ZeuS Trojan

In 2011, the source code for ZeuS 2.0.8.9 was leaked. Some groups or individuals started offering the use of ZeuS botnets on a subscription basis. According to a case study on ZeuS from students at the University of Cambridge, this “maximises earnings by providing the same service to multiple users. For the user of the service, the benefits are in a reduction in the initial financial outlay, while outsourcing the logistical and maintenance requirements, and reducing the risk of failure to achieve results.”

Cybercriminals also began creating their own ZeuS-based information stealers, make ZeuS itself something of a footnote. Citadel, GameOver, Panda Banker, Terdot, Floki, and Sphinx are some of the known ZeuS variants to date.

Before the code leak, it was rumored that the ZeuS creator would be retiring and then selling his code to a competitor called SpyEye, an up-and-coming information stealer that made heads turn for being able to remove ZeuS infections. There had been reports of a code hand-over, yes, further confirming the merging of the two malware, but the ZeuS creator didn’t quit. According to a report from Brian Krebs, the creator merely stopped selling it publicly and started creating “a more robust and private version of Zeus” instead.

In 2013, the FBI charged and arrested Aleksander “Harderman” Panin, a 24-year-old Russian male believed to be the creator of the SpyEye Trojan. That same year, Hamza Bendelladj, a 24-year-old Algerian male, was arrested and charged for developing components of SpyEye, operating botnets infected with SpyEye, and of course, fraud charges.

Is ZeuS dead?

As long as criminals continue to use bits and pieces of its code to create their own malware, ZeuS can’t be considered dead, so much as fading away slowly. However, ZeuS’s purpose, data theft, is making a comeback.

Banking trojans haven’t gone away, but in recent years their activity has been eclipsed by an epidemic of ransomware. Recently though, major ransomware operators have taken to stealing victims’ data before encrypting it, so they can threaten to leak it.

The tactic has been so successful that some ransomware actors claim to be moving away from encrypting files, and focussing entirely on finding and exfiltrating sensitive data from organisations.

In fact, following a devastating attack on Ireland’s public health system, the Conti ransomware gang issued the Health Service Executive (HSE), a free decryption key to unlock all of their affected files, convinced that simply publishing and selling the data they had stolen was leverage enough.

How long I wonder, before information stealers are another thing Biden will be phoning Putin for?