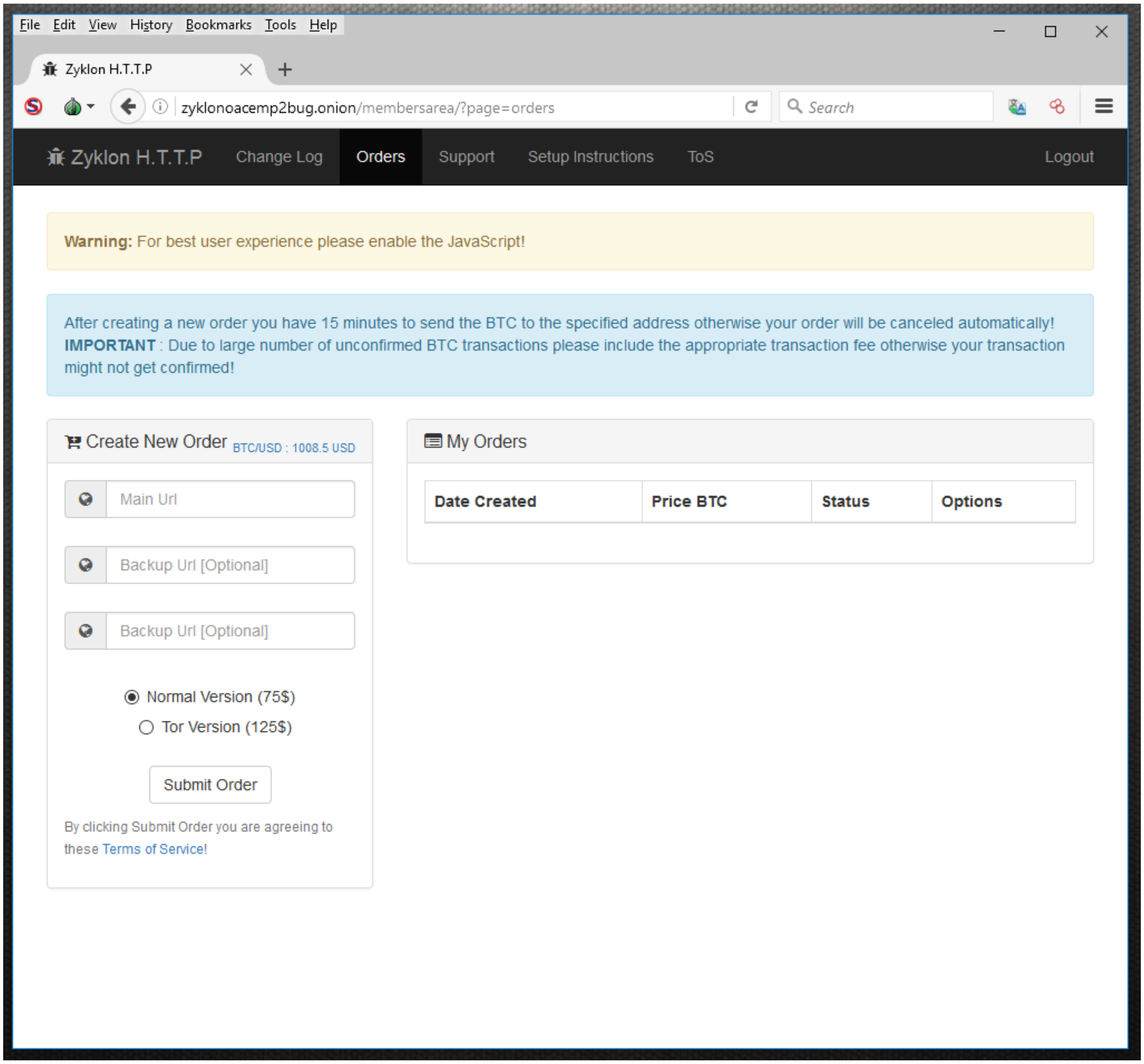
ERT Threat Alert

Zyklon HTTP Botnet

February 16th 2017

Overview

Zyklon HTTP is a botnet that is currently being sold on the Darknet (see Figure 1), HackForums and available on a number of member only communities. This botnet supports Tor for anonymization and comes loaded with a number of additional features. It allows its users to execute various types of DDoS attacks, data theft and fraud. It also features secure operation mechanisms to detect other malware and assure its availability. Zyklon targets PCs and spreads itself via a number of different methods including phishing attacks.


File Edit View History Bookmarks Tools Help
Zyklon H.T.T.P
zyklonoacemp2bug.onion/membersarea/?page=orders
Search
Zyklon H.T.T.P
Change Log
Orders
Support
Setup Instructions
ToS
Logout

Warning: For best user experience please enable the JavaScript!

After creating a new order you have 15 minutes to send the BTC to the specified address otherwise your order will be canceled automatically! **IMPORTANT** : Due to large number of unconfirmed BTC transactions please include the appropriate transaction fee otherwise your transaction might not get confirmed!

Create New Order BTC/USD : 1008.5 USD

Main Url

Backup Url [Optional]

Backup Url [Optional]

● Normal Version (75$)
○ Tor Version (125$)

Submit Order

By clicking Submit Order you are agreeing to these Terms of Service!

My Orders

Date Created	Price BTC	Status	Options

Figure 1: Zyklon H.T.T.P for sale on the darknet

Attack Methods

Distributed Denial of Service:

Zyklon HTTP v1.3 is a multi-feature botnet capable of launching multi-vector DDOS attacks from infected clients. Vectors offered in the botnet includes HTTP POST, HTTP GET, TCP, UDP, SYN and SlowLoris.

- **HTTP Flood** - It consists of seemingly legitimate session-based sets of HTTP GET or POST requests that are designed to consume a significant amount of server's resources, and can result in a denial-of-service condition - without necessarily requiring a high rate of network traffic.

- **TCP flood** – Sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or firewall. Servers need to open a state for each SYN packet that arrives and store this state in tables that have limited size and are easily filled. Once this happens, the server drop new requests, including legitimate ones.

- **UDP Flood** – The attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is “connectionless” and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. Usually, the attackers spoof the SRC IP.

- **SYN Flood** – Overwhelming a target machine by sending thousands of connection requests to it using spoofed IP addresses. The target machine attempts to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. Since a SYN-ACK packet never arrives, the massive number of half-open connections quickly fills up the server’s TCB table before it can time any connections out.

- **SlowLoris** - By sending HTTP headers in tiny chunks as slow as possible (just before the server would time out the request), the target server is forced to continue to wait for the headers to arrive. If enough connections are opened to the server in this fashion, it is unable to handle legitimate requests.

Malware Contamination:

Cloud-based malware inspection
Zyklon H.T.T.P will enumerate all startup files and upload them to the VirusTotal online malware scanner. This will lead to analyzing of samples of malicious software that resides on the system. If the file is found to be malicious, Zyklon H.T.T.P will terminate all processes associated with that file and remove the file along with the registry keys from the system. This is a great option for perpetrators to ensure that their enslaved client systems are running without disruption. The botnet user can specify files to exclude from VirusTotal, and by calculating the MD5 hash of the file Zyklon H.T.T.P will skip it while scanning.

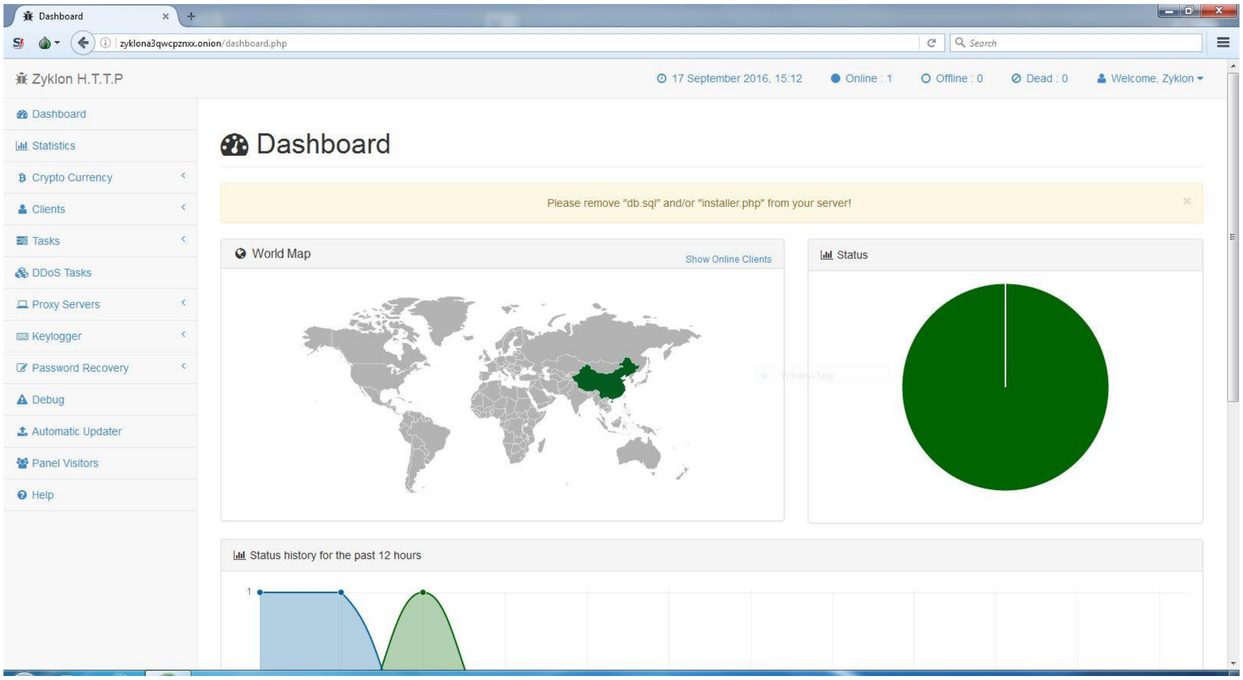
Botkiller
While the Cloud-based malware inspection relies on VirusTotal, Botkiller uses its own algorithm to determine if a file is malicious or not. This method tends to have more false-positive detections. When using this feature, Zyklon H.T.T.P will scan all processes and will check common locations that malwares reside in. It will attempt to detect injected processes and it will try to identify malware by behavioral analysis. If a file is detected as malicious the program will follow the settings specified in the botkiller feature, leading to the process termination and deletion of all associated files and registry keys. Like the Cloud-based malware inspection, this feature is keeps an enslaved client machine secure and available.

Keylogger

Keylogger is a great feature when it comes to client surveillance. It will record all keystrokes and log them to a database. The logs are sorted by dates and can be accessed from almost anywhere in the C&C panel. The control panel also lets one specify the window titles to record keystrokes for, as opposed to bloated logs with all kind of entries. Keylogger supports most if not all languages and keyboard layouts. The user can specify the maximum amount of characters that will client hold in a buffer before they are sent to the panel, or set an interval at which the logs are being uploaded to the panel.

Automatic updater

Zyklon features automatic update function that ensures that all enslaved clients are running up to date software. When executed, it compares the update file hash and installed file hash and if found different – an updated file will be downloaded and installed. This comes very handy when controlling many clients.



zyklona3qwcpznxx.onion/dashboard.php

Zyklon H.T.T.P

17 September 2016, 15:12 Online : 1 Offline : 0 Dead : 0 Welcome, Zyklon

Dashboard

Please remove "db.sql" and/or "installer.php" from your server!

Figure 2: Zyklon HTTP Panel

Data Theft:

Browser password recovery

Zyklon botnet is able to recover passwords from popular web browsers. Most noticeable ones are Google Chrome, Mozilla Firefox, Internet Explorer, Opera Browser, Chrome Canary/SXS, CoolNovo Browser, Apple Safari, Flock Browser, SeaMonkey Browser, SRWare Iron Browser and Comodo Dragon Browser.

FTP password recovery

Currently supports FTP password recovery from following FTP applications: FileZilla, SmartFTP, FlashFXP, FTPCommander, Dreamweaver, WS_FTP.

Gaming software key recovery

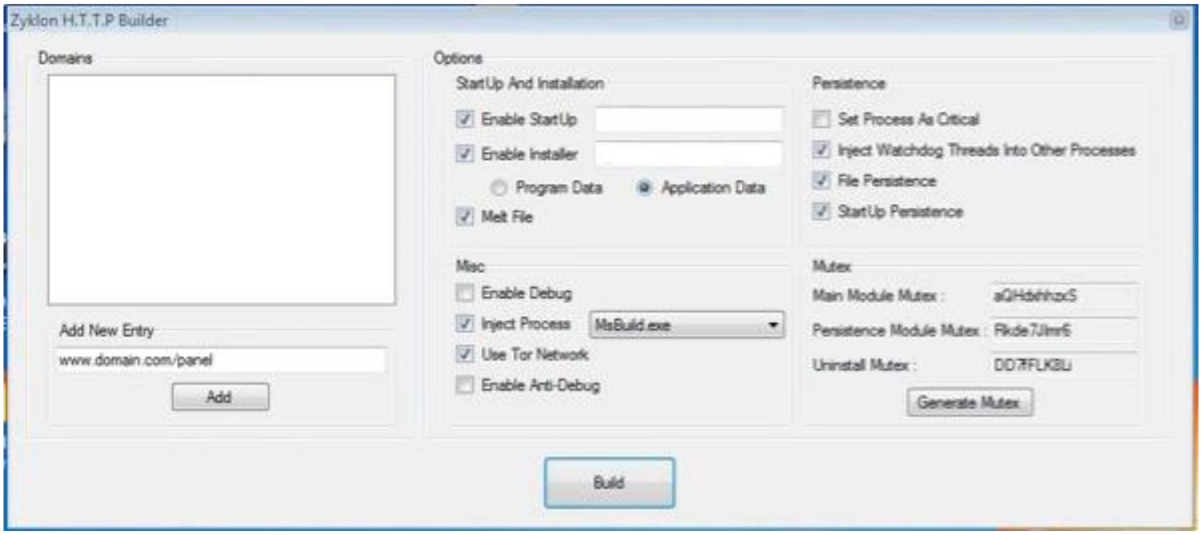
Currently supports around 50 PC gaming software's including Battlefield, Call of Duty, FIFA, NFS, Age of Empires, Quake, The Sims, Half-Life, IGI, Star Wars and many more.

License key recovery
Automatically detects and decrypts the license/serial keys of over 200+ popular software's including Office, SQL Server, Adobe, Nero and many more.

Socket Secure 5 proxy
Turn your bots into proxy servers - It automatically checks and updates a list of active proxy servers, and features reverse socket secure proxy servers, facilitating the creation of a proxy server on any client.

Email password recovery
Currently it can recover your lost email passwords from following applications: Microsoft Outlook Express, Microsoft Outlook 2002/XP/2003/2007/2010/2013, Mozilla Thunderbird, Windows Live Mail 2012, IncrediMail, Foxmail v6.x - v7.x, Windows Live Messenger, MSN Messenger, Google Talk, GMail Notifier, PaltalkScene IM, Pidgin (Formerly Gaim) Messenger, Miranda Messenger, Windows Credential Manager.

Encrypted communication
Connection between client and server is encrypted using RSA asymmetric encryption algorithm (Valid key sizes are 512-bit, 1024-bit, 2048-bit, 4096-bit) that is paired with AES-256. AES-256 keys are dynamically generated on the client and are encrypted before being stored in a session variable in the panel. After the initial key exchange, the whole communication is encrypted with AES-256.


Zyklon H.T.T.P Builder

Domains

Add New Entry: www.domain.com/panel

Options

StartUp And Installation
- ☑ Enable StartUp
- ☑ Enable Installer
- ○ Program Data ● Application Data
- ☑ Melt File

Persistence
- ☐ Set Process As Critical
- ☑ Inject Watchdog Threads Into Other Processes
- ☑ File Persistence
- ☑ StartUp Persistence

Misc
- ☐ Enable Debug
- ☑ Inject Process: MsBuild.exe
- ☑ Use Tor Network
- ☐ Enable Anti-Debug

Mutex
- Main Module Mutex : aQHdxhhzxS
- Persistence Module Mutex : Rkde7Jlmr6
- Uninstall Mutex : DD7FLK8Li

Figure 3: Zyklon Builder

* In its previous version, Zyklon was able to perform crypto mining services but this feature has been removed in the latest update. It is likely to return more mature and sophisticated in a future version, as it used to turn the infected computers into Bitcoin miners for profit – a very popular competence.

Pricing

- $75 for a basic version
- $125 for a Tor version - connects to the user panel using Tor's anonymity networking (i.e. nobody will know the location of the Command & Control server). Tor comes preloaded inside of the client and loaded at runtime so nothing has to be downloaded from the internet.
- $15 set up fee (optional) - the vendor will set up the botnet for the client on a client provided domain but will not maintain the server after setup

How to Protect Against the Zyklon H.T.T.P Botnet?

Perpetrators will create an .exe file with the Zyklon H.T.T.P Builder and send it to the victim via a number of different methods including phishing email. They do this by binding the malicious .exe file with a normal file like a popular game, app or document. Once the victim runs the malicious payload through a number of different ways the malware runs silently in the background with a keylogger and other features. These details are then sent back to the C&C panel according to the settings the attacker has configured. Once infected, there is very little an individual user can do from losing data. The attacker at this point can instruct the victims computer to carry out DDoS attacks as well.

To Avoid Bot Contamination and Guard Sensitive Data:

- Organizations shall educate their personnel on detecting phishing attempts
- Deploy an advanced bot detection solution that can cut the connection between the infected machined and the C&C server
- Secure leakage of passwords, credentials and confidential files
- Prevent turning endpoints into proxies

Key Considerations for Effective DDoS Protection

- A security solution that can protect its infrastructure from multi-vector DDoS attacks including DDoS protection from network and application-based DDoS attacks as well as volumetric DDoS attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and DDoS mitigation with cloud-based protection for volumetric DDoS attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A DDoS solution that provides DDoS protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency DDoS Service with a response team and process in place. Identify areas where help is needed from a third party.

Radware recommends IT crews to monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats when they occur.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.