PRODAFT

Threat Intelligence Insights

B&C Miks

Brute Force Attack Targeting E-Commerce Websites

Last week, the PRODAFT Threat Intelligence (PTI) team detected *brute force attacks* on e-commerce websites utilizing malicious software. The PTI team was able to obtain the visibility of the panel and detect that, so far, the malware sold under the name B&C Miks CMS has affected 3'047 victims and initiated brute force attacks on millions of e-commerce sites.

In a brute force attack, the attacker uses a tool that attempts to discover a password by trying different combinations of letters, numbers, and symbols until the right combination is found.

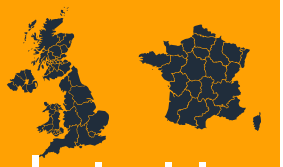
The main objective of the threat actors is to infiltrate the e-commerce websites, upload a shell to the servers, and re-sell access to other cybercriminals.

Attack Highlights

Threat Type: **Brute Force Attack**

Motivation: **Financial**

Most Targeted Countries: **UK and FR**

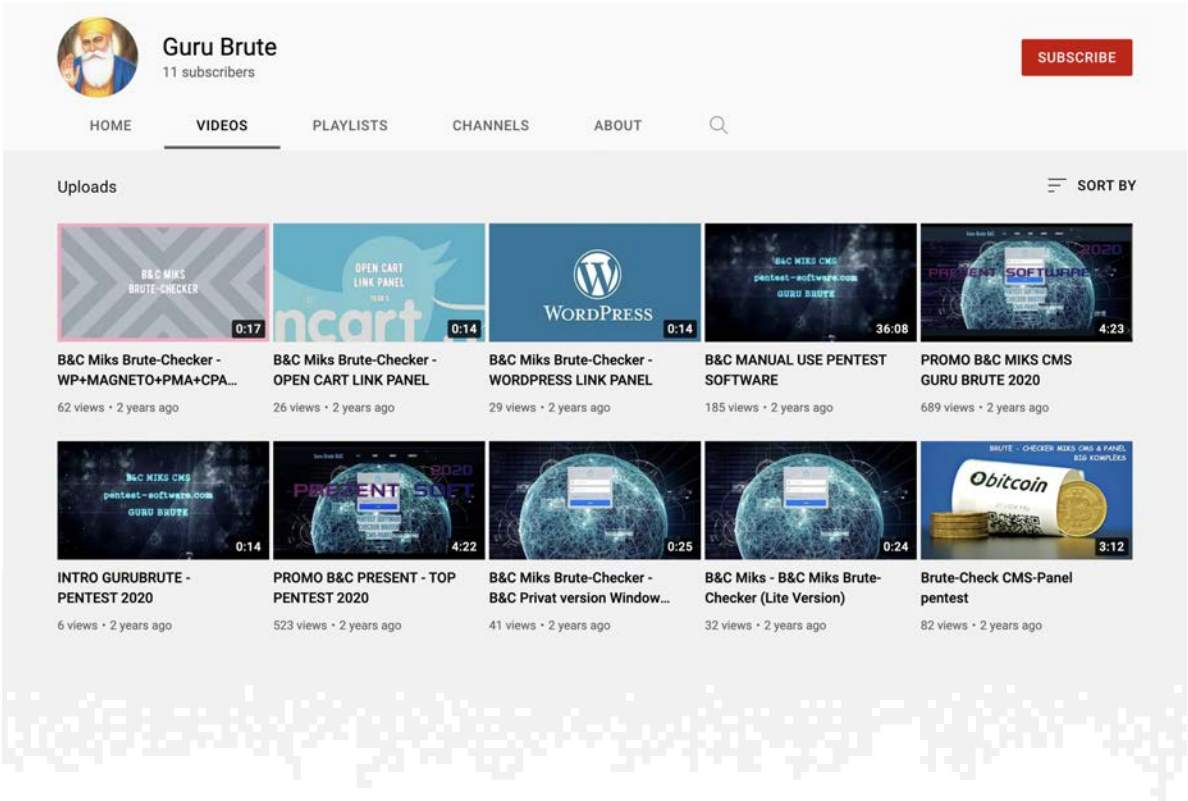


Total victims:

3'047

The Attacker

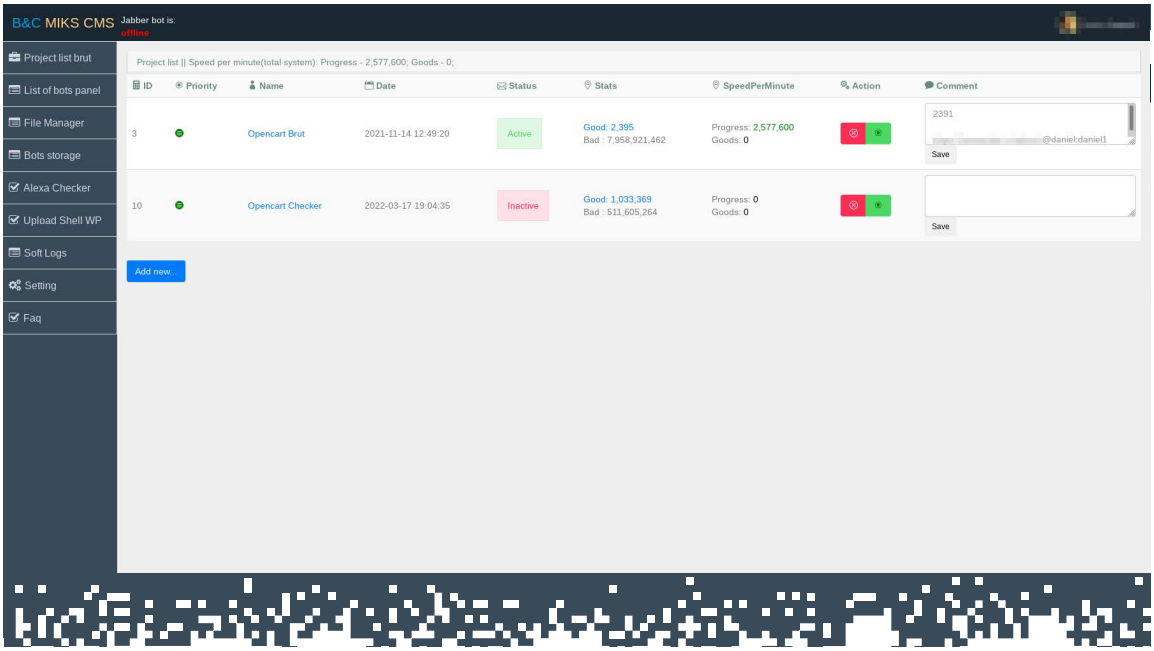
The tool is sold by a threat actor who uses the alias "guru-brute" and has been registered on forums since March 2020. On their YouTube channel, the threat actor promotes the malware that allows perpetrating brute force attacks. The threat actor communicates mainly in Russian language.



Guru Brute's YouTube Channel

The Strategy

Threat actors buy this malicious software to infect servers to obtain more network resources and brute force the credentials of e-commerce site admins. Once they have access to the administrator's username and password, they have complete control over the site. They can steal the credit card information of the e-commerce site's users or the product by shipping it to a location of their choice.



B&C Miks CMS Dashboard Page

The brute force attacks are implemented with the help of automatic shell uploads. The "shell" is a PHP script that allows the attacker to control the application server by uploading this shell/page to a website. Control of the server is needed for threat actors to be able to download files or further exploit the website.

Most malicious spam campaigns, including QBot and Emotet, utilize legitimate but compromised hosts as command and control servers to bypass the network-level intrusion detection systems. Therefore, blocking the traffic going to compromised servers plays a crucial role in the cyber threat intelligence world.

The Findings

Based on our findings, the attacks targeted thousands of e-commerce sites, and the motivation behind the attacks was financial gain. The brute force attacks compromised victims' personal information, login credentials and payment data.

The most targeted countries are the UK, France, China, Turkey, Germany, India, Russia and Singapore.

How To Prevent Brute Force Attacks

E-commerce businesses need to take action to prevent these types of attacks and deal with them effectively and efficiently. Rather than having a reactive stance, e-commerce businesses should take a proactive approach to cyber security. A proactive approach is essential for brute force attack prevention because these attacks can go undetected for long periods on your network and silently lead to data exfiltration.

Our threat intelligence platform tracks different areas and aspects of dark-web and deep-web platforms to identify and prevent these attacks quickly. With the help of the U.S.T.A. platform, you will be able to respond to cyber security threats that come your way successfully.