International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

IJSRA
Int. J. Sci. Res. Arch.
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

# Darknet and Zero-Day Exploit Analysis

Bogdan Barchuk *

*Independent researcher.*

International Journal of Science and Research Archive, 2023, 08(02), 799-811

Publication history: Received on 08 February 2023; revised on 25 April 2023; accepted on 28 April 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.2.0222

## Abstract

On the darknet, people can buy and sell illegal digital goods such as zero-day exploits, which are not yet made public. Cybercriminals value these vulnerabilities since they allow for weaknesses in security systems that pass unnoticed. In this underground community, traders, auctioneers, or leaksters can move exploits that are later used in large-scale cyber-attacks. With the help of botnets and automated tools, it is now easy for attackers to scan and hack many vulnerable systems in just a few minutes. Due to the large number of users who use them and don't update them properly, WordPress, Joomla, and Drupal are often attacked. Many times, individuals or groups that aim to harm or damage companies use these zero-day tools because the effect is strong and immediate. Because there is less distinction now between hobbyists and criminal groups, the darknet is having a bigger impact on current cybersecurity. In this paper, we discuss the way the darknet works, how zero-day exploits develop throughout their lifespan, and the increasing risk posed by tools that automate attack methods.

**Keywords:** Darknet marketplaces; Zero-day exploits; Automated bots; CMS vulnerabilities; Mass \\defacements; Vulnerability chaining

## 1. Introduction

As new technologies for hiding identities are created, the level of cybercrime rises as well. Being anonymous, cybercriminals can join efforts, trade attack tools, and run them with little chance of being caught. The darknet on the internet allows people to buy and sell illegal drugs, as well as details on weaknesses in software. Over the last decade, there has been a big shift from manual attacks on single systems to the use of automated bots and pre-programmed tools for mass attacks. Because of these tools, people with no or little technical knowledge are now able to participate in cybercrime (Hawdon, 2021).

The shift is happening due in part to the commercial sale of cyber vulnerabilities like zero-days by vendors. Zero-days, previously regarded as uncommon and worth of only top hackers, are now being openly sold, rented, or given away in various marketplace and forums in the darknet. Rapidly turning exploits into forms of profit has resulted in cybercrime-as-a-service, where individuals can buy ready-made tools for attacking systems (Zhou et al., 2020). As a result, anyone can easily get involved in transnational crime, and attacks can be made on a large scale. For this reason, individuals and countries are more at risk from nameless opponents who have access to good digital weaponry.

### 1.1. Overview

The darknet is now mainly involved in bringing about the sale and distribution of zero-day vulnerabilities, making it a secure hub for criminals, hackers, and state-organized groups. It makes it possible for people with malicious intentions to privately trade, buy, or sell software exploits that are designed to target widely used software like WordPress and Joomla. Since so many websites use these systems, making them perfect for hackers, and because third-party plugins

* Corresponding author: Bogdan Barchuk

and themes are used so often and are not updated regularly. They are, therefore, easily exposed to common hacking tricks that pirates spread in their online communities (Anjum et al., 2021).

Apart from how it provides financial services, the darknet is important for launching cyberattacks. Groups using these platforms can discuss specific bugs in content management systems and make use of helpful tools that make it faster to launch an attack. What used to be rare exploits for niche hackers is now widely available on the darknet with user-friendly interfaces that let people carry out attacks on a large scale without much work. This means that even simple-skills hackers play a part in making cyberattacks rapidly appear in large numbers (Besenyő and Gulyas, 2021). For this reason, the darknet is now a critical component in cybercrime, supporting easy and widespread use of new attack tools.

### 1.2. Problem Statement

With fast-rising darknet markets, cybersecurity is now facing a big hurdle. finding, following, and dealing with zero-day exploits. If these attacks are not known to software vendors, antivirus programs, firewalls, and intrusion detection systems aren't able to catch them. Through darknet platforms that are encrypted, zero-day vulnerabilities become more difficult to find out about, as no one's identity can be revealed. Due to being hidden, these threats are usually noticed by organizations only when an attack takes place. This problem is heightened by the fact that zero-days are now being divided, automated, and aimed at many systems quickly. Sometimes, security experts are able to react only when a breach has already brought harm to the company. Not having access to current data on darknet activities and new threats puts defenders at higher risk of attack. Therefore, the relationship between offensive capabilities and defensive skills suffers from such vulnerabilities being sold in illegal networks.

### 1.3. Objectives

The study aims to investigate how zero-day vulnerabilities are used more and more by attackers through mass tools. In the first step, it tries to discover the main ways and locations used for buying and selling exploits, including darknet markets and relevant forums. The purpose is to see how the markets allow important vulnerabilities to be used for profit. Then, the study will focus on botnets, which are software tools used to analyze, breach, and compromise systems on a large scale. The Bad Mode bot and XKyubi will be assessed by studying the cases that they encountered. In the end, the research seeks to investigate how automated hacking tools are put together and how their communities update, share their work, and improve how the tools operate. The aim of this research is to discover key ideas from the process, starting with the development of tools and followed by their active use in cyber attacks. Thus, these goals support the idea of taking action ahead of any possible threats from digital attacks.

### 1.4. Scope and Significance

The research investigates the use of darknet forums and marketplaces to trade on zero-day vulnerabilities, mainly paying attention to those that exploit content management systems such as WordPress, Joomla, and Drupal. It also examines tools that hackers use and botnets to try and compromise CMS platforms in a large way. The investigation focuses on tools, practices, and behavior of threat actors based on things seen in public repositories and archives of past defacement events. It does not include information about cyber warfare that happens at the state level or secret business intelligence systems. It is important because the study lets experts, developers, and policymakers understand the risks from zero-day exploits that appear in the darknet. To let the importance of early warning systems, disclosure of vulnerabilities, and automated defense be seen, the study investigates the entire process of exploitation. Getting familiar with these dynamics is necessary to craft better cybersecurity measures and cut down the time attackers can use to their advantage.

## 2. Literature review

### 2.1. Evolution of Defacement Culture and Bot Usage

Defacing websites has for many years represented the identity and beliefs of hackers. Early hacking actions were manual, but later on, hackers gained fame and competed with skilful cyber assaults. At first, defacements involved tampering with a singular work or object in an attempt by someone to say or show something ideologically on purpose. However, with more automated tools and bots, mass defacements on lots of websites became possible all at once.

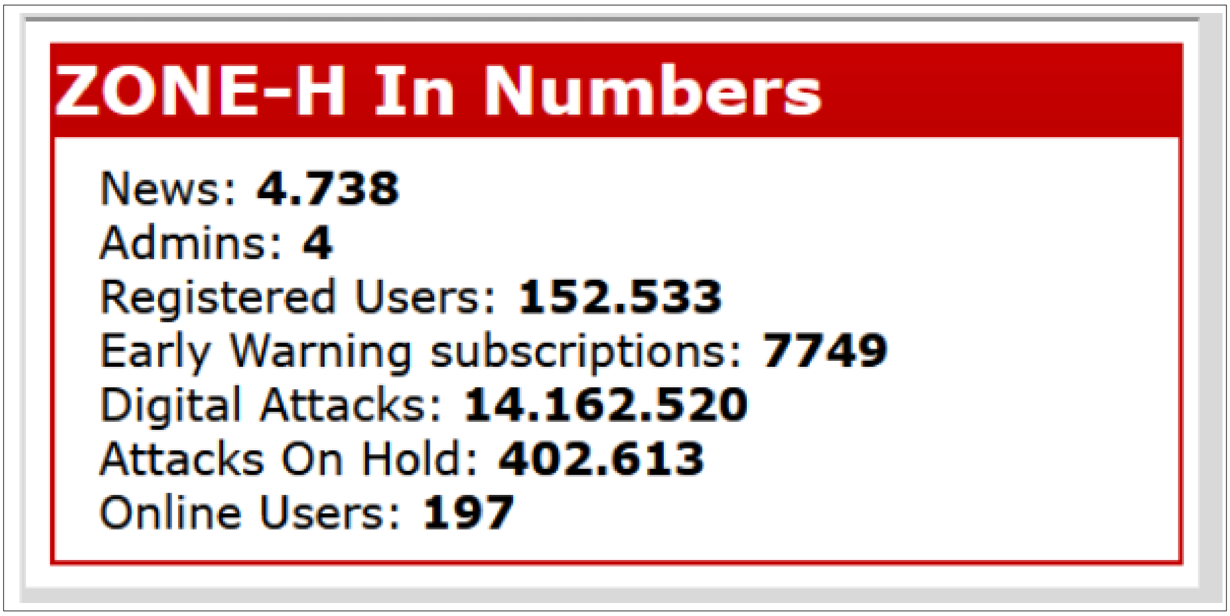
Image 1 – ZONE-H In Numbers reveals the huge size of these incidents. Zone-H's collection of more than 14 million attacks and over 152,000 registered users proves the popularity of defacement culture today. The large majority of the attacks occurred as part of mass defacements, made possible by widespread use of bots to spot and use CMS flaws.

Because bots made it easier and more valuable to attack many sites, attackers tended to go for quantities instead of trying to do things well.

During this research, we have discussed that Bad Mode and XKyubi typify the evolution of cyber vandalism. They automate most of the common steps required for an attack, making it less demanding for the attacker to succeed. With the help of mass IP generator tools, hackers can attack hundreds of systems quickly, requiring very little manual work.

This change in technology mirrors what has been happening in the history of cyberattacks, particularly relating to Distributed Denial of Service (DDoS) attacks. Brooks et al. (2022) state that the design of tools for automating DDoS attacks has progressed much like the defacement tools, which at first required only a manual approach to later become fully automated. Botnets and prebuilt exploits were also used in defacing the internet, helping the attacks to be seen and noticed by a larger number of people (Brooks et al., 2022).

In short, cyber-vandalism has changed from being done by individuals to being carried out automatically and in bulk, thanks to bot technologies that archived on Zone-H. It highlights how web attacks are becoming more common and affect an even larger number of victims.



ZONE-H In Numbers

News: **4.738**
Admins: **4**
Registered Users: **152.533**
Early Warning subscriptions: **7749**
Digital Attacks: **14.162.520**
Attacks On Hold: **402.613**
Online Users: **197**

**Figure 1** Overview of global web defacement activity and scale of bot usage, illustrating the magnitude of automated cyber vandalism from 2002 to present

### 2.2. Monthly and Daily Patterns of Web Attacks

Boosted by automation and that of programs known as bots, web attacks are now more evolved. This shift has brought about a regular pattern where attacks are carried out regularly, sometimes coming as large surges. Such attack patterns mirror the usual routines of attackers as well as the features available in the tools they choose.

Image 2 – 05/2020 and Monthly Attacks Chart clearly highlights how the numbers of attacks have gone up recently. On the top chart for May 2020, it is evident that there were sudden increases every day, and the number of attacks more than 10,000 was recorded for both May 22nd and 23rd. These spikes are rarely coincidental; Usually, they reflect attacks involving groups of bots that aim at the same set of easy-to-find vulnerabilities on a huge scale. Most attack surges happen when there is a disclosure of a public vulnerability or a leaked exploit kit gets widely distributed among hackers.

In the bottom part of the graph, you can see that attacks rose sharply in the middle of 2020. In May 2020, the number of attacks was more than 70,000, which was double the number seen in earlier months. More use of defacement and zero-day techniques is in line with this escalation. Since Bad Mode and XKyubi allow users to target dozens of websites at the same time, this is clearly increasing the number of attacks.

The usage of this pattern demonstrates a change in strategy by cyber attackers. It is not enough to hit just one group; groups seek to become noticed quickly by reaching out to many people. They may plan attacks over weekends or on specific dates to prevent a right away response and to give the attack more meaning. Now that vulnerable code can be identified and vulnerabilities spread all through the internet automatically, the actions taken daily are not set but do lead to large-scale results over time.

Due to these ups and downs, organizations require constant monitori If these systems were not present, organizations would often realize they had been part of an attack only later, after the archives listed it in Zone-H. So, it is important to recognize how often attacks occur to come up with efficient strategies.

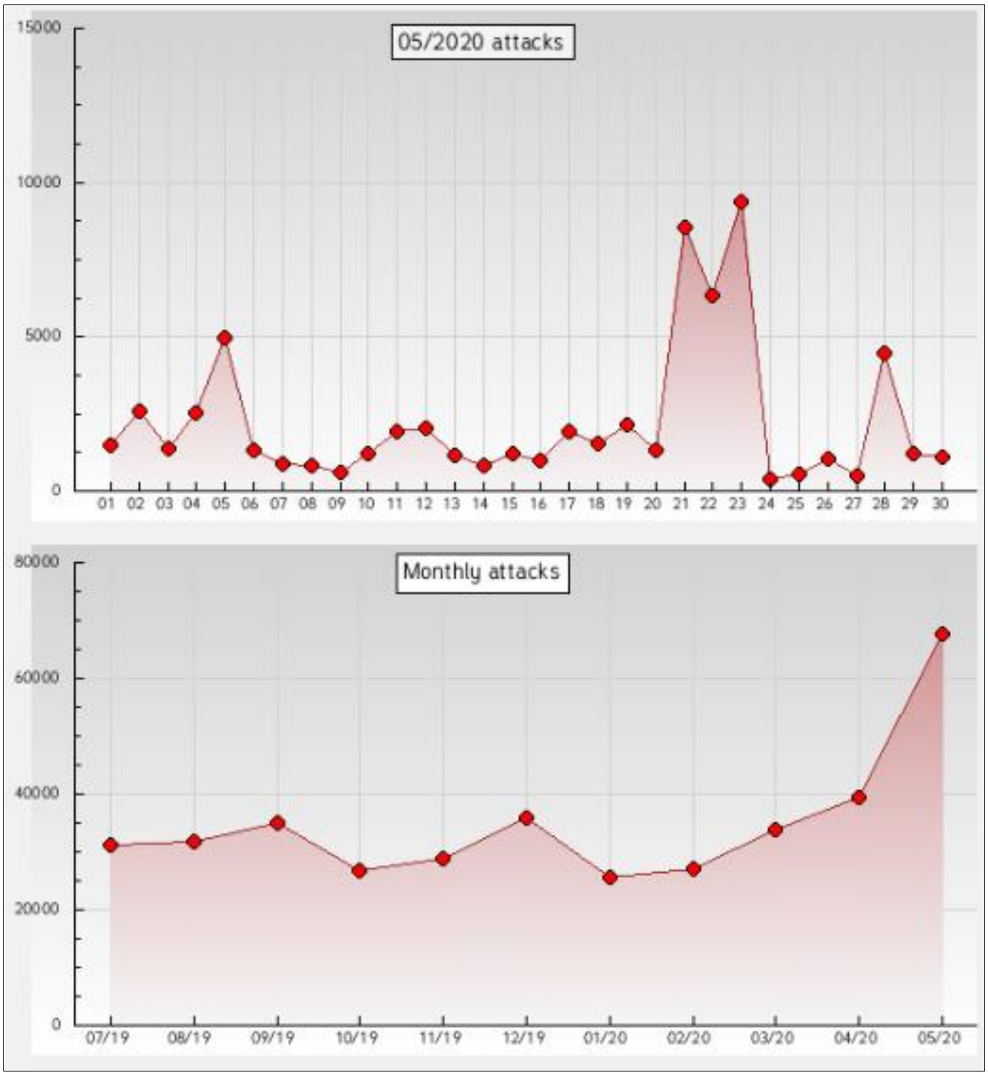


**Figure 2** Daily and monthly attack volume fluctuations in May 2020, highlighting coordinated spikes tied to automated exploitation campaigns

### 2.3. Decline in Yearly Attacks – Shift to Stealthier Exploits

Compared to the past decade, today’s cyberattacks are now less noticeable, yet they have a powerful and lasting effect. The change is easily seen when looking at the long-term data in Image 3 – Yearly Attacks, covering web defacements from 2012 to 2020. There were more than 1.4 million cyber-attacks in 2013, but the numbers have steadily declined, ending at less than 200,000 in 2020.

Just because these numbers are down does not necessarily mean cybercrime is happening any less. There was a time when numerous individual hackers and groups chose defacing websites to make their point, spread political messages, or just be destructive. Because these attacks were publicly noted, they were great ways for members of underground groups to earn a reputation. Because of improved cybersecurity and increased law enforcement, attackers switched from flashy attacks to those that are simply less noticeable.

To avoid detection, many threat actors now prefer staying in the system without making their activity known. Focus has moved from making a brand seen to keeping it strong and making it profitable. Trading zero-day vulnerabilities on darknet markets is one of the factors that have prompted this change. These flaws are instead utilized for theft of private information, deploying ransomware, or gathering information through spying, all of which must be done quietly and for a long time.

At the same time, cybercriminals are now offering their services online. Having a botnet or automated tool at hand is no longer only used to deface many websites. their main attack strategies are now gathering user credentials, selling access to servers, and elevating privileges, all done out of view within networks. On the darknet, zero-days are valuable assets, and they are often used secretly instead of being displayed for all to see.

So, the rise in targeted and economic rather than surface-level hacking, shown in Image 3, can explain why defacements have fallen. As a result of this evolution, defenders must look for threats that are made to evade detection.

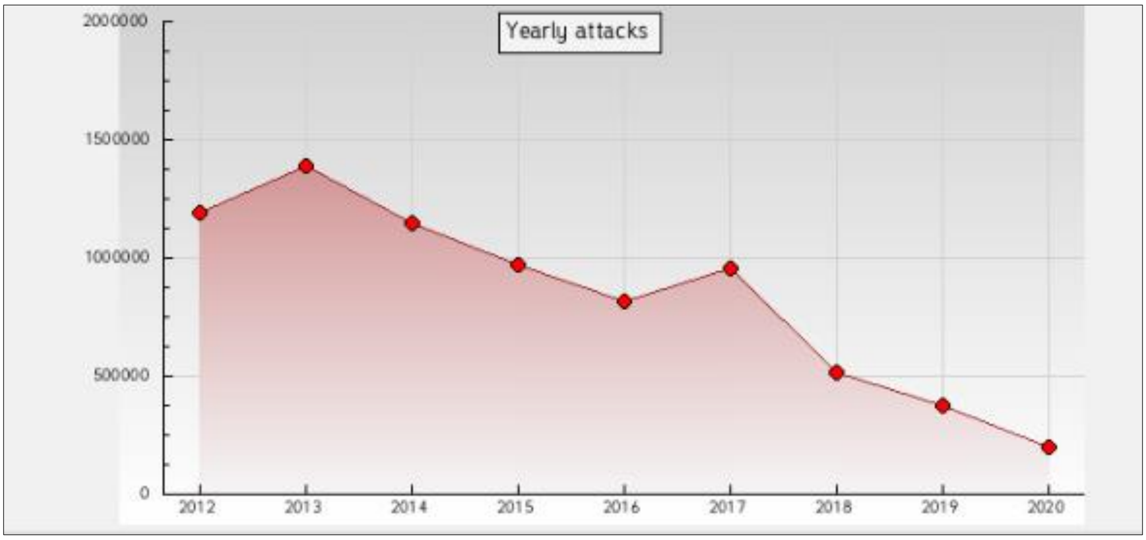


**Figure 3** Yearly trend of website defacements from 2012 to 2020 showing a decline in mass attacks as tactics shift toward stealthier exploit methods

### 2.4. Nation-State and Political Targeting via Bots

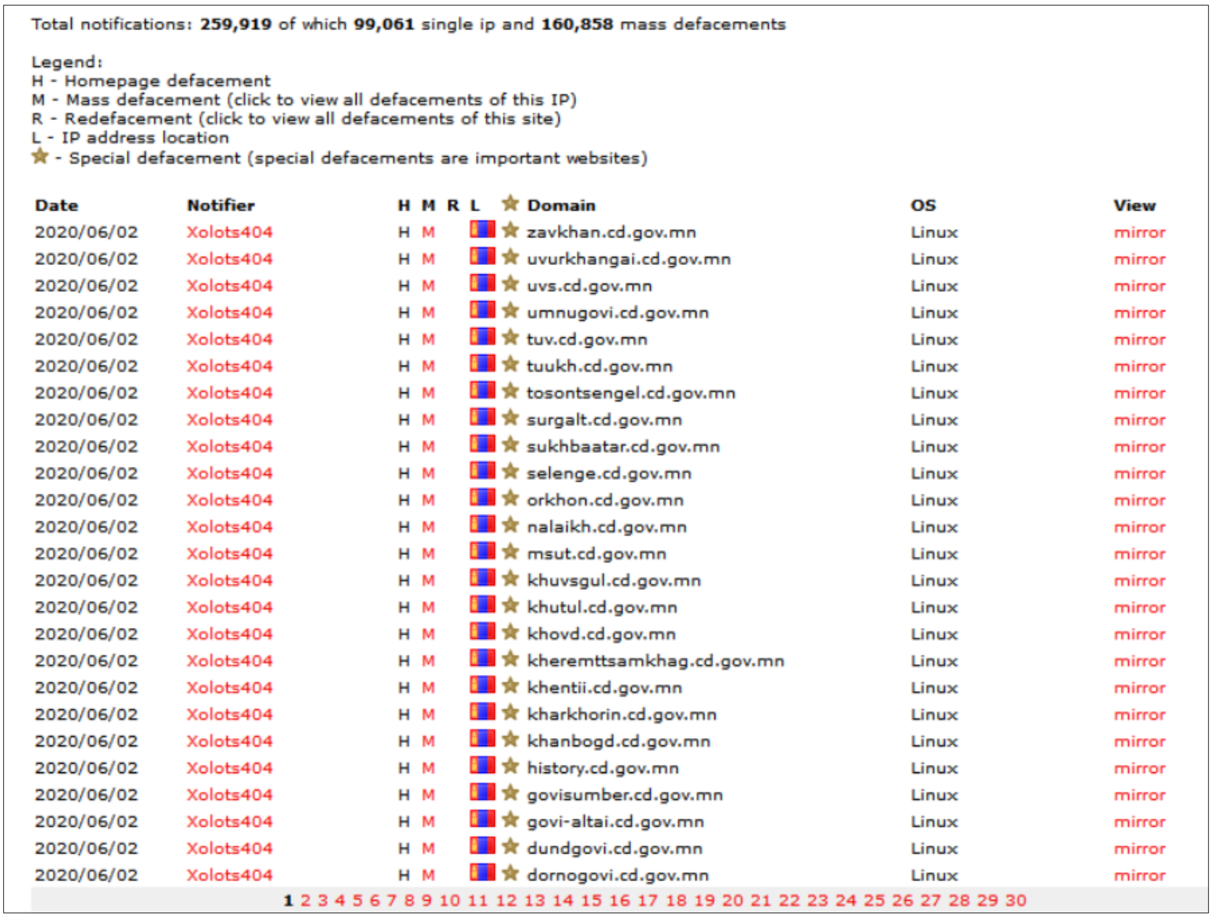
Even though most defacements are motivated by personal causes, certain defacements indicate that their motives are caused by country-wide disagreements. Defacements of government property usually include messages from political groups, aim to disrupt the reputation of the government, or try to challenge those in power. Most of these attacks are carried out with the help of bots, allowing hackers to take over and tamper with many official sites.

Image 4 – Mongolian .gov Defacements depicts a clear picture of politically driven defacements. Many government sites in Mongolia were attacked all at the same time on June 2, 2020. On Zone-H, it shows that these attacks came from the actor "Xolots404" and are classified as a Homepage attack (H) and a Mass attack (M). Since there were many government targets attacked at once, it's likely that this series of attacks was planned carefully to send a political touch, probably with the aid of a bot.

Its methodology is much like Bad Mode or XKyubi, two main types of botnets, since it can throw out lots of targets, look for subdomains, and sniff out and abuse known weaknesses. Well-configured penetration tools make it possible to access hundreds of government sites in a short time, especially when these sites have old platforms like WordPress or Joomla. As soon as the vulnerability is spotted, the bot will add a shell, modify files, and update Zone-H on the success of the attack.

The main thing that distinguishes these types of defacements is how they choose their targets and the messages they display. These sites have major importance and make them popular targets for cyber attacks. Making changes to these flags often makes them noticeable by the public and members of other communities. Even though direct evidence of Mongolia's involvement is missing, the fact that many cyberattacks target governmental organizations is clear indication of an intent to cause issues for the government.

These instances reveal that bots are involved in digital attacks and political cyberwarfare, and not only digital vandalism. Their fast compromising of various national digital assets reflects the way automation is now linked to radical ideas.



Total notifications: **259,919** of which **99,061** single ip and **160,858** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

| Date | Notifier | H | M | R | L | ★ | Domain | OS | View |
|---|---|---|---|---|---|---|---|---|---|
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | zavkhan.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | uvurkhangai.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | uvs.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | umnugovi.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | tuv.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | tuukh.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | tosontsengel.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | surgalt.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | sukhbaatar.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | selenge.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | orkhon.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | nalaikh.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | msut.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | khuvsgul.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | khutul.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | khovd.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | kheremttsamkhag.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | khentii.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | kharkhorin.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | khanbogd.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | history.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | govisumber.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | govi-altai.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | dundgovi.cd.gov.mn | Linux | mirror |
| 2020/06/02 | Xolots404 | H | M | | 🇲🇳 | ★ | dornogovi.cd.gov.mn | Linux | mirror |

**1** 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

**Figure 4** Example of politically motivated, mass defacement campaigns targeting multiple Mongolian government subdomains using automated bots

### 2.5. How the Economy of Darknet Hacking Is Arranged.

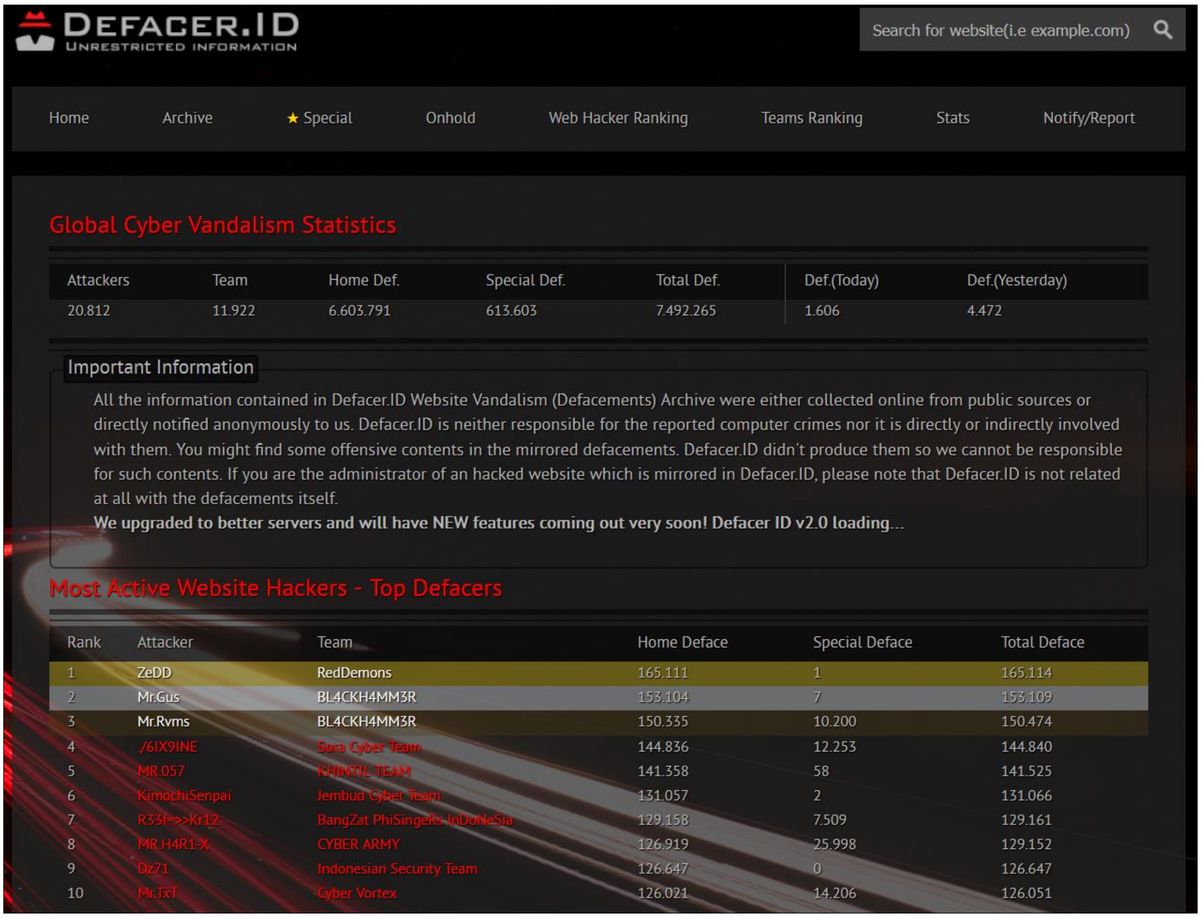
A reputation-based system and economy have made the darknet a place filled with criminals wanting to gain fame or high profits. What was once a personal attack over ideas or damage to property has become a sign of status and clout among those in the underground. Defacer.ID and other platforms collect information about cyber vandalism, arranging it in a way that highlights the size of attacks and the reputation of the attackers.

As per Defacer.ID statistics, there have been over 7.4 million cases of website defacement, and some hackers have accomplished hundreds of thousands of successful attacks. Because of these statistics, people and groups in video games are encouraged to compete, seeking both money and online prestige. Groups such as "RedDemons" and "BL4CKH4MM3R" being involved in attacks reveals the highly organized aspects of such activities, which coincide with what is seen in other darknet groups (Meland, Bayoumy, and Sindre, 2020).

Being known in the community matters a lot, as developers and affiliates in the darknet use feedback, praises from their peers, and their positions in the hierarchy to stand out and attract more clients. In addition, being in hacker rankings increases the motivation to always be active and release more exploits regularly to ensure or improve one's ranking (Sutanrikulu, Czajkowska, and Grossklags, 2020).

In addition, the level of involvement and activity in the darknet by individuals usually matches trends seen in their education and place of origin. Attackers working to take over face off, and this competition affects how many and what kind of exploits and tools become available on the darknet.

All in all, factors affecting darknet vandalism economy include both financial business and the way hackers organize themselves in communities. Public lists of tagged targets and published evidence give more motivation to vandals, combining the prospect of financial gain with social currency to support the ongoing success of online crime.



Global Cyber Vandalism Statistics

| Attackers | Team | Home Def. | Special Def. | Total Def. | Def.(Today) | Def.(Yesterday) |
|---|---|---|---|---|---|---|
| 20.812 | 11.922 | 6.603.791 | 613.603 | 7.492.265 | 1.606 | 4.472 |

Important Information

All the information contained in Defacer.ID Website Vandalism (Defacements) Archive were either collected online from public sources or directly notified anonymously to us. Defacer.ID is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Defacer.ID didn't produce them so we cannot be responsible for such contents. If you are the administrator of an hacked website which is mirrored in Defacer.ID, please note that Defacer.ID is not related at all with the defacements itself.

**We upgraded to better servers and will have NEW features coming out very soon! Defacer ID v2.0 loading...**

Most Active Website Hackers - Top Defacers

| Rank | Attacker | Team | Home Deface | Special Deface | Total Deface |
|---|---|---|---|---|---|
| 1 | ZeDD | RedDemons | 165.111 | 1 | 165.114 |
| 2 | Mr.Gus | BL4CKH4MM3R | 153.104 | 7 | 153.109 |
| 3 | Mr.Rvms | BL4CKH4MM3R | 150.335 | 10.200 | 150.474 |
| 4 | ./6IX9INE | Sora Cyber Team | 144.836 | 12.253 | 144.840 |
| 5 | MR.057 | KHINTIL TEAM | 141.358 | 58 | 141.525 |
| 6 | KimochiSenpai | Jembud Cyber Team | 131.057 | 2 | 131.066 |
| 7 | R33f=>>Kr12 | BangZat PhiSingeRs InDoNeSia | 129.158 | 7.509 | 129.161 |
| 8 | MR.H4R1-X | CYBER ARMY | 126.919 | 25.998 | 129.152 |
| 9 | Dz71 | Indonesian Security Team | 126.647 | 0 | 126.647 |
| 10 | Mr.TxT | Cyber Vortex | 126.021 | 14.206 | 126.051 |

**Figure 5** Darknet vandalism economy visualized through defacement counts and hacker rankings, emphasizing reputation and competitive behavior in underground communities

## 2.6. CMS Exploits in Circulation

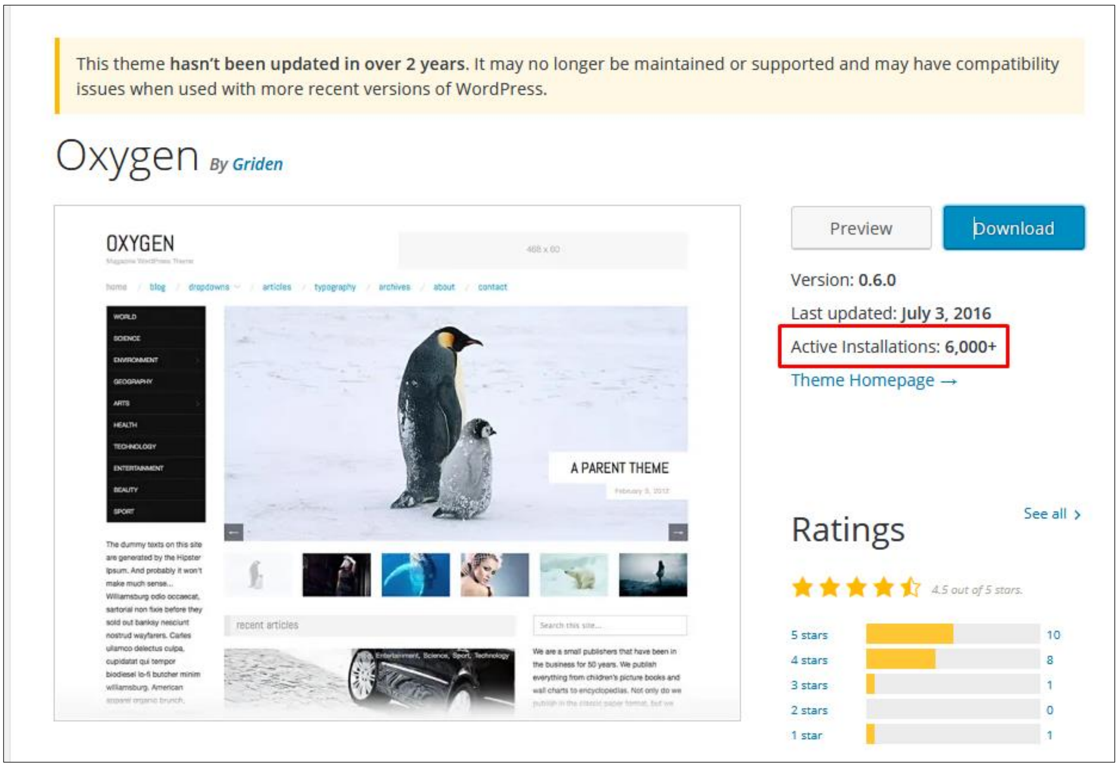
Due to how popular WordPress and similar systems are, as well as their use of multiple plugins and themes, they are now easy targets for cybercriminals. An important factor is ensuring old or no longer supported parts get the latest security fixes. The Oxygen WordPress theme, seen in Image 6, is a good example since it has more than 6,000 active users, but no updates have been made for over two years. Such subjects provide a significant chance for threat actors to take advantage of known flaws.

If themes or plugins become deprecated, their security problems are not fixed, so bots can scan and attack a huge number of websites in no time. Attackers take advantage of old components, using Bad Mode among other automated tools to scan for the versions of CMS and vulnerable plugins or themes so they can exploit them all at once. When themes such as Oxygen are not cared for, it allows hackers to use zero-day or known flaws.

Searching for these components is made easy by Google dorks that can be used with just a few keywords. Attackers usually gather a collection of sites with available vulnerabilities and leverage bots to attack them on a large scale, which very often leads to problems such as shell uploads, site defacement, or data breaches.

In addition, the importance of these events goes further than just causing damage. If a CMS platform is compromised, it can be exploited for attacks such as sending ransomware, collecting usernames, or moving into bigger networks. The large number of vulnerable themes makes it possible for many users to be vulnerable, making the risks caused by poor maintenance even greater.

All in all, old CMS themes such as Oxygen continue to be major risks for website security. They highlight the importance of applying updates quickly to avoid keeping open doors for those who try to exploit vulnerabilities.



This theme **hasn't been updated in over 2 years**. It may no longer be maintained or supported and may have compatibility issues when used with more recent versions of WordPress.

Oxygen *By Griden*

Version: **0.6.0**

Last updated: **July 3, 2016**

Active Installations: **6,000+**

Theme Homepage →

Ratings

4.5 out of 5 stars.

| | |
|---|---|
| 5 stars | 10 |
| 4 stars | 8 |
| 3 stars | 1 |
| 2 stars | 0 |
| 1 star | 1 |

**Figure 6** Example of an abandoned WordPress theme with thousands of active installations, highlighting common exploitation targets within CMS ecosystems

### 2.7. Dork-Based Discovery of Vulnerable Targets

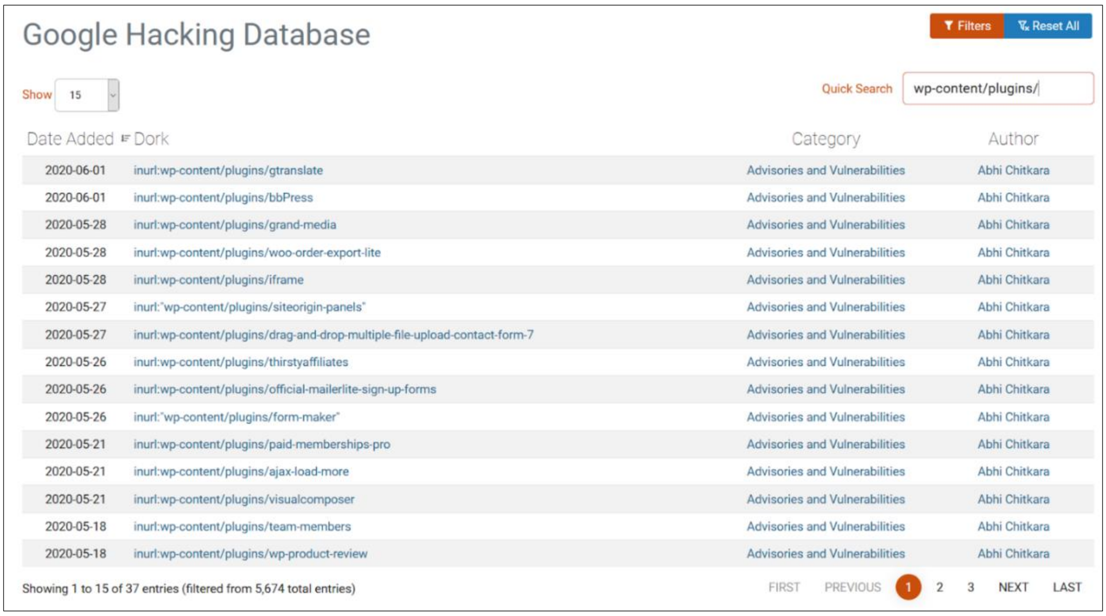
The rise of "Google dorks" has helped people search the internet more efficiently for targets that are vulnerable. Using this technique, attackers can quickly find out which components of a CMS can be used against WordPress plugins and themes. Image 7 demonstrates some active Google dorks that aim at wp-content/plugins/ and show how malicious users find vulnerable plugins to exploit.

With the help of these dorks, hackers are able to discover plugin folders linked to known security issues and set up long lists of people to target. For instance, searching with inurl:wp-content/plugins/gtranslate or inurl:wp-content/plugins/grand-media picks out plugins that have well-known security issues. The attackers make use of this knowledge to run routines and exploits against these particular websites.

The main benefit of using dorks is that they do not require complex reconnaissance. Rather than depending only on vulnerability scanners that could miss some parts of a target or operate slowly, attackers use search engines to find information on web assets that might be vulnerable. This helps find important targets that may be open to threats from outdated or poorly set up plugins much more easily.

It was indicated in the early research that bad mass exploitation bots perform a short search process, helping to easily scan, and break into insecure websites in large numbers. Looking at Image 7's Google Hacking Database, we realize that there are many plugins vulnerable to attacks.

Having these cases further reveals the need to update, secure, and isolate sensitive directories regularly. If these problems are not addressed, websites can be quickly attacked by simple automation tools, such as methods that dork.



Quick Search: wp-content/plugins/

| Date Added | Dork | Category | Author |
|---|---|---|---|
| 2020-06-01 | inurl:wp-content/plugins/gtranslate | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-06-01 | inurl:wp-content/plugins/bbPress | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-28 | inurl:wp-content/plugins/grand-media | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-28 | inurl:wp-content/plugins/woo-order-export-lite | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-28 | inurl:wp-content/plugins/iframe | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-27 | inurl:"wp-content/plugins/siteorigin-panels" | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-27 | inurl:wp-content/plugins/drag-and-drop-multiple-file-upload-contact-form-7 | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-26 | inurl:wp-content/plugins/thirstyaffiliates | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-26 | inurl:wp-content/plugins/official-mailerlite-sign-up-forms | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-26 | inurl:"wp-content/plugins/form-maker" | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-21 | inurl:wp-content/plugins/paid-memberships-pro | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-21 | inurl:wp-content/plugins/ajax-load-more | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-21 | inurl:wp-content/plugins/visualcomposer | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-18 | inurl:wp-content/plugins/team-members | Advisories and Vulnerabilities | Abhi Chitkara |
| 2020-05-18 | inurl:wp-content/plugins/wp-product-review | Advisories and Vulnerabilities | Abhi Chitkara |

Showing 1 to 15 of 37 entries (filtered from 5,674 total entries)

**Figure 7** Google dork queries used to locate vulnerable WordPress plugins, demonstrating how attackers efficiently discover exploitable sites

## 3. Methodology

### 3.1. Research Design

The study uses a descriptive-analytical research method to analyze how the darknet supports the use of zero-day exploits and automated attack tools. By studying available web archives and records of defacement, the research is able to detect patterns in cybercrime over various periods. The analysis is based on specific cases of different malicious software and botnets, such as Bad Mode and XKyubi. It enables us to look deeply into the technology and actions involved in cybercrime. Descriptive information covers how many exploits and bots are seen, and the analytical section interprets this data in terms of cybersecurity issues. It is easy to update the framework for this research, considering recent threats and constant shifts in darknet markets. As a result, the design makes it easier to see the link between exploits, how they are distributed, and the tactics of mass exploitation, which helps create better defense plans.

### 3.2. Data Collection

The information used for the study came from several open-source platforms and archives devoted to cybersecurity problems and exploit stores. Zone-H is an important archive, collecting records on millions of defacement incidents. A detailed list of known vulnerabilities and exploits can be found on Exploit-DB; GitHub has an array of free hacking tools and scripts for everyone; and Defacer.ID tracks any vandalism or activity by hackers. The Google Hacking Database was also useful in revealing which search queries attackers apply to find vulnerable websites. We used a combination of manual and automated approaches to examine bot behaviors, signatures of attacks, and patterns of vulnerabilities. Adopting this method made it possible to explore the abilities of bots and discover what can be automated in exploiting them. The data gathered covers several attack forms, popular CMS targets, and locations, supporting a detailed analysis of how mass hacking and exploit activity are carried out on the darknet.

### 3.3. Case Studies/Examples

*3.3.1. Case Study 1: The Bad Mode Bot – Yemen Routine for Mass Hacking*

The Bad Mode bot has developed significantly and is now made to attack multiple websites in amounts far greater than before. Constructed in Yemen, the bot relies on advanced means of producing IP addresses and listing subdomains, which enable it to look for a large number of potential victims at once. Rather than conducting reconnaissance manually, Bad Mode is able to rapidly check hundreds of IP addresses and related website subdomains to find out where WordPress or Joomla installations are left unguarded.

Bad Mode gets its strength mainly from automatically scanning for and using vulnerabilities. It checks the targets for a broad range of vulnerabilities by using a big library of well-established flaws found in popular CMS plugins and core parts. As soon as a vulnerable site is spotted, the bot begins to attack using vulnerability chaining. In this method, a series of exploits are used continuously during the same attack to skip past protections or raise access level, making it more likely that the attack will succeed.

Mostly, the bot takes advantage of vulnerabilities in WordPress and Joomla, such as old plugins, flaws in upload scripts, and flaws in placing content. It allows the attacker to carry out all the steps from checking for vulnerabilities to exploiting them and leaving a shell. If successful, an attacker will likely set up a web shell to allow them to access the server at any time over the internet. Hackers may exploit this access to change websites, take data, or make use of the server as a part of a large network of controlled computers.

Bad Mode is recognized for having advanced tools as well as managing activities on a huge scale. Because of automation, even those low on tech skills can use the bot to attack hundreds or thousands of sites each time. Although certain issues, for example, with function for HTTPS websites and false positive results, still exist, the popular tool is still successful due to its large user base and specialized techniques.

This bot was developed in an open way and connected to an APT group, which is a sign of a concerning trend. It is now easy for more people to access advanced hacking tools, not just members of special organizations. Because tools such as Bad Mode are readily available, more people can attempt cybercrime, putting poorly maintained websites at an increased risk.

All in all, the Bad Mode bot highlights how cyber vandalism has become something that happens on a large scale and is highly mechanized. By using large-scale scans, exploiting multiple security gaps, and self-deploying shells, the tools today are designed to increase the attack's impact with a minimal effort from the attackers. According to this case study, it is important to deal with patches immediately, manage CMS security better, and improve how such threats are detected.

#### *3.3.2. Case Study 2: The XKyubi Bot – Multi-CMS Vulnerability Chaining from Tunisia*

The XKyubi bot, made in Tunisia, shows how intelligent and smart cyberattack tools can now target many content management systems. Rather than focus on a specific CMS, XKyubi goes after vulnerabilities found in Joomla, WordPress, Drupal, and Prestashop. Its multi-platform nature helps it to compromise thousands of websites in a single burst of attacks.

The main reason XKyubi works so well is its advanced process for bedding down vulnerabilities in a chain. It means taking advantage of several vulnerabilities present in a CMS or its plugins, combining the exploits to get around security and increase access rights. Linking exploits together, XKyubi makes it possible to overcome defense systems that could stop just one exploit from succeeding. It exploits typical vulnerabilities that allow attackers to run code on remote servers, carry out SQL injection, allow file uploads, and display hidden configurations inside the CMS.

When a system is found to be vulnerable, XKyubi takes action and sets up web shells so hackers can still control the server even if users detect the attack. With this capability, actors can execute any commands they want and keep expanding their position. With XKyubi, it takes less time from the initial gathering of information to a full breach, so attack campaigns become larger and more organized.

With a modular design, XKyubi is able to use exploits for various CMS platforms, making it flexible for each target. Being flexible and assisting many platforms makes it powerful in the hands of internet criminals. It is able to detect old programs and unprotected weaknesses that happen regularly in CMS websites where security is not regularly managed.

Using the bot in actual scenarios points to the increased risk of multi-CMS exploit tools. It can carry out cyberattacks on multiple platforms even if the attackers do not have much technical expertise, raising the number of potential attackers. Also, as the report centers around well-known threats, it reveals how not applying patches in time can lead to serious issues in well-used CMS environments.

Ultimately, the XKyubi bot demonstrates how cyberattack tools are getting more flexible, automated, and efficient. Being able to use multiple types of CMSs and add shells for command execution allows attackers to compromise a lot of sites and continue doing so. In light of this example, we should make sure that all CMS platforms use proper security measures to address the rising danger from flexible automated attacks.

### 3.4. Evaluation Metrics

To determine their effectiveness, a thorough examination from different angles is needed. An important factor to look at is the number of vulnerable sites that are exposed and able to be exploited. This means computing the number of websites that run outdated CMSs, unprotected plugins, and old themes, as these are targetable by bots. A bigger pool means a larger group can be attacked with an automated system.

Bot efficiency is another important measure that shows the ratio of success to failures while trying to exploit a device. This evaluates how accurately the bot detects risks and place payloads without any mistaking or faults. Better efficiency allows the bot to hit its target with more precision and exploit it better, straightly influencing its effect.

Finally, exploit longevity sees to what extent an active vulnerability can be used by attackers. A vulnerability such as CVE-2015-8562 in Joomla is still used because many have not patched it and a lot are still using the unprotected versions. With longer-lasting exploits, there is a bigger chance for malicious software to target a device. Taken together, they show the full impact of bots and can direct how defenses are put into place.

## 4. Darknet play important role in hosting trade of exploits

### 4.1. Marketplace Structures

They are carefully built systems that make it possible for buyers and sellers to trade securely and anonymously. The forums in these marketplaces allow people to talk about security vulnerabilities, reveal exploits, and offer assistance in technical matters. Because buyers and sellers cannot confirm the other’s identity, escrow services are used in marketplaces to hold the payment until the buyer confirms getting the exploit or tool, thus protecting from possible fraud. One more important aspect is the given reputation score that rates how dependable sellers have been according to their feedback and past sales. These rankings increase buyers’ confidence and inspire sellers to keep their goods and services up to par. Access in the market may be tiered so that higher-level users can get access to unique details about zero-day attacks. Forums provide threat actors with an opportunity to collaborate and inform each other. On the whole, this combination forms a risk-controlled system for the buy and sell of zero-day exploits and hacking tools.

### 4.2. Zero-Day Pricing Models

Darknet marketplaces set prices for zero-day exploits based on a number of main factors. The kind of target is very important. Microsoft Windows or well-known CMS exploits may be sold for more on the black market because they can be used by many users. Pricing depends on the quality of exploits, so those that bypass detection and give full remote access to systems are worth more than other less powerful vulnerabilities. Additionally, uniqueness is paramount; A zero-day that is not well known and has not been repaired can be very expensive, particularly if it is kept hidden. Another important factor to keep in mind is how hard the exploit is to carry out, what knowledge is needed, and if it could help in a more significant attack. Prices may rise when time is a key factor since an urgent exploit is needed. On the whole, the process of setting price depends on the technical details, potential effects, and rarity, resulting in a market where potential buyers consider the risks and pros together with the cost.

### 4.3. Exploit Distribution and Tool Bundling

Attackers often gather a variety of attack tools together in order to exploit distribution on the darknet. These groups of bots have vulnerability scanners, exploit modules, and web shells for use after a successful attack. By bundling tools, threat actors make it possible for their tools to be easily operated by people with limited technical skill. Many packages use techniques to hide their code logic and behavior, so signature-based defenses find it harder to detect and analyze them. Toolkits from vendors are often updated regularly to take advantage of newly exposed weaknesses, stay compatible after systems are patched, and overcome security measures. This way of working means the set of tools can be effective even when there are changes in individual attacks. Thanks to the convenience and strength of bundled tools, more and more people are using them, making it much faster and easier for cyberattacks to take place.

The introduction of ways to share Kits such as Telegram, Discord, and leaked Kits played a big role.

In the past few years, exploits are more likely to be traded on Telegram and Discord than on public forums and online marketplaces. Because of the group features and encrypted messages, sellers can now talk to buyers in a more confidential and prompt manner. This movement makes the business safer from law enforcement and its competitors. So, such platforms assist in fast sharing of leaked exploit kits and zero-days with the groups they address. It is now easy for threat actors to get access, and they can work together quickly using real-time communication. The shift from talking in public forums to closed messaging highlights the growing preference for networks that are not tied to any particular organization, help criminals trust each other, and protect their privacy.

## 5. Security implications and defense strategies

### 5.1. Threat to CMS-Based Infrastructure

Large numbers of websites across the globe are powered by Content Management Systems, such as WordPress, Joomla, and Drupal. Since they are used so much, they become targets for cybercriminals. Since there are so many third-party plugins and themes available, the attack surface can get very large, and many of their components may not be updated or patched. With these weak points, attackers can unlawfully enter a site, put destructive code into it, or deface the site's pages. These targets are mainly CMS-based because bots and exploit kits make use of known issues to ramp up their attacks. Data breaches, website downtime, damaged reputation, and way for further attacks are some of the major risks in case of a compromised CMS. As a result of being widely used by many organizations and people, these CMS platforms are important to secure due to the high risk of vulnerabilities affecting large groups.

### 5.2. Limitations of Current Defense Mechanisms

There are several problems with the defenses being used against web-based attacks. Such antivirus programs are not able to identify every new or hidden exploit, so systems remain vulnerable to zero-day attacks. When patch management takes time, the problem gets worse, as the unpatched vulnerabilities can be exploited for some time after fixes are made. Sometimes, Web Application Firewalls (WAFs) cannot detect all the threats in the latest payloads and multi-stage attacks. Besides, several organizations do not have good processes for tracking attacks or reacting to threats, which makes it harder for them to address such issues in a timely manner. This makes it easy for automated tools and botnets to work without much resistance. Defense should focus on active steps to detect and stop dangers even before they can harm anyone.

### 5.3. Proactive Monitoring Approaches

It is important to use proactive monitoring methods to address new threats. Using dork alerting, defenders try to spot queries that suggest a website is at risk and act in advance before the site is attacked. With honeypots in place, you can find out about possible attacks early and understand the attacker's methods. Exploit trend mapping also records the spread and popularity of exploits, which allows security teams to get an early warning about new threats. They add to regular defenses, by offering intelligence and awareness, helping organizations to better plan how to improve their security. Being aware of the signs can help companies react faster, preventing more harm from an attack.

### 5.4. Importance of Public Vulnerability Databases

WPVulnDB, CVEDetails, and the Google Hacking Database are important in improving cybersecurity. Here, anyone involved in security can check in-depth details about reported vulnerabilities in a central spot, including how serious they are, which programs are influenced, and whether patches are available. WPVulnDB is used to cover WordPress vulnerabilities, especially the information website owners need about plugins. CVEDetails pulls together all the important Common Vulnerabilities and Exposures findings from various platforms. Attackers can use the search queries in the Google Hacking Database to find leaks in vulnerable systems. By being open to the public, these databases ensure others can learn from them and use this knowledge to stay secure. Because of them, it is easier for the community to learn about and tackle vulnerabilities at an early stage, helping lessen how much time is left for them to be used.

### 5.5. Teaching people and spreading awareness about the problem

A cybersecurity strategy should focus on informing and educating people in the community. By supporting these activities, security workers become better at defending their systems against potential threats. Programs focused on development teams highlight the need for secure coding, timely patching, and made-to-order vulnerability communication. If administrators can notice the first signs and keep their CMS updated, the probability of being exploited decreases. When everyone in the community knows what to do, they are more likely to work together, pass along information, and take action for security. Overall, focusing on education makes everyone in the organization more involved in keeping the system secure.

## 6. Conclusion

### 6.1. Summary of Key Points

This study highlights the critical role of the darknet in facilitating the distribution of mass exploitation kits and zero-day vulnerabilities.. Thanks to its method of operation, darknet marketplaces enable malicious actors to buy and exploit unknown problems in software with little delay. Such attack tools as Bad Mode and XKyubi make it possible for hackers to quickly and widely exploit and take control of malfunctioning CMS platforms. Thanks to these bots, steps such as scanning, exploiting vulnerabilities, and placing a shell for future actions can be performed by many people at once. Looking at the results in defacement archives and attack trend charts confirms that bot-based cyberattacks are still a big and constant threat. Sophisticated attackers now keep their actions hidden and make use of technology, focusing on large-scale and rapid methods. Unaddressed and unshielded weak parts in CMS leave a company at high risk. On the whole, the study suggests that more robust cybersecurity measures are needed to stop mass exploitation from the darknet.

### 6.2. Future Directions

The focus of future cybersecurity strategies needs to include handling cyber threats fueled by darknet and the use of automated attackers. Improving how exploits are investigated on the darknet can increase transparency and allow for identifying which exploits are reliable and which are not. By using AI, it is possible to predict threats and observe the actions of attackers quickly, speeding up defenses against new attacks. It is important for policies to drive businesses to amend their devices in line with stronger CMS guidelines and to plug security gaps quickly. Stricter monitoring of the darknet helps to spot and stop exploits from being shared before major incidents occur. Working together, industry, academia, and government bodies will help create effective strategies that bring together new technologies, laws, and knowledge in society. These directions aim to improve our ability to defend against cyberattacks that are launched in an automated and hidden way from the darknet.

## References

[1] Anjum, A., Kaur, D. C., Kondapalli, S., Hussain, M. A., Begum, A. U., Hassen, S. M., Adam Boush, D. M. S., Benjeed, A. O. S., and Osman Abdalraheem, D. M. H. (2021, December 20). A mysterious and darkside of the darknet: A qualitative study. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167244

[2] Besenyő, J., and Gulyas, A. (2021). The effect of the dark web on the security. Journal of Security and Sustainability Issues, 11, Article 7. https://doi.org/10.47459/jssi.2021.11.7

[3] Brooks, R. R., Yu, L., Ozcelik, I., Oakley, J., and Tusing, N. (2022). Distributed Denial of Service (DDoS): A history. IEEE Annals of the History of Computing, 44(2), 44–54. https://doi.org/10.1109/MAHC.2021.3072582

[4] Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(6). https://doi.org/10.1007/s12103-021-09652-7

[5] Meland, P. H., Bayoumy, Y. F. F., and Sindre, G. (2020). The ransomware-as-a-service economy within the darknet. Computers and Security, 92, 101762. https://doi.org/10.1016/j.cose.2020.101762

[6] Sutanrikulu, A., Czajkowska, S., and Grossklags, J. (2020). Analysis of darknet market activity as a country-specific, socio-economic and technological phenomenon. In 2020 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1–10). Boston, MA, USA. https://doi.org/10.1109/eCrime51433.2020.9493259

[7] Zhou, G., Zhuge, J., Fan, Y., Du, K., and Lu, S. (2020). A market in dream: The rapid development of anonymous cybercrime. Mobile Networks and Applications, 25(1), 259–270. https://doi.org/10.1007/s11036-019-01440-2