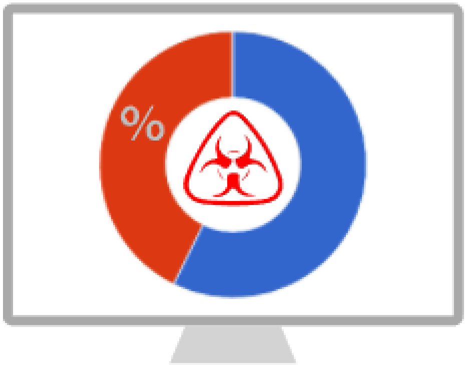
QUTTERA

ANNUAL WEBSITE MALWARE REPORT

2016

Quttera | Linked in

The data in this report provides insights on online threats in websites that were detected by Quttera automated tools and analysed by malware research team.



January 2017

Introduction

Internet technology is rapidly evolving making it much easier for both individuals and organizations to create websites and to upload their unique content in a blaze. Content Management Systems (CMS), Website in a Click services, shared hosting, and other services allow to get online almost with no effort and with minimum budget. And with the Internet of things (IoT) in the doorway, nearly every aspect of the business and personal life gets connected to the web to communicate, merchandise, exchange, provide service, etc.

On the other hand, the more data is there, - the more profit can online criminals potentially gain if they can access it illegally. Malware industry is building powerful back-end infrastructure to launch sophisticated malicious campaigns and by-pass the detection mechanisms. Online security and malware protection are the essential components of the reputable and safe business. Hence, to keep up with the pace, malware research and forensics platforms are required to process an enormous amount of data non-stop to prepare tools and methods capable of identifying and removing every new infection types and variants.

CVE Per CMS Platform

In 2016 the following vulnerabilities have been filed against top 6 Content Management Systems (CMS):

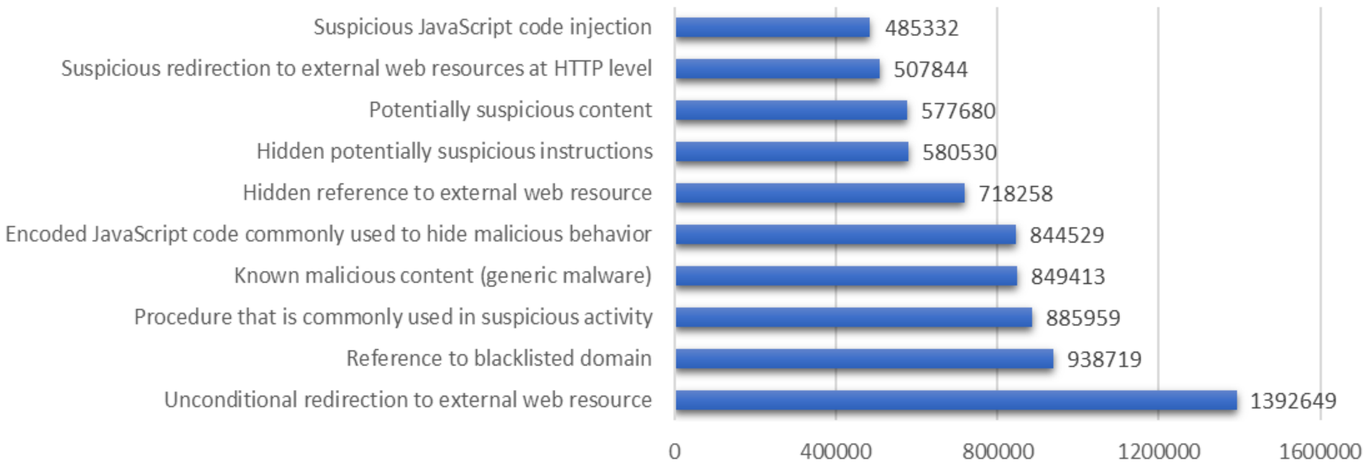
CMS	# CVE reported	Search string
WordPress	37	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress
MODX	31	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modx
Drupal	24	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=drupal
Joomla!	8	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=joomla
vBulletin	2	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vbulletin
Magento	1	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=magento

The 2016 Year Website Malware in Details | Q1 – Q4

The table below is the overall detection statistics per the threat type.

Threat Type	Q1	Q2	Q3	Q4
Encoded JavaScript code commonly used to hide malicious behavior	199,746	275,647	126,325	242,811
Reference to blacklisted domain	148,883	196,783	297,921	295,132
Potentially suspicious content	113,476	152,723	147,715	163,766
Hidden potentially suspicious instructions	144,743	147,485	142,311	145,991
Hidden reference to external web resource	133,530	130,764	231,952	222,012
Suspicious JavaScript code injection	123,008	127,540	118,674	116,110
Suspicious redirection to external web resources at HTTP level	119,319	126,612	126,465	135,448
Unconditional redirection to external web resource	321,204	425,405	325,544	320,496
Procedure that is commonly used in suspicious activity	220,119	220,690	221,801	223,349
Encoded JavaScript code commonly used to hide suspicious behavior	113,189	117,532	122,276	131,569
Malicious PHP content	29,165	29,165	29,428	29,934
Drive-by-download attack	12,281	14,166	14,067	16,595
URL generated during page execution	14,993	14,151	13,133	14,369
Known malicious content (generic malware)	212,455	212,304	211,850	212,804
Suspicious PHP content	111,438	111,527	111,466	111,288
Suspicious function call	1,851	11,350	1,837	11,606
Malicious hidden iframe	4,445	41,510	4,477	4,280
Suspicious PHP decoder	3,377	3,407	3,356	3,461
Suspicious execution behavior	8,830	1,106	12,728	12,640
Modified PDF format	758	773	960	891
JavaScript requires unreasonable amount of memory	1,133	1,168	1,193	1,131
PDF file containing potentially suspicious embedded file	2,136	2,430	2,734	2,837
Sequence of operations that is commonly used in suspicious activity	2,719	2,517	2,916	2,867
Malicious SPAM/SEO content	-	3,753	4,815	4,372

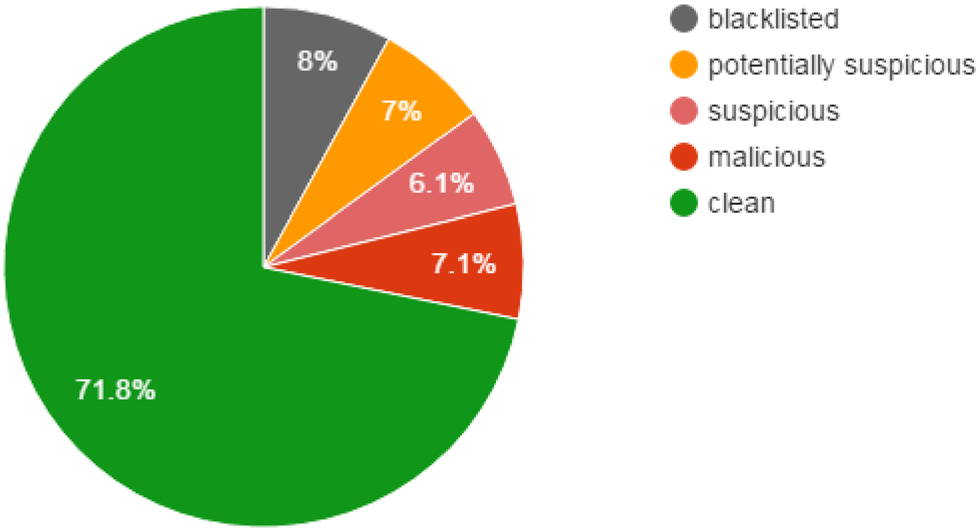
TOP 10 Online Threats



Website Severity Report

Currently, we assign severity status to a scanned domain / URL based on the detected components and their level of maliciousness to a website visitor. Ranging from Potentially Suspicious to Malicious these groups allow to estimate the immediate danger that the detected code imposes and the possibility of the False Positive. The data in this report applies to the defined/limited sample and it has been checked and verified both manually and using automated tools.

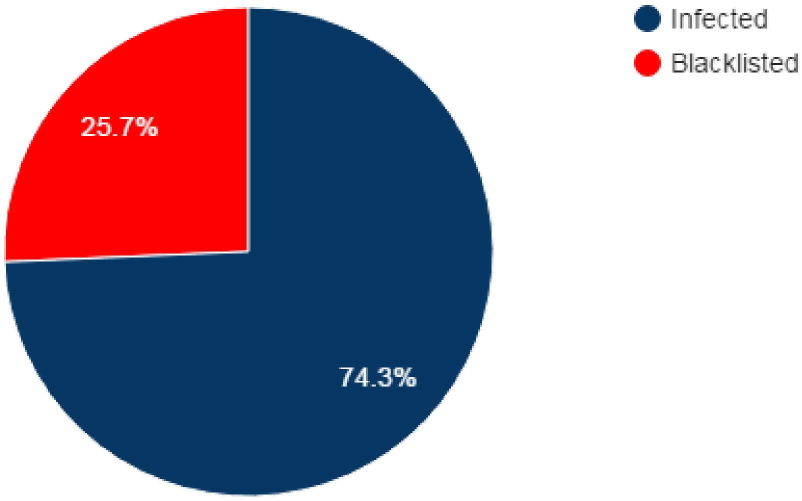
2016 | WEBSITE SEVERITY REPORT (Sample: 1,598,684 websites)



Blacklisting Report

Almost each search engine provider and security vendor manage blacklisting mechanisms. It is used to protect the customer and block the dangerous content from being accessed. In this section, we compared the blacklisting coverage against the active threat on the processed website.

2016 | 74.3% OF THE INFECTED WEBSITES WERE NOT BLOCKED BY ANY OF THE SECURITY PROVIDERS OR SEARCH ENGINES

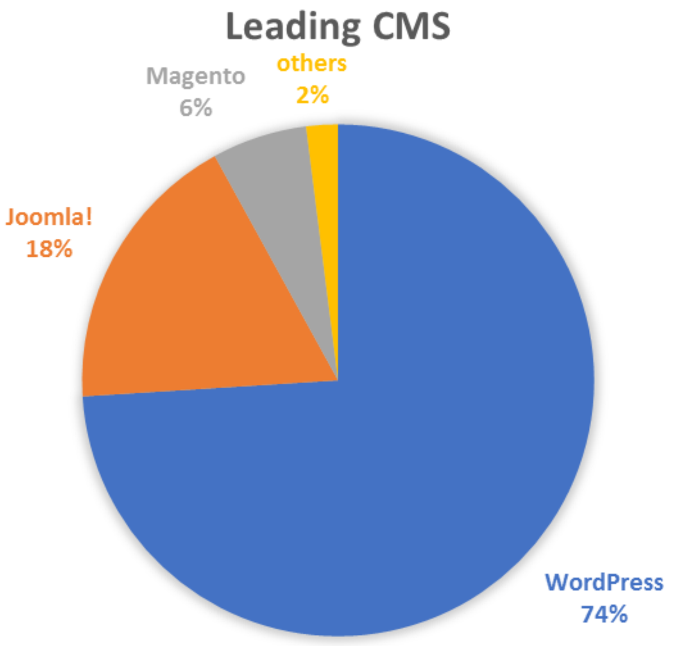


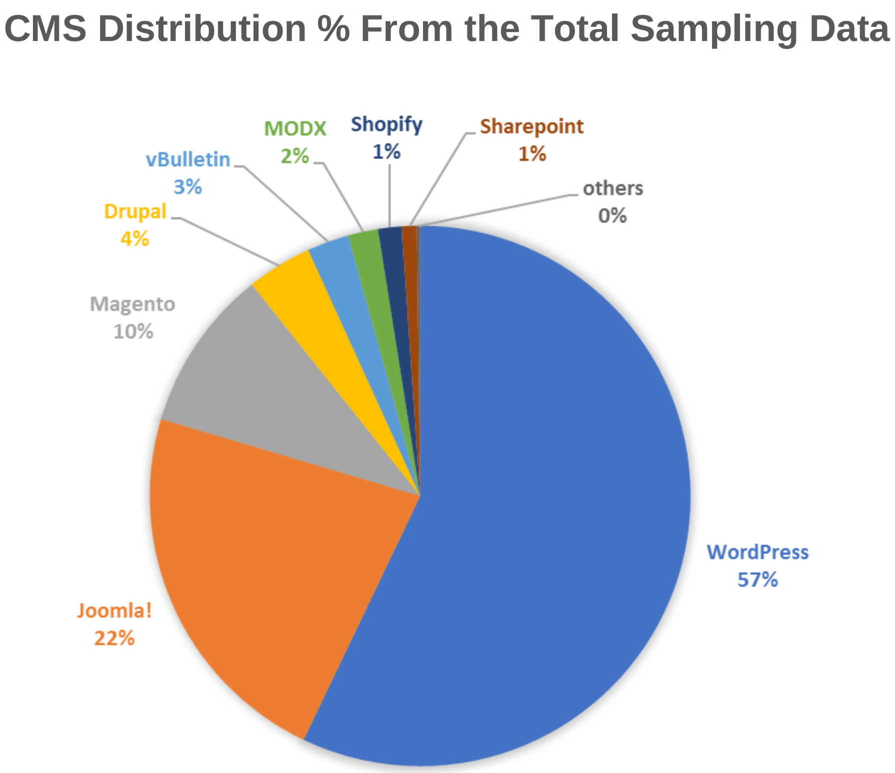
Hacking Report

The data in this section is based on the malware investigation and removal from the customers' websites during the year 2016.

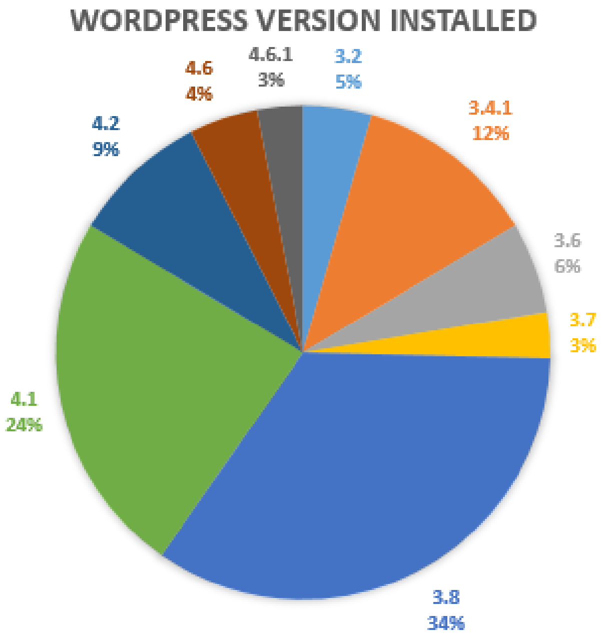
CMS Analysis

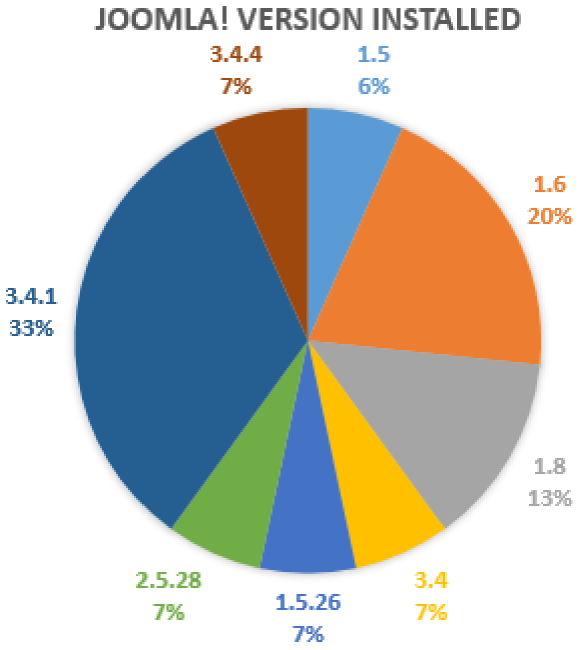
Leading platforms among the infected websites that use Content Management System (CMS) were WordPress (WP), Joomla! and Magento.

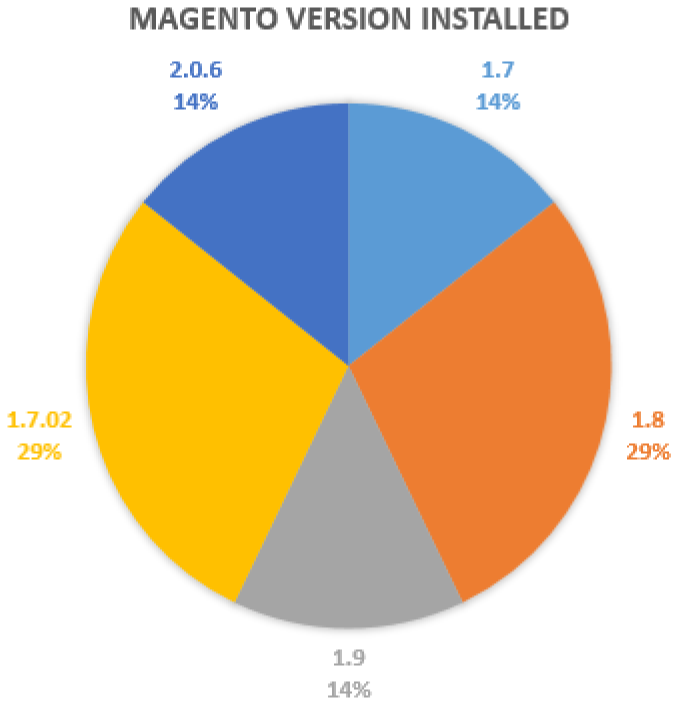




One of the common reasons of the hacking and, especially, the re-infection is the exploitation of the vulnerable and outdated version of the software and components such as plugins, themes, templates modules and other third-party components. The same applies to the CMS installations. Below are insights on the versions of the CMS as detected by our researchers at the time the website was already compromised.







Malware Incidents Insight

In this section, we outline some of the various exploitation vectors and malware types that were detected by our tools and removed by the incident response team during 2016.

SUPEE-5344

Magento based websites compromised due to the vulnerability in the installed version of the CMS.

A remote code execution (RCE) vulnerability known as the “shoplift bug” that allowed hackers to obtain Admin access to a store.
More info: https://magento.com/security/patches/supee-5344---shoplift-bug-patch

SUPEE-5994

Magento based websites compromised due to one or more vulnerabilities in the installed version of the CMS.
More info: https://magento.com/security/patches/supee-5994

SUPEE-6285

Magento based websites compromised due to one or more vulnerabilities in the installed version of the CMS.
More info: https://magento.com/security/patches/supee-6285

SUPEE-6482

Magento based websites compromised due to one or more vulnerabilities in the installed version of the CMS.
More info: https://magento.com/security/patches/supee-6482

SUPEE-6788

Magento based websites compromised due to one or more vulnerabilities in the installed version of the CMS.
More info: https://magento.com/security/patches/supee-6788

Culprit bot network

Website was a part of the Culprit bot network.

FilesMan infection

Website infected with the FilesMan backdoor malware that allows hacker to access and modify compromised site.
More info:

- https://blog.quttera.com/post/filesman-backdoor-malware-on-your-computer/
- https://blog.quttera.com/post/deobfuscation-made-easy-with-malware-decoder/

Ultimate VC Add-ons

Infection planted into the plugin files (*Trojan and others*) allowed hackers to send Spam and distribute infection.

SPAM

Among the other Spam campaigns occurred in 2016 these two stand out for their scale and ability to survive the standard security measures:

- Self-Recovering Spam Bot (more info: https://blog.quttera.com/post/self-recovering-spam-bot-launched-exploitation-from-entire-ip-sub-network/)
- Self-Recovering Black SEO & Spam Targeting WordPress (more info: https://blog.quttera.com/post/self-recovering-black-seo-spam-infection-hits-wordpress-setups/)

CVE-2015-8526

Joomla! vulnerability that allowed remote attackers to conduct PHP object injection and execute arbitrary PHP code via the HTTP.
More info: https://www.cvedetails.com/cve/CVE-2015-8562/#metasploit

Ransomware

Website infected with the *Win32/Wadhrama.A* ransoware infection
More info: https://blog.quttera.com/post/instant-ransomware-for-unpatched-websites/

Summary

The data in this report has been carefully checked and verified to give you the numerical insights on the scale of the infection being spread through the websites. We are working closely with hosting companies, security vendors and website management companies to help webmasters running safe and malware-free sites.

Links

ThreatSign – Website Anti-Malware Platform

Website Malware Scanner - API

Partnership

For more info on Quttera technology, products and services: https://quttera.com

Connect with Quttera on:

- Blog
- Twitter
- Facebook
- YouTube