# WORDPRESS ATTACKS

KATIE ELIAS & CRISTINA COLLAZOS

## OVERVIEW OF FINDINGS

WORDPRESS ATTACKS ARE MORE PREVALENT THAN EVER. THROUGH A CONTROLLED ENVIRONMENT, WE EXPLORED SUCH VULNERABILITIES AND ATTACKED WORDPRESS WEAK POINTS IN OUR VICTIM MACHINE. WE FOUND THAT MOST ATTACKS COULD HAVE BEEN PREVENTED THROUGH UPDATES & PATCHES. HOWEVER, BEST PRACTICES IN ACCESS CONTROL COULD HAVE ALSO MITIGATED THE DAMAGE.

**84%**
Security vulnerabilities on the internet that result in cross-site scripting or XSS attacks

**41%**
WordPress attacks caused by a vulnerability on the hosting platform

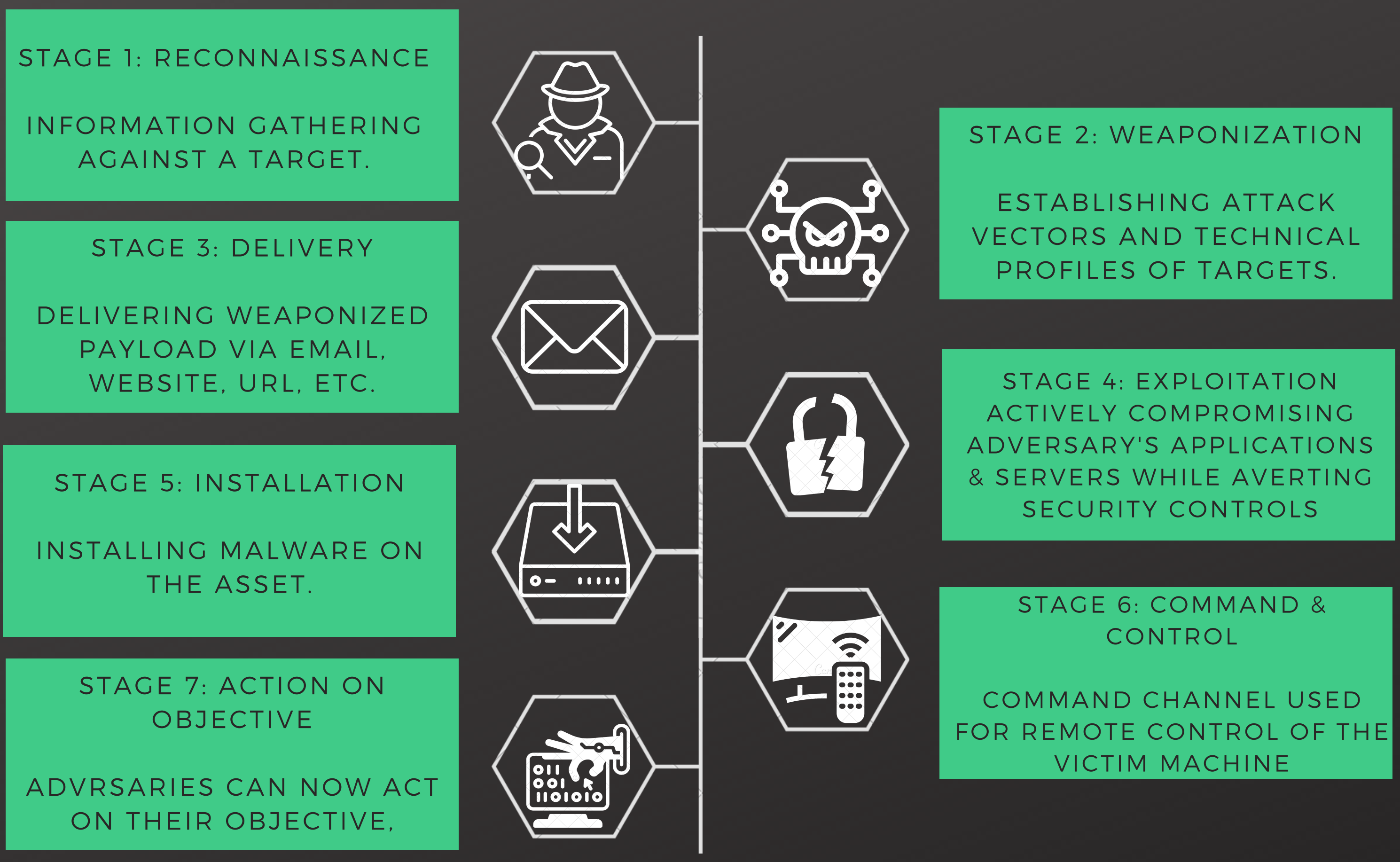
**52%**
WordPress vulnerabilities related to WordPress plugins

ACTIVE WORDPRESS WEBSITES

**1.3 Billion**

**44% OF HACKING** WAS CAUSED BY OUTDATED WORDPRESS SITES

## CYBER KILL CHAIN



STAGE 1: RECONNAISSANCE

INFORMATION GATHERING AGAINST A TARGET.

STAGE 2: WEAPONIZATION

ESTABLISHING ATTACK VECTORS AND TECHNICAL PROFILES OF TARGETS.

STAGE 3: DELIVERY

DELIVERING WEAPONIZED PAYLOAD VIA EMAIL, WEBSITE, URL, ETC.

STAGE 4: EXPLOITATION
ACTIVELY COMPROMISING ADVERSARY'S APPLICATIONS & SERVERS WHILE AVERTING SECURITY CONTROLS

STAGE 5: INSTALLATION

INSTALLING MALWARE ON THE ASSET.

STAGE 6: COMMAND & CONTROL

COMMAND CHANNEL USED FOR REMOTE CONTROL OF THE VICTIM MACHINE

STAGE 7: ACTION ON OBJECTIVE

ADVRSARIES CAN NOW ACT ON THEIR OBJECTIVE.

## VULNERABILITIES

Wordpress Enumeration

Open and unrestricted ssh access via port 22

Weak password security

SQL backup of database in a directory with unrestricted access

Unrestricted access to Wordpress directories

Escalated root privileges with the use of a python script

Brute-forceable URL directories and files

Netcat reverse shell/remote execution vulnerability

## MITIGATION STRATEGIES

Update Wordpress version and disable xmlrpc.php

Monitor and alert when SSH Port 22 is accessed by unauthorized users.

Harden password policy and error handling reporting to mitigate attempts at reconnaissance and brute force.

Monitor server traffic and alert for unauthorized attempts to access SQL Database.

Monitor and alert for attempts to use “root access” as well as “super-doer” activity.

Remove php file from root of WordPress folder and disable the plug-in for XML-RPC from all IPs with exceptions

## ABOUT THE LOCKHEED MARTIN CYBER KILL CHAIN

INSPIRED BY A MILITARY MODEL, LOCKHEED MARTIN DEVELOPED THE CYBER KILL CHAIN AS A STRUCTURED FRAMEWORK TO CLASSIFY, DEVELOP AN ATTACK VECTOR, ENGAGE, AND DISMANTLE A TARGET. THIS FRAMEWORK DETERMINES WHAT STEPS ATTACKERS MUST ACCOMPLISH IN ORDER TO CARRY OUT THEIR OBJECTIVES.

**SOURCES:** HTTPS://KINSTA.COM/BLOG/WORDPRESS-STATISTICS/
HTTPS://WWW.WHOISHOSTINGTHIS.COM/COMPARE/WORDPRESS/STATS/