Werde Digital.at

ABC

Weblogs in Gefahr – Sicherheits-Tipps für den WordPress Blog

WPROTECT

www.wprotect.de

Werde
Digital.at

Österreichische Blogger-Konferenz
am 22. und 23. April 2016 in Linz

www.abcstar.at

WordPress & Webserver
Sicherheitslösungen

www.wprotect.de

Karim-Patrick Bannour

WPROTECT

viermalvier.at
Social Multi Media

WPROTECT

MarktPlatz

Aktuelle Bedrohungen

WPROTECT

DDoS-Attacke um Website lahmzulegen

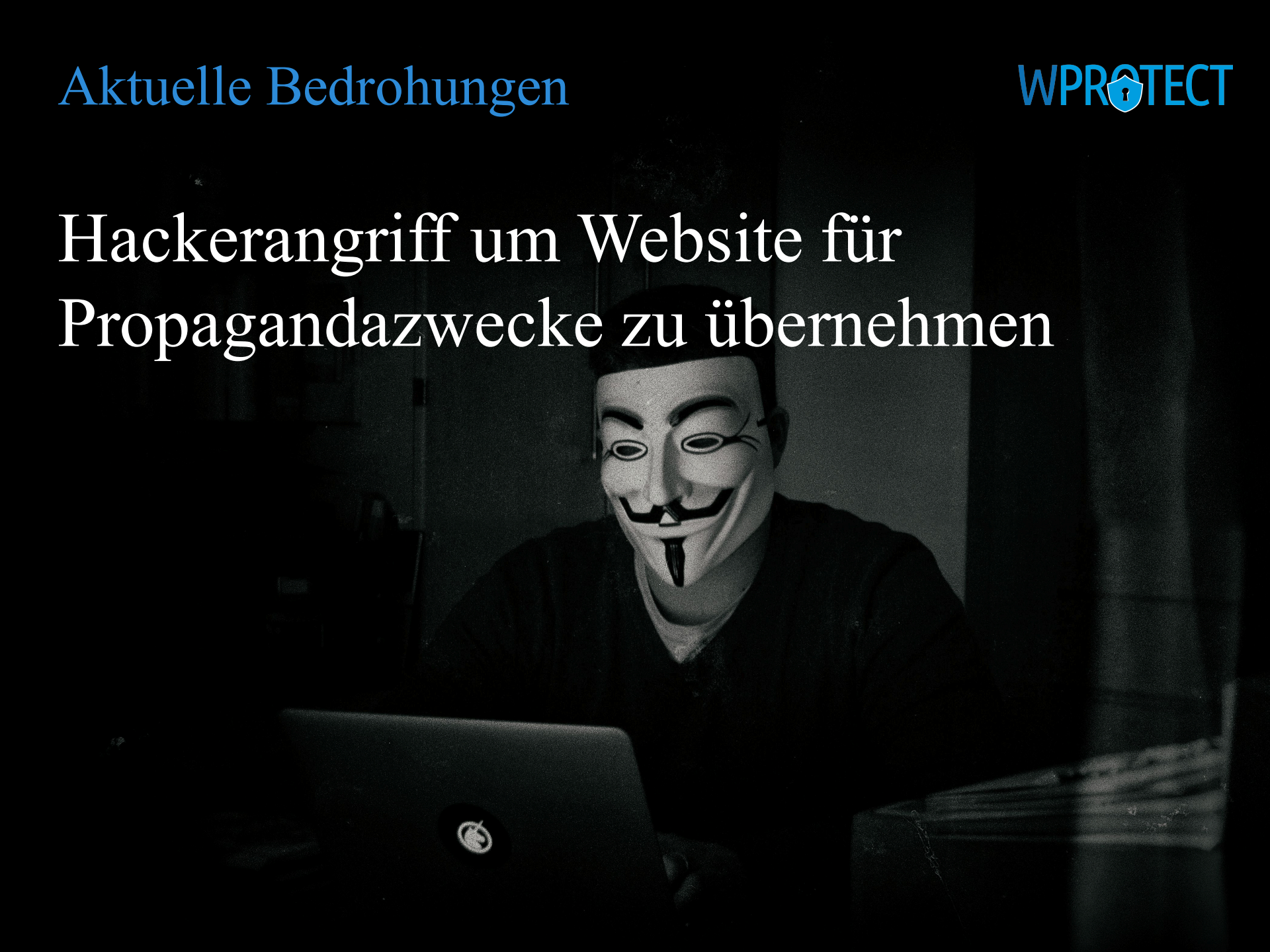
Aktuelle Bedrohungen

WPROTECT

Hackerangriff um Daten zu stehlen/verschlüsseln

WPROTECT

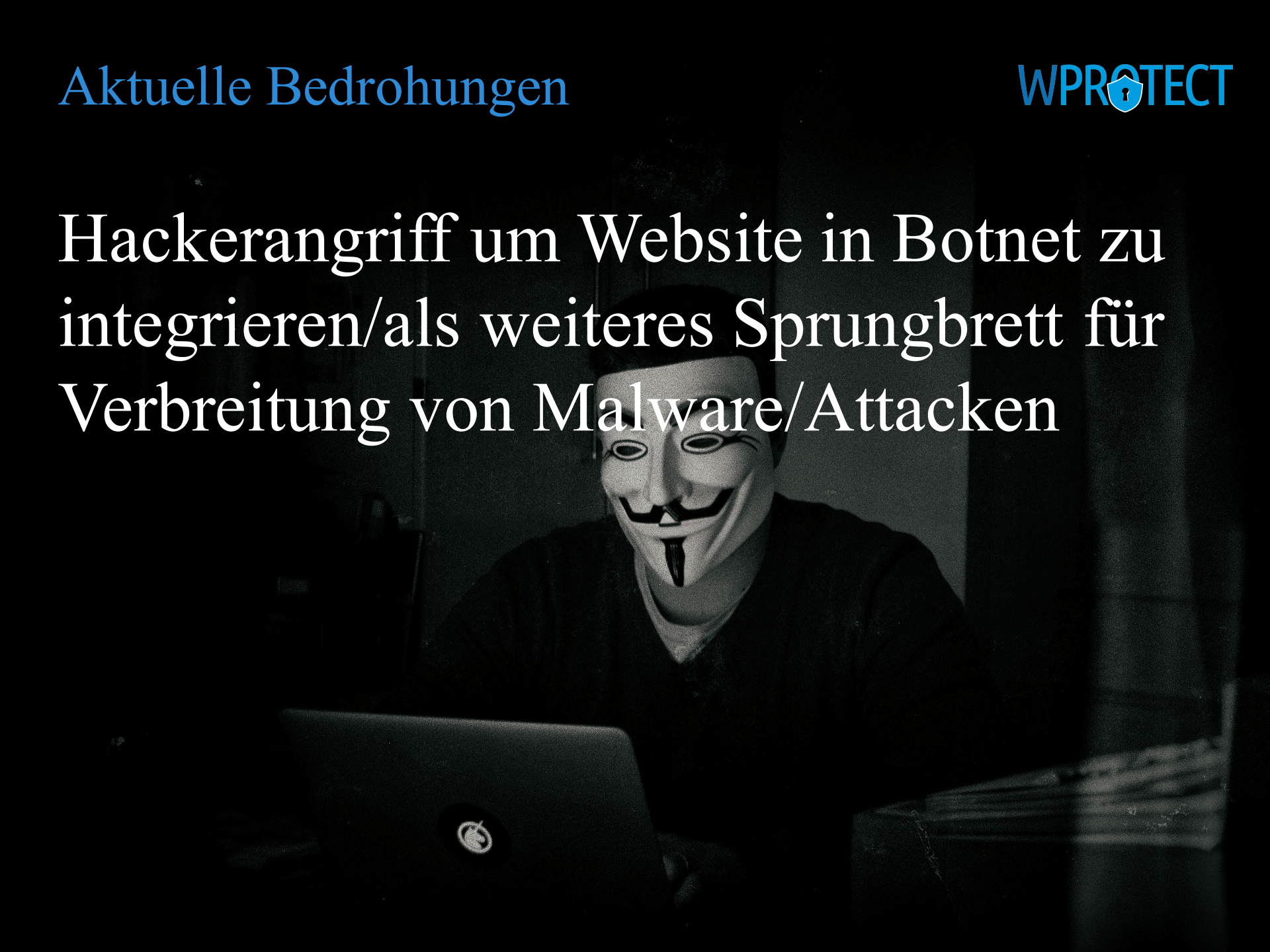
Hackerangriff um Website für Propagandazwecke zu übernehmen



Aktuelle Bedrohungen

WPROTECT

Hackerangriff um Website in Botnet zu integrieren/als weiteres Sprungbrett für Verbreitung von Malware/Attacken



WordPress Verbreitung

WPROTECT

Rund 60% aller auswertbaren Websites nutzen WordPress als CMS

Einfach zu installieren, zu warten und redaktionell zu betreuen

Cyberrisk

WPROTECT

Jedes 2. Unternehmen berichtete in diversen Umfragen, dass es bereits angegriffen wurde

Aktuelles Beispiel

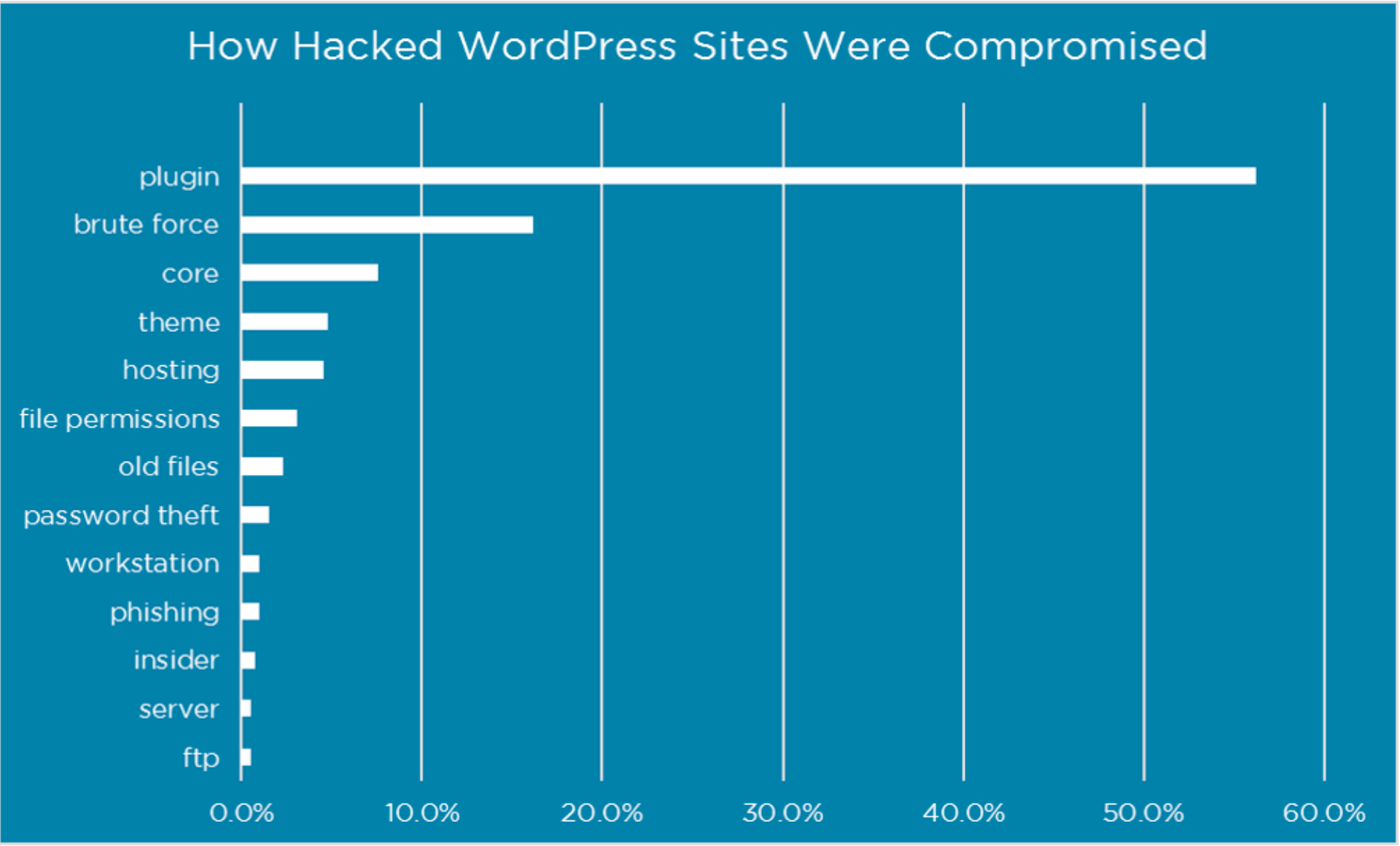
WPROTECT

Nicht aktualisieres/defektes WordPress-Plugin war ein wichtiger Angriffsvektor im Fall „Panama Papers“

https://www.wordfence.com/blog/2016/04/panama-papers-wordpress-email-connection/

WordPress Sicherheitslücken

WPROTECT



Quelle: WordFence Blog https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

WPROTECT

Tipps für mehr Sicherheit

Benutzerverwaltung

WPROTECT

- Keine Standarduser „admin“, ...
- Anzahl Admins beschränken
- Rechte sorgsam vergeben
- Autoren sollten nicht Admins sein

WordPress-Version

WPROTECT

- WordPress-Version verschleiern

Datenbank

WPROTECT

- Präfix ändern (Standard: wp_)
- Zugriff beschränken auf localhost oder bestimmte IP

Sichere Passwörter

WPROTECT

- Verwenden Sie nur sichere Passwörter (mindestens 10 Zeichen) und diese nur 1x pro Service

Beispiel: „2016 habe ich sehr viel über Wordpress Sicherheit gelernt!“

2016hisvüWSg!

Sichere Passwörter

WPROTECT

- Noch besser: Lange Passwörter über 20 Zeichen, noch schwerer zu hacken!
- Unzusammenhängende Wörter, ohne Bezug zur Website oder Autor/Admin

Stromquarantänefenstersitzung

Login

WPROTECT

- Zugriff sperren durch Verzeichnisschutz und Verschieben der login.php
- Zugriff auf /admin durch htaccess limitieren
- Dateirechte 644 und Verzeichnisse 755

Datenverkehr überwachen

WPROTECT

- Überwachen Sie Zugriffe, Netzwerktraffic usw. und setzen Sie Limits
- DDoS-Attacken und Trafficspitzen z. B. abfedern mit Cloudflare

FTP

WPROTECT

- Sichere Passwörter verwenden
- FTP-User und deren Rechte beschränken

PC sauber halten

WPROTECT

- Regelmäßige Scans mit aktueller Antiviren-Antimalware-Software

Antispam

WPROTECT

- Spamkommentare verhindern z. B. mit Antispam Bee

Loginversuche limitieren

WPROTECT

- Login mit falschem Passwort auf 3-5 Versuche einschränken, dann Sperre
- „Passwort zurücksetzen“-Funktion einschränken bzw. protokollieren

Plugin-Tipp:

- WordFence
- Limit Login Attempts

2-Faktor-Authentifizierung

WPROTECT

- Login

Malware-Scanner nutzen

WPROTECT

- Regelmäßig Scans auf Malware und Security Issues durchführen

Plugin-Tipps

- Sucuri
- Anti-Malware Scanner EMS

Google Search Console

WPROTECT

- Ehemals Google Webmaster Tools
- Schickt E-Mails wenn Malwareverdacht oder anderes Problem

Plugins sorgsam auswählen

WPROTECT

- So wenig Plugins wie möglich
- Wenn dann
  - von bekannten Entwicklern
  - regelmäßig aktualisiert
  - kompatibel mit der WP-Version
  - gut bewertet
  - hohe Installationsrate

Backups

WPROTECT

- Regelmäßig Backups machen (serverseitig oder Plugin)
- Am besten auf anderem Webserver ablegen

Plugin-Tipp:

- BackWPup

Regelmäßige Updates

WPROTECT

- WordPress Core
- Themes
- Plugins

regelmäßig aktualisieren!

Plugin-Tipp:

- Jetpack (u. a. Auto-Updates)

Themes

WPROTECT

- Nicht benötigte Themes löschen
- Nur Themes von bekannten Anbietern (egal ob FREE oder PREMIUM)

Hosting/Server

WPROTECT

- Vertrauenswürdigen Hoster auswählen
- Aktuelle PHP-Version verwenden
- Apache aktualisieren
- SSL verwenden (Tipp: Let‘s encrypt)
- Zugriff auf Server einschränken (kein root, ...)
- Automatische Sicherheitsupdates aktivieren
- usw.

Servertest: https://www.ssllabs.com/ssltest/index.html

www.wprotect.de