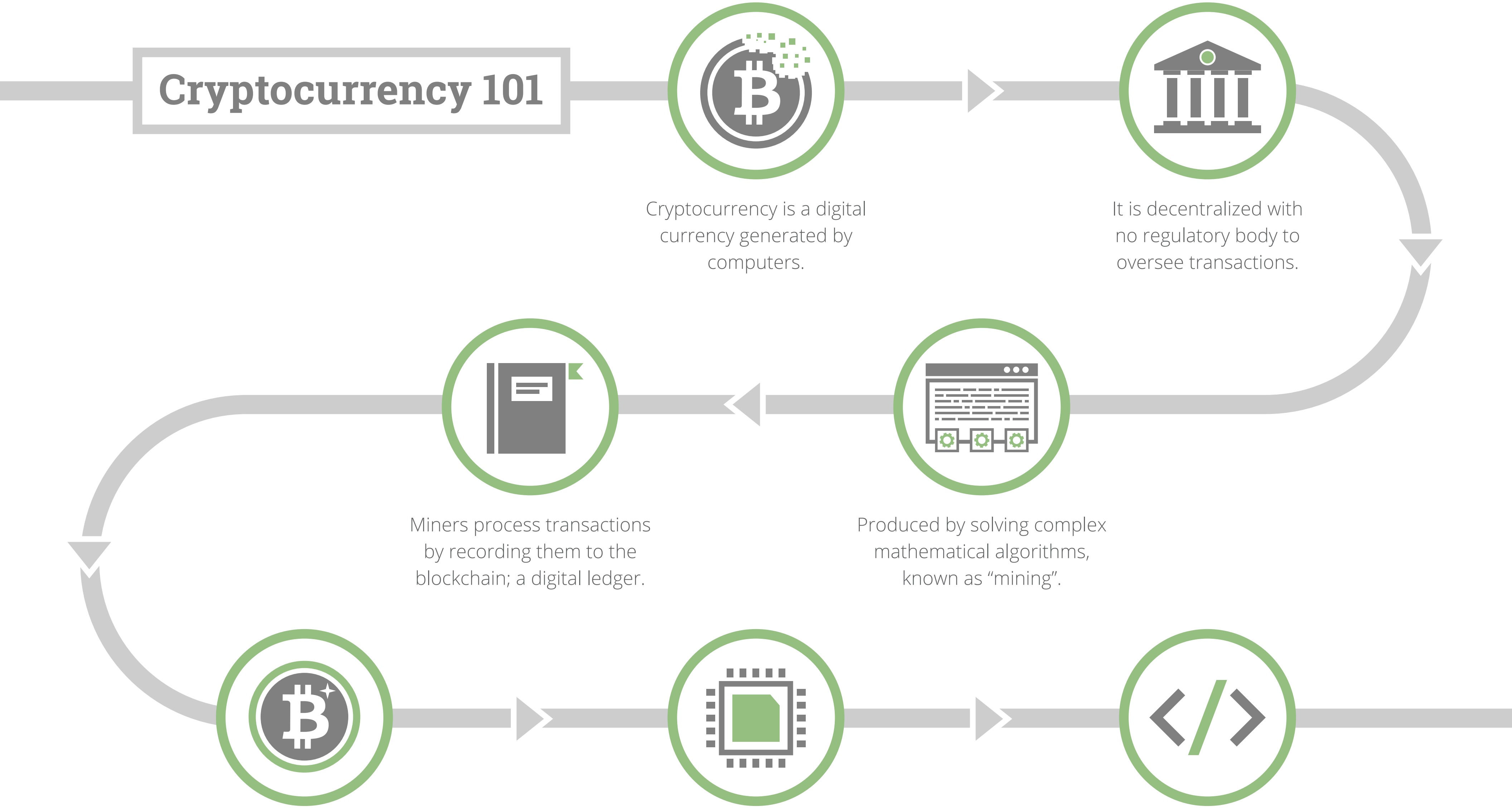
Cryptocurrency Mining Malware

Trends & Threat Predictions

sucuri

Table of Contents

Cryptocurrency 101



Cryptocurrency is a digital currency generated by computers.

It is decentralized with no regulatory body to oversee transactions.

Produced by solving complex mathematical algorithms, known as “mining”.

Miners process transactions by recording them to the blockchain; a digital ledger.

Miners are rewarded in the form of newly created coins.

Mining software on websites use excess CPU power from visitors to mine coins.

The code runs in the background without the visitor being aware of it.

The Rising Popularity of Cryptocurrencies

Since the introduction of Bitcoin in 2009, the popularity and adoption of cryptocurrencies as **digital assets have grown at a rapid pace.** Once reserved for the black market, hobbyists, mathematicians, and computer geeks, cryptocurrency is now becoming a global topic of interest with a market capitalization of over **700 billion USD.**

These digital assets are not governed or managed by central banks – instead, they are stored by the user in a personal wallet, allowing for **decentralization and anonymity** from traditional banking institutions. As adoption continues to rise, cryptocurrencies may begin to play a significant role in how goods and services are obtained by individuals and corporations alike.

Cryptocurrencies are produced by solving cryptographic and other complex mathematical algorithms, also known as “mining”. The most popular cryptocurrency, Bitcoin, takes an extraordinary amount of computing power to mine. A single bitcoin requires 215 kilowatt hours of electricity for each transaction. According to recent reports, the total energy consumption of the bitcoin network **consumes as much electricity as 2 million homes** in the United States.

The total cryptocurrency market capitalization rose 3224% during 2017 from $17 billion to $565 billion, with daily trade volumes surpassing $50 billion USD.

Abuse of Cryptominers

As the price of Bitcoin and other cryptocurrencies have risen, Sucuri has seen an influx in the number of crybercriminals looking for opportunities to monetize on the growing popularity. In 2017 alone, our research team identified **over 7,000 websites** that have been compromised by bad actors to mine Cryptocurrencies — a large majority of which are **associated with the mining of Monero,** a popular cryptocurrency.

Unlike BitCoin, Monero's algorithm does not favor GPU's and can be mined by web browsers and normal computers. It also contains **privacy features that make transactions and wallets more difficult to trace,** serving as an attractive monetary instrument to those involved in criminal activities.

Sucuri's research team noticed an increase in requests around mid-September, 2017, after CoinHive launched its mining service. CoinHive's initial version allowed website owners to install Monero coin miners using a simple snippet of Javascript. The code worked in the background of visitors' browsers, **utilizing any excess CPU power without the consent or knowledge of the website visitor.** These cryptominers served as an alternative monetization method, but the code was almost immediately abused by hackers who installed it on compromised websites.

Despite product updates to mitigate some of the abuse issues, CoinHive continues supporting webmasters who implemented the first release of the cryptominer.

> **Sucuri has identified massive cryptominer infections targeting WordPress, and Willem de Groot has reported over 2K infected Magento sites.**
>
> *Denis Sinegubko, Senior Researcher*

The Dawn of Cryptominer Infections

Cryptominers are a new opportunity for bad actors. In an effort to further monetize website infections, **hackers have begun integrating cryptominers into older malware campaigns.**

The malware used in these cryptominer infections are cleverly modified to make it more difficult for webmasters to identify and clean up. Attacks often pull payloads from a remote server, **making it easy for attackers to rapidly modify the injected content** on compromised websites.

During the initial waves of infected websites, malicious CoinHive injections used default settings that squeezed the maximum allotment of CPU power from a visitor's computer. Sucuri senior malware researcher, Denis Sinegubko, has identified advanced cryptominer parameters that have made it more difficult to detect unwanted miners on hacked websites.

In the past six months, these **infections have evolved to affect all major CMS platforms.** Attackers are abusing computer resources of website visitors to mine cryptocurrencies with little cost to themselves.

The evolution of these infections indicates that **attackers find cryptominers an effective and lucrative opportunity** and will continue to use them in their payloads.

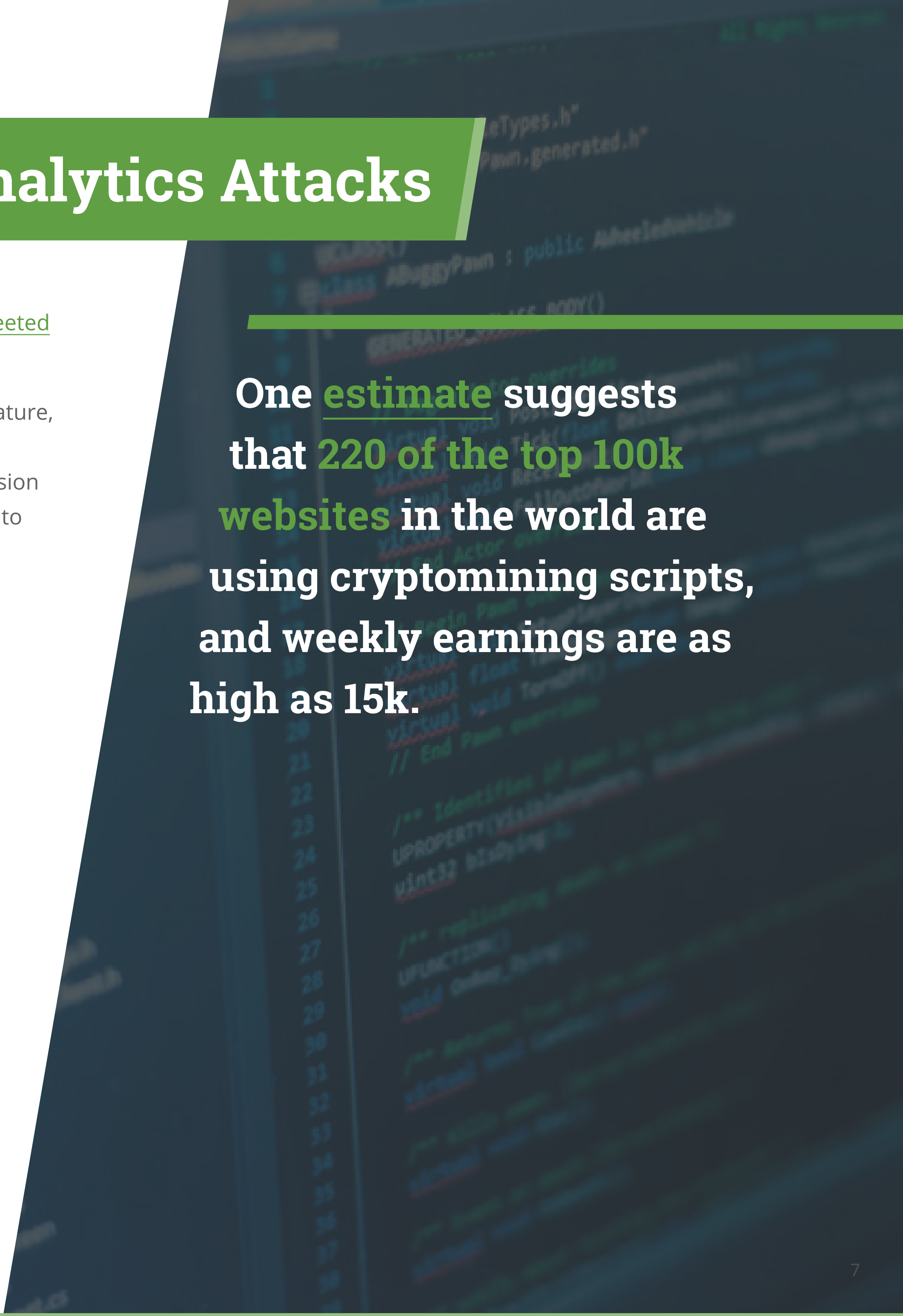
> **In the past six months, infections have evolved to affect all major CMS platforms including WordPress, Magento, Drupal and Joomla.**

Fake jQuery & Google Analytics Attacks

On October 30th, 2017, Microsoft Malware Protection services tweeted about a new cryptocurrency miner on compromised websites.

The malicious code included a number of tactics to hide its true nature, including use of a non-dotted decimal notation for the host name, utilization of a fake jQuery script name to load the obfuscated version of the CoinHive library, and replacement of miner variable names to mimic Google Analytics parameters.

Our research team identified that this particular infection is **primarily affecting WordPress sites,** and the impact is already quite significant. A quick search on PublicWWW on January 3rd, 2018 revealed a total of 4,247 infected websites. These websites also share the “cloudflare.solutions” malware that was identified April, 2017 by the Sucuri research team, suggesting that the **same attackers are responsible for this new infection.**



One estimate suggests that 220 of the top 100k websites in the world are using cryptomining scripts, and weekly earnings are as high as 15k.

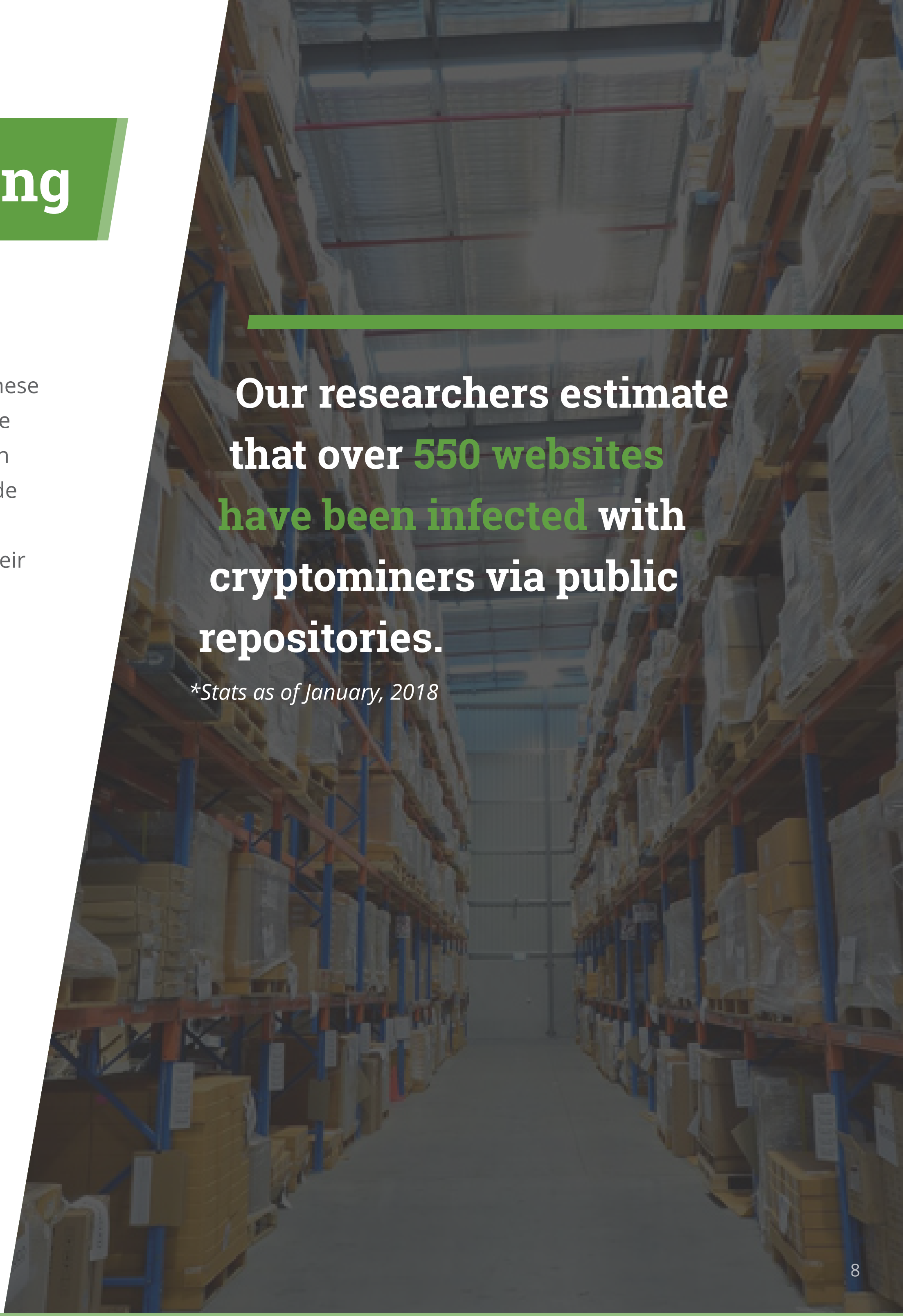
GitHub & Malware Hosting

The Cryptominer Edition

There are a plethora of public repos for cryptocurrency miners. These resources are attracting bad actors who know how to use tools like Git and GitHub and intend to modify third-party code for their own nefarious purposes. Unlike typical hackers who host malicious code in shady or compromised locations, **these black hats exploit services that normal programmers use** in order to distribute their unwelcome code.

In a recent investigation, we discovered attackers abusing the free GitHub.io service, which allows users to publish web pages directly from a GitHub repository. The attackers were distributing unwanted Javascript cryptominers and **placing the script in hidden iframes.**

Our researchers consider repository malware to be a recent distribution trend that will only continue to rise.



Our researchers estimate that over 550 websites have been infected with cryptominers via public repositories.

**Stats as of January, 2018*

Threat Predictions for 2018

Caveat: *The accuracy of these predictions largely depend on the market value of Monero and other cryptocurrencies. If the crypto market sees a large correction in the coming months, hackers may lose interest and seek other more lucrative opportunities.*

Indicative of the current threat landscape, browsing services are already beginning to implement cryptocurrency mining protection features - but these are still in the early stages of development, and aren't seen in all major browsers. As cryptocurrencies attract more users and the market capitalization continues to grow, **our researchers expect to see an increase in mass infections related to Javascript coin miners.**

A greater separation of white and black hat cryptomining platforms will likely occur in 2018 - and the **emergence of new black hat platforms will shelter the accounts and servers of bad actors** from complaints, offering further opportunities for exploitation.

In a less-than-ideal scenario, hackers will inject scripts that load malware from third-party servers maintained by cybercriminals. These scripts would load the appropriate payload for a visitor, which could include **ransomware, ads, cryptominers, scams or other unwanted malware.**

Assuming services like CoinHive stay unregulated and do not force webmasters to disclose or opt-in javascript miners, it's possible that cryptomining could become the worst type of pop-up ad - or even **evolve into a form of malvertizing.**

Cryptocurrency Mining Malware Predictions:

- **Mass infections including Javascript coinminers**
- **Increase in infections utilizing free hosting services**
- **Malicious cryptominers included in payloads**

Website Protection Against Malware & Other Threats

Sucuri offers a cloud-based **Software as a Service (SaaS) Intrusion Detection System (IDS),** built on the concept of a **Network-Based Integrity Monitoring System (NBIMS).** This monitoring platform includes both a remote and local (server-side) continuous scanning engine, providing **high visibility into the current security state of a web property.**

Included in the platform is an alerting engine for **Indicators of Compromise (IoC),** as well as a **cloud-based Web Application Firewall (WAF),** which serves as Intrusion Prevention System (IPS) to intercept and inspect all incoming HTTP/HTTPS requests and **block malicious requests** before ever reaching your website.

The platform is supported by our Security Operations Center (SOC) which provides **24/7/365 monitoring and response for all website attacks,** including:

- Detection and Removal of Malicious Cryptocurrency Miners
- Mitigation of DDoS Attacks
- Prevention of Vulnerability Exploit Attempts
- Protection Against the OWASP Top 10 (and more)
- Access Control Attacks (i.e., brute force attempts)

Our incident response team addresses all website infections. **No installation or application changes are required.** All sites are added and configured via the Sucuri dashboard. To enable the server-side scanning, a PHP agent is required at the root of the main domain.

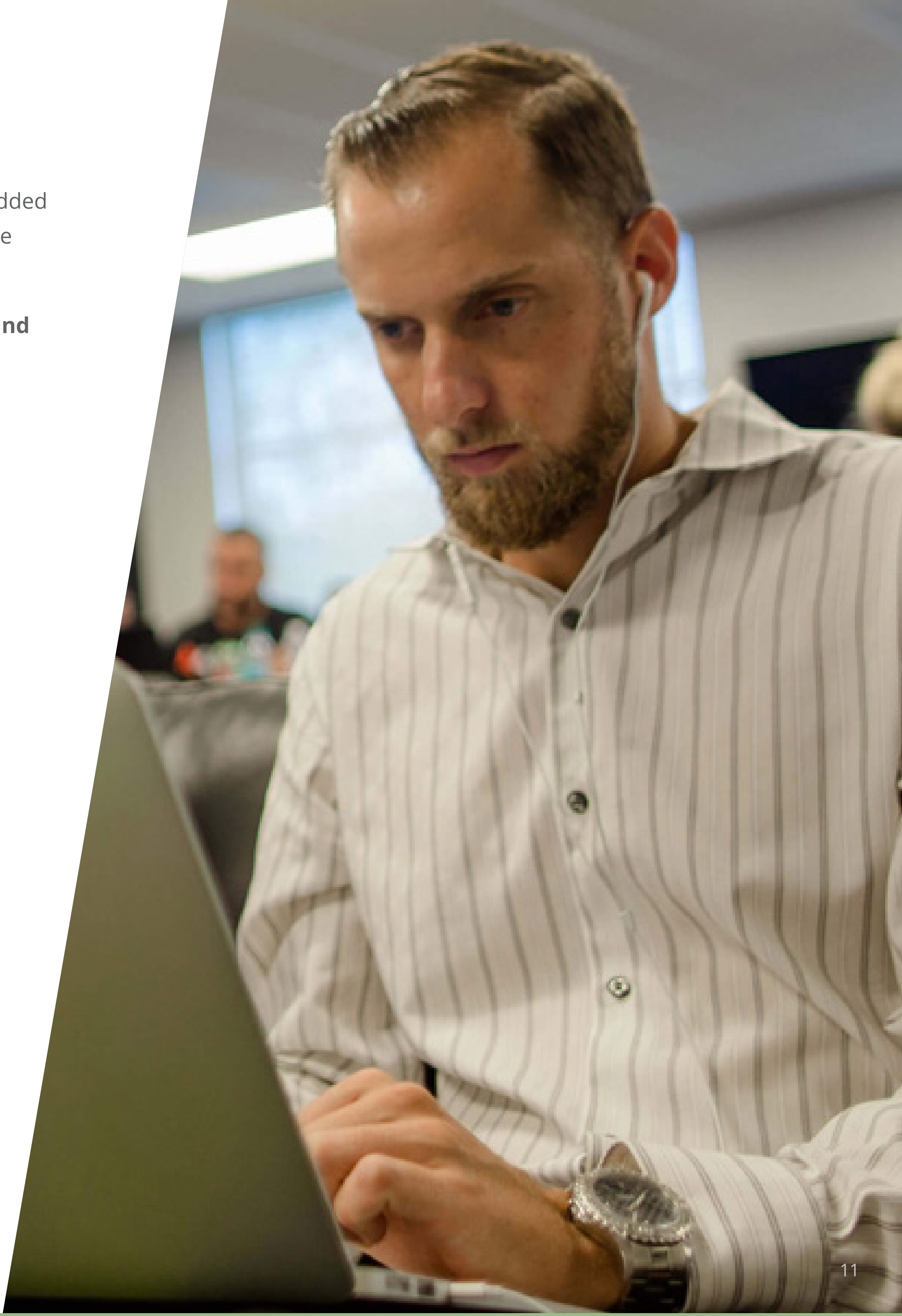
Want to cleanup or protect your website from cryptominers and other unwanted malware?

Contact us for a free consultation.

✉ enterprise@sucuri.net

☎ 1–855-670-2121

▭ sucuri.net/enterprise



Website Security Platform

Sucuri is a website security provider for demanding organizations that want to ensure the integrity and availability of their websites. Unlike other website security systems, Sucuri is a SaaS cloud-based solution built on state of the art technology, excellent customer service, and a deep passion for research.