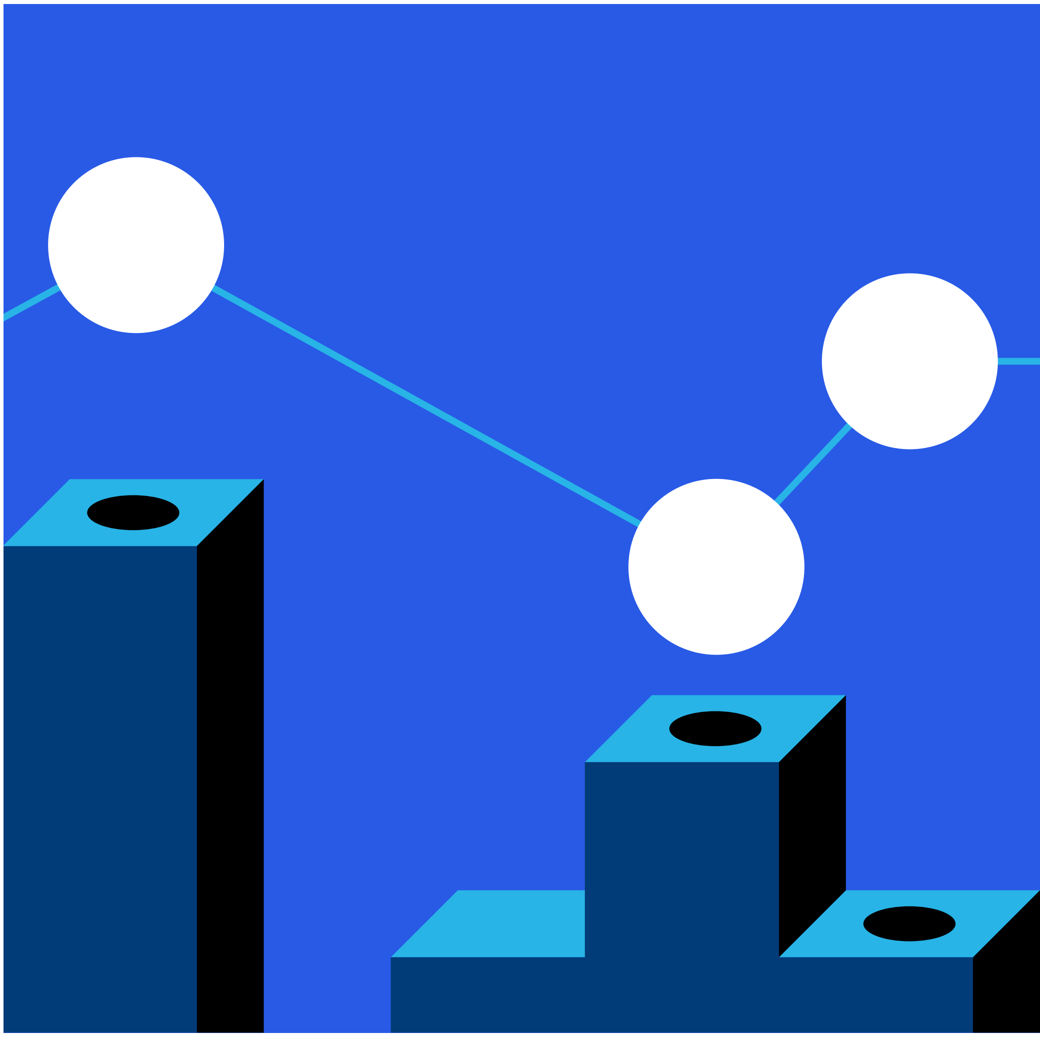
imperva



WHITEPAPER

A Guide to Protecting Cryptocurrency from Web Threats and DDos Attacks

Since the inception of Bitcoin in 2009, the volume and value of cryptocurrencies has increased dramatically. Other currencies such as Ethereum, Litecoin and Stellar have been issued and now there is a steady stream of new currencies issued in initial coin offerings (ICOs). There are now over 1,600 cryptocurrencies in circulation, with a corresponding increase in the number of currency owners. The total market capitalization of cryptocurrencies is $100 billion (as of December 15, 2018).

With this rapidly growing adoption, it is important to describe where the cryptocurrency is vulnerable and how the various players of the ecosystem can secure their investment. While the underlying blockchain technology of the cryptocurrency is in most cases natively secure, there are vulnerable points in the cryptocurrency life cycle. This paper will help improve security for participants in that cycle.

Vulnerabilities for an Emerging Cryptocurrency Industry

Here are some of the critical phases of a cryptocurrency lifetime where security is at risk:

1. ISSUERS OF THE ICO whose site (where the ICO is issued and where investors send their currency) can be attacked to interfere with not only the offering but also later support for the cryptocurrency. In one case the offering site was hacked to change the address for sending investments, thereby diverting a portion of the offering. ICOs websites have been subject to major DDoS attacks to make the site unavailable and disrupt the ICO.
2. OPERATORS OF CRYPTOCURRENCY EXCHANGES often hold millions of dollars of assets at any given point, and trade large amount of assets in real time transactions. Those sites can be overwhelmed by transactions or subject to attack.
   In some cases, DDoS attacks have caused an exchange to be unavailable for some period of time.
3. CRYPTOCURRENCY WALLET: Owners of cryptocurrency who must choose an exchange, and then protect their cryptocurrency wallet. Funds have been stolen from private and online wallets using credential-stuffing techniques with stolen credentials or phishing attacks.

Initial Coin Offering

The website or mobile application serving the cryptocurrency is vulnerable just like any site but is an especially tempting target for attackers. There have been attacks on ICO sites that delayed the offering or even siphoned off a portion of the offering cryptocurrency. In one case an attacker switched the official contribution address to the attacker's own anonymous address using a defacing attack. ICO sites are also often subject to large volumetric network or application layer DDoS attacks.

With the large amounts of transactions, ICO sites require a high level of protection using the following practices:

- AUTHENTICATION – Keep unauthorized visitors out by requiring strong passwords and two-factor authentication. Do not disclose more information than required on a failed login attempt such as which portion of the login is incorrect.
- UPDATE SOFTWARE AND OS – The many software applications used to run the site can contain vulnerabilities. Keep all the software up to date with the latest versions and patches that close detected vulnerabilities.

- **VALIDATE** all input on client input side and at server side. This will prevent injection of malicious content such as SQL injection and cross site scripting. See the OWASP Top 10 for more on web vulnerabilities.
- **ENCRYPTION** – Use HTTPS for the entire site.
- **RESTRICT ACCESS TO THE ADMIN PAGE** – Allow only selected admin users to access the site admin URLs.

Most importantly, secure your site with an enterprise-class web application firewall. A WAF will provide protection against all web application attacks and control access to your site and applications.

Currency Exchange

Those wishing to purchase or trade cryptocurrency can choose among the many exchanges that provide the service. Besides other considerations in choosing an exchange, the security measures and availability of the exchange must be considered so the stored assets are secured, and the potential trade is not impacted by unexpected delay at the exchange. Such delays can be caused by:

- A DDoS attack that causes the exchange to not be available for trades for some period of time.
- A larger volume of clean transactions than the site can handle such as database overload or server resources overload, resulting in service degradation.

In fact, cryptocurrency sites using our services are some of the most targeted in terms of industry by a DDoS attack. While these attacks were all successfully mitigated by Imperva, there have been several reports of damaging attacks on cryptocurrency exchanges.

These instances will likely continue with the growing demand for cryptocurrency. In addition, exchanges are a key target since they act as a wallet, and at any given point can store hundreds of millions of dollars of cryptocurrency. Therefore select an exchange with a proven record of being available and secure.

APIs are often the weak points of cryptocurrency exchange websites, as their payload structure is often proprietary making it harder to identify malicious rates or payloads. As a result they are often used as the vector for DDoS or other attacks.

To provide the expected level of service, an exchange must consider the following measures to mitigate the risk of service degradation.

- Provide sufficient bandwidth for the demand. This can be a constant challenge in a market where demand is rapidly increasing. Besides that challenge, it is unlikely to be sufficient to mitigate the large-scale DDoS attacks we are witnessing.
- Monitor traffic to detect when the site is under DDoS attack.
- Detect and stop malicious users by recognizing and filtering traffic such as that originating from known attack addresses, known bot agents or from locations that are known to be the major source of attacks.
- Protect against account takeover attacks, such as those employing credential stuffing, with strong web site protection as described above for the ICO site.
- Detect and stop malicious application layer requests by recognizing and filtering excessive numbers of requests from a single source or user session, known application signatures and traffic that does not conform to known HTTP protocols.

Protect your APIs, (often the weak point of website protection) as it is more challenging to inspect the legitimacy of their payload. They could either be ineffective due to false positives, or on the contrary enable vectors to attacks. Due to the difficulty of effectively implementing these measures, exchanges can implement services that provide the required level of service and protect against these attacks.

Currency Wallet

After you purchase cryptocurrency, it's stored in your digital wallet. In this way, you can receive and send cryptocurrency as you like. The wallet stores the private key that shows ownership of a public key connected to a certain amount of currency in the blockchain. Since the private key cannot be recreated, a lost key is a loss of that cryptocurrency. Also, if someone gains access to the key, he has access to the cryptocurrency funds.

As a result, safe and secure storage of the wallet is essential. The choice of wallet is very important too. Just like you can store cash in various locations – such as a wallet or pocket to have with you, a bank or a safe – a few types of wallets are available to store cryptocurrency:

1. SOFTWARE WALLET

A desktop or mobile app that provides access to the cryptocurrency. Since it is only accessible from the one device on which it is installed, the wallet provides a high level of security. However if something happens to that device you might not be able to retrieve your private key, and hence lose your currency.

2. ONLINE WALLET

The wallet is stored on a website and as other data stored in the cloud, accessible from any device. This could, however, be more vulnerable depending on the security provided by the third party. Stolen assets are often the results of credential stuffing attempts. Stolen usernames and passwords from known or less known sites are for sale on the dark web, and are stuffed on these sites, most often by botnets in the login pages, until a username/password combination works.

3. HARDWARE WALLET

A dedicated physical device built to store the keys locally provides the highest level of security. To use the wallet, users simply plug the device into an internet-enabled device, enter the device's pin and make the transaction.

Using those options, we suggest these steps to secure your cryptocurrency:

1. SMALL AMOUNTS ONLINE – Just like you usually wouldn't keep thousands of dollars in your pocket, minimize the amount of cryptocurrency that you keep in your computer or mobile device. Maintain the amounts you require for everyday use in those environments, so that the funds are easily accessible, and maintain the remaining funds in a safer environment, such as a hardware wallet.

2. BACKUP – Regardless of the type of wallet you use, make sure to keep safe backups of everything. Remember that if you lose your wallet private keys, you've lost the cryptocurrency. Keep multiple backups on different types of devices (such as USB and paper) at different secured locations so that you have alternate recovery paths.

3. **ENCRYPT** – Encrypt your wallet with a strong password that you'll never forget. Consider keeping a copy of the password in a safe location, such as a vault.
4. **SECURITY LAYERS** – Employ the additional layers of security that are available in your environment, such as two-factor authentication for login and for any transaction. Secure the environment with malware and antivirus protection.
5. **USE RECOMMENDED WALLETS** – If you use an online wallet, carefully select one that has an established reputation for secure service. Consider using a wallet that is integrated with your exchange.
6. **USE A UNIQUE PASSWORD,** not used in other websites that could be subject to unreported credential theft.

Imperva Protection

Creating a new currency and building an exchange are complex businesses. Imperva Web Application Firewall and DDoS mitigation can protect your website from the most advanced website attacks, DDoS and account takeover attacks. Imperva can provide you with additional cloud-based load balancing and failover or delivery rules solutions to maximize your site availability with ease of operation.

Web Application Firewall

Imperva's web application firewall, named by Gartner as a leading WAF for six consecutive years, analyzes all user access to your web application and protects your application from cyberattacks, while making sure that specific technologies such as web sockets are not broken. It protects against all web application attacks including OWASP Top 10 threats and blocks malicious bots. Imperva also controls which visitors can access your application with traffic filtering based on a variety of factors.

The WAF performs profiling of all aspects of the web application to detect attacks, such as preventing a site defacing attack that relies on cross site scripting. With this protection, your site can avoid the annoying validation requests, such as a Captcha, email confirmation or two-factor authentication that are prevalent on many sites.

DDoS Protection

To protect cryptocurrency exchange and foundation sites, Imperva DDoS Protection automatically detects and mitigates attacks targeting websites and web applications. Imperva is the only service provider to offer an SLA-backed guarantee to detect and block attacks in under 3 seconds. In 2019, our Behemoth 2 platform blocked a 713 Gbps (Gigabit per second) DDoS attack and other attack with more than 650 Mpps (million packets per second), with capacity to spare. We expect that capacity will be tested further as the size of attacks continues to increase.

Besides handling large volumetric attacks, Imperva specializes in protection for these types of DDoS attacks.

- Complex application, or Layer 7, attacks that target applications on your web server. These attacks require a smaller volume to be effective, measured in packets per second, but are harder to detect. The Forrester Wave reports Imperva to be among the top ranked in ability to detect and mitigate application layer attacks.

- Large scale attacks consisting of a huge volume of requests that are orchestrated via the API provided by many sites. API traffic is filtered with minimal false positives. Check out Imperva API Security for maintenance-free API security automation.

Application Delivery

Content delivery networks offer an efficient way for cryptocurrency exchanges to address exponential growth and build their business to scale. In addition to the DDoS service protection, Imperva CDN offers the following services that can help improve the robustness of cryptocurrency exchanges when under heavy load.

- Global content delivery network (CDN) improves your site's speed and performance with its intelligent caching and its high-speed storage and optimization tools. With over 40 PoPs deployed, Imperva provides significant improvement to page loading time.
- Imperva cloud load balancing enables exchanges to easily scale, add servers and failover data centers and add delivery and forwarding rules from the cloud with no downtime.
- Credential stuffing and account takeover protection with the ability to define rules that provide additional protection of login pages that prevent bots from performing credential stuffing. This mitigates major account takeover threats in the cryptocurrency domain in which hackers use stolen credentials for fraud.
- Traditional security measures against brute force attacks block high rate requests to the /login page from a given IP. However there have been recent attacks that bypass such filters by sending thousands of bots in infected computers at a very low rate. Imperva CDN can prevent attacks even at a low rate, since it can block or add a challenge to any non-human visitor reaching the /login page without slowing down the page load.
- Advanced bot classification and mitigation utilizing advanced rules.
- API protection, with extremely low false positives while keeping a high level of protection against DDoS attacks targeting APIs.

With these services in place, you can ensure that your site will always be available.

Conclusion

The variety and volume of cryptocurrencies continue to rise and attacks on cryptocurrency continue to increase in size, complexity and frequency. It is important that the associated institutions understand the need for dedicated and advanced WAF and DDoS protection services to minimize financial, operational and reputation risks associated with the attacks.

The best practices outlined in this paper will help institutions build a sound mitigation strategy. These measures include monitoring of application and network traffic, detection and filtering of malicious users and identification and blocking of malicious requests.

Imperva offers cloud-based WAF and DDoS protection services that address all of the key requirements, enabling cryptocurrency institutions to keep their websites and online applications up and running with high availability, performance and the best user experience.

ABOUT IMPERVA APPLICATION SECURITY

Imperva Application Security mitigates risk for your business with full-function defense-in-depth, providing protection wherever you choose to deploy - in the cloud, on premises, or via a hybrid model. Imperva offers advanced analytics to quickly identify the threats that matter, Web Application Firewall (WAF) solutions which block the most critical web application security risks, DDoS protection with a 3-second mitigation SLA, API Security that integrates with leading API management vendors, Bot Management for protection against all OWASP automated threats, Runtime Application Self-Protection (RASP) for security by default against known and zero-day vulnerabilities, and a developer-friendly Content Delivery Network (CDN) for the utmost performance. Through FlexProtect, our unique licensing model, you can deploy Imperva Application Security how and when you need it. FlexProtect helps protect your applications wherever they live — in the cloud, on-premises or in a hybrid configuration.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

Copyright © 2019 Imperva. All rights reserved