With more than $1.1 billion in cryptocurrency-related thefts during the past six months, the dark web hosts a thriving, illicit economy for opportunistic (and often unexperienced) cybercriminals.
Executive Summary

Cryptocurrencies. A decade ago, names such as Bitcoin, Dash, Etherem, and Monero were merely buzzwords. Fast forward to today, and they've become as recognizable as the U.S. dollar and the Euro. In many realms, these digital currencies are ushering in a new era of investing – a modern gold rush, albeit in digital form.

As was the case during the physical gold rush in the mid-1800s, there are criminals looking to exploit innocent parties of their earnings. Carbon Black has found that modern-day cybercriminals are increasingly using the dark web to facilitate cryptocurrency theft on a large scale.

During the past six months, Carbon Black looked into the dark web to determine how cryptocurrency malware is being bought and sold, fostering a burgeoning economy designed to pilfer some of the most popular cryptocurrencies on the market.

“Modern-day cybercriminals are increasingly using the dark web to facilitate cryptocurrency theft on a large scale.”

KEY RESEARCH FINDINGS

1. Our research uncovered a total of $1.1 billion in cryptocurrency-related thefts during the past six months.

2. There are currently an estimated 12,000 dark web marketplaces selling approximately 34,000 offerings related to crypto theft.

3. These malware offerings range widely in price, from as low as $1.04, to as high as $1,000 per offering. The average listing price was $224, while the “sweet spot” for pricing was around $10.

4. Cryptocurrency-stealer malware is the preferred method among crypto-targeting cybercriminals.

5. The available dark web marketplaces represent a $6.7 million illicit economy built from cryptocurrency-related malware development and sales.

6. Of the attacks we identified, cryptocurrency exchanges are the most vulnerable target for cybercriminals, with 27% of attacks targeting exchanges directly. Nearly 21% of cryptocurrency attacks target businesses, 14% target users directly and 7% target governments.

7. Although Bitcoin is still the lead cryptocurrency for legitimate cyber transactions, cybercriminals are moving to alternative and more profitable currencies, such as Monero, which is used in 44% of all attacks.
Cryptocurrency Overview

Today, there is no shortage of cryptocurrencies. Though abundant, cryptocurrencies tend to be volatile as values fluctuate day to day. Bitcoin reigns supreme as the original and oldest coin, with a value of $7,425 per coin at the time of this writing. These prices fluctuate due to a number of factors including: market demand, impending regulation and currency theft.

During our research, we explored the potential use of legitimized cryptocurrency on the dark web. More specifically, we looked at an up-and-coming currency, Zcash (with an estimated market cap of $665,208,949), which was legitimized by JPMorgan through an exclusive partnership\(^1\) in October 2017. We attempted to identify if Zcash gained popularity on the dark web through transactional use among users or through specific malware development activities.

Analysis of our collected data revealed no direct correlation between cryptocurrency and legitimacy on the dark web. While there are several listings that specifically target Zcash through illicit mining and wallet-stealer malware, the bulk of current offerings are Bitcoin-centric. This is likely due to its popularity.

While Bitcoin is king, our research revealed that cybercriminals shy away from Bitcoin when conducting illicit activity or accepting payments.\(^2\) The reason for this is simple: associated fees are too high, transactions take too long to process and criminals fear losing their ill-gotten gains. These cybercriminals appear to prefer Monero due to privacy, non-traceability\(^3\) and comparatively low transaction fees.\(^4\)
“Cybercriminals appear to prefer Monero due to privacy, non-traceability and comparatively low transaction fees.”

**Threat Overview**

We evaluated open source reporting for a six-month period to identify and quantify the largest threats posed from cryptocurrency-related crimes. During this process, we identified more than $1,148,763,000 in losses over the six-month period.

To quantify this figure, we looked at the most recent data from the United States Federal Bureau of Investigation’s (FBI) Internet Crime Center (IC3) that reported $1.3 billion in victim losses from internet crime for all of 2016.

Data collected by our research detailed a number of victims and sectors most affected by cryptocurrency-related crime. Of the identified attacks, we concluded that cryptocurrency exchanges are the most vulnerable target for cybercriminals. Attacks on these exchanges account for just over 27% of all reported incidents. These exchanges represent prime targets for cryptocurrency theft, fraud and harvesting of user information for follow-on targeting by these same criminals.
Data breaches and theft of personal information can be a critical step that enables cybercriminals to conduct targeted campaigns on cryptocurrency users. **These types of attacks on users represent 14% of cryptocurrency-related attacks.** Importantly, these incidents ultimately lead to theft of cryptocurrency and potential delivery of stealer malware or crypto-mining malware to a user’s vulnerable endpoints.

We calculated **nearly 21% of cryptocurrency attacks occur on businesses.** The majority of these attacks involve targeted deployment of illicit crypto-mining malware. This is commonly referred to as co-opted mining and involves hijacking a privately owned infrastructure to mine cryptocurrency. Cybercriminals can tailor their malware to throttle mining speed and frequency in attempts to delay detection.

These co-opted crypto-mining attacks can also target government resources in similar ways. Specifically, we identified that nearly **7% of cryptocurrency attacks targeted various governments using the same tactics, techniques and procedures (TTPs) found in private industry attacks.**

Of specific interest are recent trends in illicit and intentional mining activity targeting individuals browsing commercial and government websites. Our research found that **a growing number of websites are either intentionally deploying cryptocurrency scripts or are being used to deliver illicit mining malware to unsuspecting users.** This is most commonly referred to as “cryptojacking,” and, even if you aren’t being targeted for your own cryptocurrency, there’s a chance your endpoint may be abused for someone else’s gain.6 We found those living in countries with smaller economies are more likely to be targeted with “cryptojacking” malware, as they’re less apt to pay ransom.7
Separately, we evaluated the most targeted cryptocurrencies by cybercriminals. Bitcoin may be the most popular cryptocurrency, but the same cannot be said for its net favorability with these criminals. Interestingly, 44% of all attacks involve Monero in some form. This includes illicit mining and wallet theft. Second on the list for popular cryptocurrencies among cybercriminals is Ethereum, which comes in at a little more than 11%. Rounding out the top three is Bitcoin, accounting for about 10%. The remaining targeted cryptocurrencies are NEM, Bitcoin Gold and Tether, among others.

### Geographic Hotspots

Regarding geographic hotspots involving cryptocurrency-related attacks, we found no immediate correlation between location of the incident and overall motive for the attack. Based on the analysis of our collected data, most attacks occur against vulnerable targets of opportunity. As such, these attacks are not bound to geographic location, but rather occur in areas where significant opportunity exists, including targets with easily exploitable vulnerabilities.

This is especially true for those would-be cybercriminals purchasing inexpensive malware from the dark web as a “just-in-time” capability. These types of attacks are typically less focused than those employing more sophisticated malware.

However, we identified specific hot spots where activity most occurred within the past six months. The top five most active hot spots include: **the United States with 24 incidents, China with 10, the United Kingdom with 8, Japan with 5 and India with 5.** We should also note that these countries, along with the others identified with cryptocurrency-related attacks, have mixed legal status regarding cryptocurrencies and trading activities.
Cryptocurrency Gold Rush on the Dark Web

Dark Web Cryptocurrency Malware Findings

Our research on current malware offerings available on the dark web revealed a booming marketplace for malign cyber actors of all types. Our analysis of the marketplace suggests cryptocurrency-related malware listings are designed to cater to unskilled cyber actors, or those looking to make a quick buck from highly vulnerable victims. The listings are riddled with phrases that emphasize the sheer simplicity in using these tools. The phrases are not something we typically expect to see in offerings geared toward sophisticated actors.

“Our analysis of the marketplace suggests cryptocurrency-related malware listings are designed to cater to unskilled cyber actors, or those looking to make a quick buck from highly vulnerable victims.”

These malware offerings are often made available at rock-bottom prices. The lowest identified offering was priced at $1.04, with a max price of $1,000, and an average listing price of around $224. We also identified a sweet spot in malware pricing for cryptocurrency-related attacks at around $10.
“We identified a sweet spot in malware pricing for cryptocurrency-related attacks at around $10.”

Analysis of listing prices and malware descriptions reveal that the average listing is likely relatively unsophisticated, and detectable with proper endpoint security. Higher priced listings, including the identified $1,000 malware, enable a more technically proficient user to compile their own malware. While these are still detectable, they are capable of defeating common indicators of compromise (IOCs) and signatures.

We estimate a total of 34,286 cryptocurrency-related malware offerings are currently available on the dark web. Of the total offerings, we identified cryptocurrency-stealer malware as the preferred TTP among crypto-targeting cybercriminals. These offerings account for 65% of total listings and promise to make the buyer rich through exploitation of the target’s endpoint and subsequent draining of the targeted cryptocurrency wallet. Funds are quickly and covertly redirected to the criminal’s wallet, leaving the original owner with nothing.

Additionally, we found that covert-mining malware accounts for a little more than 10% of total offerings on the dark web. Users on the dark web acknowledge that Graphics Processing Units (GPUs) are expensive, so they recommend saving the money and co-opting a victim’s computing resources to mine cryptocurrency on behalf of the cybercriminal. Similar to stealer malware offerings, mined cryptocurrencies are directed to the wallets of the malign actors.

We also identified that mining botnets represent approximately 3.3% of these offerings. These botnets are intended to perform the same task as a covert mining malware, but these botnets substitute a single victim with a large number of co-opted machines. Depending on the targeted cryptocurrency, these botnets can generate significant income if the campaign is successful.

Lastly, we identified that 1.6% of available listings involve mobile malware packs. These malware packs are typically used to harvest legitimate credentials to steal cryptocurrency from the victim’s wallet or, alternatively, deploy malware on the device for the purpose of illicit mining.

The above data represents an estimated dark web economy currently worth $384,463. With that in mind, we extrapolated the average weekly value of the economy and estimate a 12-month total economy size of roughly $6,664,022.

$6,664,022
Current size of illicit, dark web economy for cryptocurrency-related attack offerings.
CRYPTOCURRENCY GOLD RUSH ON THE DARK WEB

The marketplace represents a significant illicit cryptocurrency-related economy, with potential for high return on investment (ROI). Most importantly, we identified specific sellers and listings that provide detailed instructions and tutorials for users to cash out their earnings. For all intents and purposes, this is easily identifiable as crypto-cleansing (think money laundering, but with blockchain), which allows users to exchange for alternative cryptocurrencies through cryptocurrency exchanges.

Additionally, well-coordinated cybercriminals (as well as state and non-state actors) are capable of cryptocurrency pump and dump schemes. These schemes target initial coin offerings (or other established currencies) and involve exchanging existing coins or purchasing the targeted currency in an effort to drive up value. This activity is intended to drive up the price of the coin for sale, and lure in legitimate users to purchase. Once the currency has achieved sufficient value, the actor sells their share of the currency for a potentially sizable margin. These activities are as illegal as the initial theft, and only serve to aid the kill chain and follow-on campaigns.

**Dark Web-Enabled Attacks**

A plethora of turnkey tools and materials are made available on the dark web that allow less adept hackers to execute successful campaigns using “just-in-time” capabilities. These capabilities negate the need for long and expensive development, testing and evaluation timelines. This significantly reduces the time between acquisition to successful campaign execution.

These ready-made capabilities also enable cybercrime syndicates and other cyber-espionage groups as use of common TTPs greatly increases anonymization. Additionally, these actors make use of commercially available capabilities, which spurs innovation that makes individual components more sophisticated. Providers are able to iterate quickly using sales of previous wares to continue development and specialization in their space.

With these factors in mind, we’ve re-interpreted the traditional “Cyber Kill Chain” as an opportunity to “purchase” all or parts of the “Cyber Kill Chain” to significantly improve the speed and overall effectiveness of a cybercampaign.
The “New” Cyber Kill Chain

**PURCHASING THE CYBER KILL CHAIN**

**PHASE 1: RECON**
- Attacker no longer needs to execute recon, potentially tipping off an impending attack or revealing true origin.
- Purchasing target information is cheap and easy. Many free alternatives also exist.

**PHASE 2: WEAPONIZATION OF EXPLOIT**
- Attacker purchases exploits and pre-weaponized documents/files that have proven success record. Weaponization tools often include the ability for the attacker to customize the file name, format and contents of the decoy file.

**PHASE 3: DELIVERY**
- The delivery infrastructure is easily purchased and constantly adapting to avoid detection and defense mechanisms. Delivery includes malicious ad networks (or exploiting vulnerabilities in legitimate ad networks) and using email-based delivery via compromised email servers with good reputation scores. Delivery methods include:
  - Malicious ad network (broad-sweeping targeting)
  - Delivery to specific target (via compromised legitimate mail server)

**PHASE 4: EXPLOITATION**
- Because the campaign can be run at a much larger scale (company-wide targeting, industry-wide targeting, compromised high-traffic websites) exploitation returns greater results than a self-developed campaign.
- Low-cost weaponization and delivery ensures success much faster than traditional campaigns.

**PHASE 4: EXPLOITATION (ALTERNATE ROUTE)**
- Alternatively, many companies have been compromised and direct access to terminals can be purchased on the dark web (bypassing the “exploitation and installation” phases entirely).

**PHASE 5: INSTALLATION**
- Commercially available RAT (Remote Administration Tools) and other long-term presence tools are easily available on the dark web and make attributions more difficult.

**PHASE 6: COMMAND & CONTROL**
- Command and control of the compromised target can be operated through rented Infrastructure-as-a-Service (IaaS) or the entire malware maintenance can be purchased and operated by a third party in a Software-as-a-Service (SaaS) model.

**PHASE 7: ACTIONS ON OBJECTIVES**
- The attacker now has first-tier access to the target network and can execute any series of attacks against the target business to include:
  - Financial theft
  - Proprietary data and customer theft
  - Lateral traversal further into the network
The Exploitable Attack Surface: Fighting Back

We evaluated threat reporting and pinpointed key tactics, techniques, and procedures (TTPs) most favored by cybercriminals. **Stealer malware is the most prevalent, being involved in 41% of incidents.** Mobile malware ranked second and is used in 22% of attacks. Mobile malware is closely followed by drive-by malware attacks at 18%.
Cybercriminals have tools and capabilities at their disposal. However, there are steps to take to avoid becoming a victim. Below are suggestions for how to avoid victimization from lurking cybercriminals looking to make quick coin. There’s no reason why investing in cryptocurrencies should feel like the Wild West.

Cybercriminals most commonly target endpoints to drain and steal the contents of cryptocurrency wallets. This can be done through internet-delivered malware and malicious mobile applications. Users should always use an endpoint security solution with prevention and detection capabilities to protect their devices. More importantly, users should avoid installing untrusted applications or following unfamiliar links.

Consider using an ad-blocker on all endpoints used to browse the internet. These ad blockers reduce the risk of having your device used to harvest cryptocurrency without your consent. This is a growing tactic for cybercriminals, and when coupled with endpoint protection, can go a long way to prevent filling someone else’s wallet.

Cryptocurrency exchanges represent a significant target of opportunity for would-be cybercriminals. Conduct extensive research to select a trustworthy exchange, and avoid reusing passwords across websites. This is especially true for wallets and exchanges. Concerned users should also avoid accessing their mobile cryptocurrency on public Wi-Fi, or on those networks with poor security.

Organizations should have steps in place to protect their financial assets and bank accounts. This would include limiting access to certain individuals and having an audit process. Store any and all cryptocurrency in an offline wallet and have a backup. Never store your cryptocurrency in an online or warm wallet (a dedicated device that must be connected to the internet to make transactions). Cold storage is best – offline in a safe that a small number of employees have access to.

Be on the lookout for secure connections with cryptocurrency exchanges, along with unexpected emails from the same. Risks involve falling victim to a common spear phishing attack or even a fraudulent website.
Conclusion

Decentralized cryptocurrencies are likely to increase in sheer quantity and in value in the short-to-mid term. However, a growing number of countries are considering current legislation or have already passed laws regulating cryptocurrencies.

In the meantime, governments and law enforcement agencies will attempt to regulate these digital currencies. In the same vein, cybercriminals will attempt to exploit the ever-increasing attack surface. Unfortunately, new investors and traders looking to jump on the crypto bandwagon will exacerbate the opportunity for exploitation.

We expect to see cryptocurrency theft and illicit mining activity expand in the mid-to-long term as security mechanisms and user awareness slowly catch up to the evolving threat. These cryptocurrencies represent an alternative and lucrative funding stream, which is especially true for criminals, as well as nation-states desperately seeking to subvert sanctions.

TTPs will evolve and adapt quickly, along with the dark web marketplaces that fuel the illicit economy. As attackers evolve, so must defenders.
References

4. https://www.monero.how/monero-transaction-fees

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has a strong heritage of innovative technology leadership in multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform - the Cb Predictive Security Cloud - Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

© 2018 Carbon Black and Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions.