Executive Summary

Digital Laundry
An analysis of online currencies, and their use in cybercrime

By Raj Samani, EMEA, McAfee
François Paget and Matthew Hart, McAfee® Labs
Recent actions by law enforcement, and the charges brought forward by prosecutors, add weight to the theory that digital currencies are a key 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 in history.

However, Liberty Reserve is not the only virtual currency that has been used by criminals, and the proliferation of these services 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—with targeted attacks on financial exchanges, and malware developed to target digital wallets.

Some currencies, such as Bitcoin, allow the creation of new currency through a process known as mining. While initially people used their own computing resources for mining, in June 2011 a JavaScript Bitcoin generator (miner), allowed high-traffic sites to employ visitors’ computers to produce Bitcoins. Although in some cases the site would explain this to visitors, the procedure could be done without their knowledge as well—in effect creating malicious bots. One rogue employee of the E-Sports Entertainment Association installed such a miner on some 14,000 computers to secretly mine Bitcoins.

Defining Digital Currencies
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.

In the report Redefining Virtual Currency, 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, which hints at an expanding noncriminal market.

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 virtual currency companies, users quickly identify new platforms to launder their funds; simply shutting down the leading platform will not solve the problem.

As Figures 1 through 4 illustrate, many illicit services accept 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.
Figure 2. Virtual currencies are accepted as payment for any number of illegal products on anonymous online marketplaces.

Figure 3. The sale of otherwise regulated products such as firearms is all the more attractive because the nature of virtual currencies makes it difficult to not only control the sale of guns, but also to trace them to perpetrators should they be used in crimes.
Ease of use is one of the biggest benefits of digital currencies and electronic money. Acquiring virtual currencies with particular exchanges may demand a registration process, but in some cases users can purchase currencies merely by providing funds.

Bitcoin is currently the leading virtual currency, 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 combines cryptography and a peer-to-peer architecture to avoid a central authority; law enforcement agencies say this also makes it more difficult to identify suspicious users and obtain transaction records.

This decentralization is not without vulnerability. For example, the Bitcoin network suffered from a denial of service (DoS) attack that forced the development team to patch the core reference design. Cyberattacks against virtual currencies are not limited to the Bitcoin network; exchanges are also falling victim.

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, crashing the Bitcoin rate from US$17.50 to almost valueless.

The development of the JavaScript Bitcoin miner brings considerable potential for the creation of bot miners. And although not all miners are malicious, their use of nefarious distribution methods creates measurable spikes in malware and bot usage generally and corresponded to the first boom in Bitcoin rates.

Recent analysis by McAfee Labs into a Bitcoin botnet found other 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. In June 2011 a half-million dollars were stolen from a Bitcoin user with the pseudonym Allivain.

Research into Bitcoins has raised concerns about potential privacy implications as well. A new academic study 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.
Conclusion
Attempts to close down virtual currency 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 DoS 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.