Cryptomining Malware Appears Across the Web | Proofpoint US

By November 29, 2017 Proofpoint Staff

Published: 2017-11-29 · Archived: 2026-04-05 15:09:05 UTC

Background

Although the first Bitcoin was mined in 2009, the value of the "cryptocurrency" and new alternatives like Litecoin and Monero have risen dramatically in recent months. Once primarily the domain of cybercriminals and underground operators attracted by anonymous transactions, Bitcoin in particular has become big business, with even the Chicago Mercantile Exchange recently announcing it would begin trading in Bitcoin futures. While still volatile, Bitcoin values alone have risen by 860% since the beginning of 2017 (Figure 1)[1], while Monero prices are up over 1200% (Figure 2). Predictably, threat actors are following the money and finding ways to target these new currencies and their users.

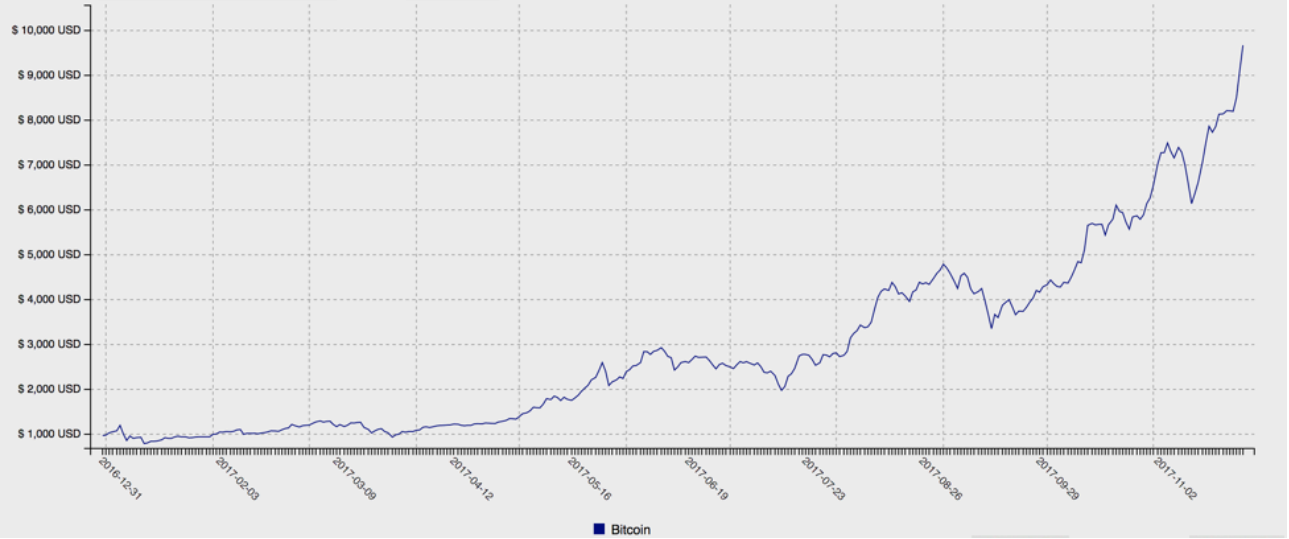

Figure 1: Bitcoin price trend, 2017 YTD, courtesy of cryptocurrencychart.com

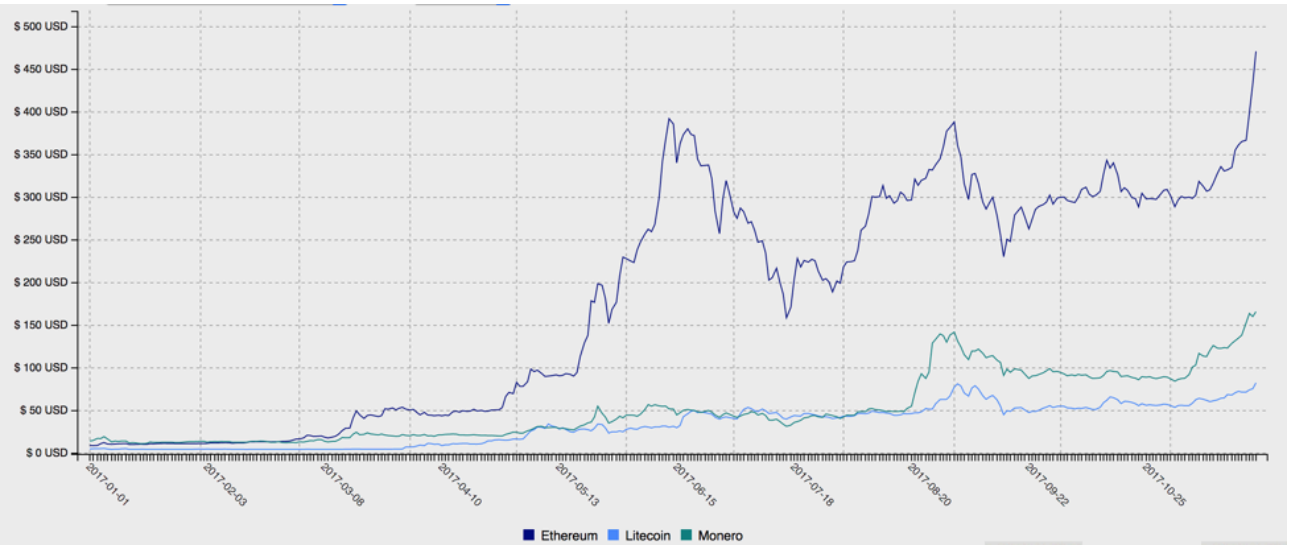

Figure 2: Ethereum, Litecoin, and Monero price trends, 2017 YTD, courtesy of cryptocurrencychart.com

Cryptocurrencies are created through a process called mining. At the simplest level, mining involves solving math problems of increasing complexity to unlock new units of currency. The increasing complexity creates scarcity, as do preset caps on the number of units that can ultimately be mined. This complexity has made it nearly impossible to mine Bitcoins outside of supercomputing environments, but alternatives like Litecoin and Monero can still be effectively mined with desktop CPU resources. Miners invest CPU cycles and energy for the potential rewards: free currency units.

Monero is one of the few valuable cryptocurrencies that can be mined with CPU power, making it the cryptocurrency of choice for many legitimate and crypto mining malware. Cryptocurrencies traditionally are mined with CPU power first, then GPU power once developers learn to increase mining speed with GPU-driven calculations. Once cryptocurrencies can only be mined efficiently with GPUs or, for even more compute-intensive mining, field programmable gate arrays (FPGAs) -- specialized hardware and chips purpose-built for a single function -- they are no longer reasonable candidates for mining with coinmining bots or browser-hijacking scripts. At this point, cybercriminals will likely move on to other currencies. For now, Monero uses the CryptoNight algorithm, which currently appears to be fastest on a CPU, but regardless of the cryptocurrency mined there is often a significant investment in hardware and energy.

Criminals are turning to cryptocurrency mining malware, or coinminers, to short circuit this investment, instead stealing energy and CPU cycles from their victims and using them to mine. At the same time, legitimate and criminal enterprises alike are exploring browser-hijacking software to mine cryptocurrencies while web surfers visit their websites or sites they have compromised for this purpose.

While mining can potentially provide those willing to invest the time and resources -- or to exploit victims with crypto mining malware -- with free cryptocurrency, most users simply buy and exchange cryptocurrencies. Some are looking to cash in on the rapidly rising prices, investing in the new currencies, storing them in wallets and utilizing specialized exchanges. Many economists are pointing to a likely bubble, particularly in Bitcoin values, but interest remains quite high among businesses and consumers.

Both cryptocurrency wallets and exchanges have been targeted by cybercriminals with phishing schemes and backdoored software. Even the relatively new category known as initial coin offerings (ICOs) have been targeted. ICOs have become an increasingly popular means for businesses to generate funds and rally investors, offering investors cryptocurrency units or tokens in exchange for potential future value. This increases the number of cryptocurrencies in circulation and potentially short-circuits regulatory requirements around securities offerings. Though not necessarily illegitimate in and of themselves, ICOs have been the targets of phishing attacks, Ponzi schemes, and other types of fraud. In spite of these concerns, ICOs raised $2.2 billion through September 2017 for companies turning to them for financing.

All of this has increased the attack surface, opportunities, and incentives for threat actors to move quickly to capitalize on widespread interest and rising prices.

Following the money

All of these elements point to a larger trend: as threat actors look for ways to directly monetize malware and infected machines, evidence that coinminers are a more than just the latest security fad continues to mount. While many people first learned about Bitcoin as the payment method to decrypt computers infected with ransomware, threat actors are once again following the money and cashing in on their newfound popularity. They are running phishing schemes, deploying malware crypto mining malware, deploying browser-based miners, and creating fraudulent wallets and other related software to victimize users.

Proofpoint research suggests that the number of new malware strains related to cryptocurrency, whether designed for direct theft of wallet credentials or using system resource abuse to mine for such currency, now exceeds the number of one-off, “script kiddie” ransomware strains that had been appearing on a daily basis in 2016 and early 2017. This appears to be a major trend among threat actors and we expect it to continue as: 1) cryptocurrencies increase in value; and 2) popular Bitcoin alternatives like Litecoin and Monero remain mineable with desktop PC resources.

Dedicated crypto mining malware

As noted above, malware designed specifically to mine cryptocurrencies is now appearing more frequently than new ransomware variants. While many of these are more amateur in nature or their developers lack the infrastructure for large-scale distribution, we have already observed coinminers in a number of very large campaigns. In May, we identified the Adylkuzz Monero miner being spread in massive network-based attacks. In other campaigns, we have seen established actors traditionally focused on banking Trojans begin to distribute coinminers, either as a rotating or secondary payload or as a new primary payload.

One such recent campaign involved an actor we track as TA516. This actor typically distributes instances of the SmokeLoader intermediate downloader, which, in turn, downloads additional malware of the actor’s choice -- often banking Trojans. Figure 3 shows a lure document from a November campaign in which TA516 distributed fake resumes with malicious macros that, if enabled, launch a PowerShell script that downloads SmokeLoader. In this instance, we observed SmokeLoader downloading a Monero coinminer. Since the middle of 2017, TA516 has used similar macro-laden documents as well as malicious JavaScript hosted on Google Drive to distribute both Panda Banker and a coinminer executable via SmokeLoader, often in the same campaigns.

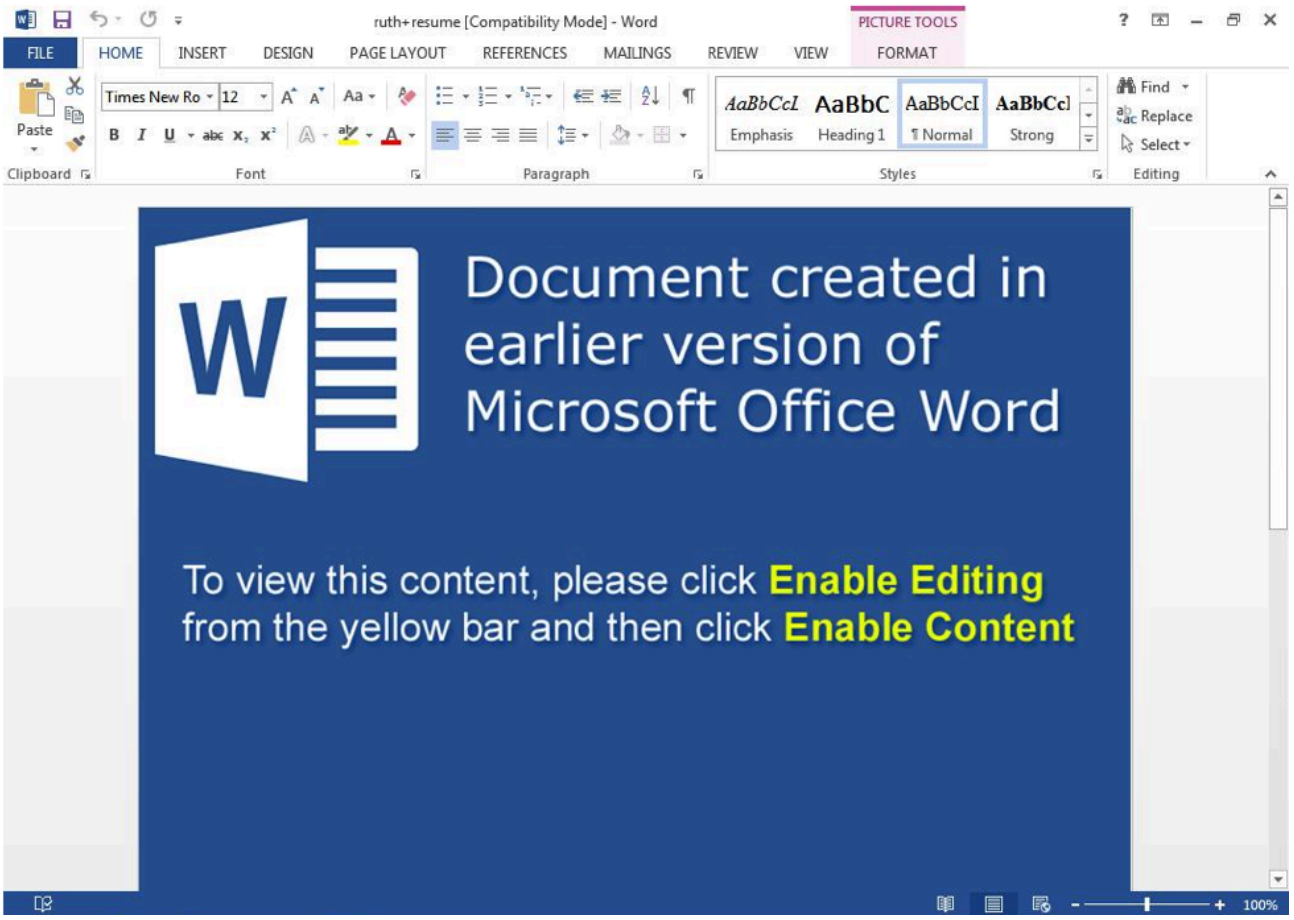

Figure 3: Fake resume lure document distributed in email by TA516

Dedicated coinminers present certain advantages for threat actors: continuous mining while machines are on, persistence mechanisms, and the ability to distribute the malware to large numbers of potential victims through email and web-based campaigns, as well as available strains for both mobile and desktop computing platforms make coinminers attractive to financially motivated actors. However, their impact on performance can make them readily detectable by end users and many desktop and gateway security products can detect and mitigate the binaries. For smaller actors, distributing at sufficient scale to mine effectively can also be problematic.

Coinmining modules

One way threat actors are addressing the distribution issue is to incorporate coinmining modules in existing malware. In particular, we have observed mainstream malware like The Trick banking Trojan add coinmining capabilities. While we initially observed coinmining in The Trick campaigns from less prominent actors, The Trick's affiliate model means that we will likely be seeing this at scale from actors like TA505 soon. AbaddonPOS, a popular point-of-sale malware, has recently incorporated the ability to steal cryptocurrency wallet credentials as well. SmokeLoader, in addition to being used to download standalone coinminers, is available on underground markets with a built-in coinminer module for an additional fee.

Browser-based minings

The Pirate Bay made headlines recently for attempting to pay for their operations by mining coins through users' browsers with Coinhive. Coinhive is a JavaScript application that can be placed on websites, using visitors' CPUs while they are on a particular page. Some sites are exploring this as an alternative to ads and paywalls, but many do not allow surfers to opt out. The Ultimate Fighting Championship recently implemented Coinhive on their pay-per-view streaming site, but faced a backlash for not informing users [16].

In other cases, Coinhive and other scripts like it are placed on compromised websites without the owners' knowledge. The practice appears to be driving increases in pirated content on illegal streaming sites - sticky sites where users spend a long time on a single page watching videos while unknowingly having CPU cycles hijacked to mine cryptocurrency.

Phishing and theft

Cryptocurrencies are generally stored in digital wallets while exchanges are used to trade cryptocurrencies for common currencies. Simply relying on the human factor and engaging in the types of phishing and direct theft with which traditional banking customers have contended for years means that phishing actors can use established practices and social engineering in the new arena of cryptocurrency.

We have previously documented increasingly sophisticated phishing schemes targeting cryptocurrency exchanges and online wallets [5] as well as backdoored wallet software [6]. Figure 4 shows a phishing template used to steal credentials for blockchain.com, the largest provider of Bitcoin wallets in the world.

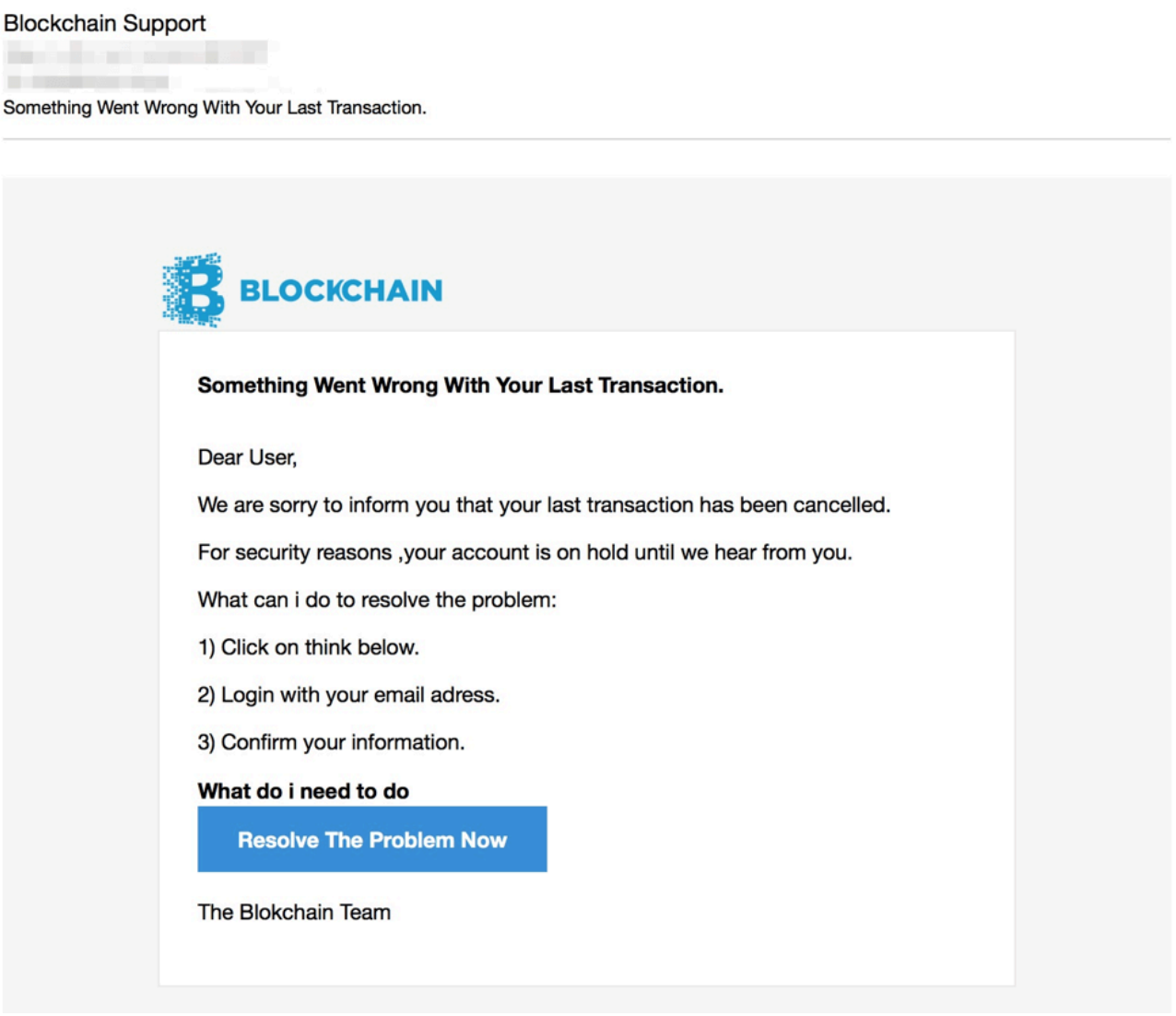

Figure 4: Blockchain email lure with stolen branding from May 2017

Figure 5 shows the download screen from a fraudulent domain distributing a backdoored version of wallet software for Litecoin cryptocurrency. The fake site uses stolen branding and the lookalike domain itecoin[.]com.

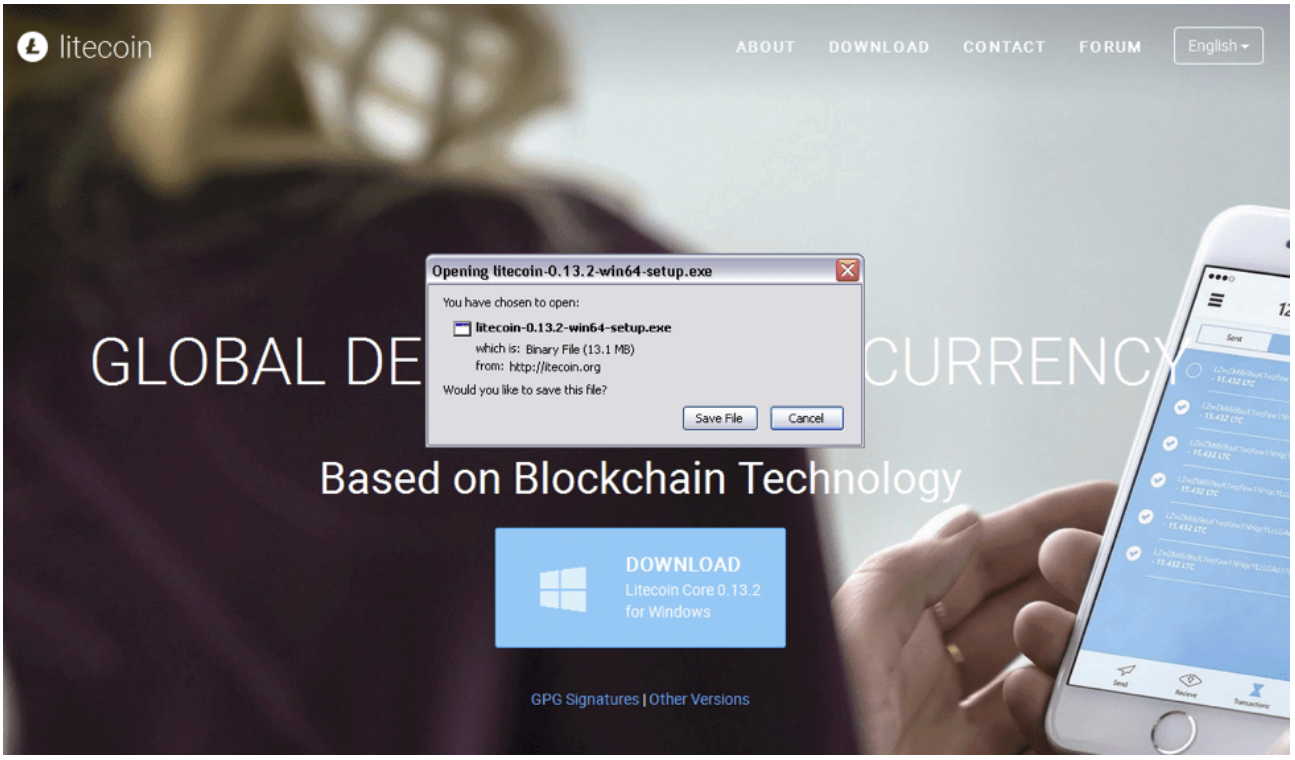

Figure 5: Backdoored Litecoin wallet downloaded from imposter site itecoin[.]org

Conclusion

Rising cryptocurrency values, increasingly mainstream use cases, and readily available malicious and browser-based tools for mining new cryptocurrencies are fueling an explosion in coinminer distribution. While we are seeing a gradual decline in the new one-off, proof-of-concept, and “script kiddie” variants of ransomware, coinminers appear to be drawing amateur and seasoned threat actors alike.

Taken in the context of massive coinminer campaigns like we observed with Adylkuzz, paywall trends, etc., it is clear that both threat actors and legitimate web sites are incorporating this technology quickly before mining becomes prohibitively CPU-intensive, as it is with Bitcoin. It appears to be an easy, modular add-on for a variety of malware and a source of residual -- if not primary -- income for threat actors.

As a result, consumers and organizations are at risk for a threat that is much more subtle than ransomware, often running undetected until PC performance is dramatically impacted by this new family of malware. These threats are coming via malicious spam campaigns, browser-based scripts, and more, necessitating the continued use of intelligent email gateways, endpoint antivirus, and intrusion detection systems that can block associated traffic.

****

References

[1] https://www.cnbc.com/2017/11/01/bitcoin-price-hits-6500-to-new-record-high-after-cme-futures-plan.html

[2] https://www.economist.com/blogs/buttonwood/2017/11/greater-fool-theory-0

[3] https://www.bleepingcomputer.com/news/security/underground-hacking-forum-admins-having-second-thoughts-about-selling-ransomware/

[4] https://www.bleepingcomputer.com/news/security/copy-pasting-malware-dev-made-63-000-from-mining-monero-on-iis-servers/

[5] https://www.proofpoint.com/us/threat-insight/post/follow-money-phishing-schemes-go-after-cryptocurrency

[6] https://www.proofpoint.com/us/threat-insight/post/backdoored-litecoin-wallet-spread-typosquatted-domains

[7] https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

[8] https://community.rsa.com/community/products/netwitness/blog/2017/07/20/an-introduction-to-cryptocurrency

[9] https://www.theguardian.com/technology/2017/sep/13/from-silk-road-to-atms-the-history-of-bitcoin

[10] https://www.theregister.co.uk/2017/11/07/ufc_coin_hive/

[11] https://www.reuters.com/article/us-sec-ico/wall-street-regulator-warns-celebrities-individuals-touting-digital-coins-idUSKBN1D1652

[12] http://money.cnn.com/2017/11/27/investing/bitcoin-price-new-high/

[13] https://www.arbornetworks.com/blog/asert/snatchloader-reloaded/

[14] https://seekingalpha.com/article/4127707-just-sold-half-bitcoin

[15] https://motherboard.vice.com/en_us/article/ne7nvm/is-the-pirate-bays-in-browser-cryptocurrency-mining-better-than-its-crappy-ads

[16] https://www.theregister.co.uk/2017/11/07/ufc_coin_hive/
