

Cryptocurrency-Mining Malware in the Underground

Research Brief



TrendLabs Security Intelligence Blog

Fernando Mercês

Senior Threat Researcher


May 2018

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



Crime follows the money, as the saying goes, and once again, cybercriminals have acted accordingly. The underground is flooded with so many offerings of cryptocurrency malware that it must be hard for the criminals themselves to determine which is best. This kind of malware, also known as cryptomalware, has a clear goal, which is to make money out of cryptocurrency transactions. This can be achieved through two different methods: stealing cryptocurrency and mining cryptocurrency on victims' devices surreptitiously (without the victims noticing), a process also known as cryptojacking. In this research brief, we discuss how cryptocurrency-mining malware is being peddled in the underground and how the advertised features compare against one another.

How cryptocurrency malware is advertised

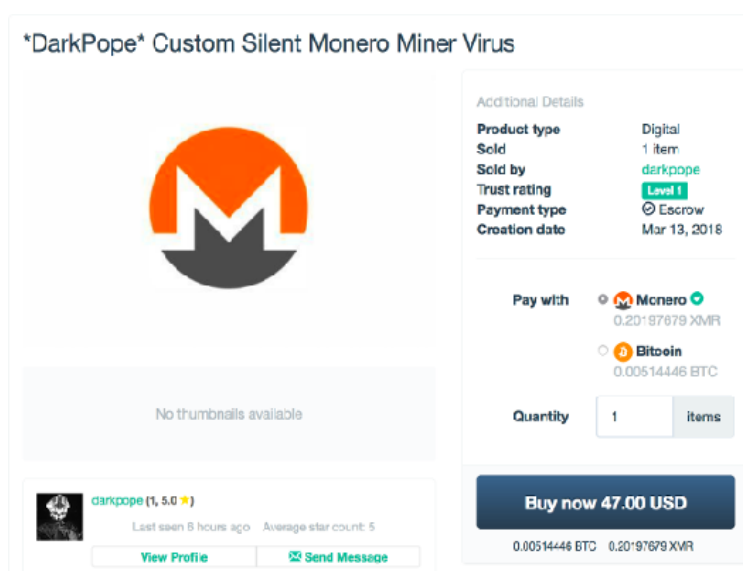


Figure 1. Posting for DarkPope custom malware

One of the latest offerings we've spotted in the underground market is a piece of malware called DarkPope. It's a Monero (XMR) cryptocurrency-mining malware built

from scratch and customized for each buyer. The price is US\$47, and the product description is as follows:

This listing is for a custom made Silent Monero Miner

How does it work:

Once infected, your victims computer will start to mine the crypto-currency Monero (XMR) for you in the background. It will be custom built just for you with your own attached Monero address for the revenues. All you have to do is to spread it as much as you can and money will come automatically. Please provide a Monero address for setup.

What you will receive:

- Custom made .exe file with your own Monero address attached to receive instant revenues
- Website to check current profits and connected victim miners
- 10+ Spreading-Guides
- 24/7 holy support

FAQ:

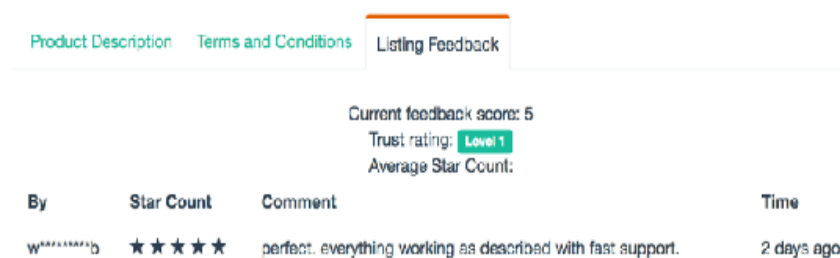
- Yes, other Altcoins are possible too upon request.
- Yes, the software will try to start again after reboot of the computer.
- Yes, the software starts again after termination of the miner process in task manager.
- No, it is not FUD by default, but will get easily through Windows Defender and Security Essentials. There are a lot of tutorials out there and people keep selling crypters on the markets. You should consider some of these options.
- Yes, it does work on x64 and x32 operating system architectures.
- You can make a Monero address at mymonero(.)com
- Yes, you'll be able to verify if it is really mining to your address and that I'm not scamming you.

Please contact me for clarification of any further questions.

ALWAYS USE PGP ENCRYPTION FOR COMMUNICATION. STAY SAFE.

Figure 2. DarkPope description

Apart from a wide range of options and features, the malware developer offers 24x7 support.



The screenshot shows a user interface for a listing. At the top, there are three tabs: 'Product Description', 'Terms and Conditions', and 'Listing Feedback', with the last one being active. Below the tabs, the feedback summary shows a 'Current feedback score: 5', 'Trust rating: Level 1' (in a green box), and 'Average Star Count:'. Below this is a table of feedback comments.

| By | Star Count | Comment | Time |
|---------|------------|---|------------|
| w*****b | ★★★★★ | perfect. everything working as described with fast support. | 2 days ago |

Figure 3. Customer feedback on DarkPope

The same actor also offers cryptocurrency-stealing malware for bitcoin (BTC) wallet addresses:

This listing is for a custom made Bitcoin Virus / Bitcoin Switcheroo / Bitcoin Address Switcher

How does it work:

Once infected, every copied Bitcoin address on the victims computer will get replaced by one of yours. The address will get changed when the victim pastes the address to send coins to somebody. To remain unsuspecting I will attach 10.000 addresses to your virus and the virus will choose the most similar address automatically. So bitcoins will get send to you by 'accident'. All you have to do, is to spread it as much as you can and coins will come automatically.

What you will receive:

- Custom made .exe file with 10.000 addresses attached
- Easy tool to check all your addresses for potential balances
- Explanation about how to cash out funds to your wallet
- 10+ Spreading-Guides
- 24/7 holy support

FAQ:

- Yes, the software will try to start again after reboot of the computer
- Yes, the software starts again after termination of the process in task manager
- No, it is not FUD by default, but will get easily through Windows Defender and Security Essentials. There are a lot of tutorials out there and people keep selling crypters on the markets. You should consider some of these options.
- Yes, it does work on x64 and x32 operating system architectures.
- No, you don't have to send me your Bitcoin address.

Figure 4. Cryptocurrency-stealing malware description

As stated by the developer, the malware changes the destination address in bitcoin transactions in memory. An interesting feature is finding similar addresses for replacement from a pool of 10,000 addresses so that once the bitcoin addresses are infected, victims would likely not notice the change and conclude the transactions, giving their coins to whoever buys this malware in the underground. This one costs US\$97, as this screenshot shows:

DarkPope Bitcoin Address Switcher Virus

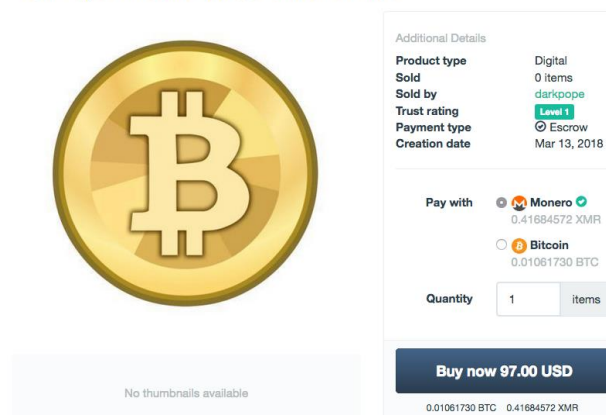


Figure 5. Posting for DarkPope bitcoin address switcher

Comparison of cryptocurrency malware offerings in the underground

Given the amount of cryptocurrency-mining malware for sale in the underground, it's infeasible to categorize or study all of it. However, we have selected 10 different recent offerings from this year and last year to serve as a basis for comparison:

| Name | Release Date | Targeted Cryptocurrency | Price |
|----------------|--------------|--|----------------------|
| xSlappz | May 8, 2017 | Zcash (ZEC) | US\$25 |
| Aqius | Oct 27, 2017 | Monero (XMR) | US\$20 |
| Flacon | Nov 24, 2017 | Ethereum (ETH), Monero (XMR) | US\$150 - 500 |
| Decadence | Nov 30, 2017 | Monero (XMR) | US\$40 – 1,000 |
| DeluxeSoftware | Jan 18, 2018 | Ethereum (ETH), Monero (XMR) | 5% profit fee |
| OverSeer | Jan 26, 2018 | Electroneum (ETN), Monero (XMR), Zcash (ZEC) | US\$15 - 90 |
| Deejayngo | Feb 12, 2018 | Ethereum (ETH), Monero (XMR) | US\$30 |
| Tommis | Feb 23, 2018 | Bitcoin (BTC) | US\$40 |
| Fluxminer | Mar 24, 2018 | Ethereum (ETH) | US\$3.99 |
| Dylan | Apr 12, 2018 | Monero (XMR) | US\$5 per .exe built |

Table 1. Comparison of cryptocurrency-mining malware offerings

As you can see, the prices started considerably low last year, then went through some spikes, and are now low again. With only US\$5, a criminal can already get a working cryptocurrency-mining malware. We have also noticed that Monero is the cybercriminals' preferred cryptocurrency.

However, don't let these 10 different offerings make you think that there aren't more. We see new offerings regularly and hundreds of new detections daily, especially if we count web-based cryptocurrency-mining malware. For instance, a simple search for pages using one of the most common Monero-mining services returned more than 25,000 results:

<Q>

css files

js files

Search

↑

Too many results? Try a phrase search with quotes: "coinhive.min.js"

Q

query syntax

29451 websites in 0.05 s.

CSV

CSV +snippets

| Rank | Domain | Snippets |
|--------|--------------------------------------|---|
| 1 424 | primewire.ag | ://coinhive.com/lib/coinhive.min.js"></script> <script> |
| 1 461 | mejortorrent.com | ed"?Module:{};self.CoinHive=self.CoinHive {};sNAME:"worker-asmjs.min.js?v7",REQUIRES_AU nhive.com/lib/,"ASMJS_NAME:"worker-asmjs |
| 2 586 | gowatchfreemovies.to | ://coinhive.com/lib/coinhive.min.js"></script> <script> |
| 3 400 | moonbit.co.in | javascript" src="js/coinhive.min.js?v3"></script> <scri |
| 3 742 | xpau.se | ://coinhive.com/lib/coinhive.min.js"></script> <script> |
| 7 588 | animesorion.tv | ://coinhive.com/lib/coinhive.min.js"></script> <script> |
| 7 956 | xmoviesforyou.com | ://coinhive.com/lib/coinhive.min.js" type="text/rockets |
| 9 955 | seriesdanko.to | //coin-hive.com/lib/coinhive.min.js"></script> <script> |
| 10 154 | avxhm.se | })(); { if (!window.coinhive_check_count) { wind 3.3.6/css/bootstrap.min.css" rel="stylesheet" shee ype="application/json"> { "@context": " |
| 10 643 | dpstream.net | ://coinhive.com/lib/coinhive.min.js"></script> <script> |
| 10 770 | mejorenvo.com | ed"?Module:{};self.CoinHive=self.CoinHive {};sNAME:"worker-asmjs.min.js?v7",REQUIRES_AU ebook.net/es_ES/all.js?ver=3.1.1#xfbml=1"> |
| 11 692 | adguard.com | ryptocurrency-miner-coinhive" target="_blank" re et" href="/css/main.min.css?version=895"> < g.src = u + "piwik.js"; s.parentNode.inse |
| 12 178 | xrysol.online | ://coinhive.com/lib/coinhive.min.js"></script><script>v |

Figure 6. Search results for Monero-mining services

Notice that not all of these domains are compromised. They may be intentionally mining Monero, either warning their visitors of the fact or not, but we believe that there is a high chance that some of them are malicious.

In addition, the offerings are not restricted to miners. Stealers are also there, albeit in lower numbers. This screenshot shows an offering for a piece of cryptocurrency-stealing malware called Pony for 0.0023 BTC (approximately US\$20):

Pony 2.2 Cryptocoin stealer

Sold by: **Pickstone** (2) (/0) **Trust: 100%**

0.0023 BTC

Question?

Sold 0 times since Jan 30, 2018

Escrow:
Class: Digital
Ships from: Hell

Shipping time: 1 Days
Ship to: Worldwide
Auto-shipping: **Yes**

Shipping Method: Instant


Tracking Number: **No**

Buy Now

Figure 7. Posting for cryptocurrency-stealing malware

Varying features and price points

Different features make for varying price points. For instance, Decadence Miner starts at US\$40 but it can cost up to US\$1,000, depending on the features chosen by the buyer:



Decadence Miner
Published on Nov 27, 2017

THIS IS MY CPU SILENT MINER WITH ADMIN CONTROL PANEL. ON THIS VIDEO IM SHARING HOW HE'S WORKING.

GENERAL PLAN:

The whole application was written by C++
Miner is completely hidden from taskmanager and monitor system resources softwares
Can be run without admin permissions
Can be joined with other application (has no conflicts)
Can be easily crypted by third-party crypters
The protect from process closing
All folders and files is hidden
Process restoration
Dynamic threads / cores calculation
Running delays
Autorun with system start
FUD (0-5 defects)
(optional) Fake messages, alerts after miner has started work
PRICE: 40\$

PRO PLAN:

Extend General plan
You will get manual with 14 ways of spreading your miner
Client support 24/7
Free daily cleaning of file
Free changing of mining currency and loggers
The subsequent updates are free
PRICE: 70\$

EXTENDED PLAN:

Extend Pro plan
Exclusive control panel for your workers (with an opportunity to give tasks)
Free help with setup panel, hosting etc.
FUD (0-5 defects) with the same RUNTIME
Unique stab
Up to 5 wallets on 1 account
An opportunity to sell 4 copies of general plan to others (100% payback)
PRICE: 100\$

PRIVATE PLAN:

Extend all planes
Completely FUD (without defects)
Individual work with the client to get maximum profit of his goals (100% private)
PRICE: 1000\$

ADDITIONAL MODULES:

1. Substitutions BTC address to yours - 15\$
2. Data stealer(grabber) with control panel - 50\$

Figure 8. Decadence Miner and its features

Additional features such as graphics processing unit (GPU) support, web-based control panel, remote access tool (RAT) capabilities, and crypting services usually increase the price of the cryptomalware. This is also the case with OverSeer, which offers different plans for hiring cryptocurrency-mining malware services:



Figure 9. OverSeer and its package offerings

The current limited profitability of cryptocurrency-mining malware

Despite the large number of malware samples and offerings, we are not aware of large amounts of money being made with cryptocurrency-mining malware. Among all the reports on attacks involving it, apparently the most successful one was when a threat actor compromised thousands of websites in the U.S. and the U.K. and subsequently embedded a cryptominer in them. The malware stayed active for four hours, but the wallet used to receive the mined Monero coins had no more than [US\\$24](#) by the end of the attack, when the websites were cleaned. Of course, the more popular a website is, the quicker the victims will notice and let the website administrators know about the irregularities. From there, the cleaning process starts and the mining campaign ends.

It's not the same for cryptocurrency-stealing malware, though. In March, researchers reported a [cryptostealing campaign](#) that made around 8.8 BTC (approximately US\$80,000 at the time of reporting) after cybercriminals were able to put trojanized versions of legitimate software in a popular software download website.

Conclusion

It was actually hard to finish this publication, considering that new cryptocurrency malware conversations kept appearing every day in multiple places. We believe this is a huge trend, one that is unlikely to go away anytime soon. We have seen miners moving from bitcoin to Ethereum and now embracing Monero and Zcash. Some criminals have also started conversations about MoneroV, which hasn't even been released yet. And then there's the multiplicity of versions across the web, mobile, and the internet of things (IoT) — basically, all platforms may be affected.

Of course, criminals won't make a huge amount of money out of 10,000 Internet Protocol (IP) cameras, but maybe a million routers that can facilitate a [large-scale attack](#) could work for them. If we combine the risk of cryptomalware (including both the cryptocurrency-mining kind and the cryptocurrency-stealing one) with unpatched vulnerabilities, botnets, and other threats, we'll have a serious problem to reckon with.





Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection.

With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

©2018 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO