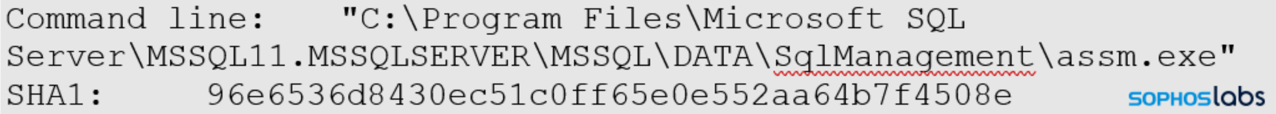
MrbMiner: Cryptojacking to bypass international sanctions

news.sophos.com/en-us/2021/01/21/mrbminer-cryptojacking-to-bypass-international-sanctions/

January 21, 2021

While searching through our telemetry, we found a handful of logs where a database server process (sqlservr.exe) launched a downloader executable that seemed to spontaneously appear on the server. The downloader retrieved a cryptominer called MrbMiner. Based on open-source intelligence, the miner appears to have been created, hosted, and controlled by a small software development company based in Iran.

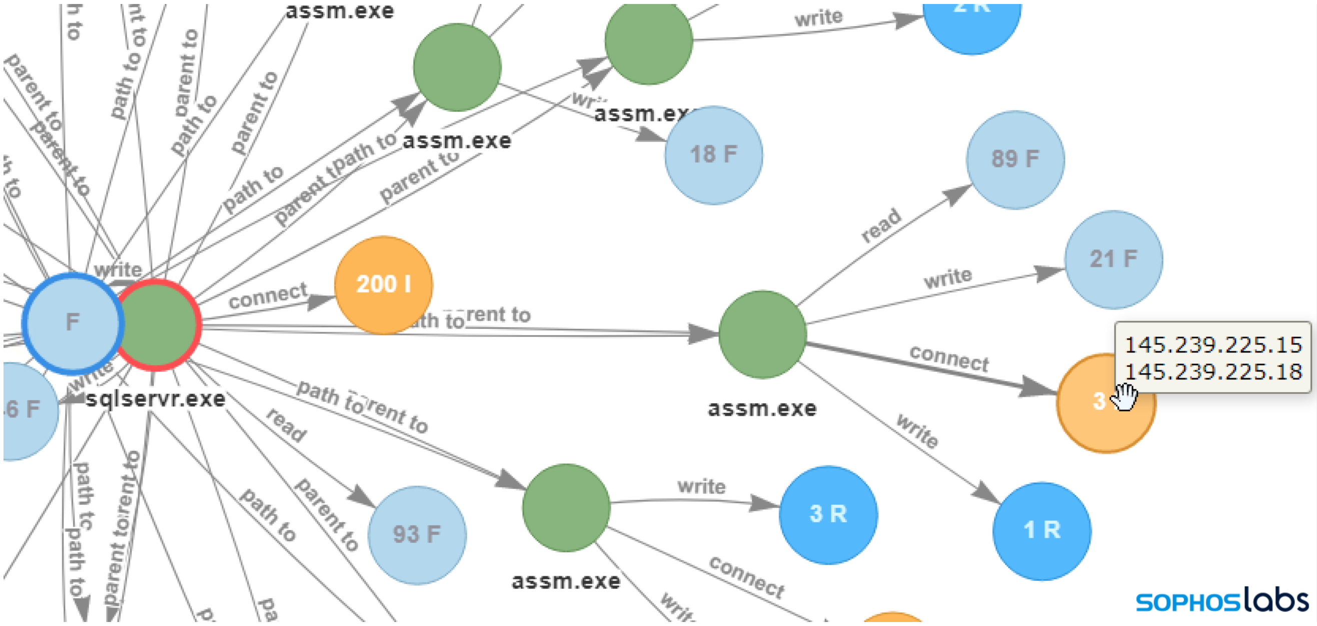


```
Command line:    "C:\Program Files\Microsoft SQL
Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\SqlManagement\assm.exe"
SHA1:      96e6536d8430ec51c0ff65e0e552aa64b7f4508e
```

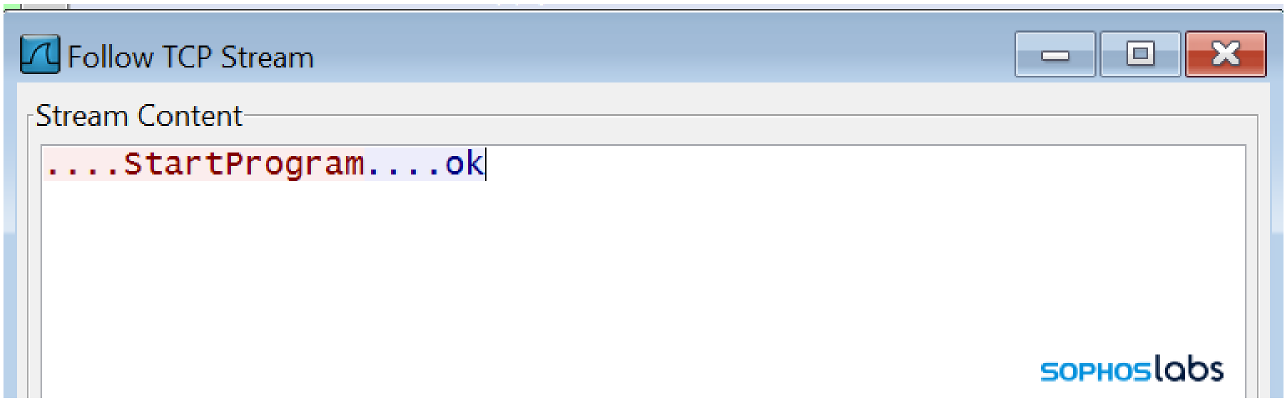
MrbMiner was downloaded by an executable run from the Microsoft SQL server directory

While our records don't reveal exactly how the malware gained a foothold on the database servers, it stands to reason the attackers may have used similar techniques as the MyKings, Lemon_Duck, or Kingminer miners, whose attack methods we have documented in previous articles.

When IT admins want to host a database, they have certain performance requirements: The ability to process lots of data reads and writes, and enough RAM and processor overhead to respond promptly to queries. As a result, servers hosting databases fall on the beefier side of the performance scale, which is why they're an excellent target for attackers whose goals include the distribution of cryptocurrency miners. People who live in countries that are under strict international financial sanctions, like Iran, can leverage cryptocurrency to bypass the traditional banking system.

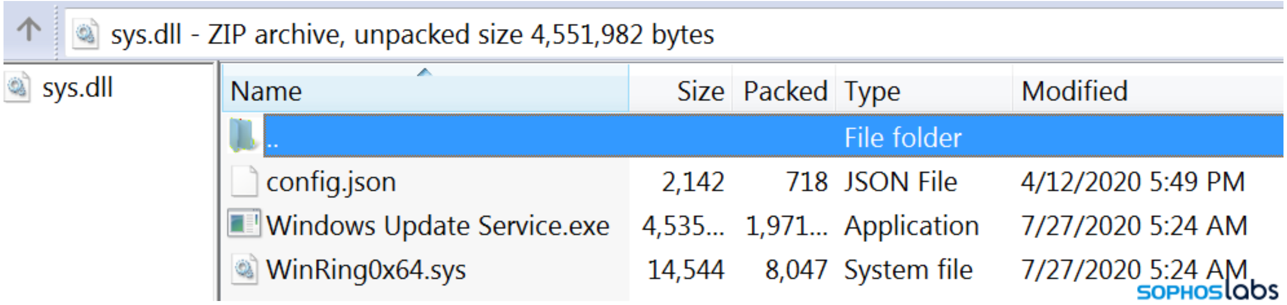


The Mrbminer investigation begins with the Microsoft SQL Server (sqlservr.exe) process launching a file called **assm.exe**, a downloader Trojan. The assm.exe program downloads the cryptominer payload from a web server, then connects to its command-and-control server to report the successful download and execution of the miner.



```
....StartProgram....ok
```

In most cases, the payload was a file named **sys.dll**, which (despite its file suffix) was not a Windows DLL but a zip archive containing a cryptominer binary, configuration file, and related files.



sys.dll - ZIP archive, unpacked size 4,551,982 bytes

sys.dll

Name	Size	Packed	Type	Modified
..			File folder	
config.json	2,142	718	JSON File	4/12/2020 5:49 PM
Windows Update Service.exe	4,535...	1,971...	Application	7/27/2020 5:24 AM
WinRing0x64.sys	14,544	8,047	System file	7/27/2020 5:24 AM

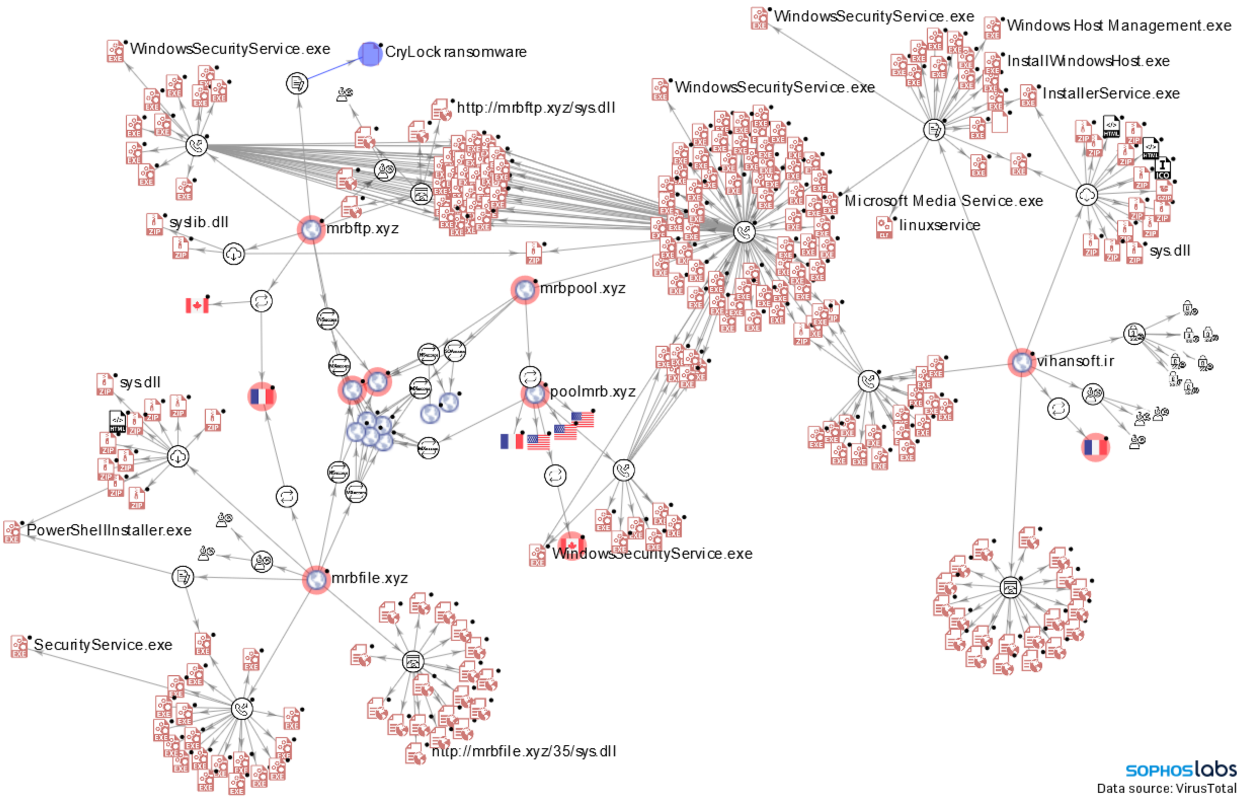
We also found a copy of this same sys.dll payload available from a Github user account that has been subsequently shut down. Several of the servers also hosted a Linux build of the cryptominer payload, but its configuration file used a different cryptocurrency wallet address than the Windows version did.

The MrbMiner cryptojacking payload included a kernel-level device driver (**WinRing0x64.sys**), and a miner executable named **Windows Update Service.exe** to obfuscate its purpose. The executable was a modified version of the XMRig miner.

The WinRing0x64.sys file is a kernel driver (publicly available on its creator's Github page) that allows userland applications to access *ring0*-level resources. It gives the attacker access to features like the CPU's model-specific register, and can read from or write to memory, directly. In particular, cryptominers use this driver to modify the MSR registers in order to disable CPU prefetchers, which results in a 6-7% performance improvement. This driver is a standard functionality that had been added to XMRig miners beginning around December, 2019.

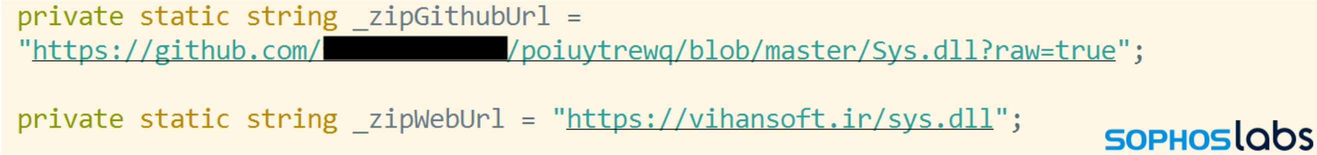
Suspicious file naming convention shared across source domains

The MrbMiner samples we initially found came in a zip named sys.dll. Under further scrutiny, we found a large network of related files and URLs hosting them.


WindowsSecurityService.exe
CryLock ransomware
http://mrbftp.xyz/sys.dll
WindowsSecurityService.exe
WindowsSecurityService.exe
Windows Host Management.exe
InstallWindowsHost.exe
InstallerService.exe
Microsoft Media Service.exe
linuxservice
sys.dll
syslib.dll
mrbftp.xyz
mrbpool.xyz
vihansoft.ir
sys dll
poolmrb.xyz
PowerShellInstaller.exe
WindowsSecurityService.exe
mrbfile.xyz
SecurityService.exe
http://mrbfile.xyz/35/sys.dll
SOPHOSlabs

Data source: VirusTotal

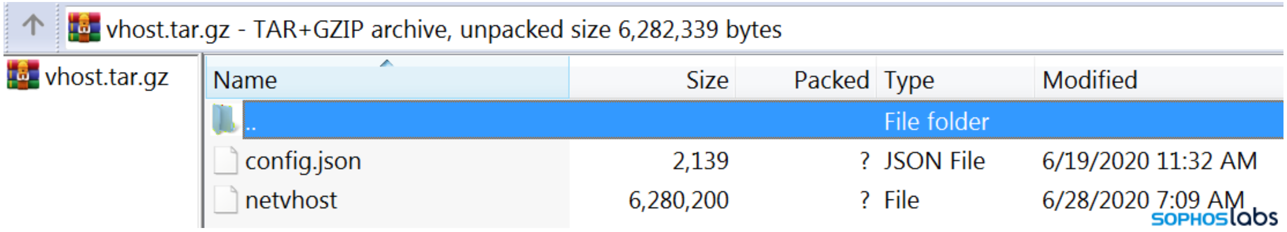
We began by digging into the domain hardcoded into the miner’s configuration file, **vihansoft.ir**.



```
private static string _zipGithubUrl =
"https://github.com/[redacted]/poiuytrewq/blob/master/Sys.dll?raw=true";

private static string _zipWebUrl = "https://vihansoft.ir/sys.dll";
```

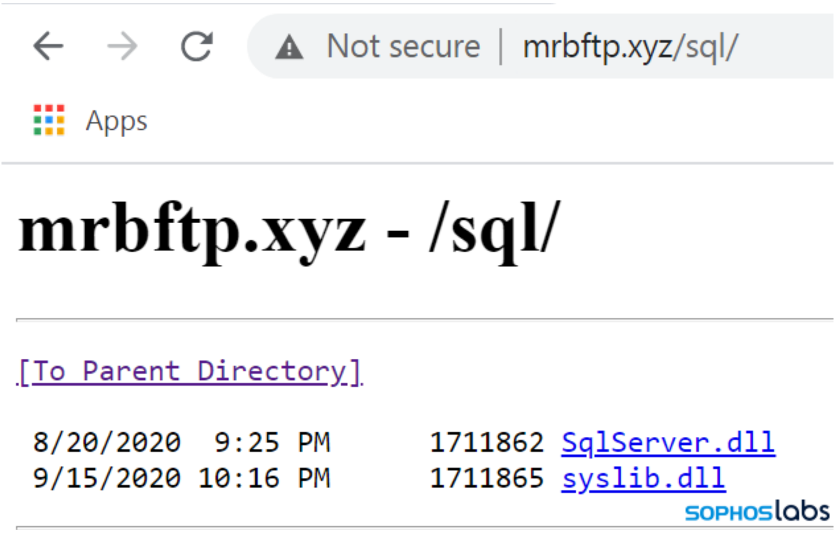
This domain connected to lots of other zip files containing copies of the miner, including ones named agentx.dll and hostx.dll. These deliberately-misnamed zip archives variously contained payloads named **Windows Security Service.exe, Windows Host Management.exe, Install Windows Host.exe, Installer Service.exe, Microsoft Media Service.exe**, and (Linux) ELF executables named **linuxservice** and **netvhost**.



vhost.tar.gz - TAR+GZIP archive, unpacked size 6,282,339 bytes

Name	Size	Packed	Type	Modified
..			File folder	
config.json	2,139	?	JSON File	6/19/2020 11:32 AM
netvhost	6,280,200	?	File	6/28/2020 7:09 AM

Many of the identical files had been downloaded from other domains, including mrbfile.xyz and mrbftp.xyz. Several other malicious files had also been hosted on these sites, with zips named sys.dll and syslib.dll, and payloads inside the archives named **Windows Security Service.exe, SecurityService.exe,** and **PowerShellInstaller.exe.**



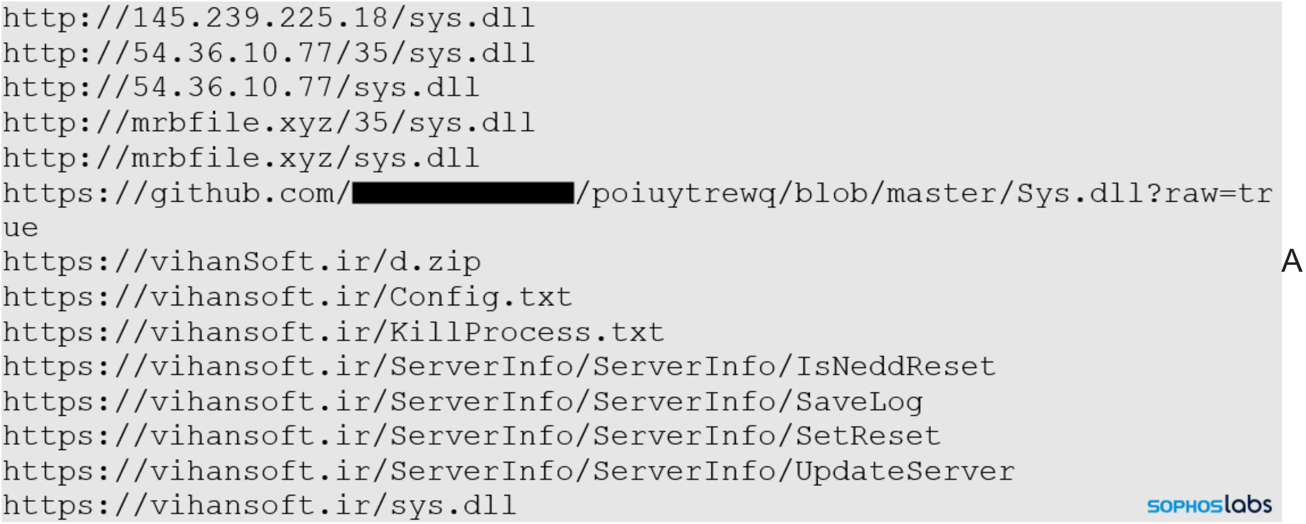
mrbftp.xyz - /sql/

[To Parent Directory]

```
 8/20/2020  9:25 PM      1711862 SqlServer.dll
 9/15/2020 10:16 PM      1711865 syslib.dll
```

Making an attribution

In many ways, the attack seemed typical of most cryptominer attacks we've seen targeting internet-facing servers. Where it was distinctly different was that the attacker themselves appears to have thrown caution to the wind about concealing their identity; A lot of the records relating to the miner's configuration, its domains and IP addresses, point to a single point of origin: a small software company based in Iran.



```
http://145.239.225.18/sys.dll
http://54.36.10.77/35/sys.dll
http://54.36.10.77/sys.dll
http://mrbfile.xyz/35/sys.dll
http://mrbfile.xyz/sys.dll
https://github.com/[redacted]/poiuytrewq/blob/master/Sys.dll?raw=tr
ue
https://vihanSoft.ir/d.zip
https://vihansoft.ir/Config.txt
https://vihansoft.ir/KillProcess.txt
https://vihansoft.ir/ServerInfo/ServerInfo/IsNeddReset
https://vihansoft.ir/ServerInfo/ServerInfo/SaveLog
https://vihansoft.ir/ServerInfo/ServerInfo/SetReset
https://vihansoft.ir/ServerInfo/ServerInfo/UpdateServer
https://vihansoft.ir/sys.dll
```

A list of URLs that have hosted MrbMiner downloads or related files

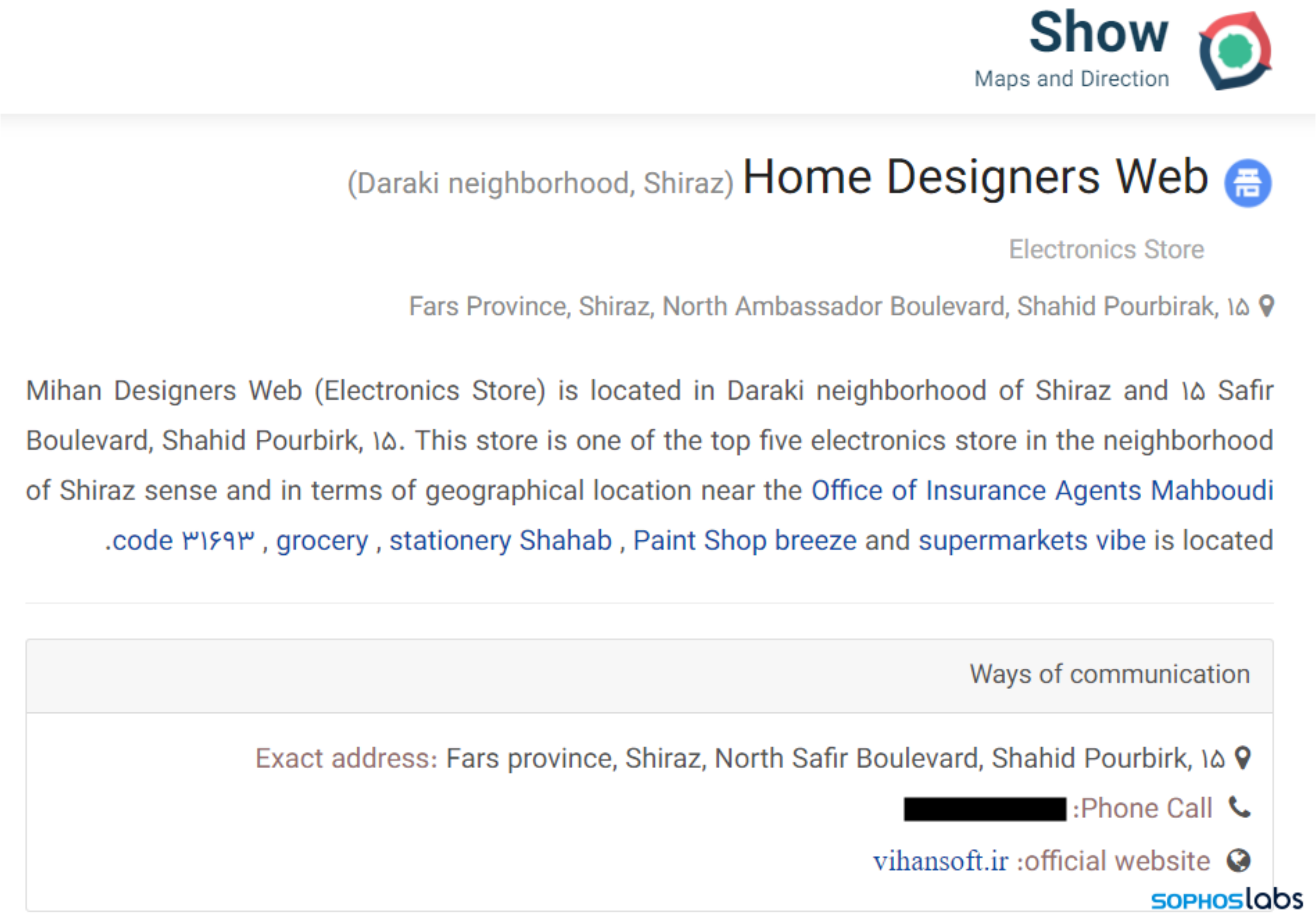
One reason cryptocurrency mining attacks are so frustrating is that it is hard to leverage law enforcement to address the problem. The source of the miners are, usually, anonymous, as is the destination of the harvested cryptocurrency value. But the MrbMiner creator may be easier to determine.

The payload location and the C2 server addresses are both hardcoded into the downloader.

One domain, used as both a C2 and a payload server, was vihansoft.ir, registered to a software development company based in Iran. Payloads were also downloaded directly from the same IP address used to host vihansoft.ir (and from a few other domains which contained the string "mrb," such as mrbfile.xyz).

When we see web domains that belong to a legitimate business implicated in an attack, it’s much more common that the attackers simply took advantage of a website to (temporarily, in most cases) use its web hosting capabilities to create a “dead drop” where they can host the malware payload. But in this case, the domain’s owner is implicated in spreading the malware.

We found a reference to the business behind vihansoft.ir in the Persian-language mapping website neshan.org. Similar to Google Maps or Waze, Neshan includes business information as part of its mapping services, and the entry for a company that lists vihansoft.ir as its website, and names its managing director.



(Daraki neighborhood, Shiraz) Home Designers Web

Electronics Store

Fars Province, Shiraz, North Ambassador Boulevard, Shahid Pourbirak, ۱۵

Mihan Designers Web (Electronics Store) is located in Daraki neighborhood of Shiraz and ۱۵ Safir Boulevard, Shahid Pourbirk, ۱۵. This store is one of the top five electronics store in the neighborhood of Shiraz sense and in terms of geographical location near the Office of Insurance Agents Mahboudi .code ۳۱۶۹۳ , grocery , stationery Shahab , Paint Shop breeze and supermarkets vibe is located

Ways of communication

Exact address: Fars province, Shiraz, North Safir Boulevard, Shahid Pourbirk, ۱۵

[redacted] :Phone Call

vihansoft.ir :official website

A machine-translated version of the Neshan website identifies the owners of the vihansoft domain

We found the miner downloads in the web root of the vihansoft domain, in a repository under a now-shuttered Github user account, and on the mrbfile.xyz and mrbftp.xyz domains, as well as on a small number of IP addresses.

The compiled cryptominer binaries were compressed into zip files that contained .PDB debug info. These strings are artifacts of the compiler used on the machine where the executable was built. The PDB debug strings included a build path with the line ” C:\Users\_____\” in it (with the name redacted here), indicating the user account under which the binary was compiled. This string matches the name associated with the Github account.

Cryptocurrency data was sent to wallets on the poolmrb.xyz and mrbpool.xyz domains as well as to the pool.supportxmr.com domain. Miner malware downloaded from the vihansoft.ir, mrbfile, and mrbftp domains communicated with the poolmrb/mrbpool domains.

Neither the “mrb” domains nor vihansoft had any usable WHOIS information, but they did have one other thing in common: They all used the same WHOIS privacy service, WhoisGuard, based in Panama, to conceal the domain ownership information.

Detection and IoCs

Cryptominer samples of MrbMiner are detected in Sophos Endpoint Protection under the definition **Troj/Miner-ZD***.*

Additional indicators of compromise have been published to the SophosLabs Github.