KryptoCibule: The multitasking multicurrency cryptostealer

welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

September 2, 2020

ESET researchers analyze a previously undocumented trojan that is spread via malicious torrents and uses multiple tricks to squeeze cryptocoins from its victims while staying under the radar

ESET researchers analyze a previously undocumented trojan that is spread via malicious torrents and uses multiple tricks to squeeze cryptocoins from its victims while staying under the radar

ESET researchers have uncovered a hitherto undocumented malware family that we named KryptoCibule. This malware is a triple threat in regard to cryptocurrencies. It uses the victim's resources to mine coins, tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files, all while deploying multiple techniques to avoid detection. KryptoCibule makes extensive use of the Tor network and the BitTorrent protocol in its communication infrastructure.

The malware, written in C#, also employs some legitimate software. Some, such as Tor and the Transmission torrent client, are bundled with the installer; others are downloaded at runtime, including Apache httpd and the Buru SFTP server. An overview of the various components and their interactions is shown in Figure 1.

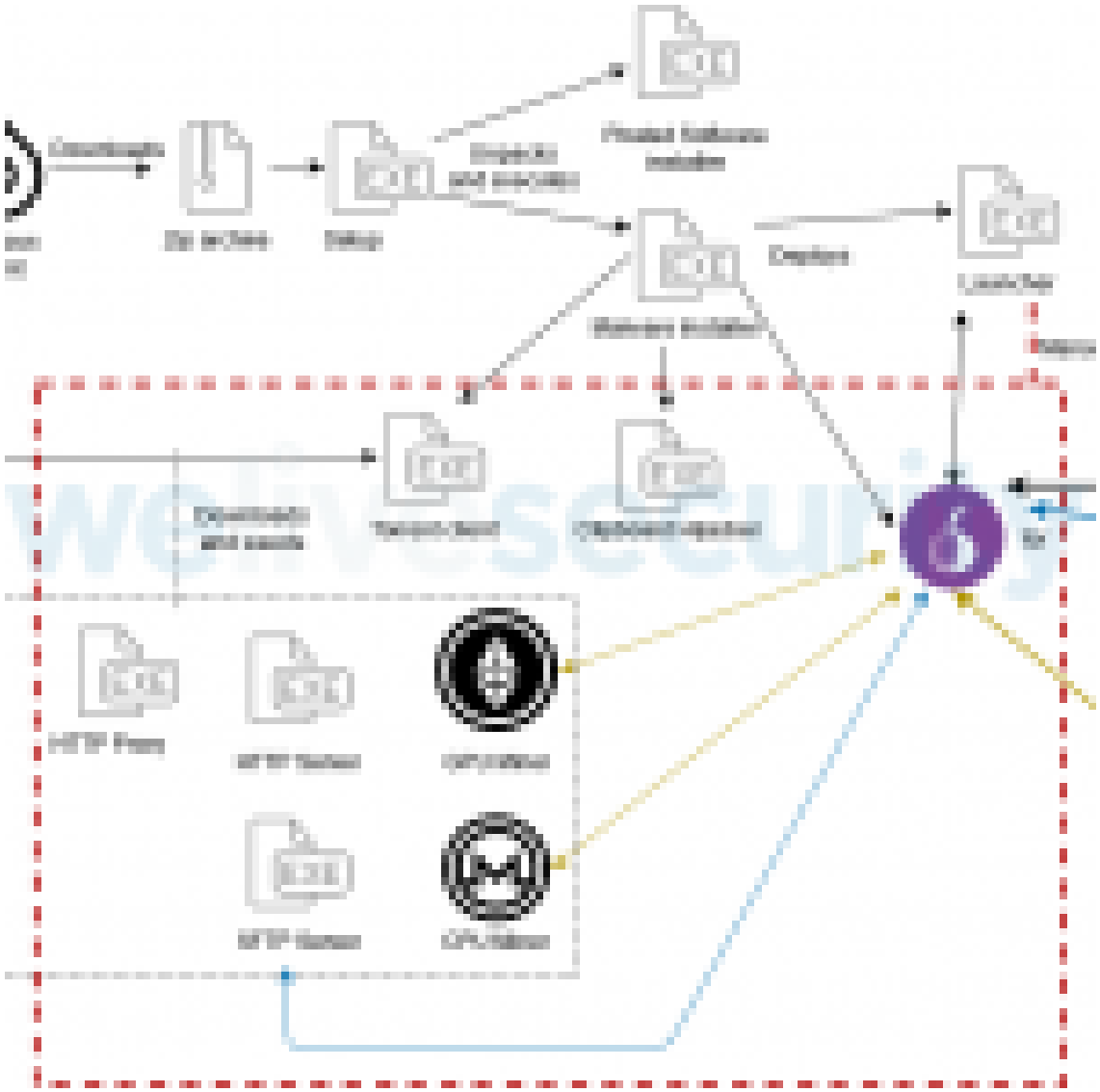

Figure 1. KryptoCibule components and tools

When the malware is first executed, the host is assigned a unique identifier with the format {adjective}-{noun} where {adjective} and {noun} are random words taken from two hardcoded lists which provide over 10 million unique combinations. This identifier is then used to identify the host in communications with the C&C servers.

On top of the crypto-related components, KryptoCibule also has RAT functionality. Among the commands it supports are EXEC, which allows execution of arbitrary commands and SHELL, which downloads a PowerShell script from the C&C. This script then loads a backdoor generated with the post-exploitation tool Pupy.

The name KryptoCibule derives from the Czech and Slovak words for “crypto” and “onion”.

Timeline

We have uncovered multiple versions of this malware, enabling us to trace its evolution all the way back to December 2018. Figure 2 shows the changes made over time to KryptoCibule.

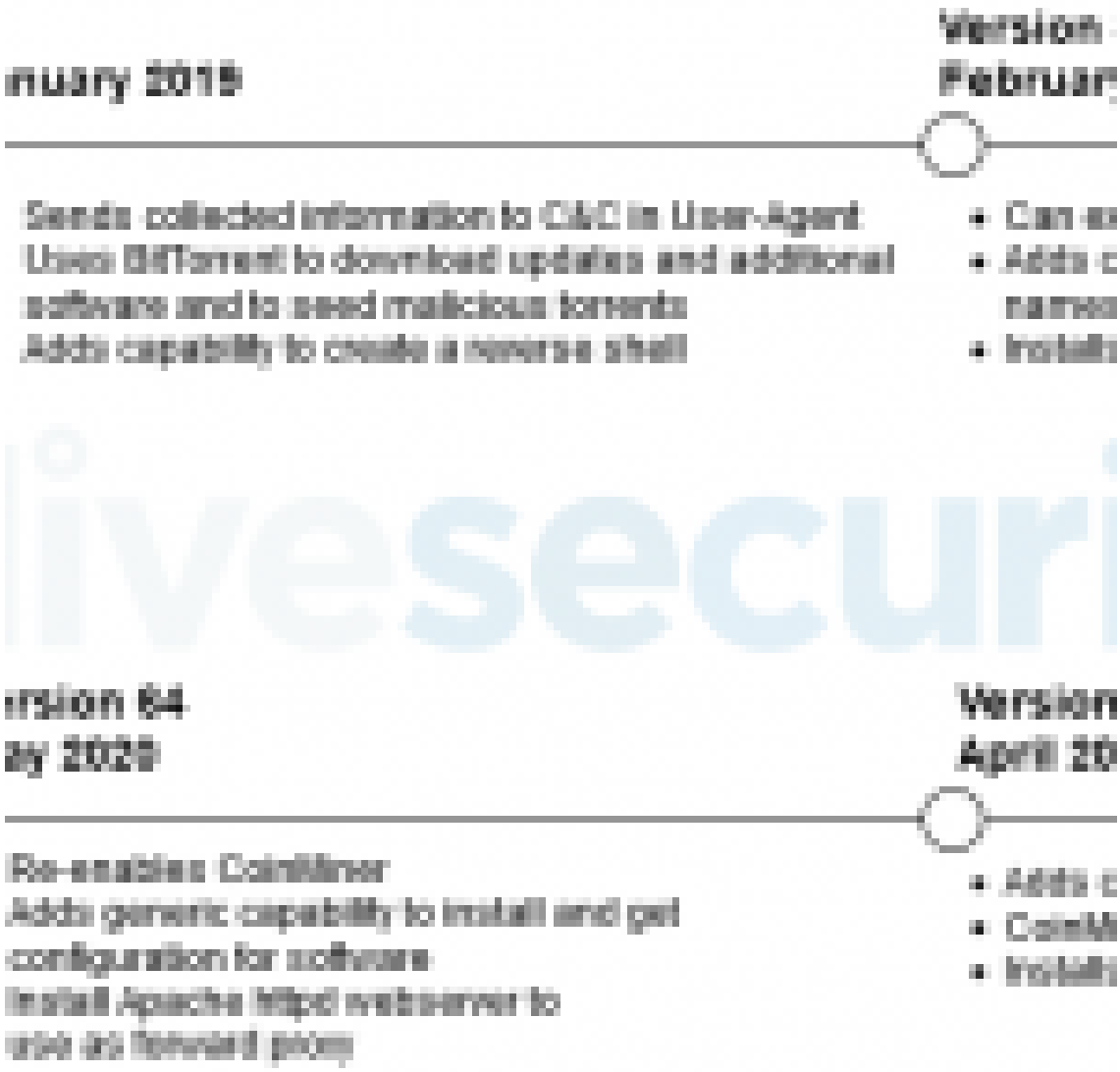

Figure 2. Timeline of updates and functionality changes

Targets

According to ESET telemetry (shown in Figure 3), the malware seems to target mostly users in Czechia (the Czech Republic) and Slovakia. This reflects the user base of the site on which the infected torrents are found.

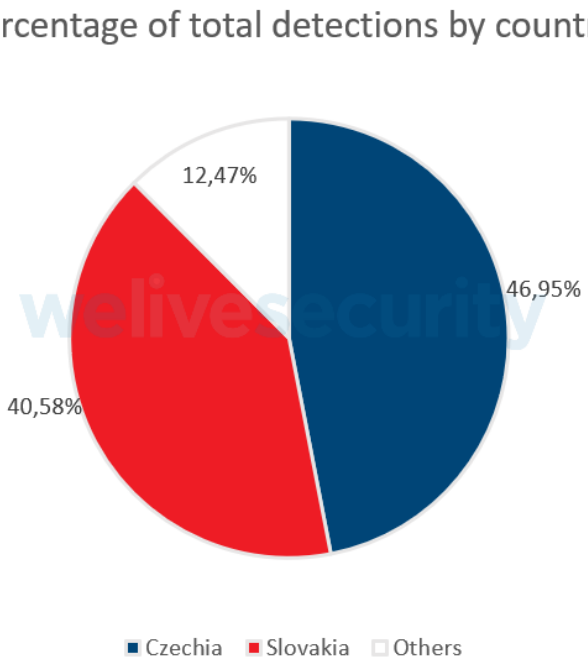

Figure 3. In our telemetry data, over 85% of detections were located in Czechia and Slovakia

Almost all the malicious torrents were available on uloz.to; a popular (At the time of this writing, this website and its localized variant (ulozto.cz and ulozto.sk respectively) are both in the Alexa top 50 most visited sites in Czechia and in the top 75 most visited sites for Slovakia) file sharing site in Czechia and Slovakia (see Figure 4). We'll explain how these torrents are used to spread KryptoCibule in the next section.

Figure 4. One of the malicious torrents on uloz.to

As detailed in the *Anti-detection and anti-analysis techniques* section below, KryptoCibule specifically checks for ESET, Avast, and AVG endpoint security products; ESET is headquartered in Slovakia, while the other two are owned by Avast, which is headquartered in Czechia.

Torrents

KryptoCibule makes use of the BitTorrent protocol to spread to new victims and to download additional tools and updates.

Initial Compromise

KryptoCibule is spread through malicious torrents for ZIP files whose contents masquerade as installers for cracked or pirated software and games. Although other files may be included, as seen in Figure 5, there are five that are common to all KryptoCibule installer archives. packed.001 is the malware, while packed.002 is the installer for the expected software. Both are XOR-encrypted with keys contained in Setup.exe.

When Setup.exe is executed, it decodes both the malware and the expected installer files. It then launches the malware – in the background – and the expected installer – front and center – giving the victim no indication that anything is amiss.

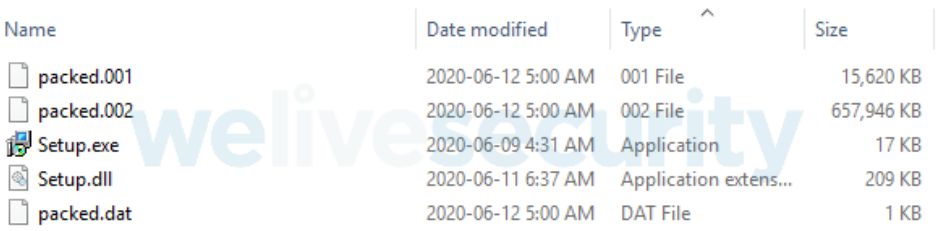

Figure 5. Content of the Dead.Cells.Incl.All.DLC archive with only the minimum common set of KryptoCibule installer files shown

Additional software and updates

The BitTorrent protocol is also used to download updates to the malware, and additional software.

KryptoCibule installs the transmission-daemon torrent client and manages it by issuing commands via its RPC interface on port 9091 with transmission-remote. The RPC interface uses the hardcoded credentials superman:krypton.

To install further software for the malware's use, such as the SFTP server, the Launcher component makes an HTTP GET request to %C&C%/softwareinfo?title=<software name> and receives a JSON response containing a magnet URI (Magnet links are a type of URI that identify files by using a cryptographic hash of their contents rather than their location. These links may also include metadata about the file. They are commonly used in the BitTorrent protocol to identify files to be shared. See https://www.bittorrent.com/blog/2016/01/27/reshaping-the-internet-whats-a-magnet-link/) for the torrent to download and other information indicating how to install and execute the program. Figure 6 shows an example of such a response.

```
1  {"Magnet": "magnet:?xt=urn[:]btih:67yd647nivxhumoedvwnwnzve55b3bxj&dn=free-BuruServer-x64-v1.7.3.zip", "Version": 1,"ExecutableRelativePath": "", "ExecutableFileName": "buru.exe","ExecutableArgs": "run", "InstallFile": "", "HasCustomConfig": true}
```

Figure 6. Sample response for a GET /softwareinfo?title=ssh_server request

The mechanism for getting updates is similar. The malware first gets global settings via HTTP from %C&C%/settingsv5. Among other things, this response contains a magnet URI for the latest version of the malware. It then makes a GET request to %C&C%/version to get the most recent version number. If the local version is lower than that version, the torrent is downloaded and installed.

Torrents are added to Transmission using the following command:

transmission-remote localhost -n superman:krypton -a "<magnet URI>"

A hardcoded list of 50 trackers (In the BitTorrent protocol, a tracker is a server that helps clients find and coordinate with peers to transfer files. See https://en.wikipedia.org/wiki/BitTorrent_tracker.) is used to get peers for all torrents.

Seeding malicious torrents

Victims are also used to seed (In the BitTorrent protocol, a seed is a peer that has a complete torrent and that lets others download that torrent's files from it. See https://help.bittorrent.com/support/solutions/articles/29000023347-what-is-seeding-.) both the torrents used by the malware and the malicious torrents that help spread it. Infected hosts get a list of magnet URIs from %C&C%/magnets, download them all and keep seeding them. This ensures that these files are widely available for others to download, which helps speed up the downloads and provides redundancy.

Anti-detection and anti-analysis techniques

This malware leverages a variety of techniques to avoid detection, along with some basic anti-analysis protections.

It starts with the initial access vector. The executable contained inside the ZIP archive is a rather benign installer program that masquerades as the legitimate InstallShield program. This file is scrambled with the open source program Obfuscar. This same tool is used on all of the malware's custom executables. The malicious code itself is located inside an XOR-encrypted file, the key being a GUID hardcoded in Setup.exe.

The malware is then installed to the hardcoded path %ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\update and uses legitimate Adobe Acrobat Reader executable names for the bundled Tor executable and its own. Some of the files contained in the install folder can be seen in Figure 7.

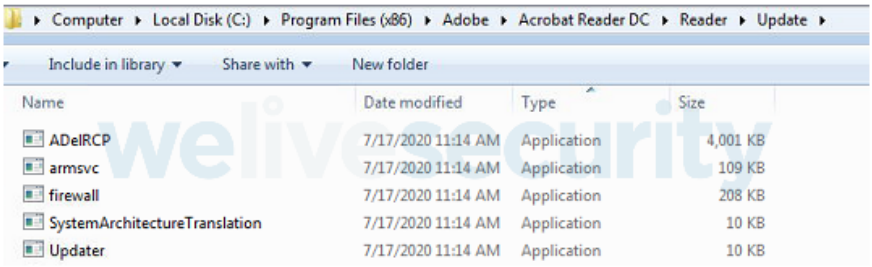

Figure 7. Some of the files in the install folder. Armsvc.exe is the malware and ADelRCP.exe is the Tor executable. Both filenames are actually used by Adobe Reader.

To achieve persistence, KryptoCibule creates a scheduled task to be run every five minutes with the following command. Once again, it uses an Adobe Reader-related name.

schtasks.exe /CREATE /SC MINUTE /MO 5 /TN "**Adobe Update Task**" /TR \""%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\Update\armsvc.exe\"" [/RL HIGHEST] /F [/RU SYSTEM]

Before first executing its payload and on every iteration of the main loop, the malware performs a check for running analysis software using the following list. If any process with a matching name is found, it stops all running components and exits.

- cain
- filemon
- netmon
- netstat
- nmwifi
- perfmon
- processhacker
- procexp
- procexp64
- procmon
- regmon
- tasklist
- taskmgr
- tcpvcon
- tcpview
- wireshark

Antivirus evasion

Before initializing the cryptominer components, the malware performs a case-insensitive check of the rootSecurityCenter2\AntiVirusProduct WMI object for the strings avast, avg and eset, as seen in the decompiled code in Figure 8. Should any of these strings be detected If any of them were detected, the cryptominer

components will not be installed.

```
private bool isTargetAVInstalled(IEnumerable<string> antiviruses)
{
    using (IEnumerator<string> enumerator = antiviruses.GetEnumerator())
    {
        while (enumerator.MoveNext())
        {
            if (enumerator.Current.ToLowerInvariant().strContains(new string[]
            {
                ProgramStrings.str_avast(),
                ProgramStrings.str_avg(),
                ProgramStrings.str_eset()
            }))
            {
                return true;
            }
        }
        return false;
    }
    bool result;
    return result;
}
```


Figure 8. Cleaned up decompiled code of the function used to check for specific security products

Whenever the malware installs itself, an update or a new component, the install path used is excluded from Windows Defender automatic scanning by issuing the following command:

powershell -c “Add-MpPreference -ExclusionPath ‘<install path>'”

It also creates firewall rules using innocuous-looking names to explicitly allow inbound and outbound traffic from its components. A rule to block outbound traffic from the ESET Kernel Service (ekrn.exe) is also created by the function shown in Figure 9.

Figure 9. Function that blocks outbound traffic from ekrn.exe in the Windows Firewall

Tor network usage

KryptoCibule brings along the tor.exe command line tool, masquerading as ADelRCP.exe, and a configuration file (seen in Figure 10) as libstringutils.dll.

```
SOCKSPolicy accept 127.0.0.1
SOCKSPolicy reject *

SocksPort 127.0.0.1:9050 PreferSOCKSNoAuth

# MaxClientCircuitsPending 1024

HiddenServiceDir default
HiddenServiceVersion 3
HiddenServicePort 9091 127.0.0.1:9091
HiddenServicePort 9999 127.0.0.1:9999
HiddenServicePort 9187 127.0.0.1:9187
HiddenServicePort 9188 127.0.0.1:9188
HiddenServicePort 12461 127.0.0.1:12461
```


Figure 10. The Tor configuration file used by the latest version of the malware

This sets up a SOCKS proxy on port 9050 that is used by the malware to relay all communications with the C&C servers through the Tor network. This has the dual benefit of encrypting the communications and making it virtually impossible to trace the actual server or servers behind these URIs.

The second part of the configuration file sets up onion services (In Tor, onion services are a way of making a service running on a certain port only reachable via the Tor network.) on the victimized host. These are accessible by the operators over the Tor network. When first starting up these services, Tor automatically generates a .onion URI for the host. This unique hostname is then sent to %C&C%/transferhost/<unique name>. We will discuss how these onion services are used in the upcoming sections.

Port Number	Service
9091	Transmission Daemon RPC interface
9999	Apache httpd server
9187	Buru SFTP server
9188	Buru Web Admin
12461	MiniWeb HTTP server

The onion URIs for two C&C servers are contained in the malware. One of these provides a REST API that the malware uses for most communications, while the other is used to download files. Additional URIs can be obtained one at a time with a request to %C&C%/server. Some older versions of the malware use these to download updates via port 12461. We believe that these URIs point to other infected hosts. The versions of the malware that use them have code to place their downloaded updates into a directory served by the MiniWeb HTTP server on that same port.

We were able to identify one IP address for the file server C&C in our telemetry data.

Acquiring cryptocurrency

KryptoCibule has three components that leverage infected hosts in order to obtain cryptocurrencies.

Cryptomining

The latest versions of KryptoCibule use XMRig, an open source program that mines Monero using the CPU, and kawpowminer, another open source program that mines Ethereum using the GPU. The second one is only used if a dedicated GPU is found on the host. Both of these programs are set up to connect to an operator-controlled mining

server over the Tor proxy.

On every iteration of the main loop, the malware checks the battery level and the time since the last user input. It then starts or stops the miner processes based on this information. If the host has received no user input in the last 3 minutes and has at least 30% battery, both the GPU and CPU miners are run without limits. Otherwise, the GPU miner is suspended, and the CPU miner is limited to one thread. If the battery level is under 10%, both miners are stopped. This is done to reduce the likelihood of being noticed by the victim.

Clipboard hijacking

The second component masquerades as SystemArchitectureTranslation.exe. It uses the AddClipboardFormatListener function to monitor changes to the clipboard and to apply the replacement rules obtained from %C&C%/regexes to its content. The code for this listener is shown in Figure 11. The value 0x31D corresponds to the WM_CLIPBOARDUPDATE constant.

These rules, in the form <regular_expresssion>!<wallet>, match the format of cryptocurrency wallet addresses and replace them with addresses of wallets controlled by the malware operator. This is an attempt to redirect transactions made by the victim to the operator's wallets. This component uses a FileSystemWatcher to reload replacement rules whenever the settings.cfg file is changed.

Figure 11. Decompiled code for the listener function used by the clipboard hook

At the time of this writing, the wallets used by the clipboard hijacking component had received a little over US$1800 in Bitcoin and Ethereum. One such wallet is shown in Figure 12. By correlating wallets used as sources in the same transactions as known ones, we were able to uncover at least four additional Bitcoin wallets that likely belong to KryptoCibule's operators.

Figure 12. A Bitcoin wallet used by the clipboard-hijacking component

File exfiltration

The third component walks through the filesystem of each available drive and looks for filenames that contain certain terms. A list of such terms we obtained during our investigation is shown in Figure 13.

```
1  ["wallet.dat", "utc--2014", "utc--2015", "utc--2016", "utc--2017", "utc--2018", "utc--2019", "utc--2020",
   ".address.txt", "electrum", "bitcoin", "litecoin", "ethereum", "cardano", "zcash", "monero", "cripto", "krypto",
   "binance", "tradeogre", "coinbase", "tether", "daedalus", "stellar", "tezos", "chainlink", "blockchain", "verge",
   "bittrex", "ontology", "vechain", "doge", "qtum", "augur", "omisego", "digibyte", "seele", "enjin", "steem",
   "bytecoin", "zilliqa", "zcoin", "miner", "xmrig", "xmr-stak","electroneum", "heslo", "waves", "banka", "crypto",
   "hesla", "seed", "metamask", "antminer", "trezor", "ledger", "private", "trx", "exodus", "password", "jaxx",
   "guarda", "atomic.exe", "copay.exe", "Green Address Wallet.exe", "msigna.exe", "ArmoryQT.exe", ".ssh",
   ".aws", "Desktop"]
```

Figure 13. A list of words to search for, taken from the GET %C&C%/settingsv5 response

Most terms refer to cryptocurrencies, wallets or miners, but a few more generic ones like crypto (in several languages), seed and password are present also. The list contains similar terms in Czech and Slovak such as heslo, hesla and banka (these are the words for “password”, “passwords” and “bank”, respectively). A few terms also correspond to paths or files that could provide other interesting data (Desktop, private) including private keys (.ssh, .aws). It gathers the full path of each of the matching files and sends the list to %C&C%/found/<unique name>.

We believe that this works in tandem with the SFTP server running as an onion service on port 9187. This server creates mappings for every available drive and makes them available using credentials hardcoded in the malware. The gathered paths can thus be used for file exfiltration by having an attacker-controlled machine request them from the infected host over SFTP.

KryptoCibule also installs a legitimate Apache httpd server that is configured to act as a forward proxy without any restrictions and that is reachable as an onion service on port 9999.

Conclusion

The KryptoCibule malware has been in the wild since late 2018 and is still active, but it doesn’t seem to have attracted much attention until now. Its use of legitimate open-source tools along with the wide range of anti-detection methods deployed are likely responsible for this. The relatively low number of victims (in the hundreds) and their being mostly confined to two countries may also contribute to this. New capabilities have regularly been added to KryptoCibule over its lifetime and it continues to be under active development.

Presumably the malware operators were able to earn more money by stealing wallets and mining cryptocurrencies than what we found in the wallets used by the clipboard hijacking component. The revenue generated by that component alone does not seem enough to justify the development effort observed.

Indicators of Compromise (IoCs)

The comprehensive list of Indicators of Compromise (IoCs) and samples can be found in our GitHub repository.

Samples

SHA-1	Filename	ESET detection name
3BCEF852639F85803974943FC34EFF2D6D7D916D	armsvc.exe	MSIL/KryptoCibule.A
352743EBE6A0638CC0614216AD000B6A43C4D46E	SystemArchitectureTranslation.exe	MSIL/KryptoCibule.A
70480D5F4CB10DE42DD2C863DDF57102BE6FA9E0	Updater.exe	MSIL/KryptoCibule.A
2E568CDF9B28824FBA1D7C16D8D0BE1D73A3FEBA	Setup.exe	MSIL/KryptoCibule.A

Network

- rlwryismmgjijryr55u5rqlbqghqvrwxe5qgxupuviyysxkky5wah6yd.onion
- 4dtu3lxrpx6nn7snjovoc3ldiy4x67k7qsrgzftvkrttoqbwnsuirhqd.onion
- v6lajszeqfkt3h2nptorindpf3mow5p3thrx2vuqbqzbv3tjrcqmgdqd.onion

Scheduled Tasks

Name	Executable Path
GoogleUpdateTask	%LocalAppData%\Microsoft\Architecture\SystemArchitectureTranslation.exe

Name	Executable Path
Adobe Update Task	%ProgramFiles(X86)%\Adobe\Acrobat Reader DC\Reader\Update\armsvc.exe

MITRE ATT&CK techniques

This table was built using version 7 *of the ATT&CK framework.*

Tactic	ID	Name	Description
Initial Access	T1189	Drive-by Compromise	KryptoCibule is spread through torrent and file-sharing websites.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	KryptoCibule directly executes PowerShell commands. Some commands received from the C&C use PowerShell.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Commands received from the KryptoCibule C&C are executed with cmd.exe.	
T1106	Native API	KryptoCibule uses the System.Diagnostics.Process C# class to run processes.	
T1204.002	User Execution: Malicious File	KryptoCibule requires victims to run an installer from a downloaded torrent.	
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	KryptoCibule attains persistence by creating a scheduled task to run the main executable every five minutes.
Defense Evasion	T1027	Obfuscated Files or Information	KryptoCibule executables are obfuscated with Obfuscar.
T1036	Masquerading	KryptoCibule components use misleading names and a configuration file masquerades as a DLL.	
T1036.004	Masquerading: Masquerade Task or Service	KryptoCibule tasks are named after legitimate and benign looking software.	
T1036.005	Masquerading: Match Legitimate Name or Location	KryptoCibule uses paths and filenames that match those of Adobe Reader for malware and Tor client. BuruServer uses paths and filenames for OpenSSH. Transmission is installed to Java runtime directories.	
T1140	Deobfuscate/Decode Files or Information	The files that come with the KryptoCibule installer are XOR-encrypted. PowerShell commands from the KryptoCibule C&C are base64-encoded.	

Tactic	ID	Name	Description
	T1497	Virtualization/Sandbox Evasion	The KryptoCibule payload is not executed if an analysis tool is detected.
	T1497.002	Virtualization/Sandbox Evasion: User Activity Based Checks	KryptoCibule uses the time since last input to set limits on cryptominer CPU usage.
	T1562.001	Impair Defenses: Disable or Modify Tools	KryptoCibule uses Add-MpPreference -ExclusionPath to exclude malware and installed tools from Windows Defender scanning.
	T1562.004	Impair Defenses: Disable or Modify System Firewall	KryptoCibule uses advfirewall firewall add rule to allow its tools and block the ESET Kernel Service.
	T1564.003	Hide Artifacts: Hidden Window	KryptoCibule hides process windows using the windowstyle hidden option.
Discovery	T1057	Process Discovery	KryptoCibule uses System.Diagnostics.Process.GetProcesses to get a list of running processes.
	T1082	System Information Discovery	KryptoCibule obtains information about host's timezone, locale, power status, OS and hardware.
	T1083	File and Directory Discovery	KryptoCibule has a component that looks for files on the local file system.
	T1518.001	Software Discovery: Security Software Discovery	KryptoCibule looks for antivirus software in the root\\SecurityCenter2 → AntivirusProduct ManagementObject. The cryptominer component is not installed if it detects an installed antivirus product.
Collection	T1005	Data from Local System	KryptoCibule learches all attached drives for a list of filenames .
	T1119	Automated Collection	KryptoCibule programmatically collect paths for files to be exfiltrated.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	KryptoCibule uses HTTP for C&C communication.
	T1071.002	File Transfer Protocols	KryptoCibule downloads updates and additional tools via BitTorrent.

Tactic	ID	Name	Description
	T1090.003	Proxy: Multi-hop Proxy	KryptoCibule bundles Tor and uses it as a SOCKS proxy to communicate with its C&C.
	T1105	Ingress Tool Transfer	KryptoCibule downloads additional tools using BitTorrent.
	T1568	Dynamic Resolution	KryptoCibule gets additional onion URIs over HTTP.
	T1571	Non-Standard Port	KryptoCibule uses port 9187 for SFTP server, and 9999 and 12461 for HTTP servers.
Exfiltration	T1020	Automated Exfiltration	Logs, file locations and system info are automatically collected and sent to the KryptoCibule C&C.
	T1041	Exfiltration Over C2 Channel	Logs, file locations and system info are sent via the KryptoCibule HTTP C&C channel.
	T1048	Exfiltration Over Alternative Protocol	KryptoCibule exfiltrates files over SFTP.
Impact	T1496	Resource Hijacking	KryptoCibule uses XMRig and Kawpowminer to mine cryptocurrency on victim systems.
	T1565	Data Manipulation	KryptoCibule replaces cryptocurrency wallet addresses in the clipboard in an attempt to hijack transfers.

2 Sep 2020 - 11:30AM