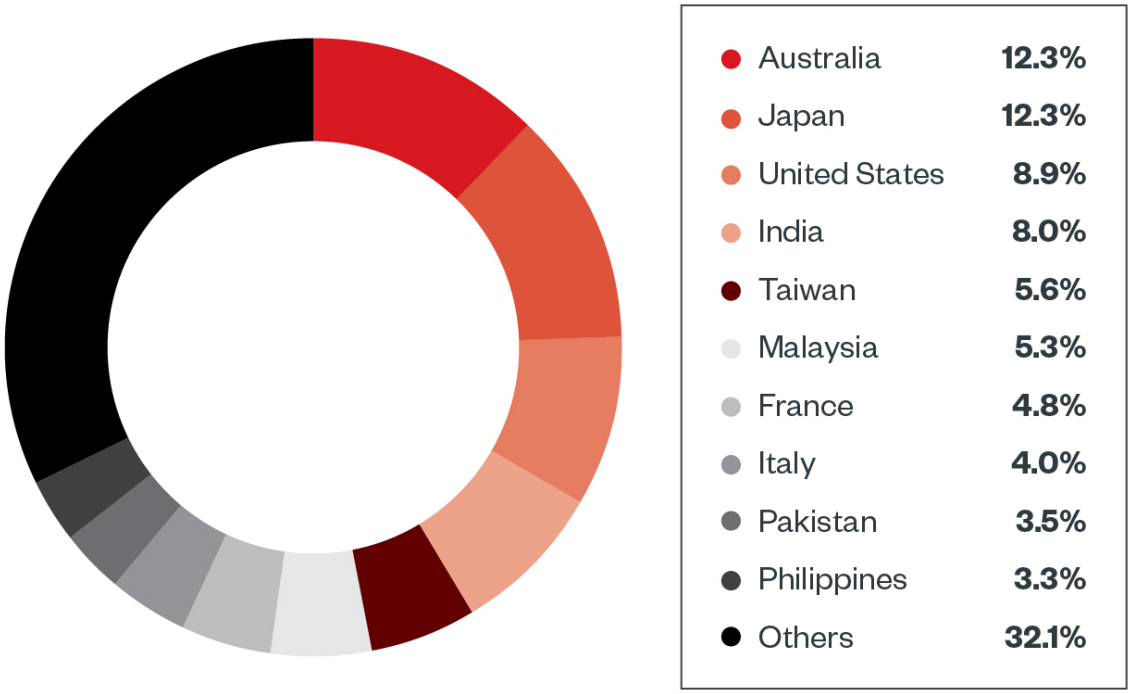
ViperSoftX Updates Encryption, Steals Data

trendmicro.com/en_us/research/23/d/vipersoftx-updates-encryption-steals-data.html

April 24, 2023



ViperSoftX, a type of information-stealing software, has been primarily reported as focusing on cryptocurrencies, making headlines in 2022 for its execution technique of hiding malicious code inside log files. Since it was first documented in November, we observed this malware campaign differentiating itself from its previous iteration with the use of DLL sideloading for its arrival and execution technique. We also noted that this update includes a more sophisticated encryption method of byte remapping and a monthly change in command-and-control (C&C) server. Without the correct byte map, the encrypted shellcode, including all components and relevant data, cannot be correctly decrypted, making decryption and analysis of the shellcode more time-consuming for analysts.

We've noted a significant number of victims in the consumer and enterprise sectors, with Australia, Japan, and the United States as the top three countries affected by ViperSoftX in the consumer category. Meanwhile, victim organizations from Southeast Asian countries comprised the enterprise sector.

Figure 1. Top 10 countries affected by ViperSoftX in both the consumer and enterprise sectors
Source: Trend Micro™ Smart Protection Network™ (SPN)

Arrival routine

For majority of cases, ViperSoftX typically arrives as a software crack, an activator or a patcher, or a key generator (keygen). In blocking and detecting these illicit software solutions, we have come to believe that the people behind these kinds of software try to convince users looking for bootleg software versions that these are not malicious and are simply flagged as "false positives." It is also a common gimmick for cybercriminals to pose malware as a keygen or an activator. Actors behind ViperSoftX take this narrative a step further by using actual non-malicious software to hide and pose as typical illegal software versions. ViperSoftX uses these files as "carriers" of the main malware encrypted within the overlay.

While the malicious actors abuse neither definitive software nor target any definitive applications, they commonly use multimedia editors or video format converters, cryptocurrency coinminer apps, phone-related desktop apps, and system cleaner apps. Through all the samples we analyzed, we consistently observed the following binary carriers:

1. *gup.exe* from Notepad++
2. *firefox.exe* from Tor
3. *ErrorReportClient.exe* from Magix, a type of multimedia-editing software

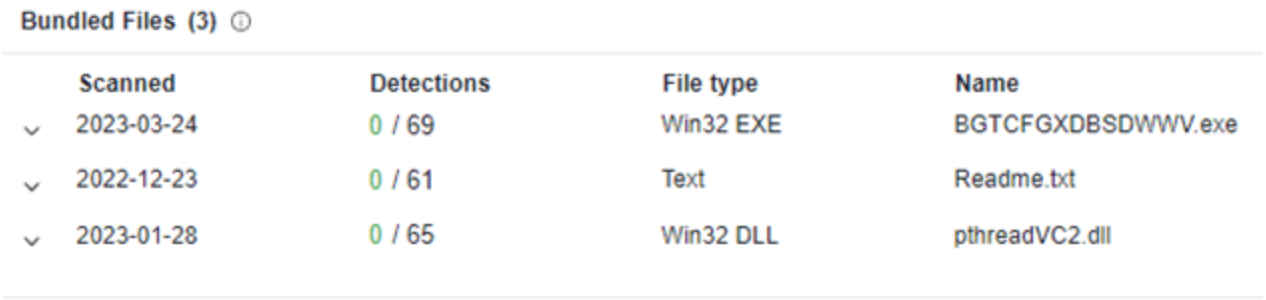


Figure 2. Typical arrival package of the malware

The malware arrives as a package of the carrier executable and the decryptor/loader DLL, typically downloaded from the websites or torrents of (illegal) software solutions. For the most part, the malware is posed as a software activator, patcher, or keygen, among other similar software executables. The malicious routine starts after the software executables have been included and run in the system.

We also noticed that ViperSoftX's primary C&C servers for the second stage download would change on a monthly basis:

- February: *chatgigi2[.]com*

- March: *arrowlchat[.]com*
- April: *static-cdn-349[.]net*

Infection routine

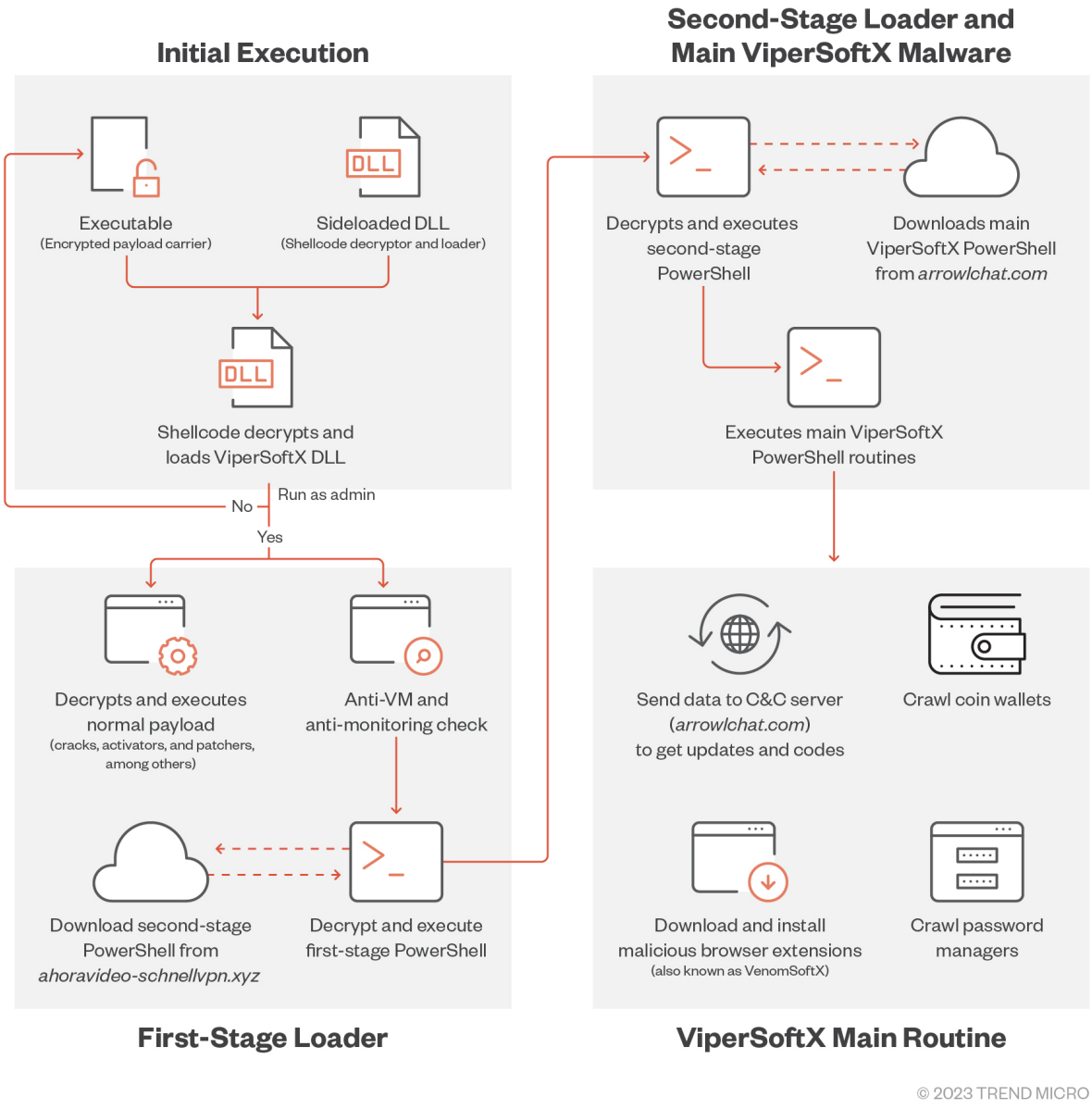


Figure 3. Execution flow of ViperSoftX

ViperSoftX first checks for a few virtualization strings and monitoring tools to check if the system is running a virtual machine (VM). Using WQL command *SELECT Manufacturer, Model FROM Win32_ComputerSystem* to query *ROOT\CIMV2*, it checks for the following strings:

- *VMWare*
- *Virtual*

The malware checks if there are monitoring tools, specifically Process Monitor, running in the current machine with the following strings:

- *procmon*
- *procmon64*
- *procmon64a*

Lastly, ViperSoftX checks for a few installed and active antivirus products, namely:

- Windows Defender
- ESET

If all checks pass, the malware proceeds to decrypt the PowerShell code and starts downloading the main ViperSoftX routine. From there, the routine is its standard multistage download and execution routine.

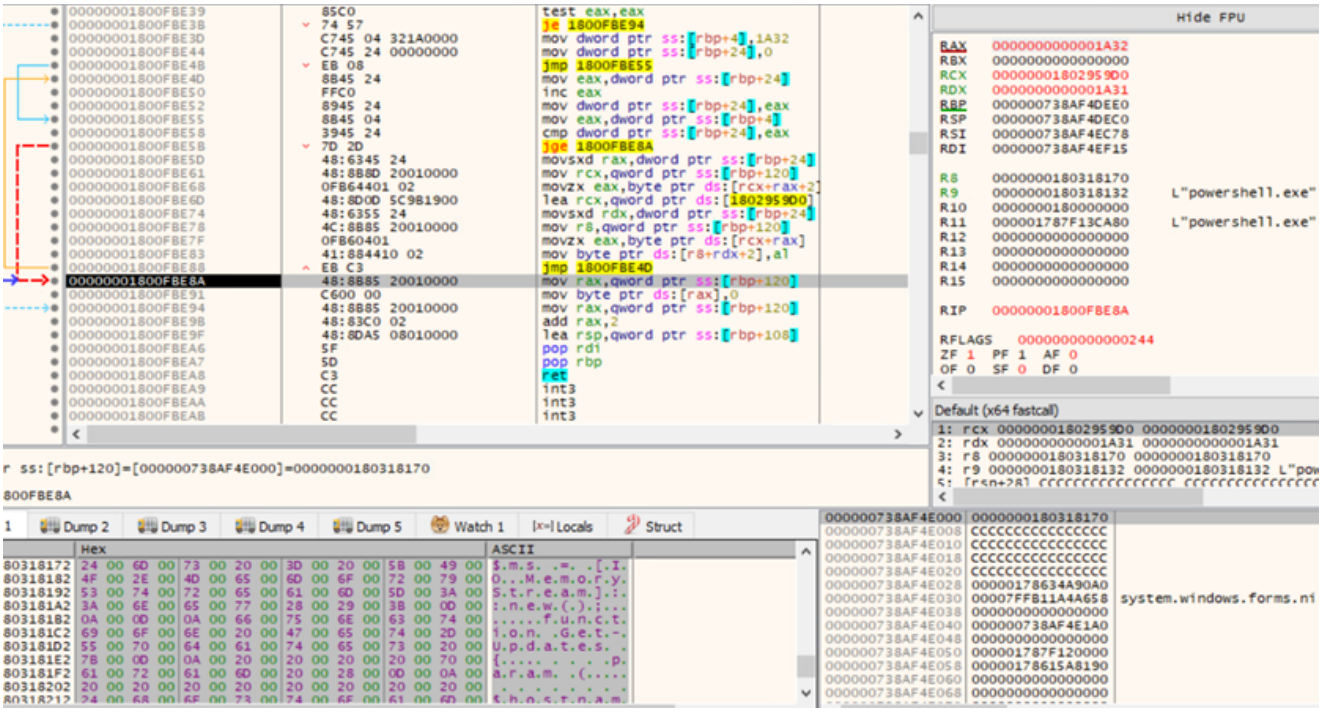


Figure 4. Execution of the first-stage PowerShell downloader after passing through blacklisting

Unique encryption

Byte mapping is a considerably simple technique. It does not require any complex computations, and the only operation it requires is to put the correct byte in the correct location. For their part, cybercriminals benefit from this malware as it reduces the presence and actions made by a large graph of objects.

Unlike the typical bitwise operations from typical decryption routines, ViperSoftX uses byte remapping to ensure that the shellcode cannot be easily decrypted without the correct byte map, weaving a cross-stitch template to the palette of 256 (*0x100h*) bytes. Though this is a very rigid method of hiding its codes, it provides some level of protection against forced decryption.

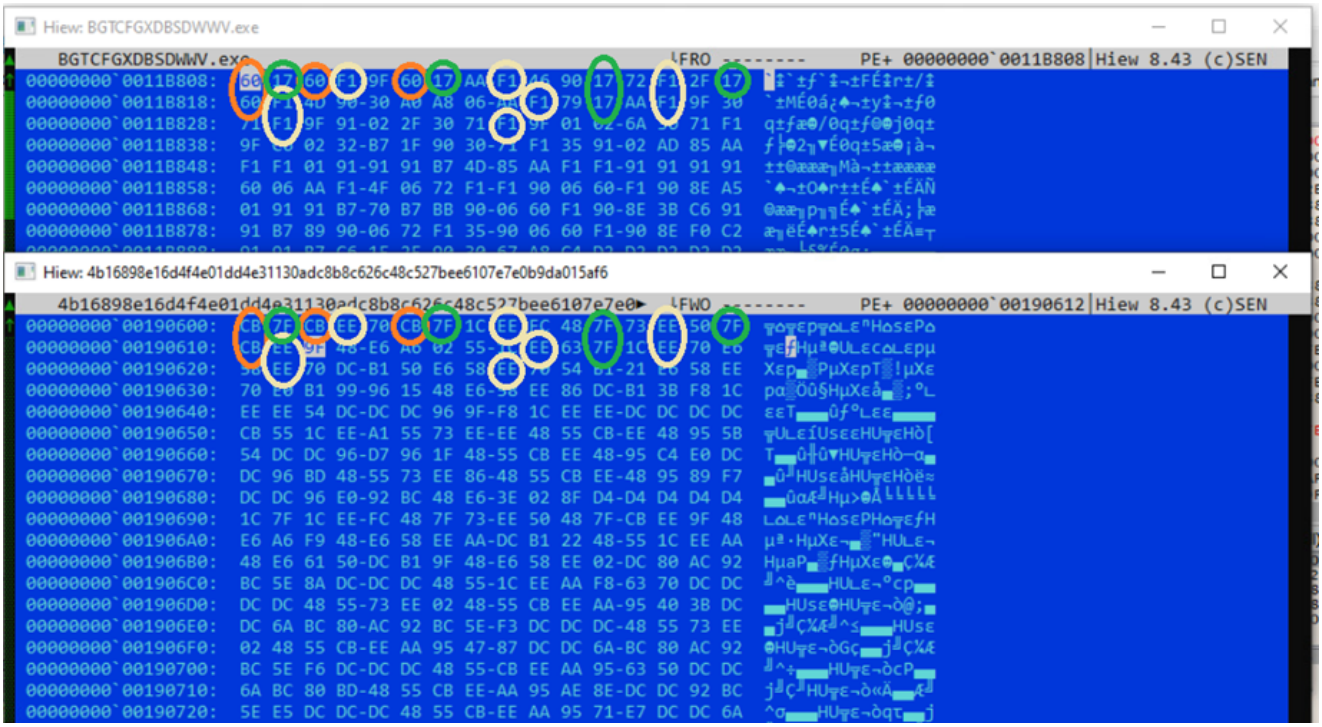


Figure 5. Comparison of two ViperSoftX carrier executables with byte remapping.
Note: The bytes of the encrypted section is a specific index on the byte map found in the sideloaded DLL. Comparing the mapping of the first four bytes on two samples shows that their offsets within the encrypted region remain the same since they result in a similar shellcode even if they are composed of different bytes per binary.

When the screenshots of the two carrier executables are compared, the number (or code) changed but the location/offset remains the same. The same is true for all the other bytes. While analysts will see the pattern of the arrangement, it is unlikely that they would be able to decrypt this without the correct sequence of bytes used in the mapping. If this pattern is a text or a string, it would not be difficult to apply brute force. However, considering this is a byte character (with 256 different bytes) and an assembly code instruction at that, brute-forcing it would unlikely yield correctly decrypted results.

We have also found that each sideloader DLL has its own pair of executable and byte map, and a decryption attempt returns an incorrectly rearranged shellcode if used with another ViperSoftX-related executable. This ensures that the shellcode will not be decrypted without the correct DLL since the latter contains the correct byte map. Moreover, all the strings,

binaries, and other relevant data within the ViperSoftX DLL also gets decrypted the same way. Afterward, the shellcode will then decrypt and load the main ViperSoftX DLL embedded within the carrier.

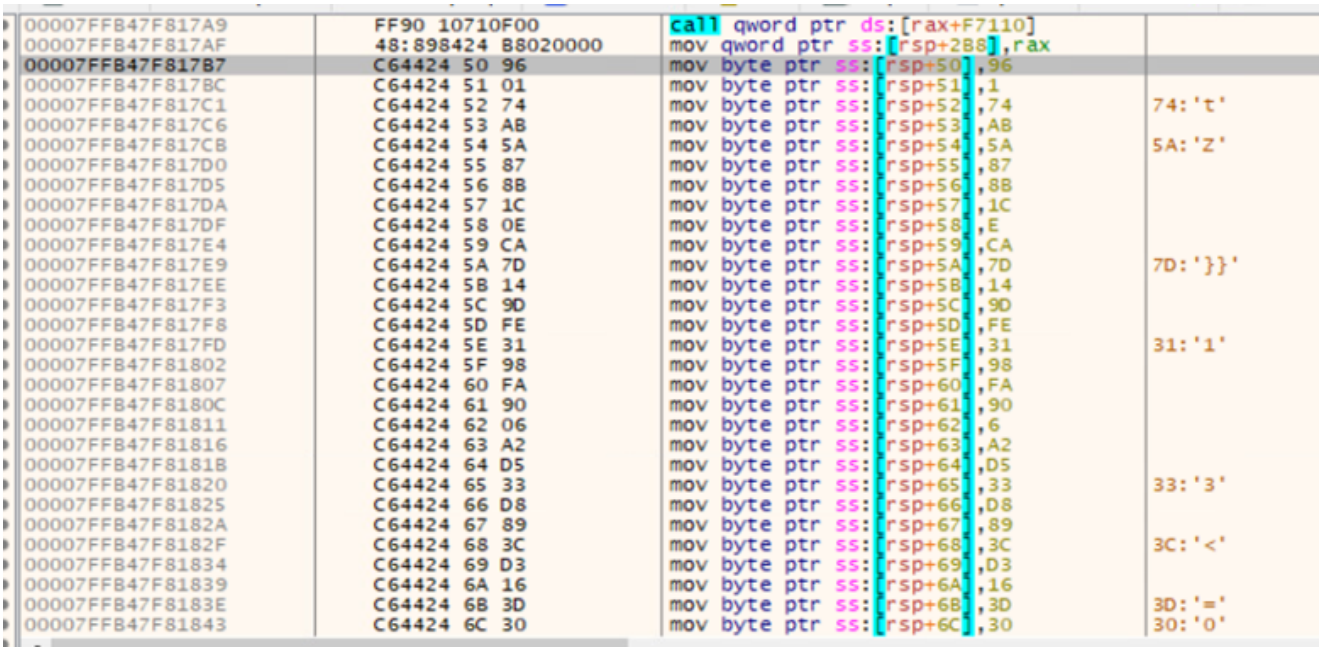


Figure 6. ViperSoftX DLL containing the hard-coded byte map (256 bytes long denoting specific bytes from “0x00” to “0xff”)

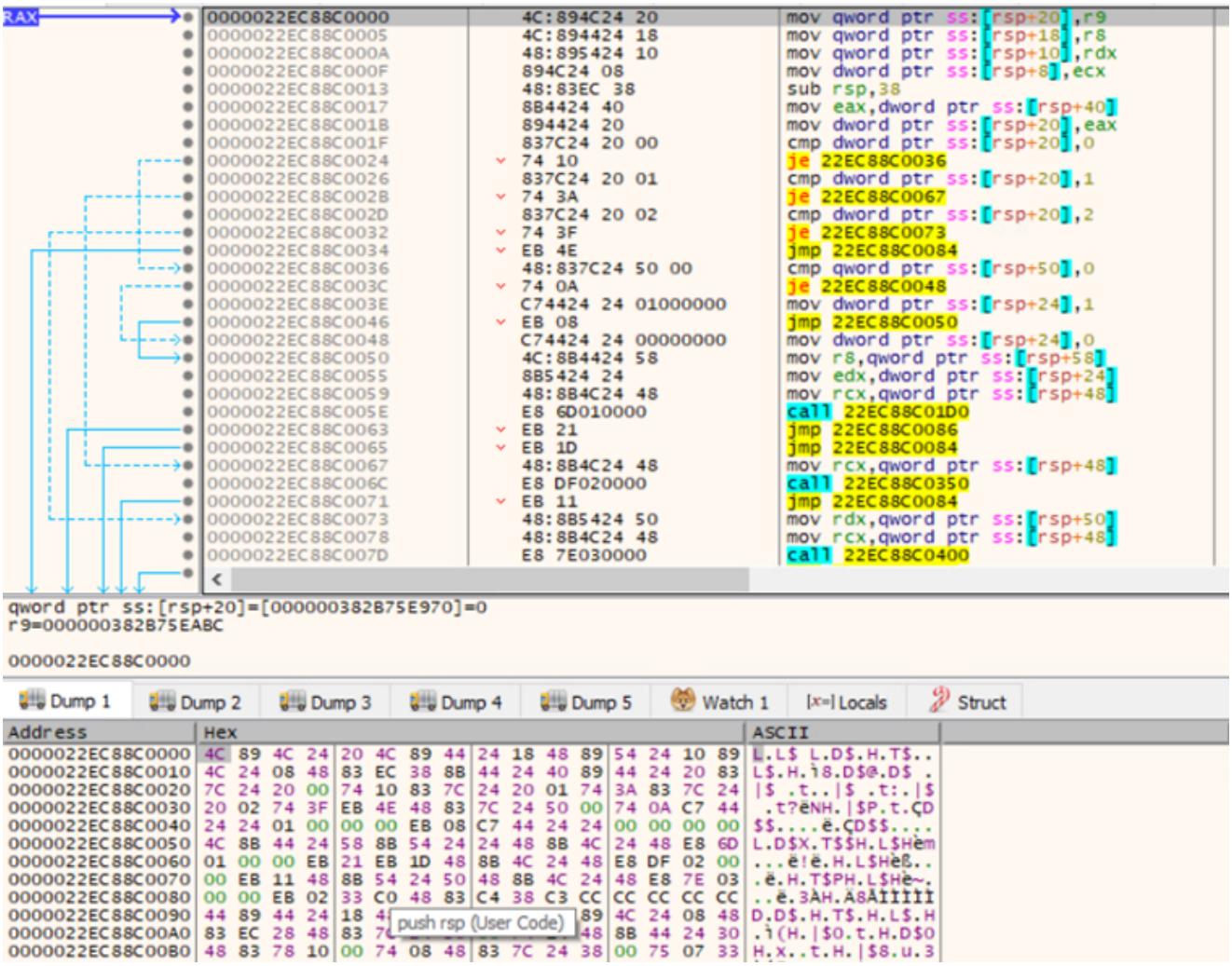


Figure 7. The actual bytes of the decrypted shellcode

This technique for encryption-decryption is not new but is mostly popular with script malware. As of this writing, the most recent piece of malware that uses this technique is the JavaScript- or Windows Scripting File-packed Magniber ransomware. Considering the former is a type of script malware, however, this technique for encryption-decryption is easily more discernable during analysis because both the encrypted data and the mapping are in the same file. In contrast to our ViperSoftX sample, which is a full binary file, the table becomes harder to find. Furthermore, since the data to be decrypted is in another file, the routine becomes even more difficult to investigate, as analysts would need the correct pair for decryption.

Password theft

Since it was first documented, ViperSoftX has been known as a cryptocurrency stealer. However, we found from our investigations that ViperSoftX can check not only for cryptocurrencies but also for a few password managers. It also uses some basic anti-C&C analyses by disallowing communications using web browsers.

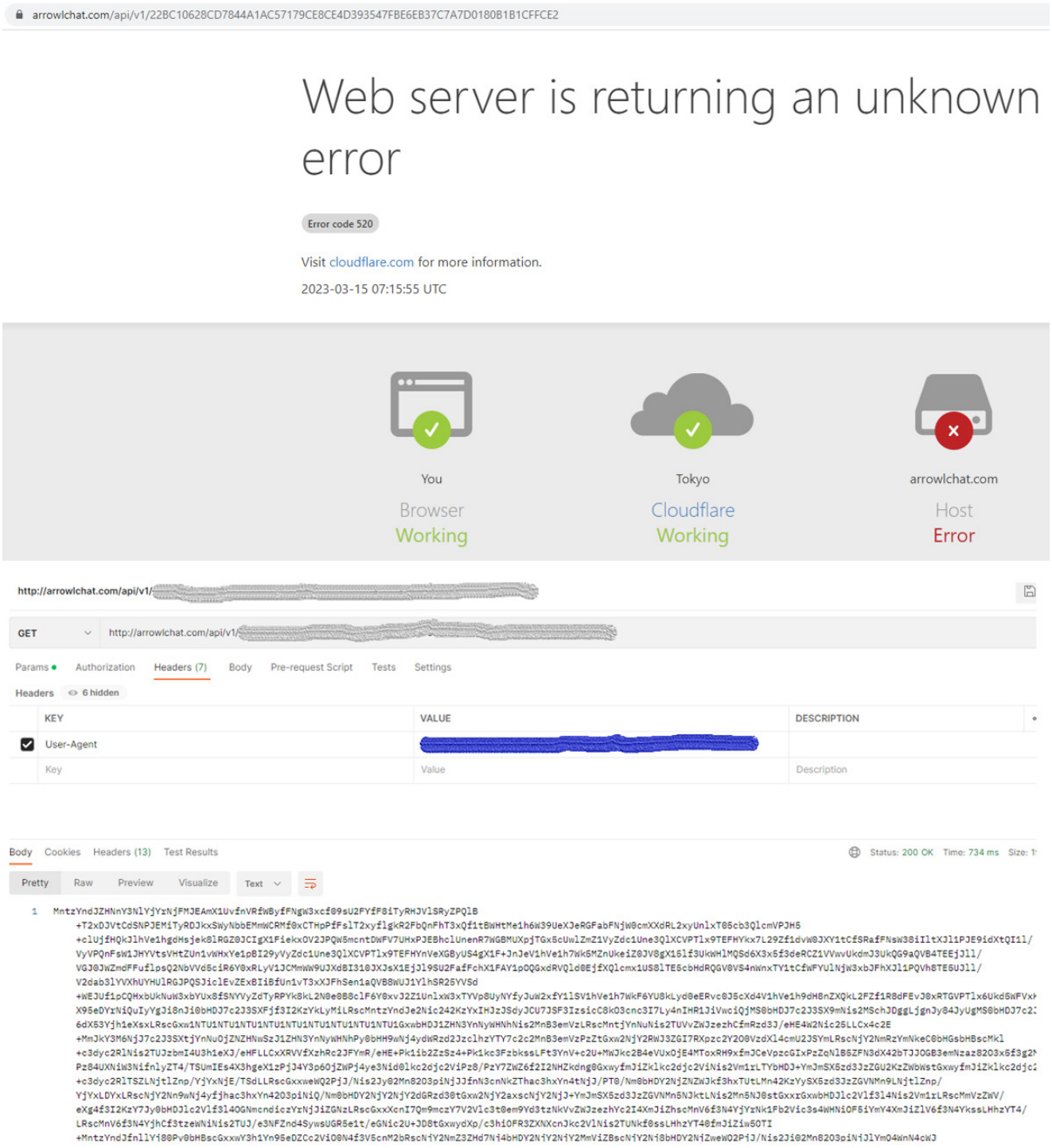


Figure 8. Response when accessing the C&C via web browsers (top), and modifying the user-agent to access the C&C and return encoded data (bottom)

It still downloads a PowerShell code (the main ViperSoftX script) to crawl through different paths in the system for cryptocurrency wallets. ViperSoftX scans for these cryptocurrency wallets in local directories:

- Armory
- Atomic Wallet
- Binance

- Bitcoin
- Blockstream Green
- Coinomi
- Delta
- Electrum
- Exodus
- Guarda
- Jaxx Liberty
- Ledger Live
- Trezor Bridge

The malware also checks for the following wallets via browser extensions:

- Binance
- Coin98
- Coinbase
- Jaxx Liberty
- MetaMask
- Mew CX (now Enkrypt)

Install browser components:

- Brave Browser
- Chrome
- Firefox
- Microsoft Edge
- Opera

The updated version of ViperSoftX includes a check mechanism for two password managers, namely KeePass 2 and 1Password. Noting the malware's capability to scann KeePass, we looked into the possible abuse of the KeePass security gap CVE-2023-24055, which forces the application to dump stored passwords in plain text (a feature already disabled in recent patches and versions). According to our investigation, although there are low numbers of victims related to the exploit, the said detections do not appear related to ViperSoftX victims.

```
$searchPaths = @(
    "$env:USERPROFILE\Desktop",
    "$env:USERPROFILE\OneDrive\Desktop",
    ([Environment]::GetFolderPath("Desktop")),
    "$env:PUBLIC\Desktop",
    "$env:ALLUSERSPROFILE\Microsoft\Windows\Start Menu\Programs",
    "$env:APPDATA\Microsoft\Windows\Start Menu\Programs",
    "$env:APPDATA\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar"
);

$searchEntries = @(
    [pscustomobject]@{
        root    = '%appdata%'
        targets =
        [pscustomobject]@{
            name = 'Exodus-A'
            path = 'Exodus'
        },
        [pscustomobject]@{
            name = 'Atomic-A'
            path = 'Atomic Wallet'
        },
        [pscustomobject]@{
            name = 'Electrum-A'
            path = 'Electrum'
        },
        [pscustomobject]@{
            name = 'Ledger-A'
```

Figure 9. PowerShell code searching for the browser link files to inject a command line and load malicious extensions

```
        [pscustomobject]@{
            name = 'Coinbase-B'
            path = 'hnfanknocfeofbddgcijnmhnfnkdnaad'
        }
    },
    [pscustomobject]@{
        root    = '%SystemDrive%'
        targets =
        [pscustomobject]@{
            name = 'KeePass-A'
            path = 'Program Files (x86)\KeePass Password Safe 2\KeePass.exe.config'
        },
        [pscustomobject]@{
            name = 'KeePass-B'
            path = 'Program Files\KeePass Password Safe 2\KeePass.exe.config'
        }
    },
      [pscustomobject]@{
        root    = '%localappdata%'
        targets =
        [pscustomobject]@{
            name = '1Password'
            path = '1Password'
        }
    }
```

Figure 10. ViperSoftX scanning browser extensions and directories for wallets and password managers

Victims affected: Consumers and businesses alike

Due to the nature of its arrival technique, we primarily assumed that the targets and victims would be regular users. However, we were surprised to see that the enterprise sector made up over 40% of the total number of victims. It is also notable that the leading countries and regions affected by the malware campaign are Australia and Japan with almost the same numbers, while US came at a close third with almost half as much victims at the consumer level. On the other hand, the majority of the affected enterprise sector can be found in Asia.

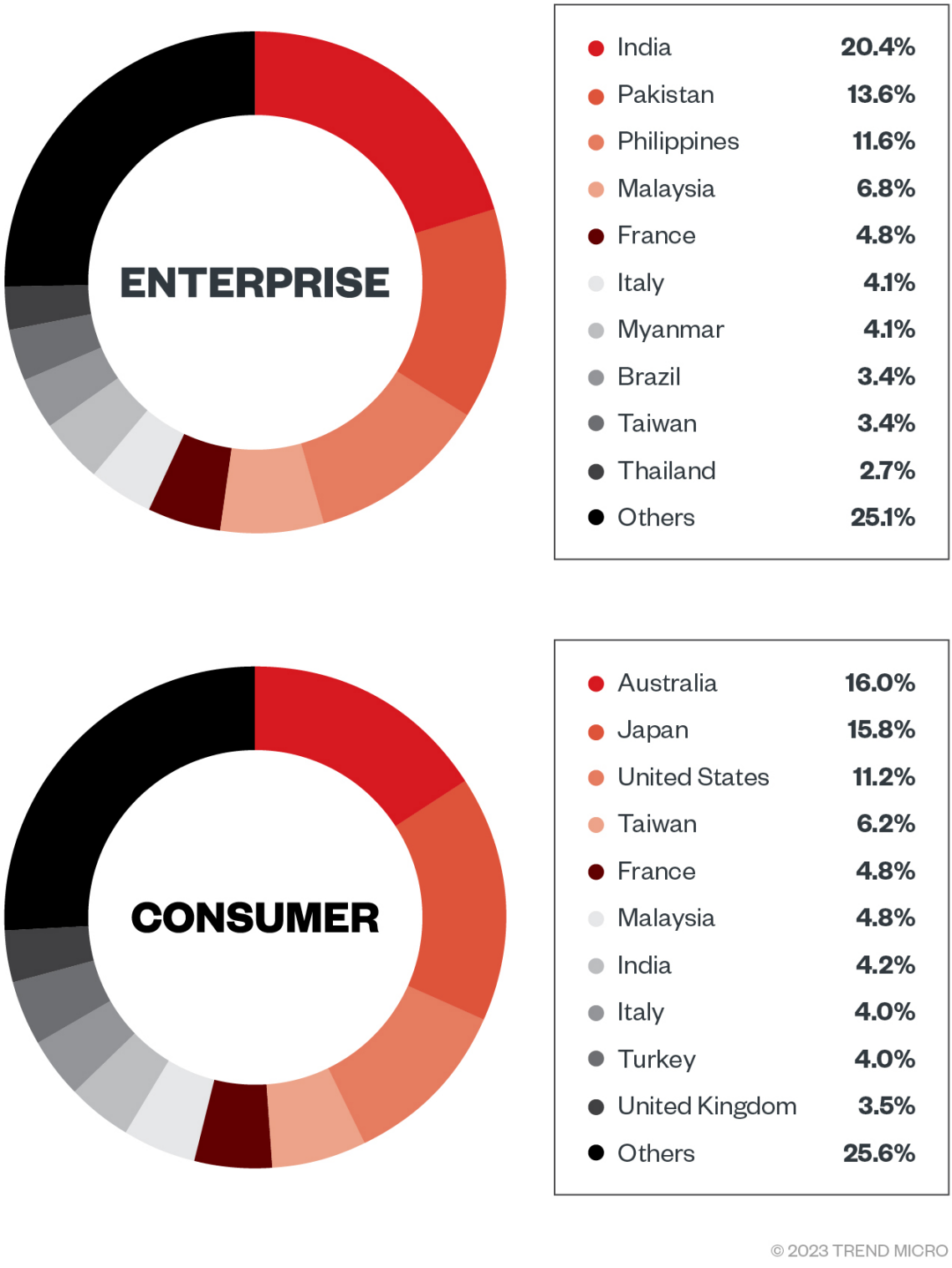


Figure 11. Top 10 countries affected by ViperSoftX malware in the enterprise (top) and consumer (bottom) sectors
Source: Trend Micro Smart Protection Network (SPN)

Conclusion and insights

While other cybercriminals use sideloading to load another non-binary component (usually the encrypted payload, which comes together as a package with the normal executable and the sideloaded DLL), the chosen techniques of the actors behind ViperSoftX (which involve using WMI Query Language (WQL), DLL sideloading/DLL load order hijacking, PowerShell reflective loading, browser hijacking, and C&C protection) are sophisticated.

The cybercriminals behind ViperSoftX are also skilled enough to execute a seamless chain for malware execution while staying under the radar of authorities by selecting one of the most effective methods for delivering malware to consumers. Although we have observed some changes throughout their campaigns, the pace of ViperSoftX's development can be considered slow compared to other types of stealer malware.

The group behind this malware has been doing this for a number of years, and it knows its target systems based on the simultaneous use of techniques to steal cryptocurrencies and passwords. In this respect, we believe there are actually at least two groups responsible for this ViperSoftX campaign based on the malware's C&C communication. As the first set of players, the main group is responsible for the deployments. On the other hand, considering the monthly change of C&C servers and communication exchange, we believe in the possibility of another group involved based on the different coding or C&C scheme. ViperSoftX uses a domain-generating algorithm (DGA) to hide its C&C server and generate useless traffic. From the DGA technique, we observed that majority of the activities are dominated by the main group, which utilizes a simple DGA. However, there are a number of activities that appear to use a different DGA. We do not discount the possibility that these can either be older samples or different operators entirely.

While ViperSoftX appears to be targeting consumers considering its chosen means for entry, we found it interesting that it also affects the business sector. One possible theory behind why businesses are affected by this campaign has to do with recent layoffs and possible budget cuts. While some users might be looking to freelance and upend their incomes while in between jobs, others might have been prompted to download tools from unofficial platforms to "save costs" and circumvent tools not found in office-issued devices. Nonetheless, we strongly recommend that users download the software and applications they need from official platforms. Cracks and other illegally owned software will only work for certain periods since majority of license verification methods are now done in the cloud. If features such as updates to circumvent the replacement of cracks or patches are disabled, users would then be putting their respective systems at greater risk of attacks or infections.

Here are some additional recommendations to prevent the risks of infection from malware types like ViperSoftX:

- Download software and applications from official platforms and sources.
- Instead of downloading illegal software, choose alternative freeware solutions from reputable sources and platforms.

- Download security solutions that can detect and block malicious components in seemingly legitimate and non-malicious software and applications.

Trend Micro solutions

Trend Micro customers are protected from threats like ViperSoftX with Trend Micro Vision One™, which provides multilayered protection and behavior detection, thereby blocking questionable behavior and tools before a piece of malware can do any damage. Implementing a multifaceted approach can aid organizations in securing potential entry points into their systems such as endpoint, email, web, and network. With the help of security solutions that can identify malevolent elements and questionable activities, enterprises can be safeguarded via automated protection while also ensuring that no significant incidents go unnoticed.

Indicators of Compromise (IOCs)

The list of IOCs can be downloaded here.