Technical analysis: The silent torrent of VileRAT

stairwell.com/resources/technical-analysis-the-silent-torrent-of-vilerat/

Research

Written by **Threat Research**at Stairwell

January 31, 2024
Authors: Silas Cutler, Evelyne Diaz Araque, Vincent Zell, Alex Hegyi, Matt Richard, and Chris St. Myers

On 26 January 2024, Stairwell's Threat Research team identified a new variant of VileRAT that has been in use since at least August 2023. Based on public reports and observed filenames, we believe that this variant is being distributed through fake software piracy sites in order to broadly infect systems.

The following report will provide background information on the activities of the group thought to be behind VileRAT, a technical overview of this recently observed activity (including details of two modified installers of the Nulloy media player that have been used to execute the malware), as well as indicators of compromise and a Python decoder script.

Who is behind VileRAT?

VileRAT is a Python-based malware family believed to be unique to the Evilnum threat group (also tracked as DeathStalker). This malware is consistently seen being deployed by an accompanying loader known as VileLoader, used to run VileRAT in-memory, limiting on-disk artifacts. The functionality of VileRAT is consistent with traditional remote access tools, providing attackers with the ability to remotely capture keystrokes, execute commands, and harvest information. VileRAT is modular and extensible, allowing actors to deploy additional functionality through the framework.

Public reporting has assessed Evilnum operates as a mercenary, hack-for-hire service with a history of targeting governments, law firms, financial firms, and cryptocurrency-related entities in the Americas, UK, EU, and the Middle East. Kaspersky researchers have linked the group to the Powersing, Janicab, and PowerPepper campaigns – Powersing being the first, detected in 2018.

Evilnum’s past tactics, techniques, and procedures (TTPs) have included sending emails designed to deliver malicious LNK attachments, Word documents, and links to executable files, as well as utilizing companies’ public chatbots. The group is known to avoid direct financial gain and focus instead on the collection of sensitive business information (investment and trading info, software licenses and platform credentials, credit cards, proof of identity documents, VPN configuration, and more) to potentially function as an “information broker” in financial forums.

VileRAT technical analysis

Stairwell has observed new activity and has identified new variants of VileRAT being deployed by modified versions of legitimate installers that contain VileLoader. This appears to be a new TTP in contrast with their past use of malicious documents and LNK files. The diagram from the 2022 Kaspersky report and a version showing recent activity by Stairwell is shown below:

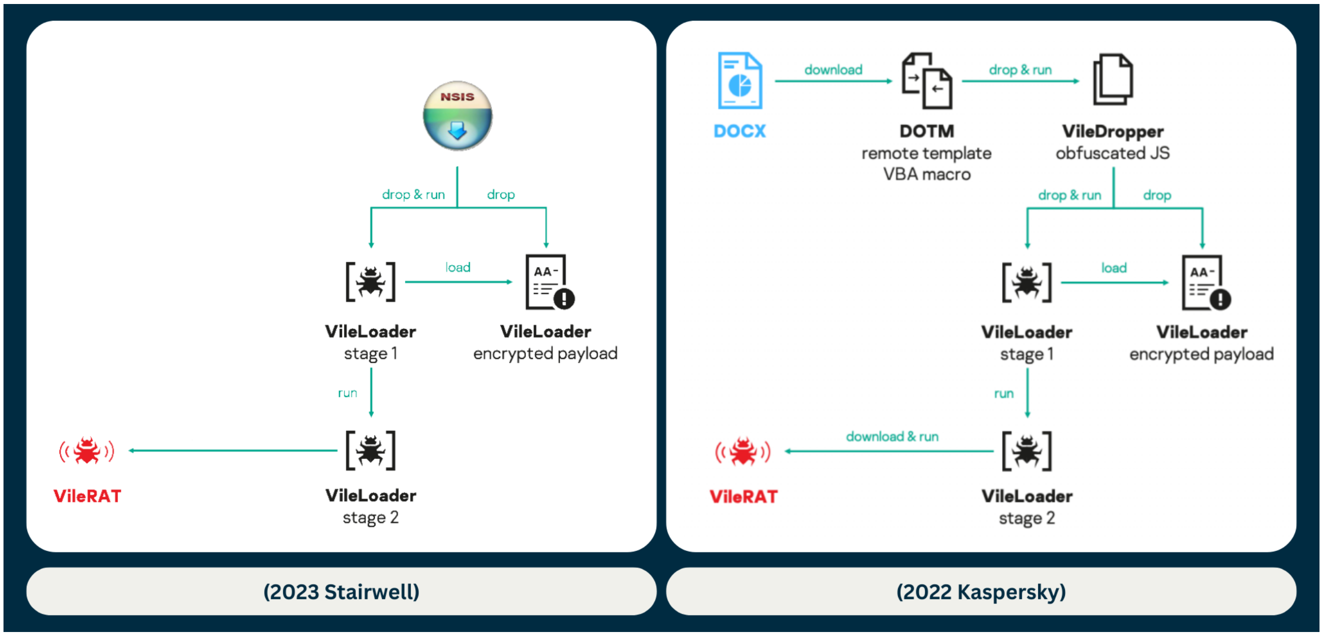

Figure 1: Comparison of VileRAT deployment in 2023 and 2022

Analysis in this report is based on a malicious installer for the Nulloy media player used to deploy VileLoader named `install.exe` (SHA256 hash: `21ae1d88e675c9a2d51a2f68beadf24a21c1b16f58fc042ff97ad8e52501300d`). This NSIS Installer was signed on 13 August 2023 13:21:00 UTC from GLOSUB LLC.

VileLoader is packaged inside the Nulloy installer under the name `Plugins/platforms/NvStTest.exe` (SHA256 hash: `552f9c111bdf18479b2195933649b8dbf80d65113b6d8743ecc9562a4e065a77`) and started by the NSIS install script when the installer is run. The relevant section of the NSIS install script is shown below:

```
SetOutPath $_OUTDIR
StrCpy $0 $INSTDIR\Plugins\platforms\NvStTest.exe
Exec "$\"$0$\" Ri28"
Pop $0
```

This copy of VileLoader (NvStTest.exe) is a modified version of a legitimate NVIDIA 3D Vision Test Application (SHA256 hash: `d799c32ddea3e0fa8219563d0b662cfe759231cfb90b23e60bf75a53f1391cd1`). When executed, it validates the passed command line argument (Ri28 is passed by default from the installer) before dynamically resolving imports related to file loading and process execution. This tradecraft is consistent with VileLoader samples originating back to 2020.

The VileRAT payload is contained in a second file written by the NDIS installer to `Plugins/platforms/wctSBWZ.tmp` (SHA256 hash: `76f93a5d5a1b6bacb6ce474e8388819a3fdb50be51b0ee59bafdfabf5cc6cbb6`). This payload and its filename are both obfuscated using XOR-based encoding methods, denoted in previous public reporting by Kaspersky as the *Type B XOR algorithm*. An example Python function to decode the payload filename within *NvStTest* is included in the Appendix.

VileRAT's core component is stored in a compressed, Xored, and base64 encoded buffer, within the payload unpacked from VileLoader. Within the decoded output is a JSON configuration for the implant, that contains the time VileRAT was started, control servers, and the encryption key for C2 communication.

```
{
    "aidm": 1706308776,
    "u": "259364724529279232",
    "did": "bHNjb3deRlpcQVhEUVtCXkpRWE5eQFETTlpHWl1HEEJUX0FfQ1tYT1wPEBoVBRc=",
    "is": 1706308780,
    "mas": "GtFm",
    "lfs": 0,
    "dl": [
        "eriegentsfsepara.com",
        "licncesispervicear.com",
        "naightdecipientc.com",
        "nscormationw.com",
        "yclearneriegen.com"
    ]
}
```

Assessment

Prior activity from Evilnum has reportedly leveraged spear phishing as the primary method for gaining access to targets and focused on collecting sensitive financial information.

Based on the number of submissions to public malware repositories for the installers, reports of pirated games opening Nulloy, and feedback from our industry peers, Stairwell assessed the total number of systems infected by this variant of VileRAT is between 1k – 10k.

Despite the increased exposure risk, the piracy ecosystem is highly temporal; file-sharing sites are regularly shut down due to copyright violations or removed from search engine results. This regularly changing landscape presents a challenge for tracking actor activity. While sophisticated threat actors such as OnionDuke and APT37 have previously leveraged software piracy for broad exploitation campaigns, the observed by Evilnum is a distinctive shift in tactics from their publicly documented history.

Appendix

Files Indicators

install.exe

21ae1d88e675c9a2d51a2f68beadf24a21c1b16f58fc042ff97ad8e52501300d

2023-07-01 21:09:39

Malicious Nulloy NSIS installer

install.exe

3812aa78d548cbf9e7667569803a437dd38805f538f4cc79d42b96e547367c56

2023-07-01 21:09:39

Malicious Nulloy NSIS installer

NvStTest.exe

552f9c111bdf18479b2195933649b8dbf80d65113b6d8743ecc9562a4e065a77

Thu Jan 17 18:28:57 2019 UTC

VileLoader

NvStTest.exe

66258788b114f08cbddbe03732e8bb8c6b314e5b0f6b69d3a48ad2eb7d615a3a

Thu Jan 17 18:28:57 2019 UTC

VileLoader

wctSBWZ.tmp

76f93a5d5a1b6bacb6ce474e8388819a3fdb50be51b0ee59bafdfabf5cc6cbb6

Encrypted VileRAT payload

wctOFKS.tmp

a9c46388c5a118e90f767992ba23516505f9ed0acd2a4ede11f60cc274912f88

Encrypted VileRAT payload

Network indicators

eriegentsfsepara[.]com

2023-07-28 06:06:18.00

VileRAT C2 domain

licncesispervicear[.]com

2023-07-28 06:06:14.00

VileRAT C2 domain

naightdecipientc[.]com

2023-07-28 06:06:22.00

VileRAT C2 domain

nscormationw[.]com

2023-07-28 06:06:05.00

VileRAT C2 domain

yclearneriegen[.]com

2023-07-28 06:06:22.00

VileRAT C2 domain

lymckensecuryre[.]com

2023-07-28 00:00:00.00

VileRAT C2 domain

atedhilarlymcken[.]com

2023-07-28 00:00:00.00

VileRAT C2 domain

petropicalnorma[.]com

2023-07-28 00:00:00.00

VileRAT C2 domain

normaticalacycurat[.]com

2023-07-28 00:00:00.00

VileRAT C2 domain

lacycuratedhila[.]com

2023-07-28 00:00:00.00

VileRAT C2 domain

Python string decoder

A copy of this script is available on the Stairwell Threat Research GitHub page.

```
#!/usr/bin/env python3
# Author: Silas Cutler ([email protected])

import sys

def type_b_decode(indata):
    res = ""
    data_offset = indata[0] + 5
    key = indata[1:data_offset-2]
    for index, data in enumerate(indata[data_offset:]):
        if data == 0:
            break
        r = (data ^ key[index % len(key)]) & 0xFF
        res += chr(r)
    return res

if __name__ == "__main__":
    import base64
    indata =
base64.b64decode('GdMhue0p3M7PzXkPvSwB9cIHTEWiCOZvNMYYAAAApCHa7V3cnc+PeVi9dgHbwnNMKKJ
45m80AAAA')
    decode(indata)
```

YARA rules

```
rule VileLoader
{
        meta:
                author= "Silas Cutler ([email protected])"
                description = "Detection for VileLoader observed in 2023-2014"
                hash =
"552f9c111bdf18479b2195933649b8dbf80d65113b6d8743ecc9562a4e065a77"
        strings:
                // Stack clearing at the start of WinMain()
                $ = { 81 EC 98 04 00 00 8B 45 08 C7 84 24 E4 00 00 00 00 00 00 00 C7
84 24 68 01 00 00 00 00 00 00 C7 84 24 64 01 00 00 00 00 00 C7 84 24 60 01 00 00
00 00 00 00 C7 84 24 E0 00 00 00 00 00 00 00 C7 84 24 DC 00 00 00 00 00 00 00 C7 84
24 94 00 00 00 00 00 00 00 }

                // Setup before import resolve:
                $ = { 8B 45 08 89 04 24 C7 44 24 04 68 42 00 00 E8 }

                // Argument check
                $ = { 8B 84 24 88 00 00 00 8B 8C 24 C0 00 00 00 83 E9 01 0F B7 04 48
83 F8 22 }

        condition:
                all of them
}

rule VileRAT_encoded_payload
{
    meta:
        author= "Stairwell Research Team"
        description = "Detection for VileLoader tmp file containing VileRat, observed
in 2023-2014"
        hash = "a9c46388c5a118e90f767992ba23516505f9ed0acd2a4ede11f60cc274912f88"
        hash = "76f93a5d5a1b6bacb6ce474e8388819a3fdb50be51b0ee59bafdfabf5cc6cbb6"
    condition:
        uint32(0x0) < 0x3290 and uint32(0x0) > 0x3000 and uint16(0x2) == 0x0 and
uint32(uint8(4) + 5) < uint32(0) and uint16(uint8(4) + 9) == uint16(0x5) and
uint32(0x5) != 0x00
}
```