

VIPKeyLogger Infostealer in the Wild

 forcepoint.com/blog/x-labs/vipkeylogger-infostealer-malware

December 13, 2024

Data Security,Awareness

December 13, 2024 |

0 min read

 VIPKeyLogger Infostealer

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:

 InfoStealers-wild-image-1.png

Email file:

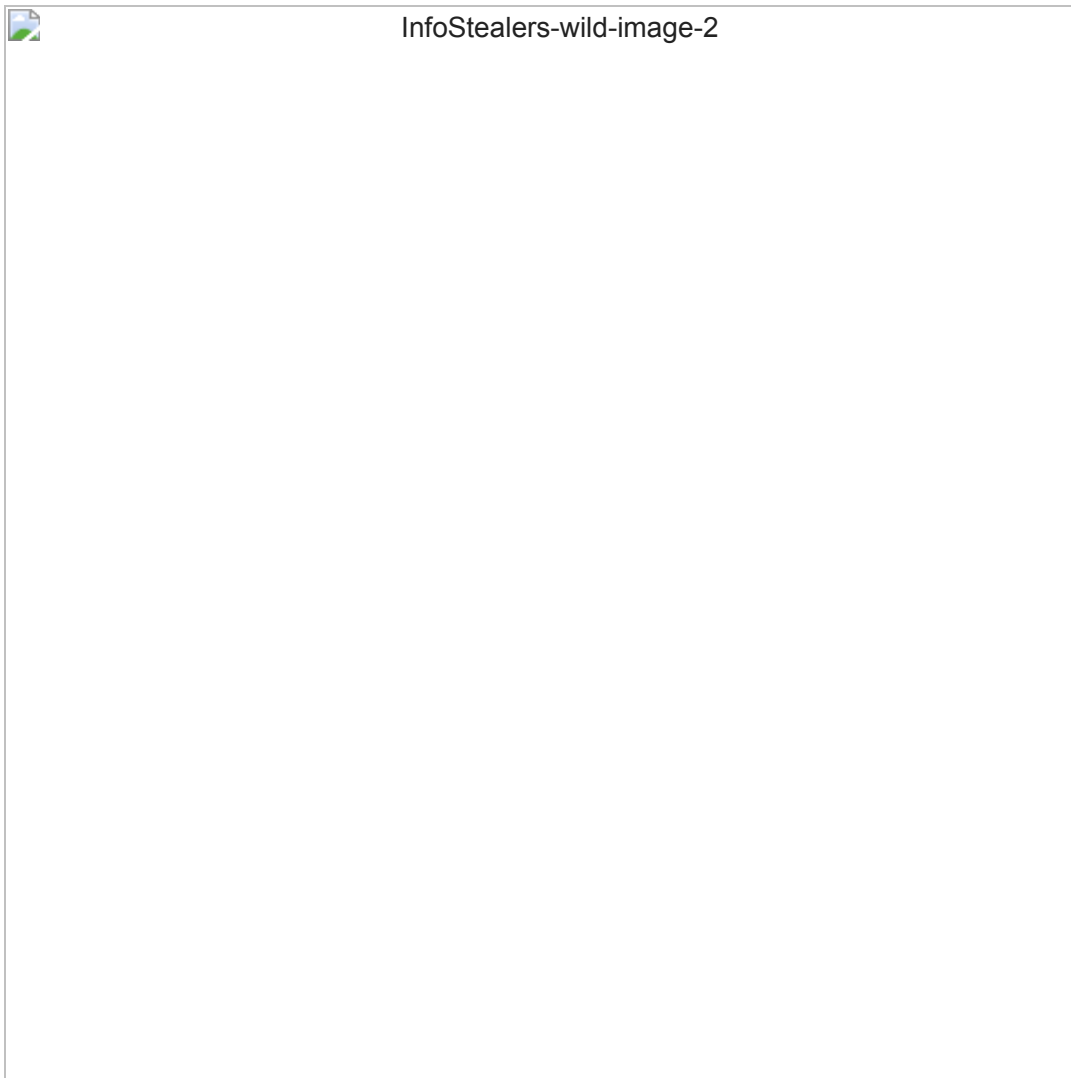


Fig. 1 - Original email

Malicious Doc file

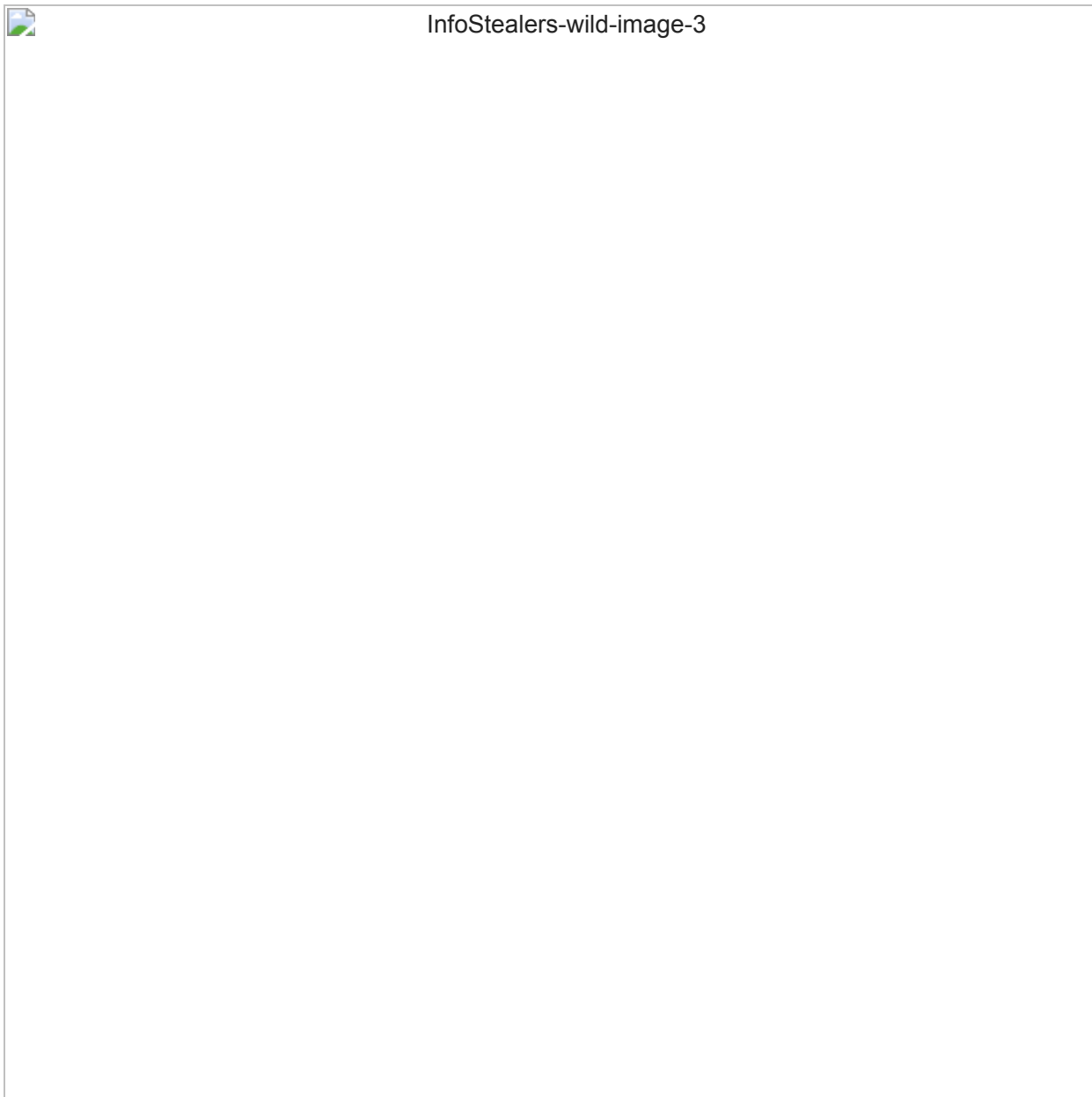


Fig. 2 - Malicious document

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.



InfoStealers-wild-image-4

Fig. 3 - File header

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



InfoStealers-wild-image-5

Fig. 4 - Dump of RTF file

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



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.



InfoStealers-wild-image-7

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](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:

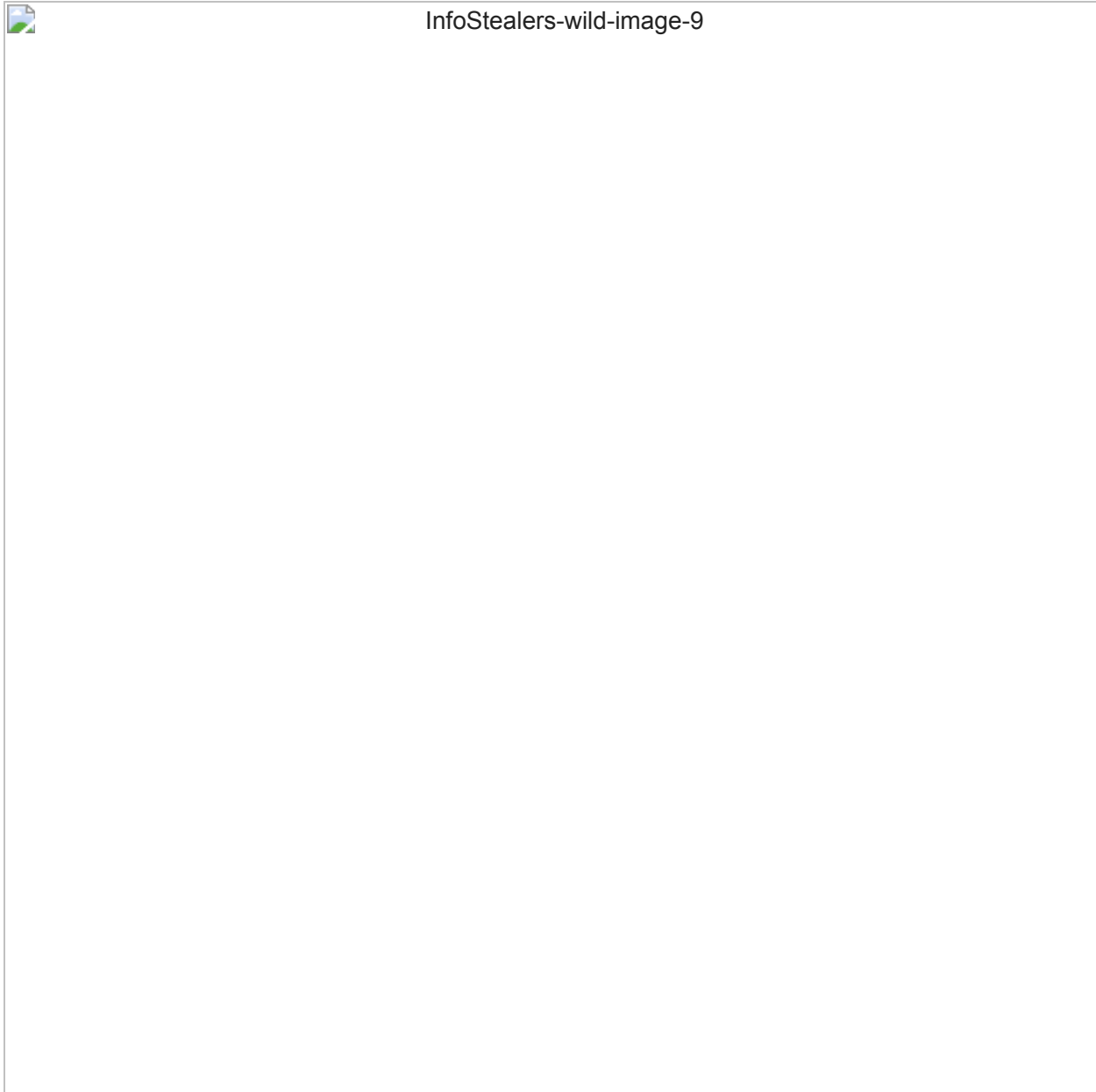


Fig. 7 - .NET compiled file

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.

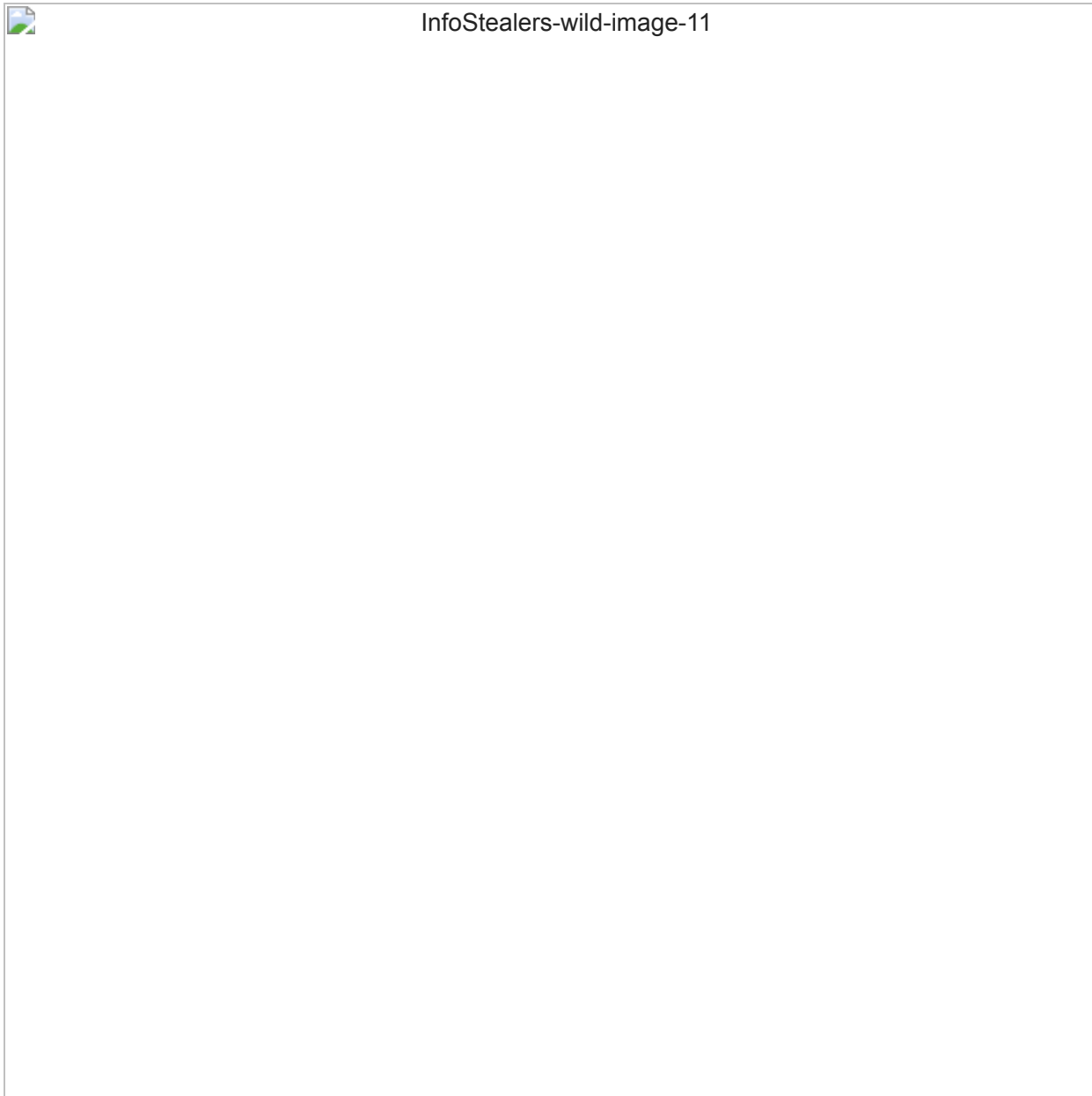


Fig. 9 - Main Initialization

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



Fig. 10 - Stenographic 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:



InfoStealers-wild-image-13

Fig. 11 - Harvested data types



InfoStealers-wild-image-14

Fig. 11.2 - Examples of exfiltrated data



InfoStealers-wild-image-15

Fig 11.3 - More examples of exfiltrated data



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



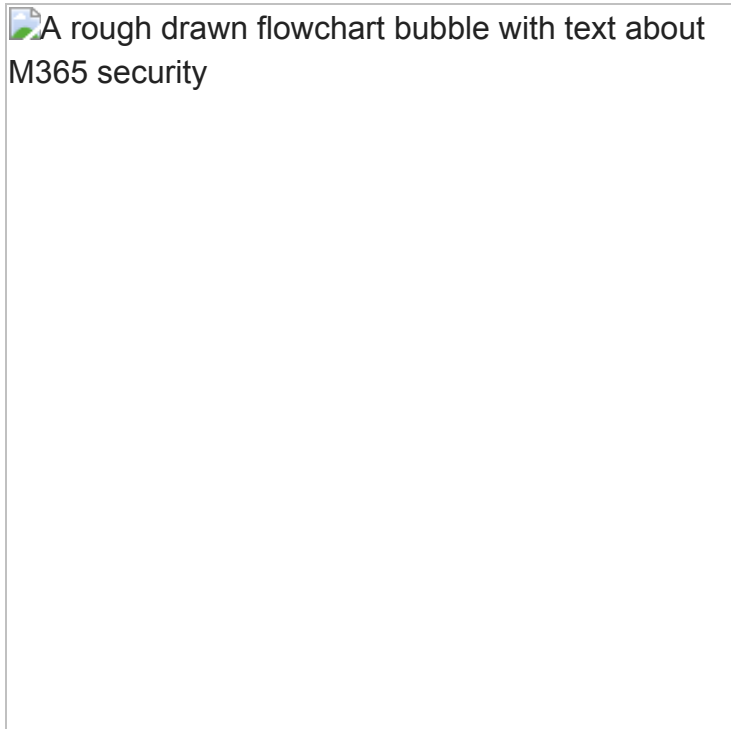
Prashant Kumar

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](#)



Microsoft 365 Data Security Playbook

Forcepoint

X-Labs

Get insight, analysis & news straight to your inbox

Cybersecurity
