ANDROID SPYWARE TARGETING RESIDENTS OF GILGIT BALTISTAN - PA

Microsoft has released a functionality, which is very new and enables the developers to use port forwarding on their systems to expose locally hosted applications over the internet. This functionality aids developers to expose their systems directly on the internet without the need to host their applications on any server. The functionality is like Live Preview in the VSCode which allows the developers to host their websites locally but now with added functionality, they can forward the local ports over the internet. Thus, anyone on the internet can access the applications developed.

This functionality is definitely very useful for the developers, however, opens a vast range of attack vectors. So far, we have not noticed any exploits or active attacks in the market however, we are sure this will very soon be used by the threat actors for C2 communications as well as data exfiltration.

As VSCode is known software in the community and is Microsoft-signed, this raises fewer alerts compared to non-signed binaries as well as the application behavior.

More details can be found here.

In this research article, our focus is to highlight the use case of data exfiltration using the same functionality. Assuming adversaries have already compromised the end user system and now hold active domain credentials. Information gathering reveals that the user is a developer and is using the latest version of Microsoft Visual Studio Code. The threat actors now plan to exfiltrate the data.

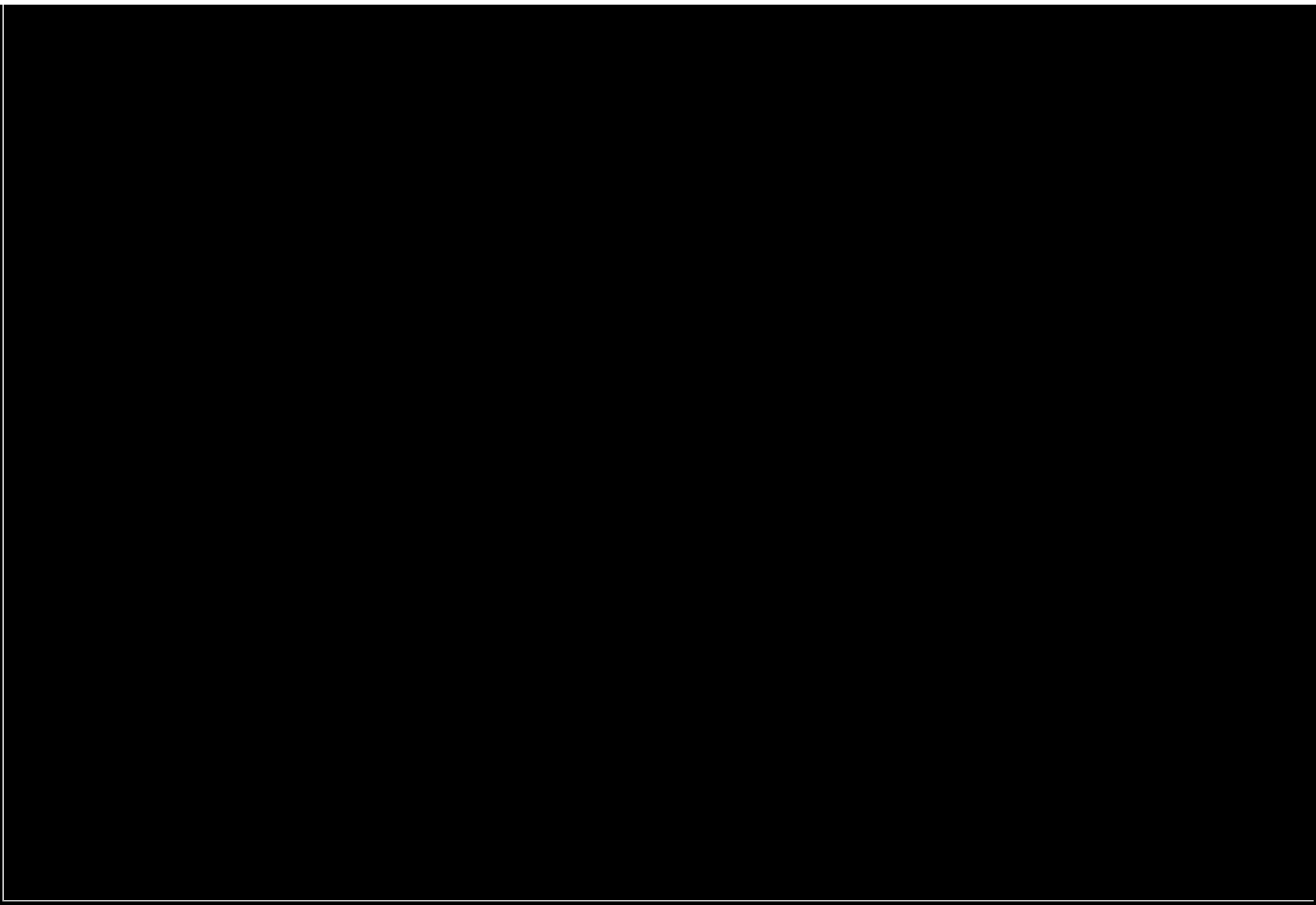
Now, there will be two use cases for the forwarded forts to be exploited.

1. The developer has set up forward ports in public mode.
2. The developer has set up forward ports in private mode.

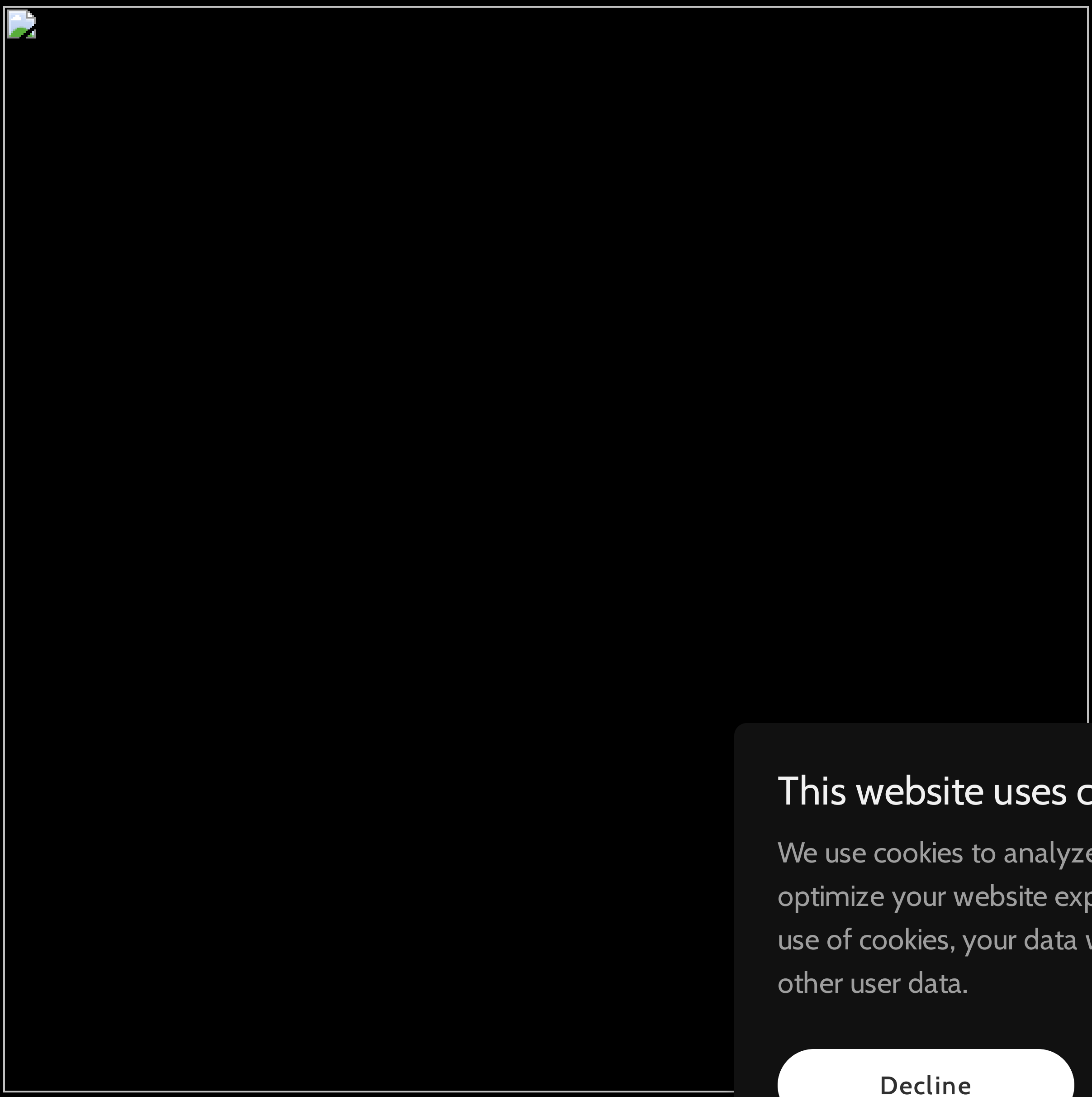
Limitations for these ports are provided by Microsoft on their website.

Scenario 1 (Public Mode)

Assuming the developer already set up public mode for the for
in the field.



As the developer has an active folder present along with the local web server (built-in/any) running on the machine, the URL is accessed by the threat actor revealing all the files within this folder over the internet. In this, case assuming that the threat actor has placed the PCI files in the folder and is now able to download the same over the internet.



This goes the other way around as well, adversaries hosting malware, C2, keyloggers, etc locally and

This goes the other way around as well, adversaries hosting malware, C2, keyloggers, etc locally and then exposing the URLs to the public and using the same to download malicious files onto the end user system.

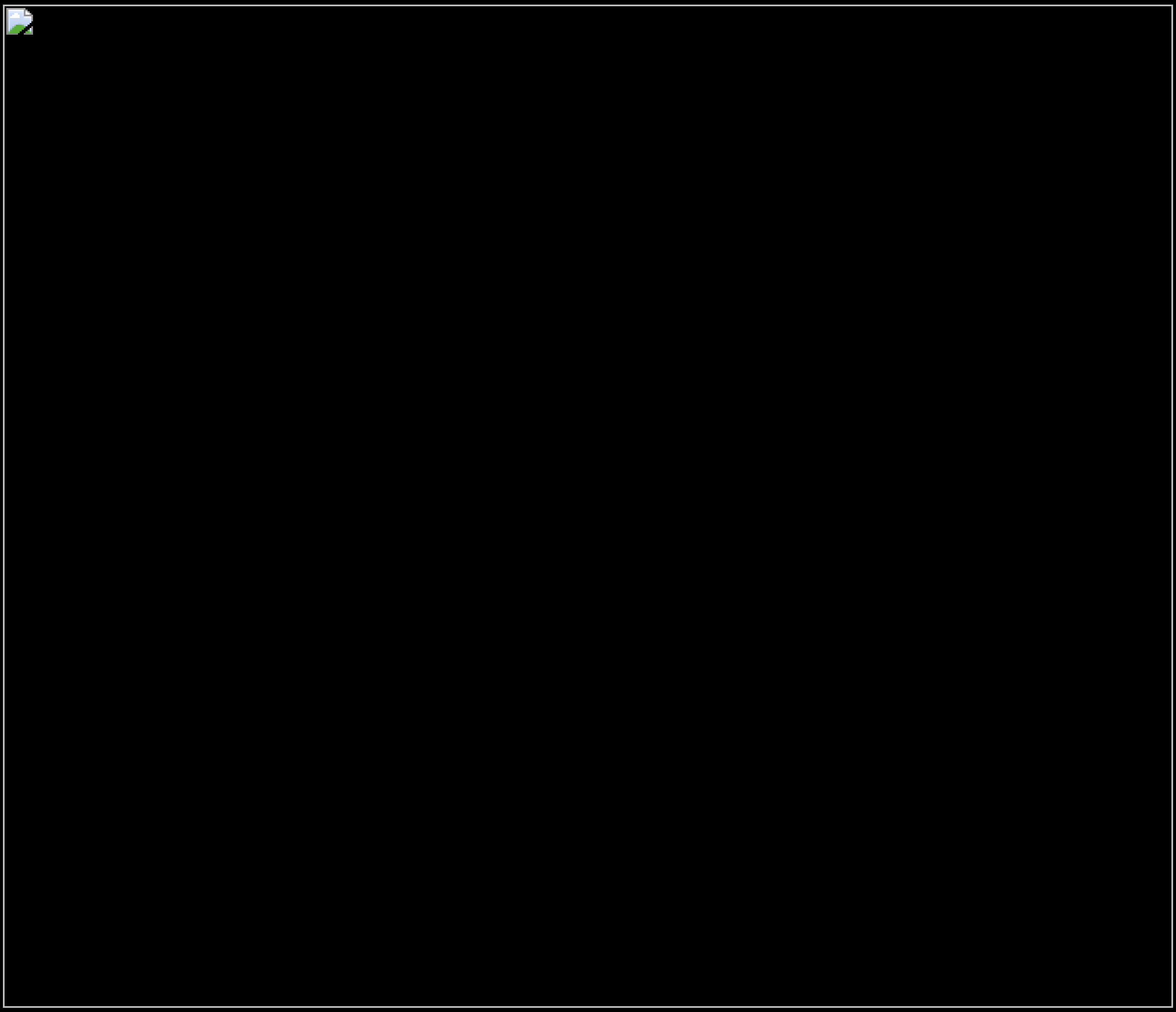
Scenario 2 (Private Mode)

In case the developer has set the settings to private mode, these can still be changed to public with a single click. However, in case these cannot be changed, the threat actor is required to have access to the users GitHub account which in most cases threat actor will not have access to. In case, they have access to the users GitHub account, they can easily log in and access the URLs.

Capability Development Cyber Essentials Review Cyber Threat Intelligence Darkweb Breach Monitoring
Digital Forensics Incident Response Malware Analysis Threat & Risk Assessment Threat Hunting
Virtual CISO (vCISO) Privacy Statement Get a quote

Phishing Campaigns

This functionality can not only be used for data exfiltration but also for hosting Phishing pages as well. The pages will be hosted on the threat actors' local machine but exposed over the internet using the forwarded ports. Thus, giving an ease to the threat actors to use the functionality without the need of hosting the application at any hosting provider.



DevTunnels URLs

These URLs are generated automatically on the runtime, and during our analysis on Mac machine, the URL is generated as below.

1. Initial Random Code for the system (Static)
2. Port (Dynamic as defined by the user).
3. MS Domain (*.euw.devtunnels.ms)

So, the final URL will look like as below.

https[:]//potato-5500[.]euw[.]devtunnels[.]ms

Detections

It is important to put detections in place for these URLs on a wildcard basis. These are not being exploited in the wild but we are sure this will become an attack vector very soon. The URLs are generated on the above pattern. Thus, the detections will be on a wildcard basis i.e.

1. *.euw.devtunnels.ms
2. *.*.devtunnels.ms

Author
- Kamran Saifullah

Published
- 10th September, 2023