Amadey stealer plugin adds Mikrotik and Outlook harvesting

medium.com/walmartglobaltech/amadey-stealer-plugin-adds-mikrotik-and-outlook-harvesting-518efe724ce4

Jason Reaves July 8, 2021

Jason Reaves

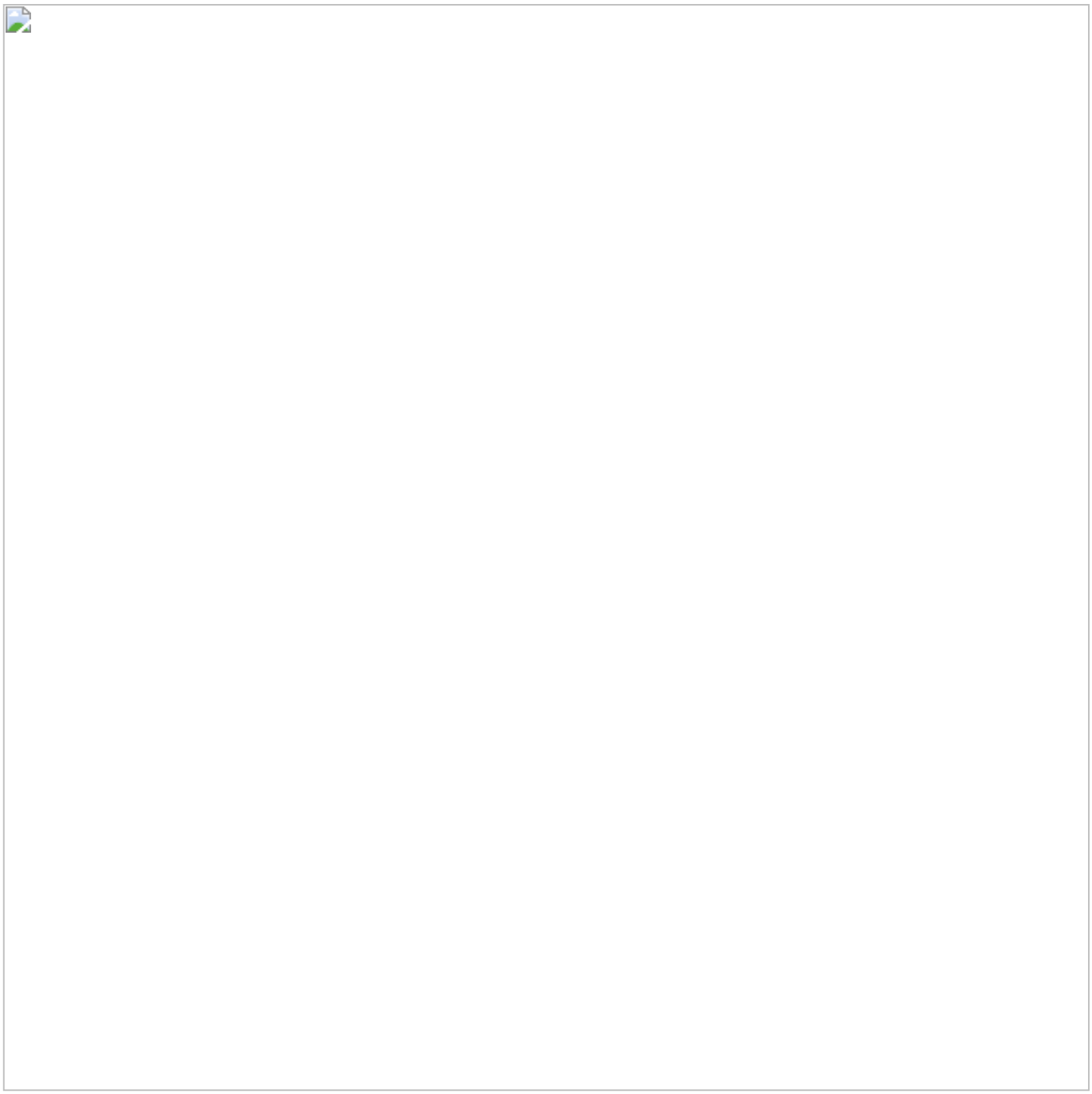
Jul 8, 2021

.

2 min read

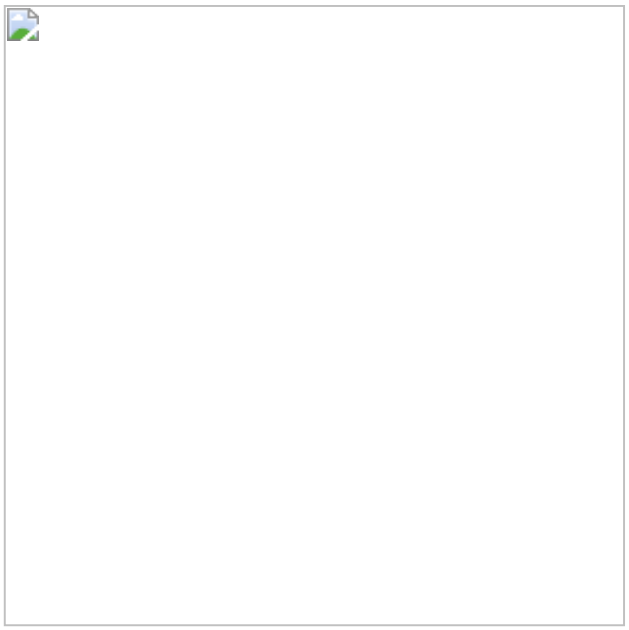
By: Jason Reaves and Harold Ogden

Last year Zscaler[3] wrote an article detailing a new version of Amadey “a2020 Amadey” that came with two new plugins ‘cred.dll’ and ‘scr.dll’. Recently, Amadey has been updated again to a new version “a2021 Amadey.” This article aims to go over some interesting additions to their stealer plugin component.

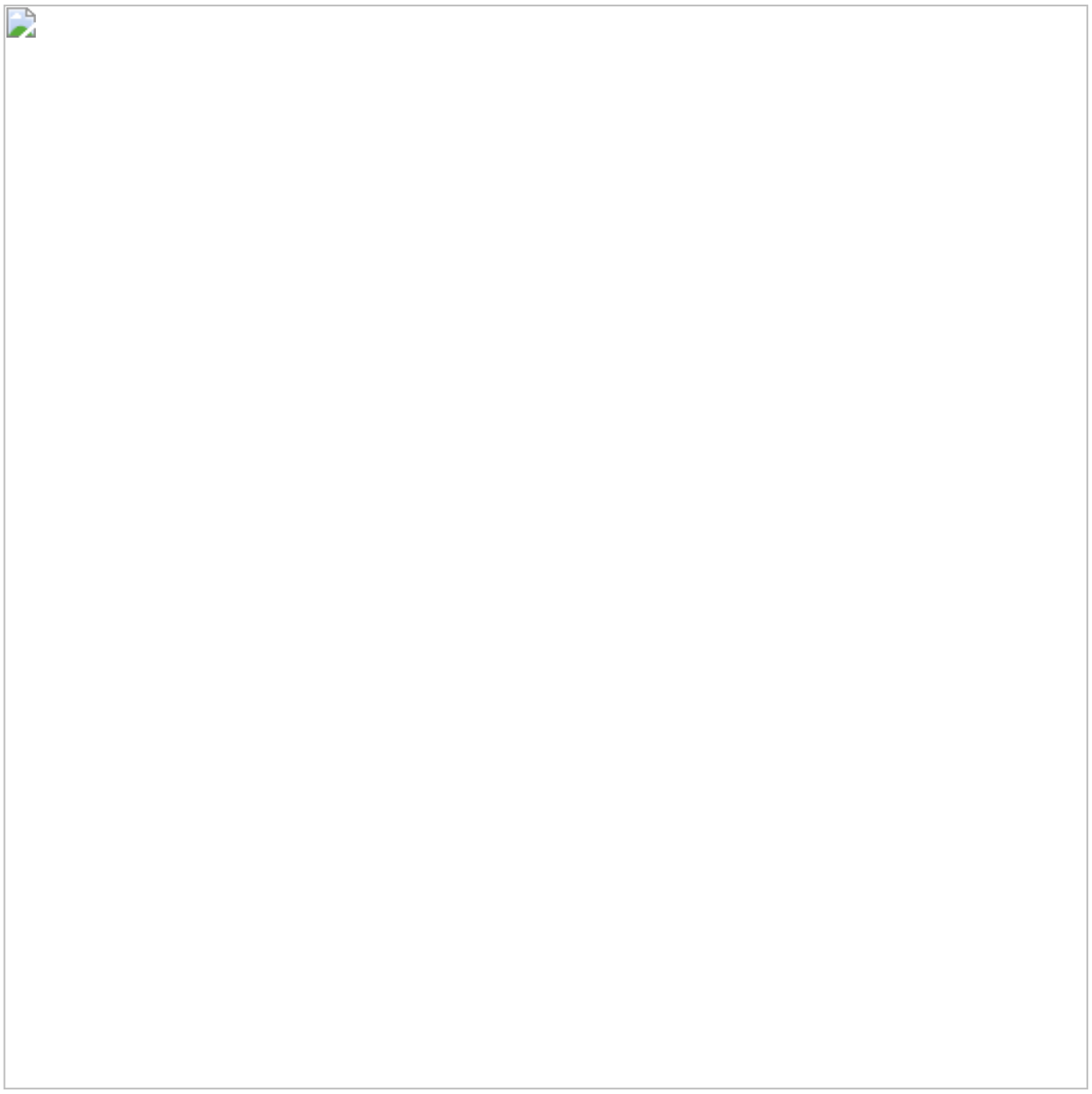


2021 Amadey Panel

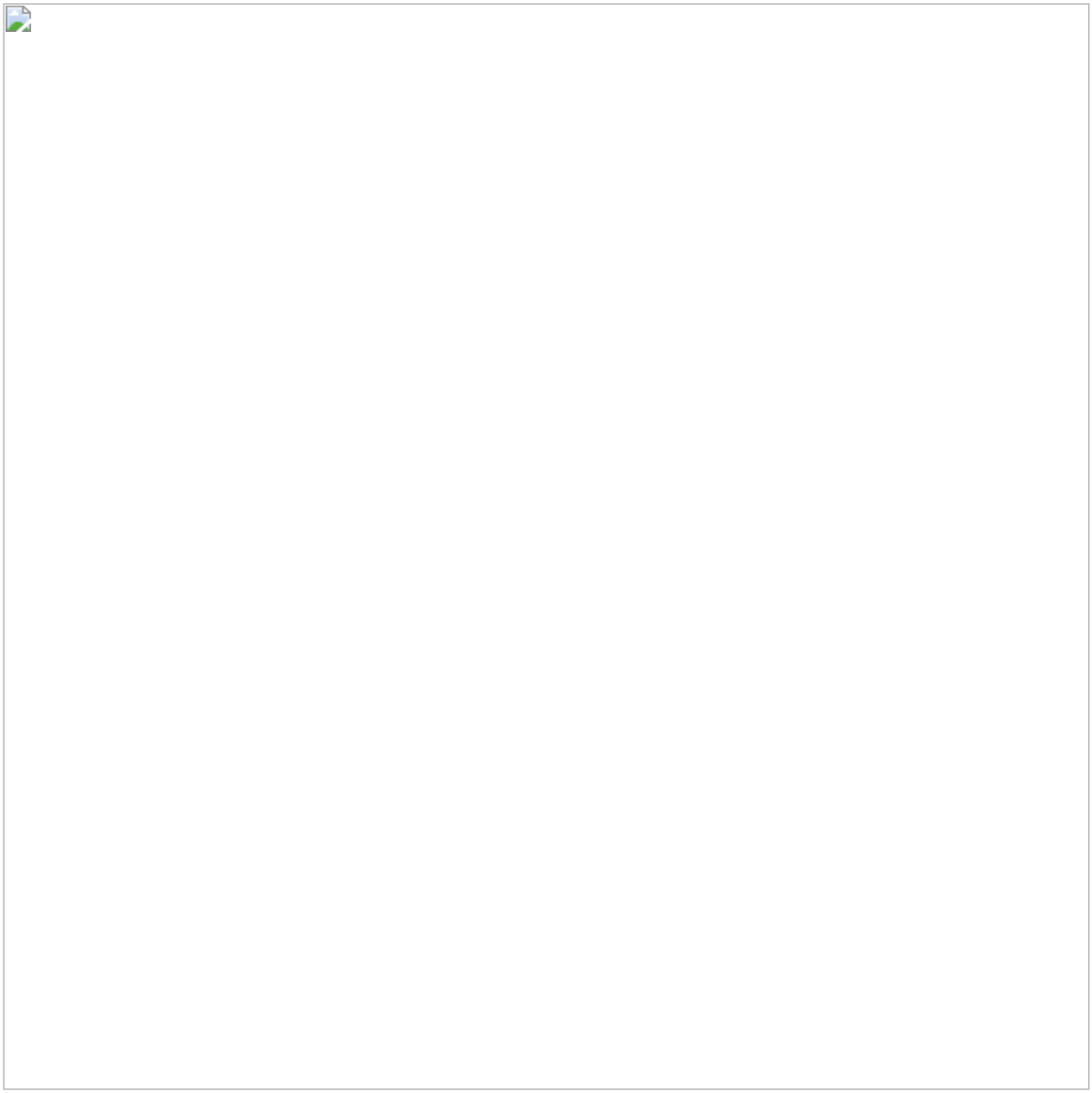
With this new version comes some interesting additions to the ‘cred’ stealer plugin as they have added functionality for harvesting Mikrotik router data and Outlook data:



Older versions of Mikrotiks Winbox[1] would give the option to export you data to a ‘WBX’ file which would store the usernames and passwords for your managed devices unencrypted along with a Addresses.cdb file which is also stored unecrypted. Freely available tools also exist to help parse these files[2] for recovering lost credentials.



Another addition is the parsing of Outlook profiles from registry in order to harvest account data:



Loaders such as Amadey continue to update their toolsets for selling on the underground and the addition of Outlook account and Mikrotik account harvesting shouldn't surprise anyone as both can be valuable data sets for criminal activities.

IOCs

```
d860bd740863e9280761ad3162d4b135d7e8cac7a9aaf302a92496e3217beb95b7eecf0ae1204a0301509d9d
```

References

1:https://forum.mikrotik.com/viewtopic.php?t=111705

2:https://github.com/jabb3rd/RouterOS_Tools

3:https://www.zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat