Amadey stealer plugin adds Mikrotik and Outlook harvesting

By Jason Reaves

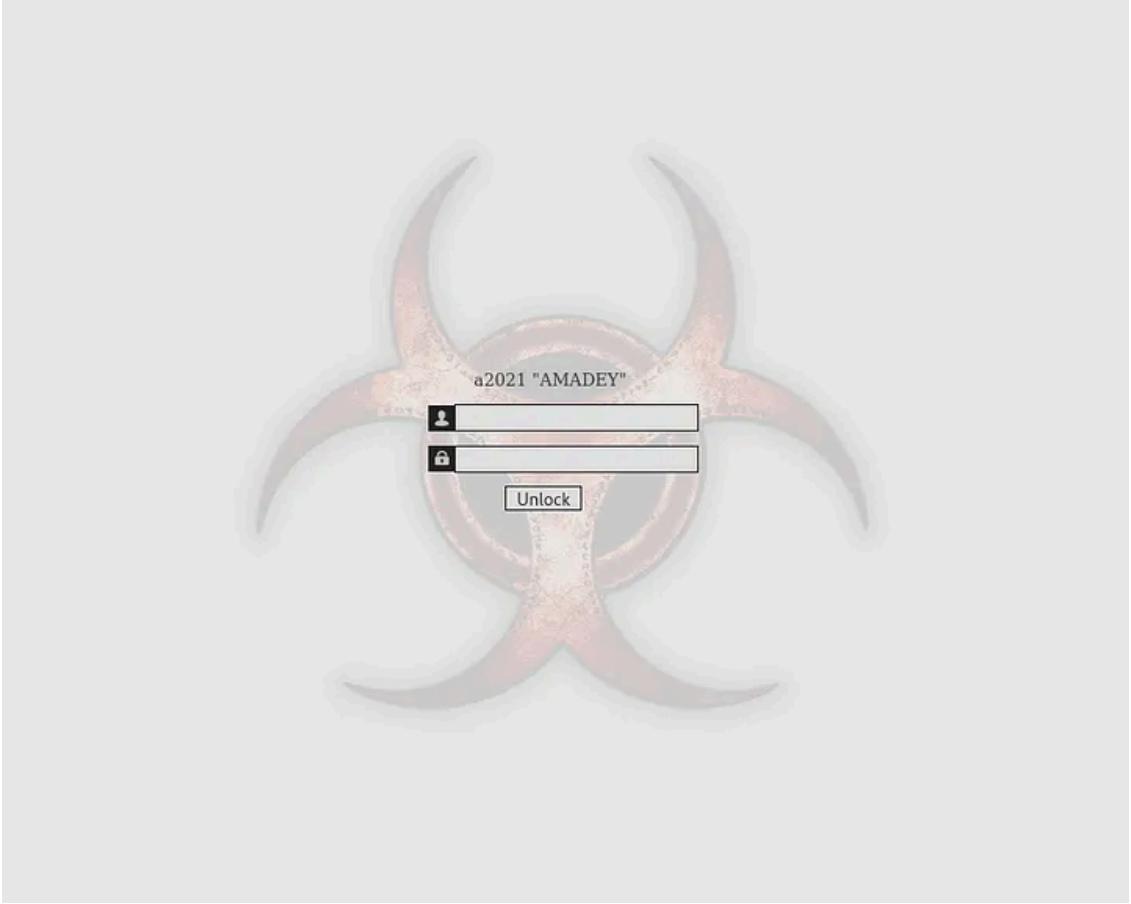
Published: 2021-07-08 · Archived: 2026-04-05 12:43:30 UTC

By: Jason Reaves and Harold Ogden

Press enter or click to view image in full size

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.

Press enter or click to view image in full size



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:

```
lea     eax, [ebp+var_4]
call    FileZilla_416604
push    [ebp+var_4]
lea     eax, [ebp+var_8]
call    Pidgin_4170E4
push    [ebp+var_8]
lea     eax, [ebp+var_C]
call    TotalCommanderFTP_417B0C
push    [ebp+var_C]
lea     eax, [ebp+var_10]
call    VNC_418DBC
push    [ebp+var_10]
lea     eax, [ebp+var_14]
call    WinSCP_419CA0
push    [ebp+var_14]
lea     eax, [ebp+var_18]
call    EmailData_415D94
push    [ebp+var_18]
lea     eax, [ebp+var_1C]
call    Mikrotik_40E6D8
push    [ebp+var_1C]
mov     eax, ebx
```

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.

```
_str__Mikrotik_Winbo dd 0FFFFFFFFh           ; _top
                                             ; DATA XREF: Mikrotik_40E6D8+34↑o
                                             ; Mikrotik_40E6D8+55↑o
                dd 30                        ; Len
                db '\Mikrotik\Winbox\Addresses.cdb',0; Text
                align 10h
_str_own        dd 0FFFFFFFFh                ; _top
                                             ; DATA XREF: Mikrotik_40E6D8+6D↑o
                dd 3                         ; Len
                db 'own',0                   ; Text
_str_M2         dd 0FFFFFFFFh                ; _top
                                             ; DATA XREF: Mikrotik_40E6D8+DF↑o
                dd 2                         ; Len
                db 'M2',0                    ; Text
                align 4
```

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

Press enter or click to view image in full size

```
                db 'Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Su';
                db 'bsystem\Profiles\Outlook\',0; Text
                align 4
_str_EMail      dd 0FFFFFFFFh           ; _top ; DATA XREF: sub_4156EC+1C9↑o
                                        ; sub_4156EC+1DD↑o ...
                dd 5                    ; Len
                db 'EMail',0            ; Text
                align 4
_str_email      dd 0FFFFFFFFh           ; _top ; DATA XREF: sub_4156EC+249↑o
                dd 5                    ; Len
                db 'email',0            ; Text
                align 4
_str_Outlook    dd 0FFFFFFFFh           ; _top ; DATA XREF: sub_4156EC+255↑o
                dd 7                    ; Len
                db 'Outlook',0          ; Text
_str_IMAP_User  dd 0FFFFFFFFh           ; _top
                                        ; DATA XREF: sub_4156EC:loc_415966↑o
                                        ; sub_4156EC+28E↑o ...
                dd 9                    ; Len
                db 'IMAP User',0        ; Text
                align 10h
_str_IMAP_Password dd 0FFFFFFFFh          ; _top
                                        ; DATA XREF: sub_4156EC:loc_4159FF↑o
                                        ; sub_4156EC+327↑o ...
                dd 13                   ; Len
                db 'IMAP Password',0    ; Text
                align 4
_str_POP3_User  dd 0FFFFFFFFh           ; _top
                                        ; DATA XREF: sub_4156EC:loc_415A96↑o
                                        ; sub_4156EC+3BE↑o ...
                dd 9                    ; Len
                db 'POP3 User',0        ; Text
                align 4
_str_POP3_Password dd 0FFFFFFFFh          ; _top
                                        ; DATA XREF: sub_4156EC:loc_415B2F↑o
                                        ; sub_4156EC+457↑o ...
                dd 13                   ; Len
                db 'POP3 Password',0    ; Text
```

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

```
d860bd740863e9280761ad3162d4b135d7e8cac7a9aaf302a92496e3217beb95
b7eecf0ae1204a0301509d9dd1ad1a7329463ed5
fa07c8de6db23c1be2ee8da97c5621f7fc006469f84e2835195fc943de43d544
d8932ee7ff3b37f1f566dd70233aab7e8f388558
```

References

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

Get Jason Reaves's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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

---

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