APT Attack Simulation 29

Date:5/17/2023

```
ess logged k [if] metalogramical vess traces
                                                                                                                                                                                                                                                                       e[get]script sec={#wq3 *Ft ontocs >
                                                                                                                                                                                                                                                                                       a7:/q.s) {logged = online.click}
                                                                                                                                                                                                                                                                                                 igger.warning) #keu_input <ch
                                                   then prote acceptage and being
                                                                                                                                                                                                                                                                                                       e") add string < status > (_ a3*5
      function logged wimput losses facation daugett #
                                                                                                                                                                                                                                                                                                             n) local cone in terms
      function logged: # input steller function logged: #
 then script sice (true) - Purknown) mw4:80a?
                                                                                                                                                                                                                                                                                                           tatus and mess is - wylocole)
                                                            script-sre-cftrue local config
                                                                                                                                                                                                                                                                                                          ess: status [true]
                     #key input cehasion (d fews mn4:h6tl8
                                                                                                                                                                                                                                                                                                           log origin set (278,56,34,#) if
                              // script src = address [status?] code <
                                                                                                                                                                                                                                                                                                              click }
   command w macress denial // script src=[error]
                                                                                                                                                                                                                                                                                                       Key inpulsarial distriction of the same
then script src [true] (?unknown) m#4:80a?:/
                                                                                                                                                                                                                                                                                                      Status 2 2
                                                                                                                                                                        status omm
                                                           script src=[true] local.confi
                                                                                                                                                                 (245, 23, 068, 789,
                                                                                                                                                                                                                                               k.command | # >> a
                                                                             logged: # Input false fun
                                                                                                                                                                n name kimg> = spa
                                                                                                                                                                                                                                           ress logged < [If] n
                                                                                                                                                                                                                                                                                                             OQ.OF INPT
                                      function login credentials {logged:
                                                                                                                                                              put.new(create))
                                                                                                                                                                                                                                            ent.name[get]sc
                                                                                                                                                                                                                                                                                                                 STORES SECTION
                                                                                 // script src= address
                                                                                                                                                                 atus?] code < [tr
                                                                                                                                                                                                                                               tus (m#4:88a7:
                                   [lock.command]# >> access:denial //
                                                                                                                                                                     t src= erro
                                                                                                                                                                                                                                                                                                             F.Warning F. W.Kottokshill Cooks
                                                                                                                                                                                                                                                       de logged (†
                                                   then script src [true] [?unk
                                                                                                                                                                                                                           statu
                                                                                                                                                                                                                                                                                                              ) add string c status > ( a3 5
     sunction logged: # innut.faise function books w
                                                                                                                                                                                                                   onfig sc
   for chien based windut-false function based w
                                                                                                                                                                                                                  onfig sc
                                                                                                                                                                                                                   onf sc
 then yes so, are - true; / curvors was named and as statu
              the second of th
                      error and the state of the stat
then sorpt are trace of an examinimum will be able to status command if ("true") add string as
                                                                                                   is the incolconfig = (245, 23,068,789,048) [lock.command]#>>>
                                                                                                                                                        set (278,56,34,#) If = frame <imq> =s
```

Authors

Abdallah Mohammed

<u>Github</u>

Abdulrahman Mohammed (De3vil) Github

Hossam Ehab (0xHossam)

Github

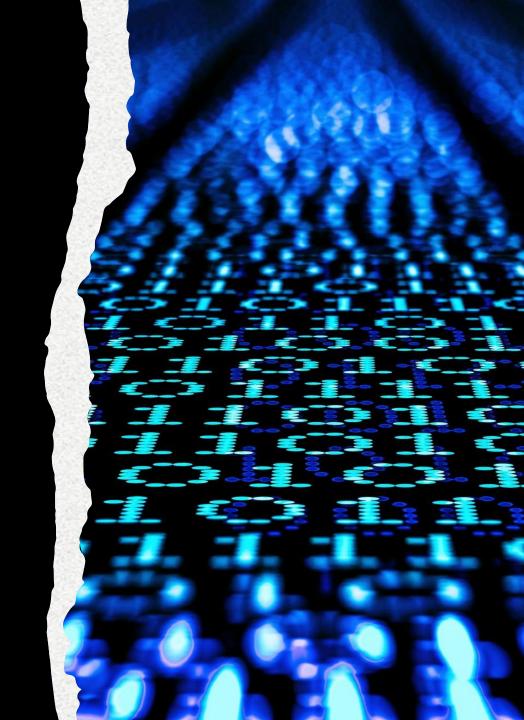
Documentation

How does the attack work?



First stage

- The attack begins with an email that contains a specially crafted HTML page that includes a malicious code. Upon opening the malicious page, an ISO file is downloaded that contains the malicious files.
 - The malicious file performs two actions
 - 1- Drops an ISO file (Second Stage)
 - 2- Sends a request to a malicious SMB server controlled by the attackers to steal the user's NTLM Hash for lateral spread.



Second stage

- The ISO file is opened and contains a forged lnk file that appears to be a PDF file from its icon, but it actually points to an exe file. When the exe file is executed, it opens the PDF file.
- Upon execution of the malicious exe file, the PDF file is also executed. DLL and bin files are loaded, a registry key is added for persistence, and the DLL runs During this stage.
 - At this point, the attacker enables UAC bypass, gains system administrator privileges, hijack Windows Defender, and loads the malicious DLL instead of the original file. This allows the attacker to invisibly direct the malicious functions on the victim's machine, download more malware, and achieve system persistence.

Third stage

• The DLL acts as a Loader to read the encrypted bin file and decrypt it in memory and try to hide from detection and run.