Snagging Creds From Locked Machines With LAN Turtle Or USB Armory

Neue Methoden erfordern neue Maßnahmen. Unter diesem Hyperlink

https://room362.com/post/2016/snagging-creds-from-locked-machines/
https://lanturtle.com/wiki/#!index.md

wird beschrieben, wie einfach es ist, einen gesperrten Computer wieder zugänglich zu machen. - Ich möchte mir gar nicht ausmalen was mit den gestohlenen Anmeldedaten alles angefangen wird.

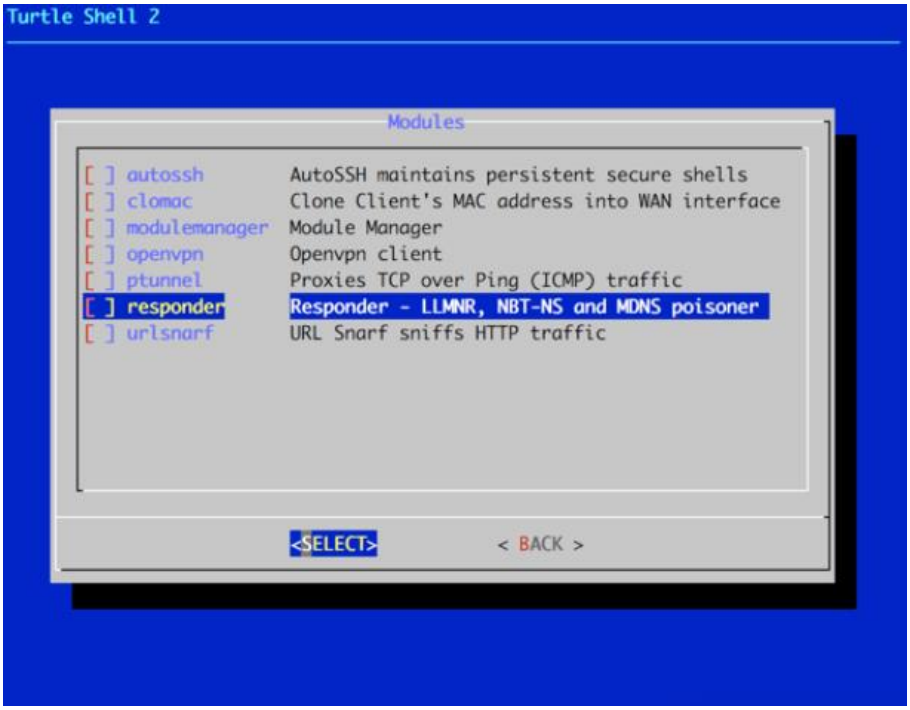
Das zum Einsatz kommende USB Gerät ist letzten Endes ein USB >Netzwerk Adapter/Gateway mit spezieller Firmware. Das Zusammenspiel mit einer dafür entwickelten Software macht es für Unternehmen zu einer wirklichen Bedrohung.

Das USB-Gerät ein kleiner Mini PC, der sich nach dem Anstecken an den physischen PC als neue Netzwerkkarte ausgibt und auch ohne Probleme von Windows installiert und über DHCP eingerichtet wird.

Und das im gesperrten Zustand!

Auf diesem Mini PC am USB-Port läuft ein Linux mit einem speziellen Responder, der auf alle Netzwerkanfragen antwortet. Dieser ist ab jetzt das Default-Gateway und DNS-Server in einem und bietet dem lokalen PC eine Proxy-Konfigurations-Datei an. Ab jetzt läuft der gesamte Netzwerkverkehr über diesen Mini PC. Der darauf laufende Responder antwortet jetzt auf alle Anfragen und erzwingt vom lokalen PC eine Authentifizierung. Das war`s.

Windows lieferte dem Angreifer die lokalen Anmeldeinformationen frei Haus.



USB Armory Bundle

http://hackerwarehouse.com/product/usb-armory/

Lan Turtle:

https://lanturtle.com/

Snagging Creds From Locked Machines With LAN Turtle Or USB Armory

Das Problem:

Das eigentliche Problem ist, das Windows standardmäßig PnP Geräten vertraut und diese auch während eines gesperrten Bildschirms nach anstecken an den dafür vorgesehen Port installiert und betriebsbereit macht.

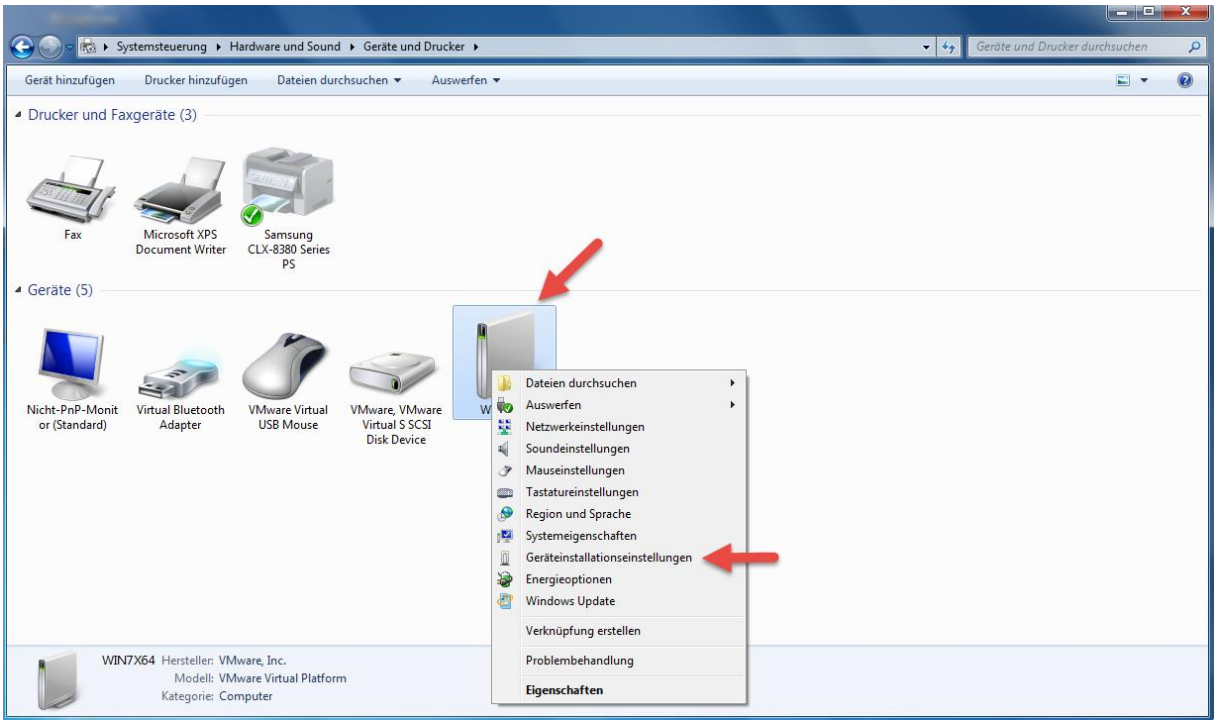
Lösung 1:

Wer jetzt eine DLP Lösung wie z.B. die von Trend Micro im Einsatz hat und die Unternehmens USB-Geräte mit einer White-List pflegt und zulässt, hat keine Probleme zu befürchten.

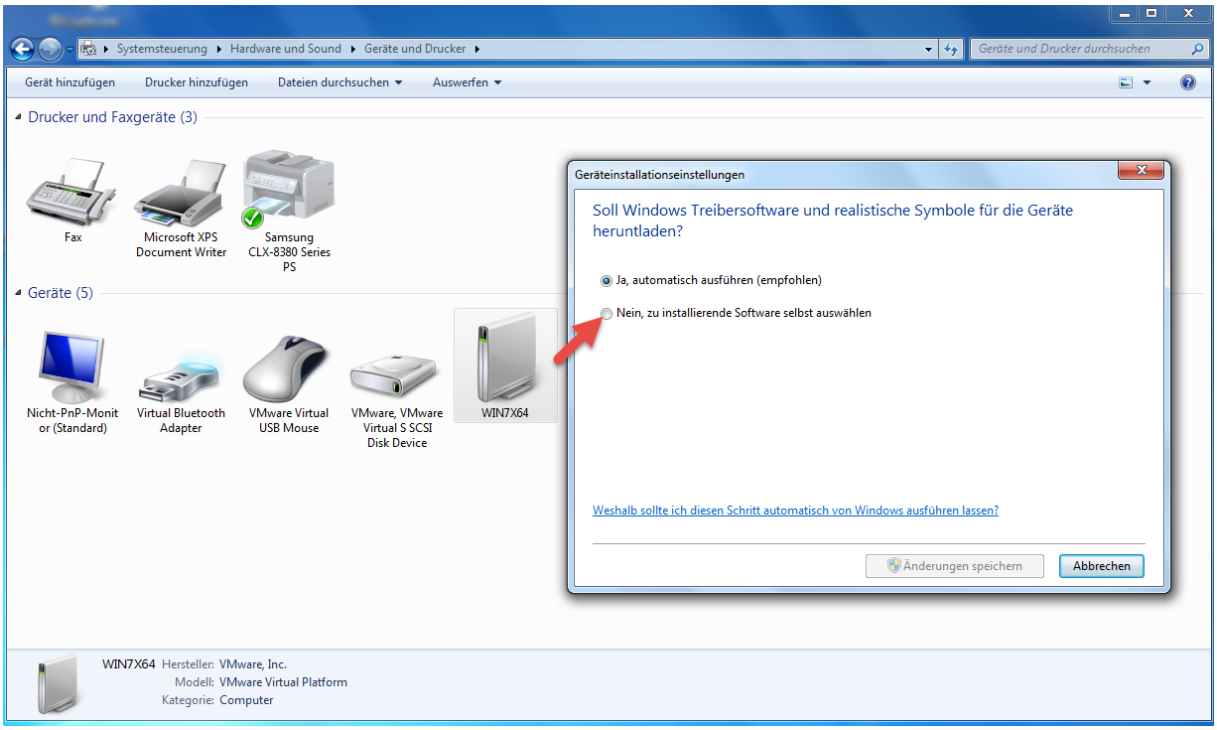
Lösung 2:

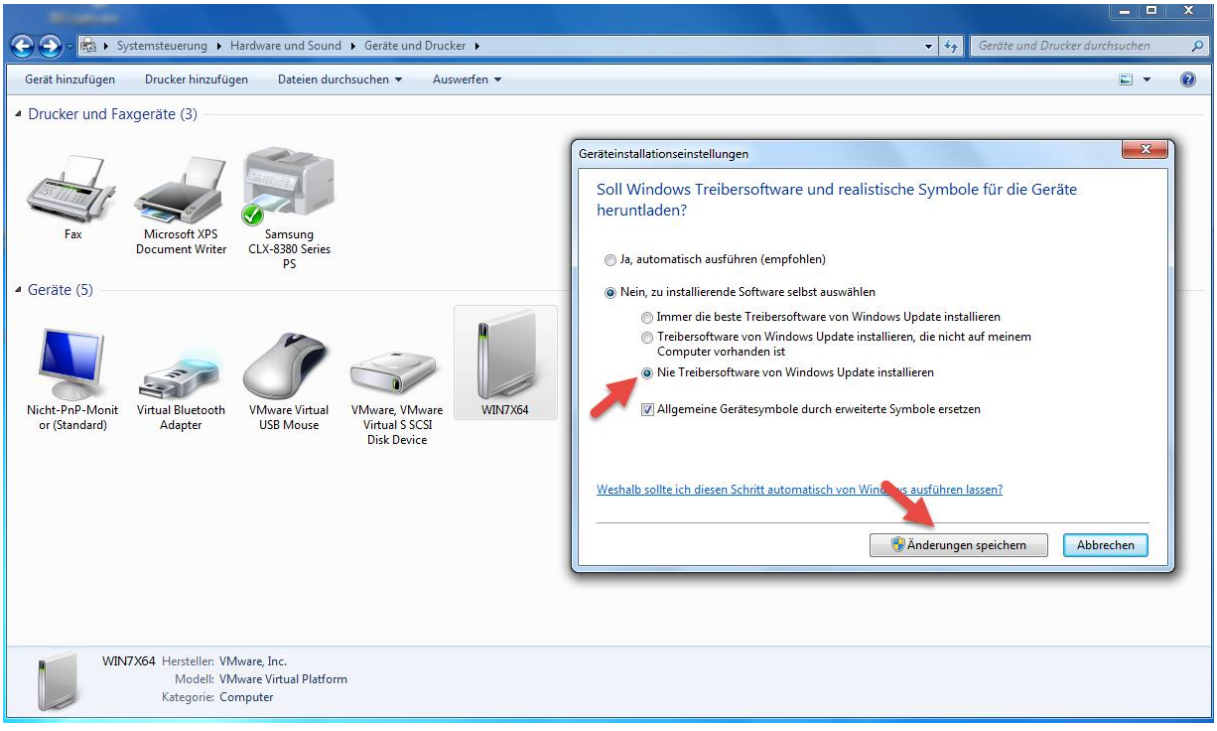
Um diese Methode des snaggens zu erschweren gehen wir wie folgt vor und deaktivieren den automatischen Treiber Download. Somit kann die angesteckte/unbekannte Hardware nicht installiert werden.

Manuelle Abschaltung des Treiber Downloads:



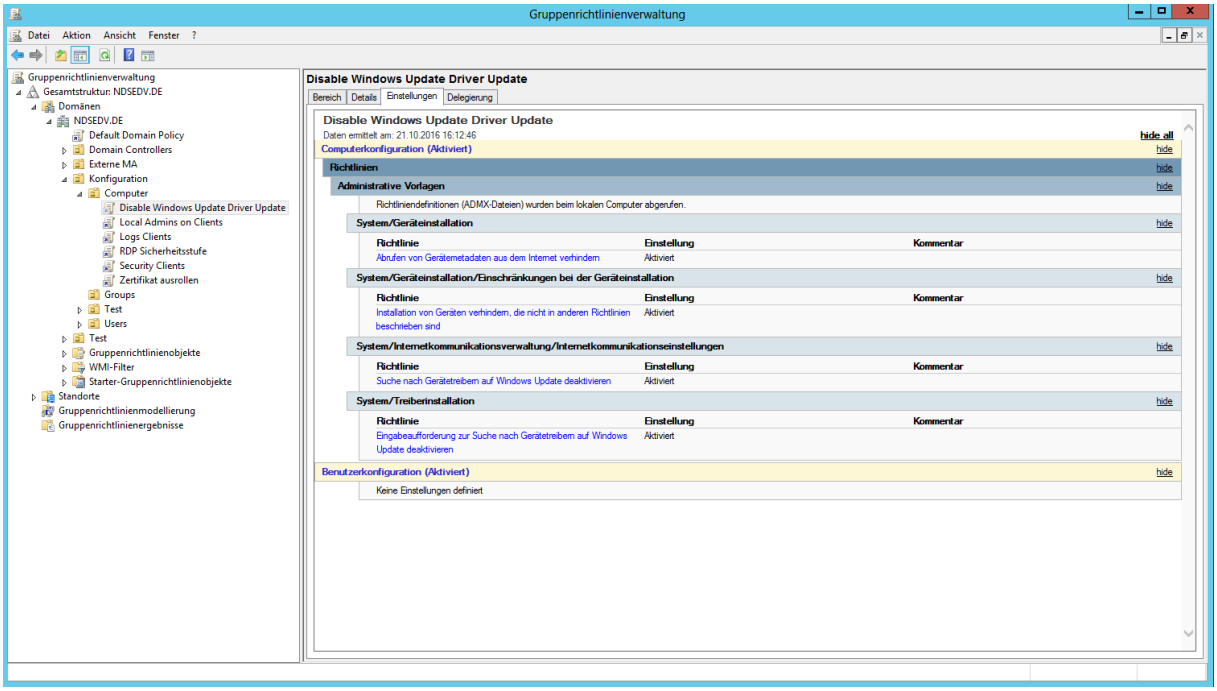
Snagging Creds From Locked Machines With LAN Turtle Or USB Armory



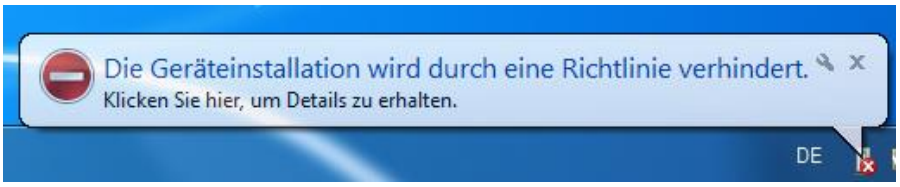


Erstellt von Jörn Walter www.der-windows-papst.de – 01.07.16 / 21.10.16

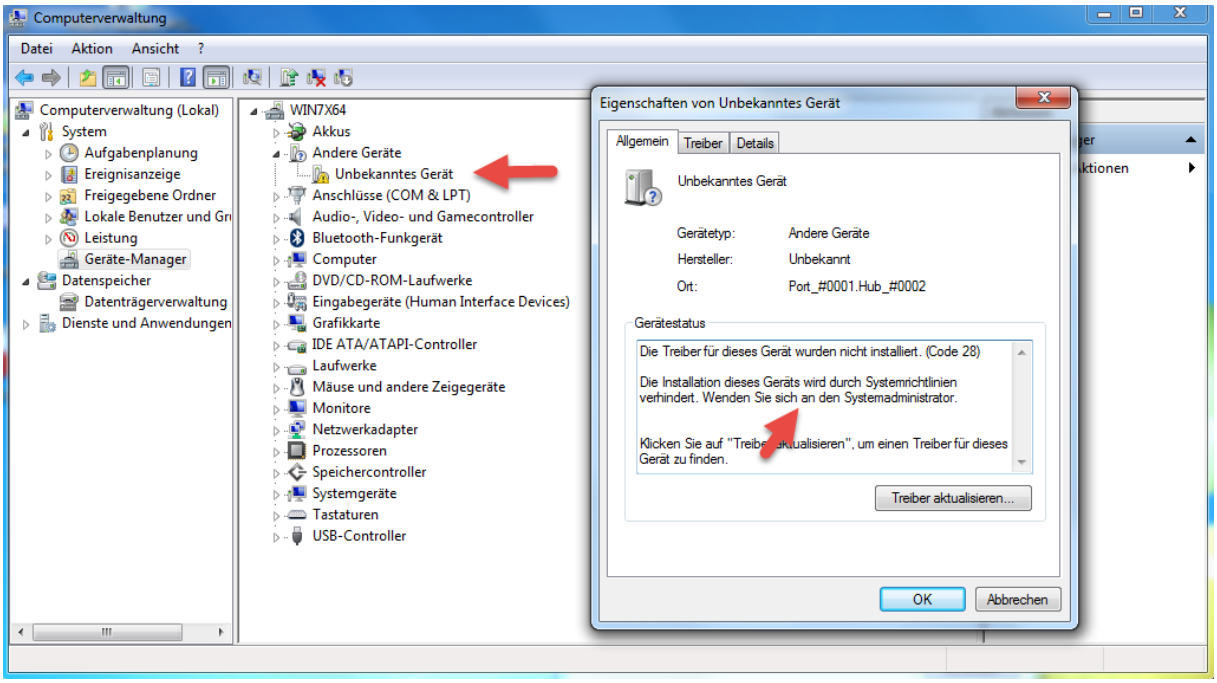
Um das Ganze unternehmensweit umzusetzen sollte eine Gruppenrichtlinie mit folgenden Einstellungen erstellt werden.



Diese Richtlinieneinstellungen führen unter z.B. Windows 7 zu diesem Ergebnis:



In der **Computerverwaltung > Geräte-Manager** sieht das so aus:



Snagging Creds From Locked Machines With LAN Turtle Or USB Armory

Registry-Key zum Abschalten von automatischen Treiber Update über Windows Update:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"ExcludeWUDriversInQualityUpdate"=dword:00000001
```

Registry-Key zum Einschalten von automatischen Treiber Update über Windows Update:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"ExcludeWUDriversInQualityUpdate"=dword:00000000
```