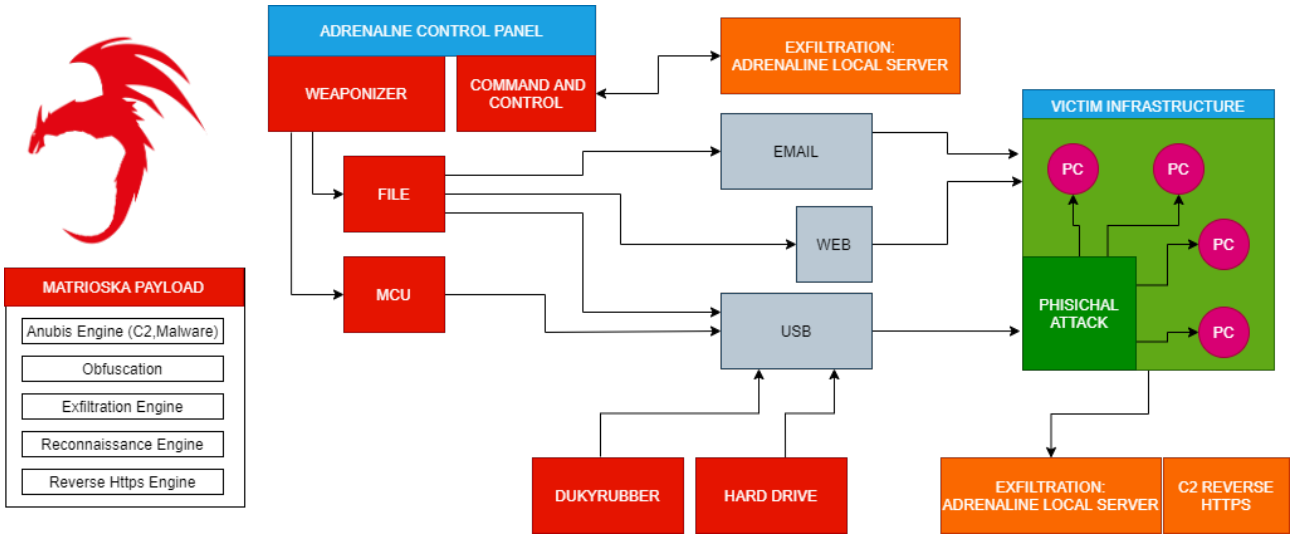
Adrenaline Operative Manual. Ver 0.4(EN)

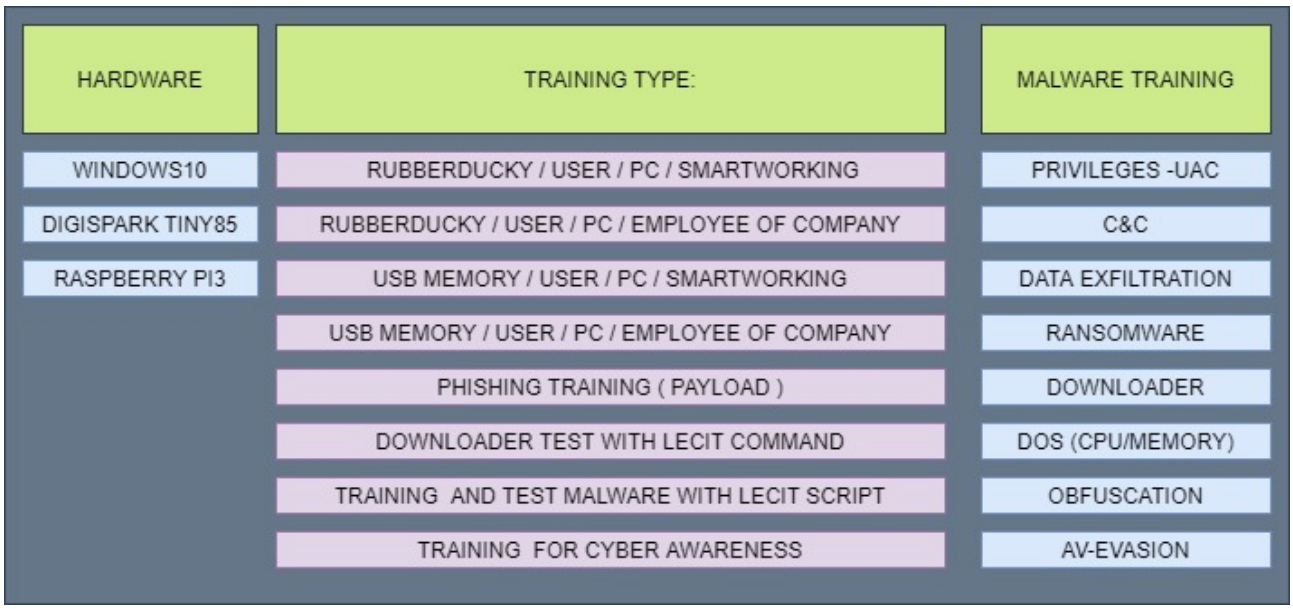
Adrenaline RT is a software to become aware of your safety system and personnel training.

Adrenaline RT works with updated windows10 systems, simple and intuitive interface to create training attacks usable by Cybersec Awareness & Training, RedTeam, Pentester, Ethical Hacker, Public Employee, and Private User.



Sgneep.com/adrenaline/

Adrenaline RT Training Program:



Requirements:

- Adrenaline RT License Key and Password
- RaspberryPi3 with USB BOOT enabled
- Digi-Spark Tiny85
- PC With win10 -64 BIT (Pentest-Machine)
- PC with win10 -32/64 BIT (Target-Machine)

Mode and Target: Attack & Training, for Microsoft Windows 10 32/64Bit Target

Main Adrenaline features:

- Cybersec Awareness Training
- Phishing: PDF + Code #C (Trojan-Downloader)
- Phishing: PDF + powershell code (Trojan-Downloader)
- Phishing: PDF + batch code (Trojan Downloader)
- Phishing: PDF + .vbs code (Trojan-Downloader)
- Attack: Ransom Class Shuffler Payload (FUD)
- Attack: CPU and Memory connection (DOS)
- Attack: * UAC-Bypass (fodhelper.exe + SgneepAvEvasion for Win-Defender)
- Attack: Downloader Test: powershell Wget, batch Wget, Native Curl, BITS, …
- Physical: program RubberDucky Firmware + digispark-Tiny85 PCB
- Physical: config RubberDucky Matryoshka in Payload or enable TestMode
- Reconn: Read network specifications (exfiltration)
- Reconn: Read Hw / Sw specifications (exfiltration)
- Reconn: Read Wi-Fi account (exfiltration)
- Reconn: Read all password file
- Installation: C2 Payload
- Installation: “Matryoshka” Payload
- Installation: ForkBomb Payload
- Installation: Auto-Start (add Register Key)
- Installation: Privileges Escalation
-C2: inject and run new Script to Target folder (“%tmp%”).
-C2: payload exit

Attack Simulation and Cybersec Awareness:

Reconn: This is not your own attack. In this phase the machine data is exfiltrated. This is system data and is of strategic importance, useful for the RedTeam or Pentester to set up the next attack. You can try this feature in the “Quick Scan” section.

Phishing: Train with Phishing Attack Simulations. To protect itself from this phenomenon, every organization must inevitably invest in the "human factor", training the ability of each user to recognize a Phishing attack.

Ducky-Rubber: for this type of attack you need the digiSpark tiny85 or compatible circuit. Once programmed with Adrenaline, the Tiny85 transforms into a USB keyboard. The Digispark Tiny85 or similar model is sold in PCB format, useful for building your pentest gadget and carrying out training tests.

Usb-Memory-Stick: for this type of attack, a memory key with the prepackaged payload is enough. It must be accompanied by social engineering techniques

Matrioska: “Adrenaline Matrioska” is a payload capable of C2 Installer, Shuffler Installer, ForkBomb Installer, * UAC-Bypass, Data Exfiltration, Startup Process Manipulation, Log Generator. All Log files generated by Adrenaline Matrioska are contained in the % TMP% folder

UAC-Bypass: Generally it is blocked by Windows Defender. However, the injection takes place anyway thanks to SgneepAvEvasion.

C2 Command And Control: Generally not blocked by Antivirus engines. It is used to inject more code into the victim's computer. It can be inserted into the victim's machine being trained via RubberDucky attack, File with Trojan, or Phishing attack.

DOS Attack: It is used to test the consequences of a Fork Bomb (a process is executed that will execute itself exponentially, it will occupy all the resources of the Target PC such as RAM, CPU, HDrive. The training test is set to stop after a few seconds and it is for demonstration purposes only.

Adrenaline-Local-Server: is used to collect data exfiltrated by training attacks.

Adrenaline Malware Simulator, Training and Weaponizer

Phishing Attack Training

Malware Attack Training and Simulation

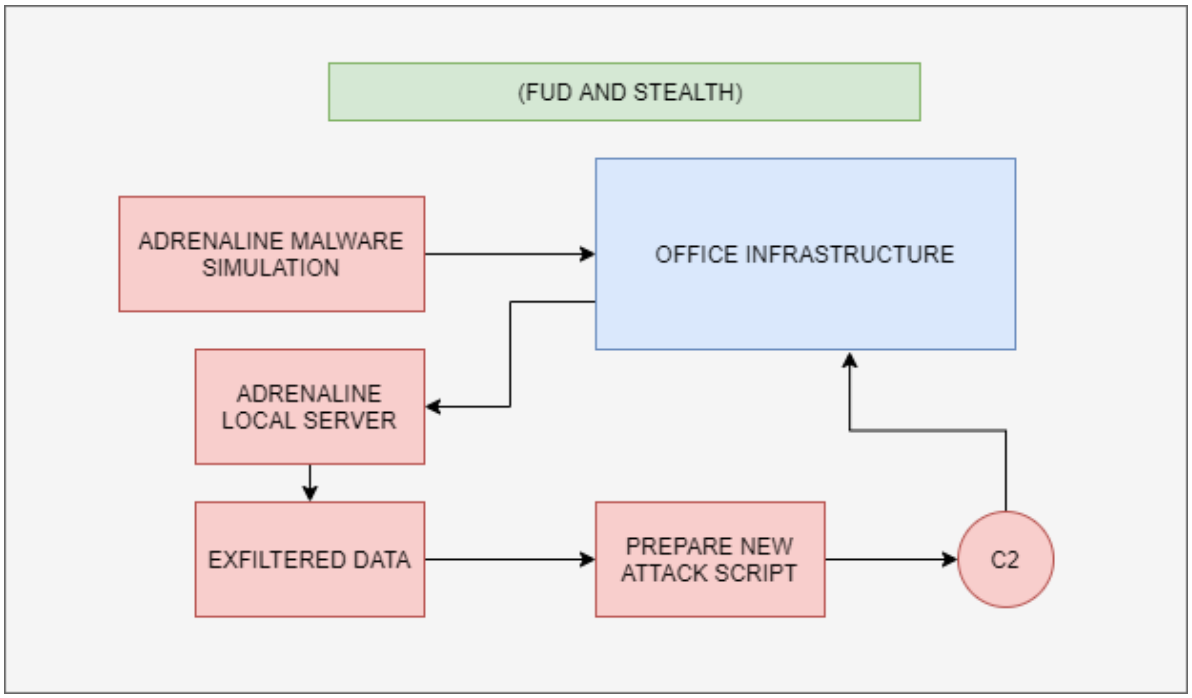
Ransom Class Attack Training and Simulation

Ducky-Rubber Training and Simulation

Trojan Attack Training and Simulation

Command & Control Training and Simulation

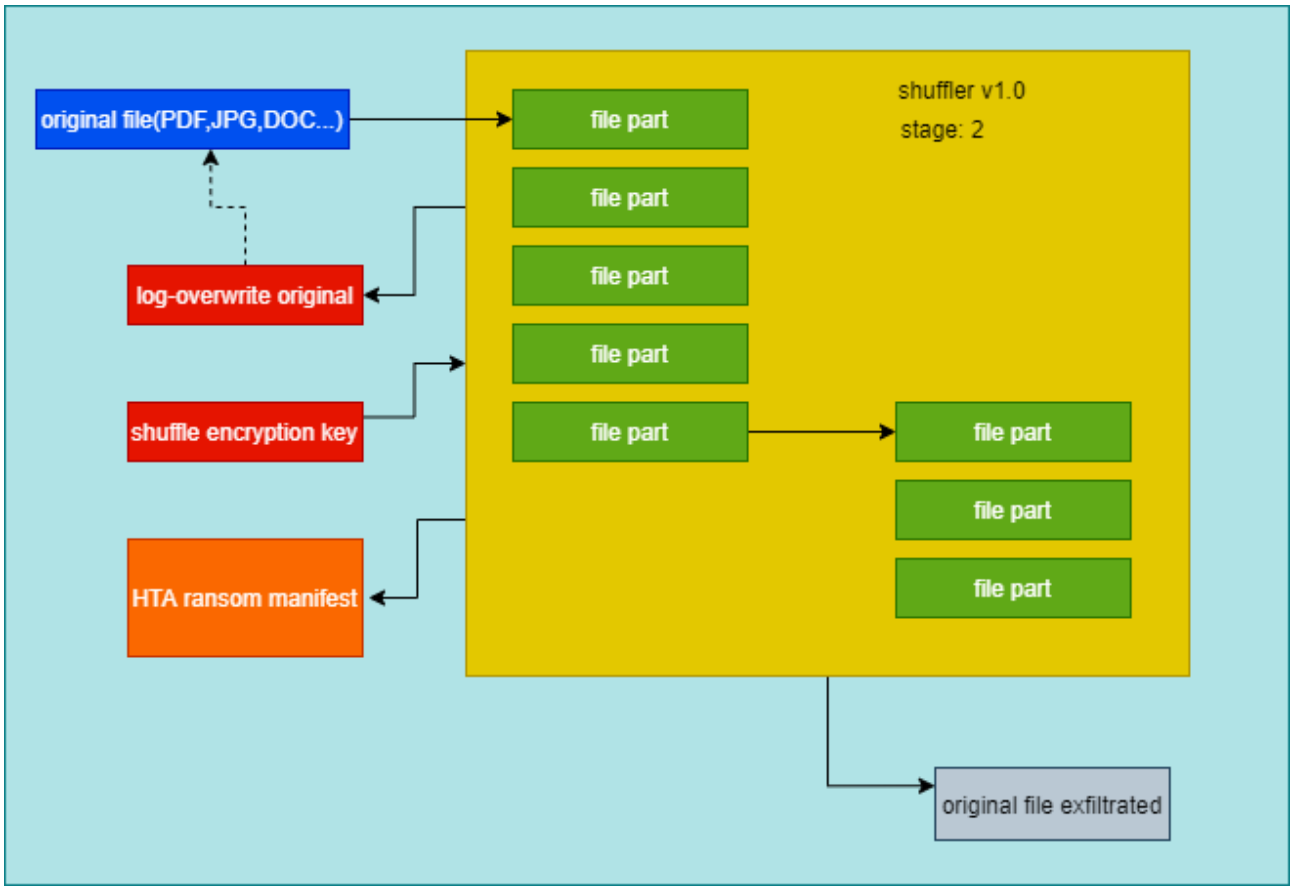
Exfiltered Data Simulation



Adrenaline Shuffler Encrypter, ransom class.

Warning!! uFor security reason this payload encrypt only *“anubis.test”* file in %tmp% folder.

"Adrenaline Shuffler" is used to train the staff employed and test the AV environment used in Windows 10 32/64 Bit, it is also of the Ransom type, so it requests redemption with a demonstration page using MSHTA (*resealable with CTRL+ALT+DEL*) . The main feature is the ability to encrypt the file by breaking it down into small pieces and shuffling them by renaming them. Our test only works on the "*pentest.anubis*" file, so for security reasons the file must be created first on the victim machine of the user to be trained.



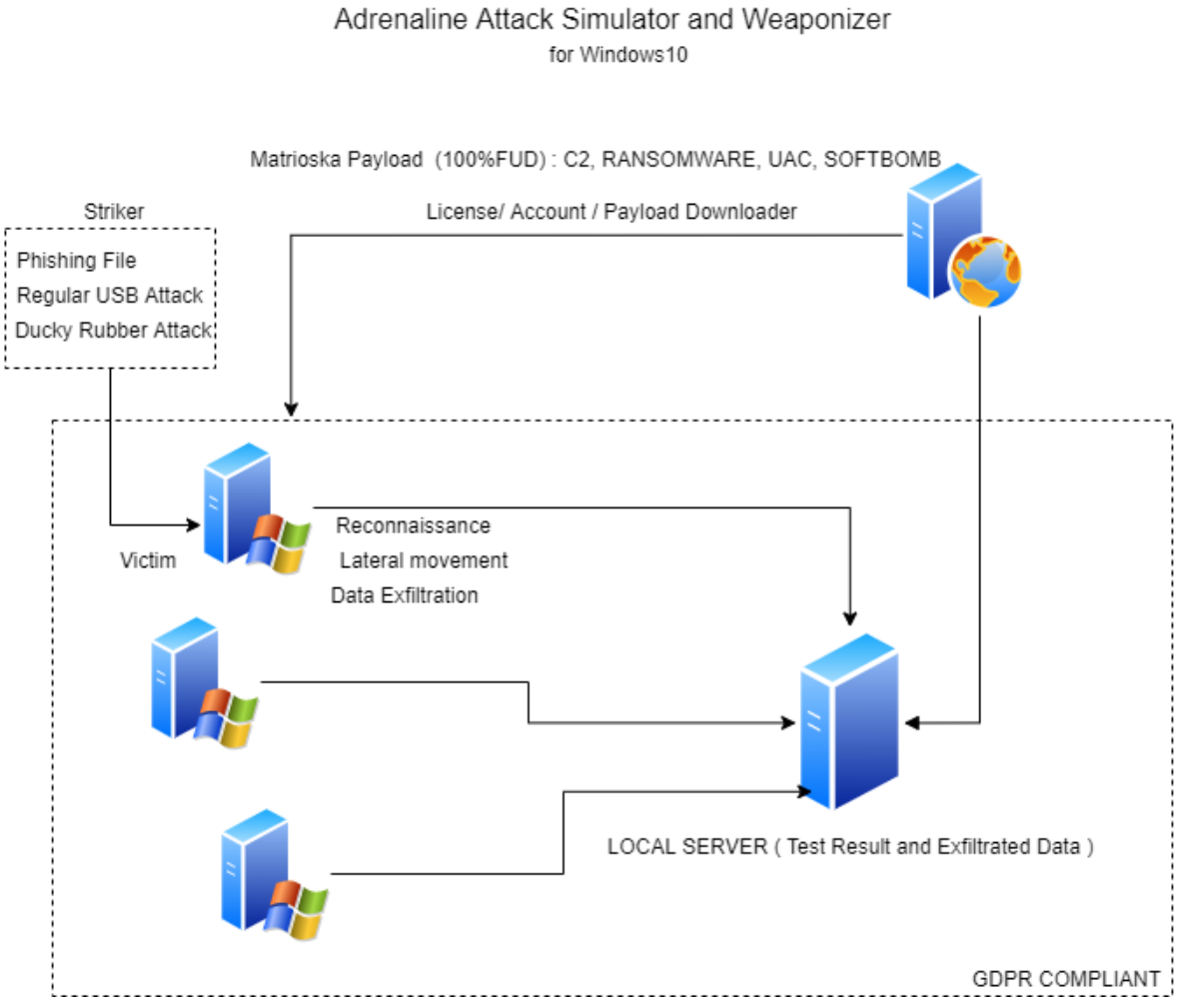
“Adrenaline Local Server” work with RaspberryPi3.

You can access the local server directly from the Adrenaline RT interface or directly from the Local Adrenaline server (available for RaspberryPi3 Hardware)

For security reasons it is not possible to access the Adrenaline Server remotely.

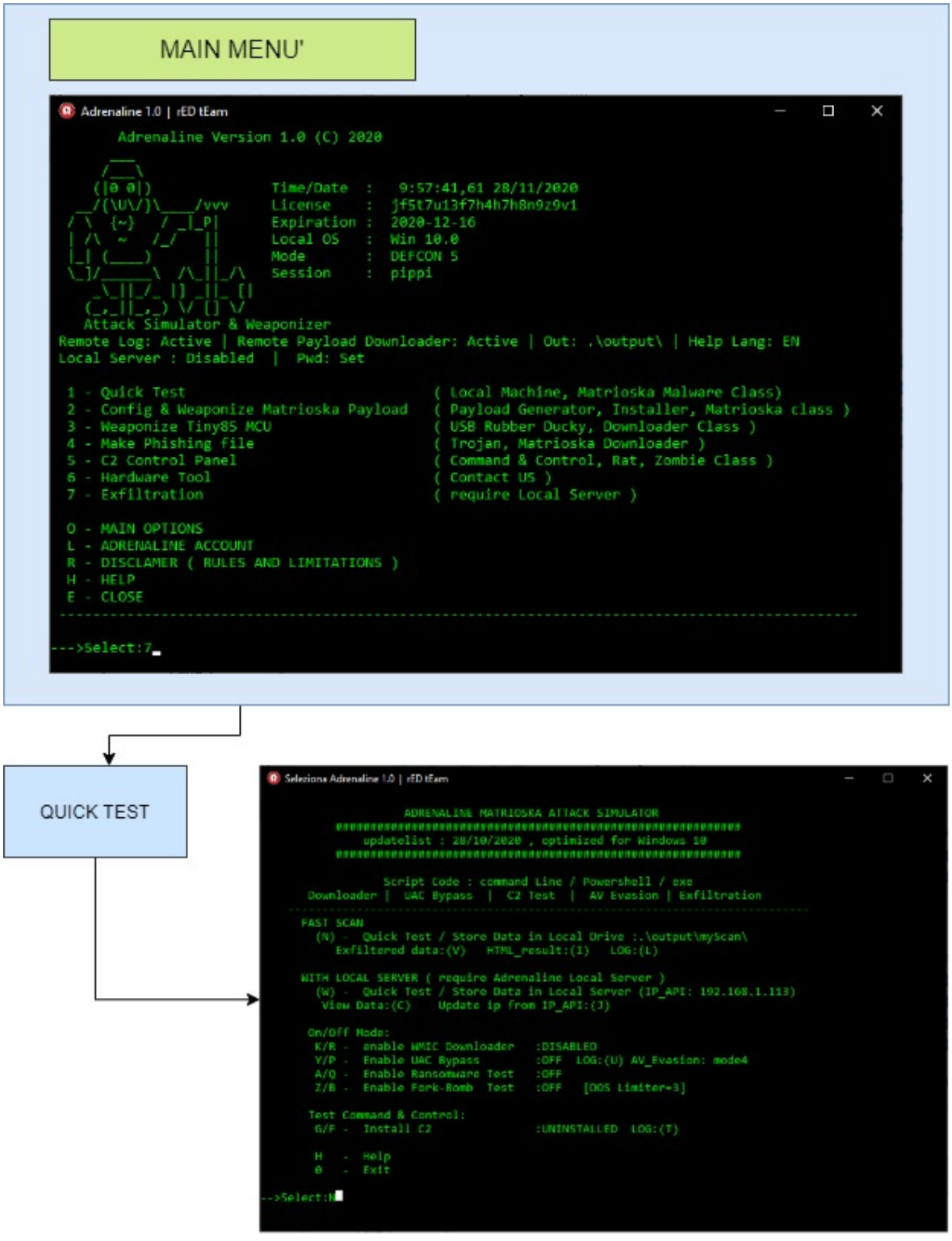
This test is recommended for small and large Windows 10 PC networks. If the simulated attack is carried out successfully, the Adrenaline server collects all the exfiltration information and PDF reporting.

The “Local-Adrenaline server” requires Internet connection and DHCP.



Main Adrenaline RT Interface:

This is the starting point of Adrenaline. Here you can organize your simulated attacks.



In this section (*button 1*) you can perform a quick scan in the Target machine. No files are destroyed or exfiltrated off your pc or subnet directly by Adrenaline.

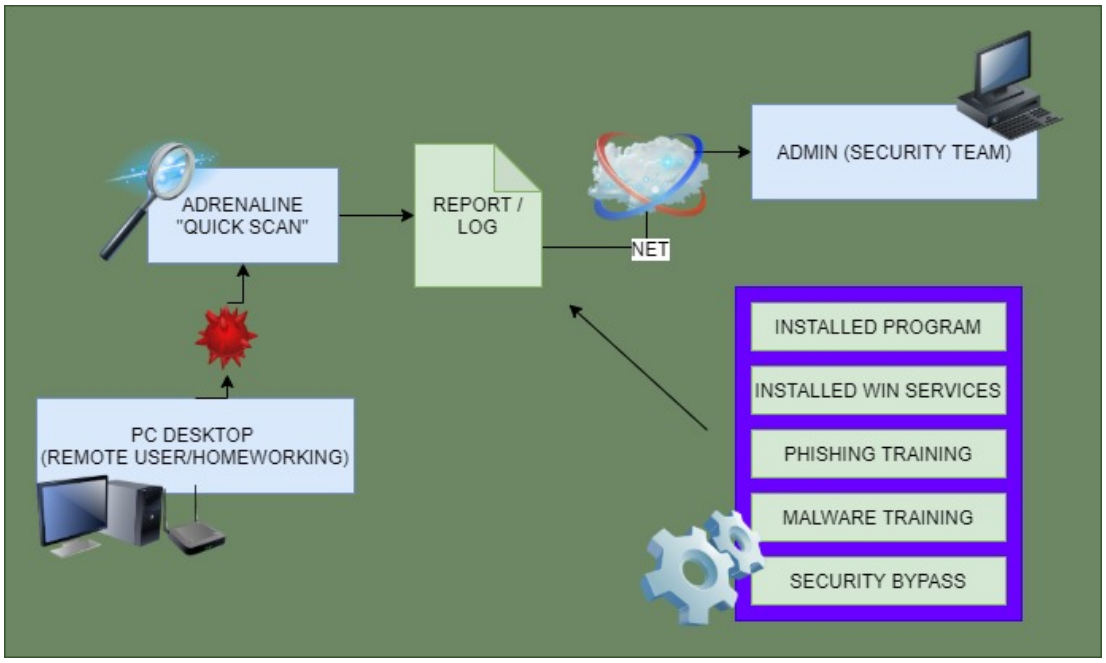
“Quick Test” Setup:

Useful for testing the operator and the machine in the SmartWorking environment:

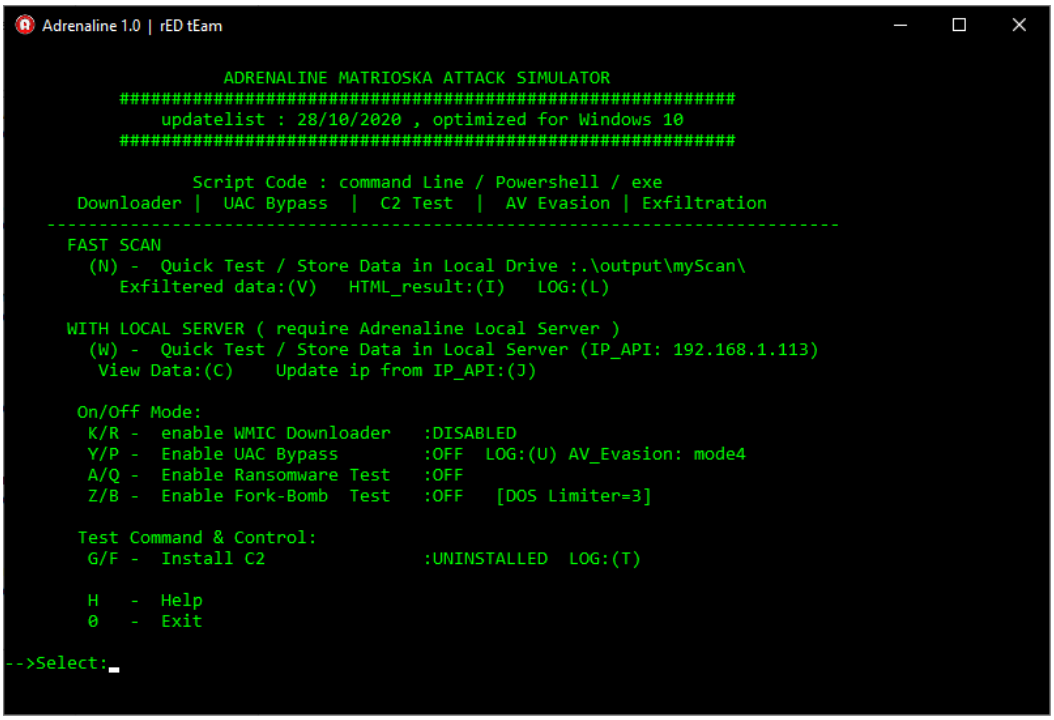
To generate the Test Payload to be inserted on remote machines use the command: 3

The payload will be created to be redistributed on Remote PCs equipped with Microsoft Windows 10

The administrator can view the log reports with the consent and sending of the operator



(operation in Smart Working).



The administrator can view the log reports directly from the "Adrenaline Local Server" or on the machine itself (operation in infrastructure or subnet)

Launch Quick Test (**N** key)

Launch Quick Test and store exfiltered data into “Adrenaline Local Server” (**W** key)

It is possible to view the exfiltrated data (key **V**).

It is possible to view the general report of the attack in HTML format

It is possible to view the log file that matryoshka payload leaves after its start (**L** key)

It is possible to perform a scan and send the data to the Local server (**W** key)

It is possible to install the C2 payload, which can be controlled from the local "Adrenaline Server" server

- Install : key **G**
- Uninstall : key **F**

It is possible to try the “Fork-Bomb” software payload test (**Z/B** key)

It is possible to try the payload test with Ransomware Shuffler (key **A/Q**)

It is possible to try the UAC bypass payload (**Y/P** key)

Reconn and Exfiltrate :

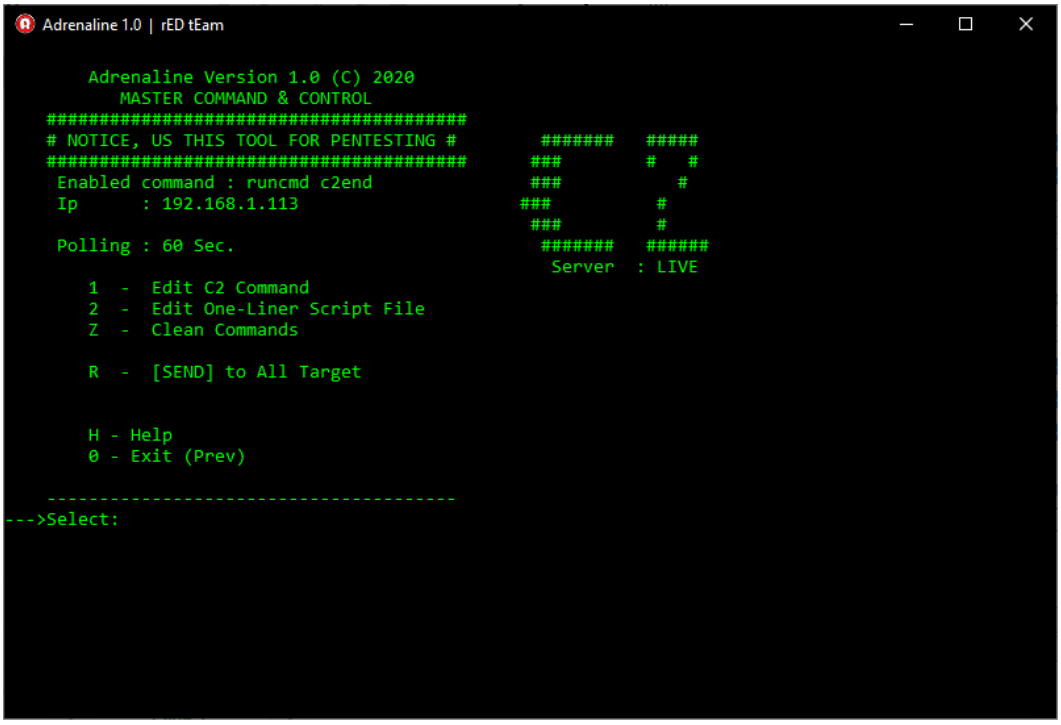
At the end of the operation, you can clean up the *%TMP%* temporary files folder. All Adrenaline log files and information are saved in this folder, so you can subsequently analyze the effectiveness of the attack.

In the “local test” (option N), information is shown in real time.

Quick Scan:

C2 Interface (Command & Control):

The C2 payload installed in the victim's target machine waits for the command from the “Adrenaline Local Server”.



Edit C2 Command (option 1):

Enter the command you want to execute in the Target machine (w10)

Edit the Batch Script in the File to be executed in the Target machine (w10)

Commands supported and executed on the Target machine:

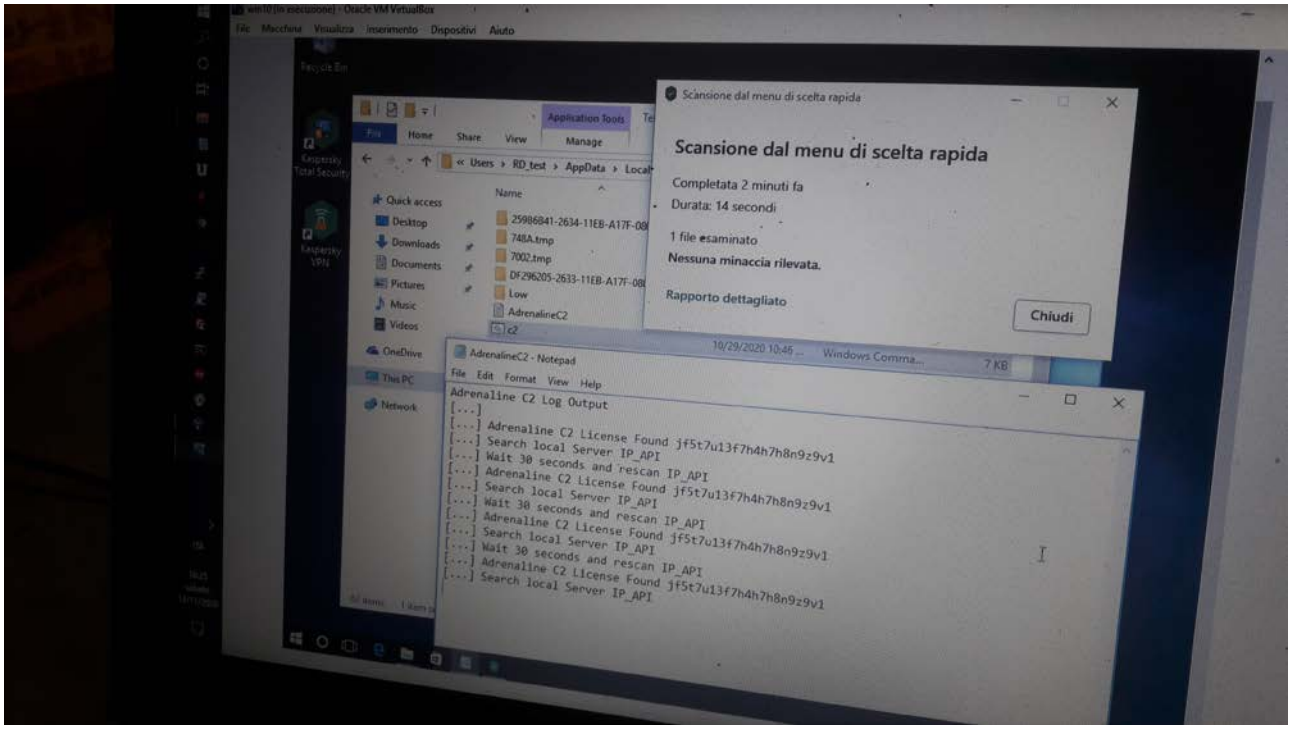
“runcmd”: run the Script Loaded from Adrenaline Local Server (2) in Target Machine

“Exit”: closes the C2.exe payload in the target machine

Edit C2 One-Liner (option 2)

Insert your one-liner script command in text file.

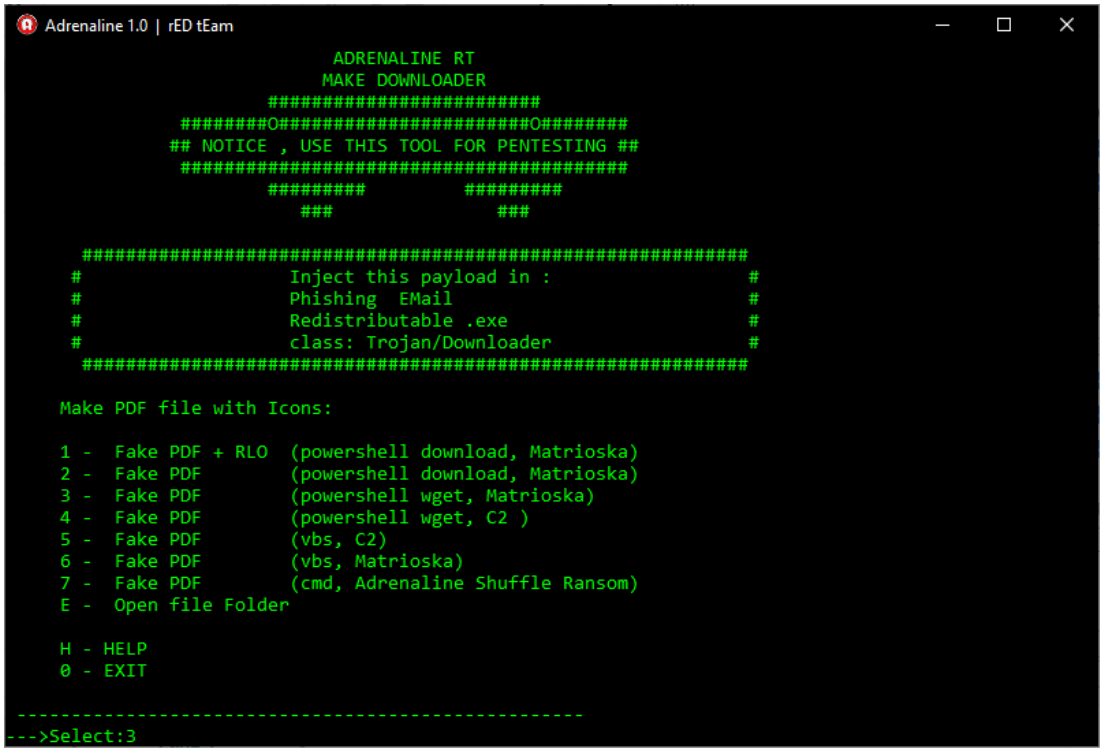
C2 Output: %tmp%\C2.log



Phishing Attack and Training the Human Factor

(1) Prepare phishing PDF file with Adrenaline RT
(2) Prepare new email with link or attach PDF file
(3) Start Phishing attack to the victim Mail address
(4) Check Log file in the Victim test (%TMP%), or connect to “Local Adrenaline Server

Press 1 to 7 and Open File Folder (E): FINISH!!, your PDF Payload file is Ready



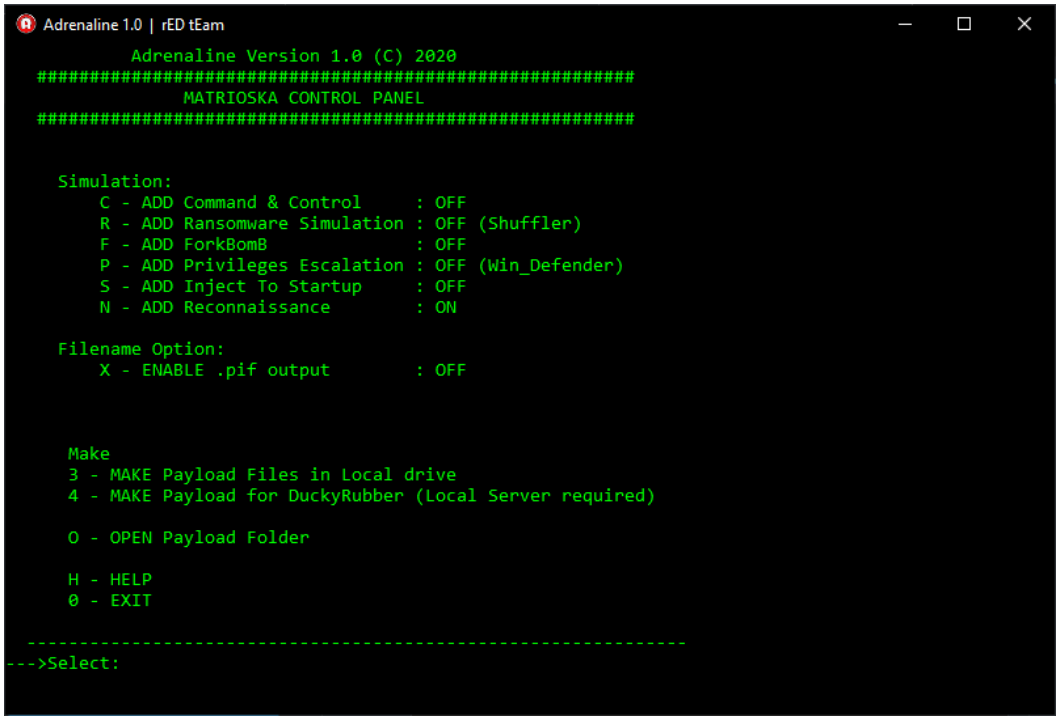
Here you can create the phishing test .EXE file.

The generated file contains the downloader which will download the payload to the victim's computer.

You can choose between a payload such as Matryoshka / C2 or Ransomware

Prepare a file with the Payload to redistribute.

It is used for training via memory key and to immediately test the protection of your AntiVirus / AntiMalware

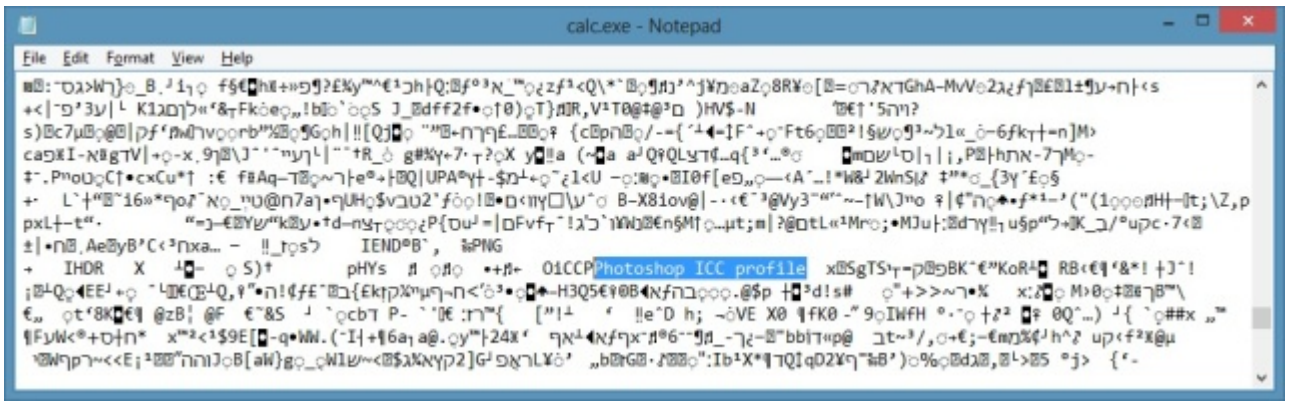


Enable .pif (option X): enabling this option a file with the appearance of a link is generated. Used to disguise the file extension, Microsoft Windows recognizes it as a normal link.

Payload generation (option 3):

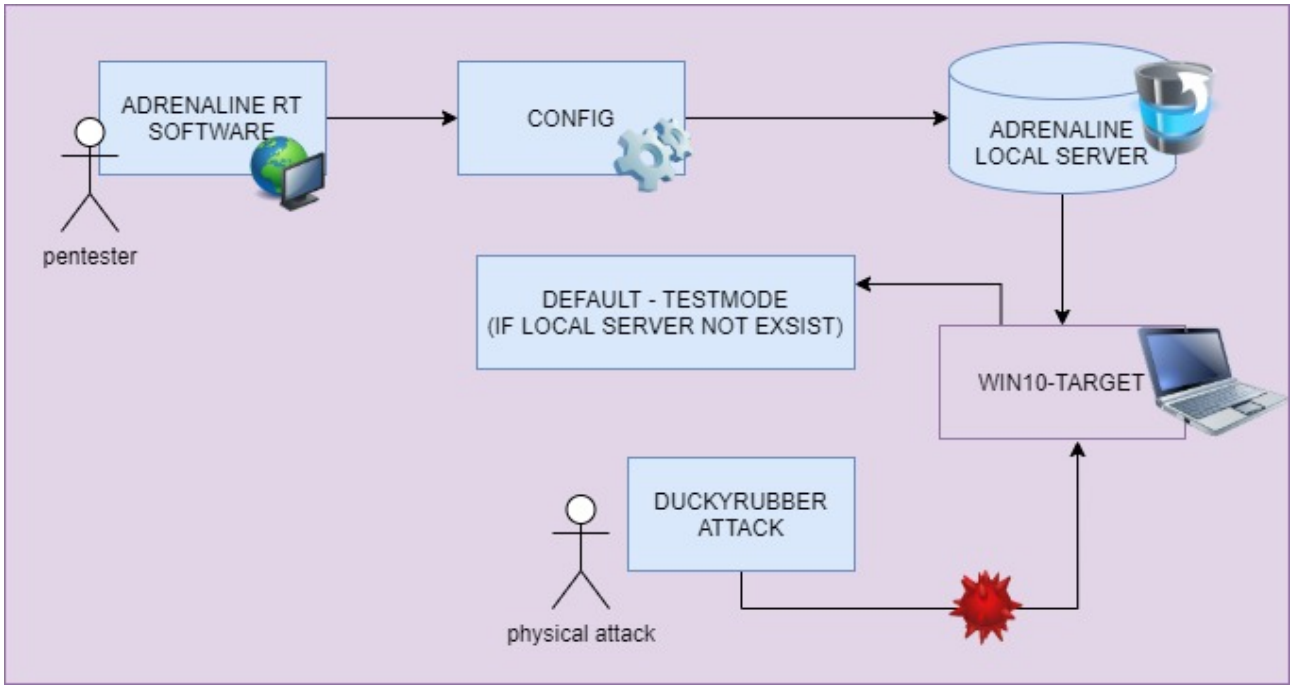
You can configure (C-N option) and generate the Payload. After creating it (option 3) we can reach the training “Malware” through (option O) of the menu.

!! ATTENTION !! The generated Payload is obfuscated.



DuckyRubber Payload configuration (option 4):

Configure the options for attacks based on RubberDucky USB (in RubberDucky mode the configuration file resides on the "Adrenaline Local Server". If the "Adrenaline Local Server" is not found, the Payload will automatically work in Default mode (Matrioska-Reconn)



Make your DuckyRubber and prepare the new pentest attack or training test:

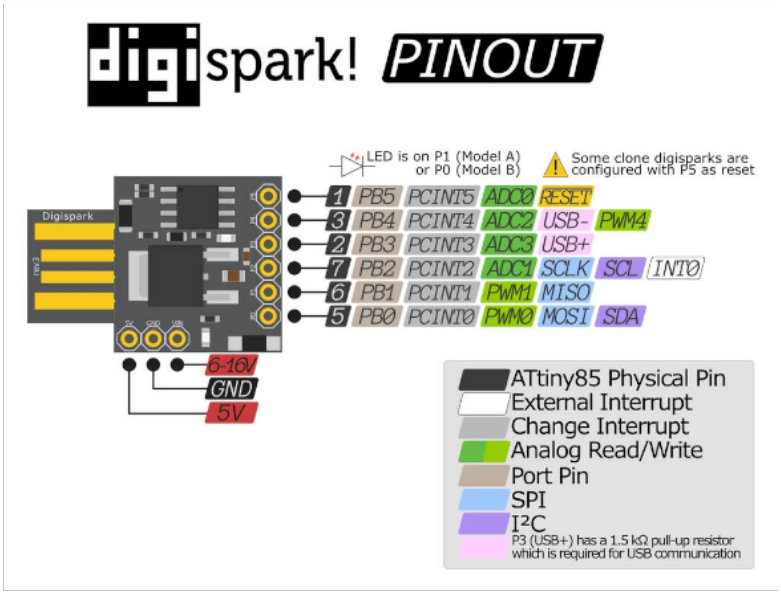
In this section we see how to prepare a Ducky-Rubber key

System requirements:

- Arduino version 1.5.8 (not another version)
- Digistump Driver
- DigiSpark Tiny85 Hardware (Amazon / Ebay)

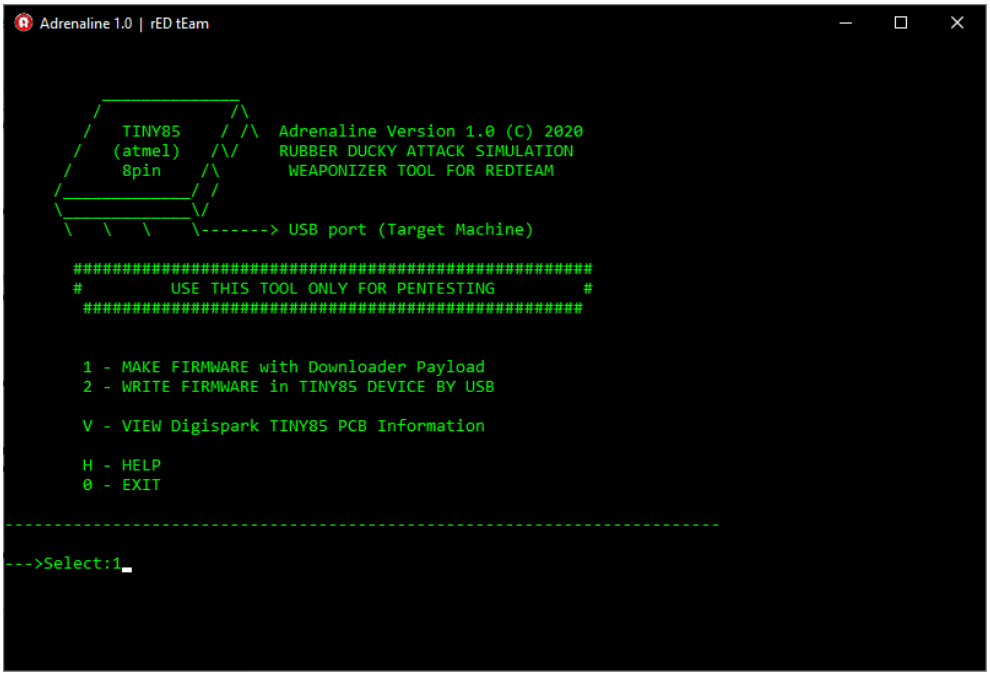
DigiSpark USB is sold by AliExpress, Ebay and Amazon for about 1/2 $.

!!NOTICE!! All 9 I/O pins are not required, use only USB port.



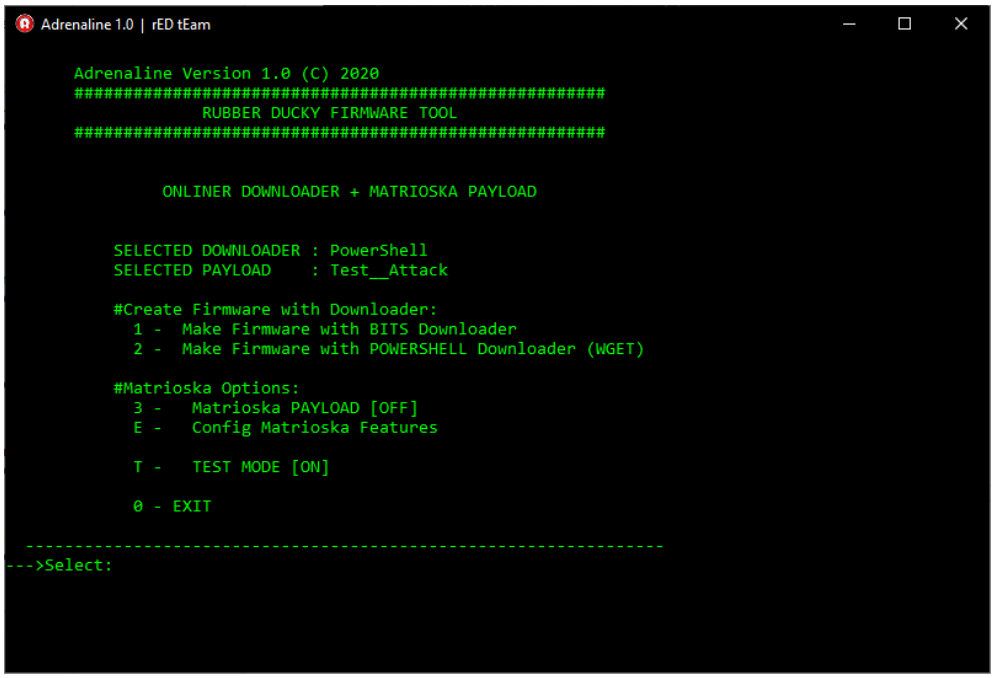
Configure and Program the Adrenaline Rubber-Ducky (Tiny85):

First we need to prepare the Firmware that calls the Matrioska or TestMode Payload. Then we **press option 1** (MAKE FIRMWARE)



STEP 1 - Make Firmware:

Select Powershell Script or BITS downloader, **option 1 or 2:**



If you want to proceed with a simple field test, make sure the "TEST MODE" (T) option is in the ON state. Basically it is a safe way to test the DuckyRubber device even on your Win10 PC. If the attack is successful, the log file is generated in the% TMP% folder of Windows 10.

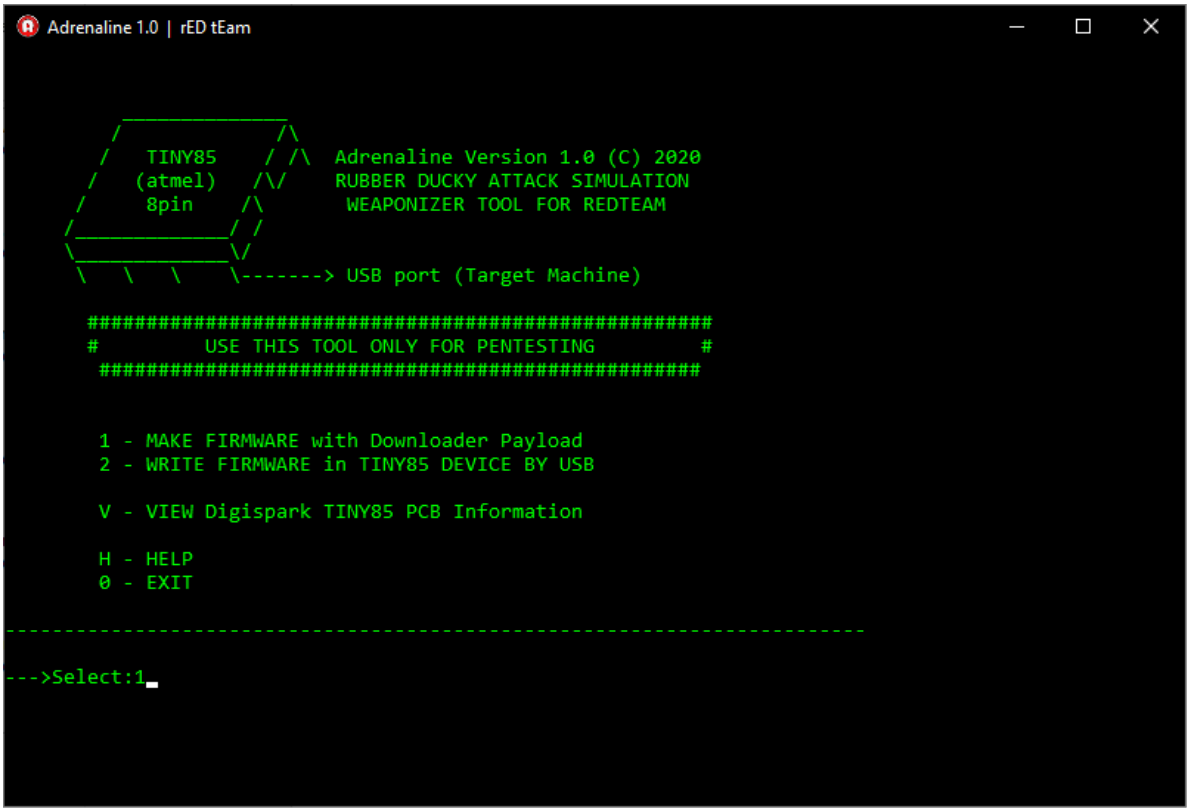
Warning! If "Test Mode" is enabled then "Matrioska Payload" always assumes the OFF status.

To generate the Firmware for Ducky-Rubber with the powershell downloader set, use (2)

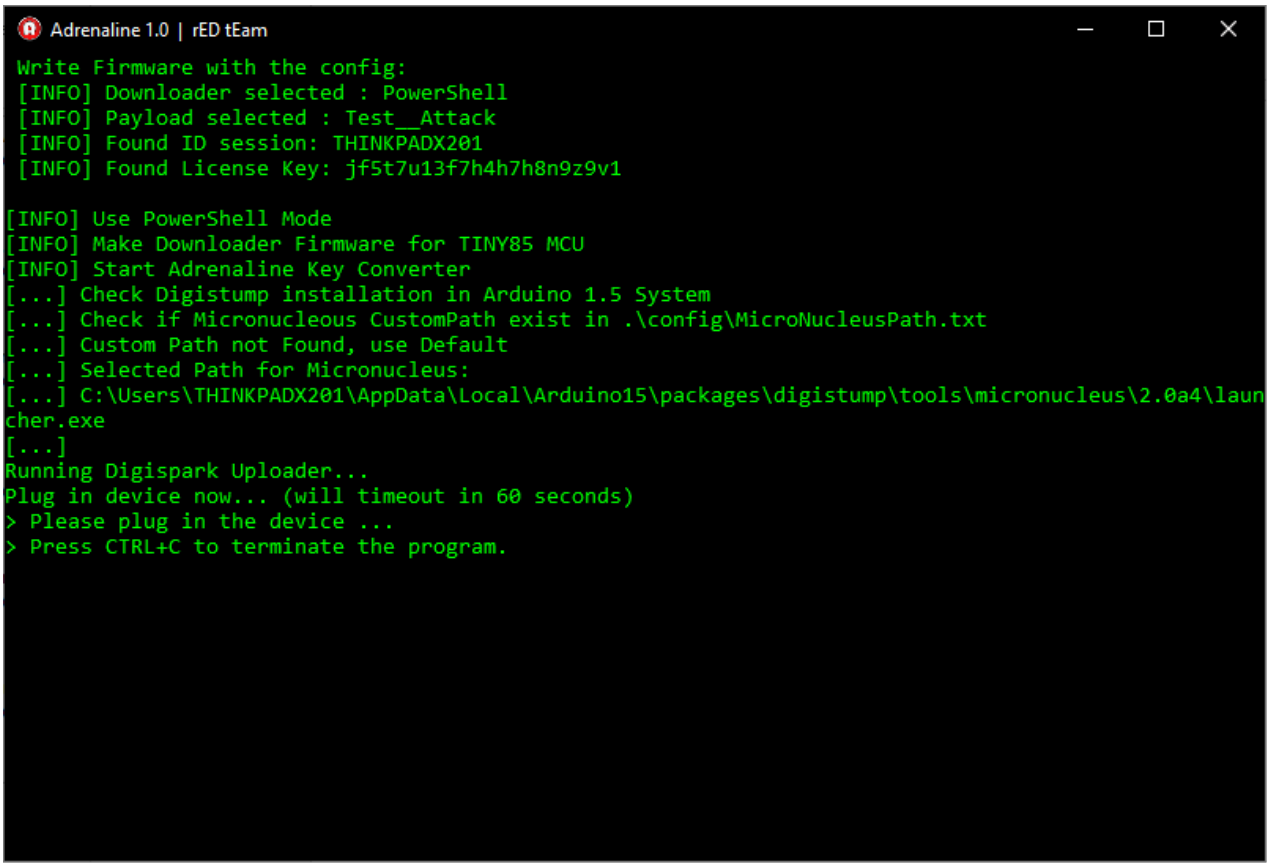
In addition, a proof of success is left in the% tmp% folder of win10, which can be recalled with the following command: notepad% tmp% / *. Log

STEP 2 - WRITE FIRMWARE IN TINY85MCU:

select option 2:



Programming a Ducky-Rubber device is very simple with Adrenaline. Within minutes you will be able to get the device programmed as a full Downloader.



Adrenaline is waiting for the device to be inserted into the USB port to be programmed.

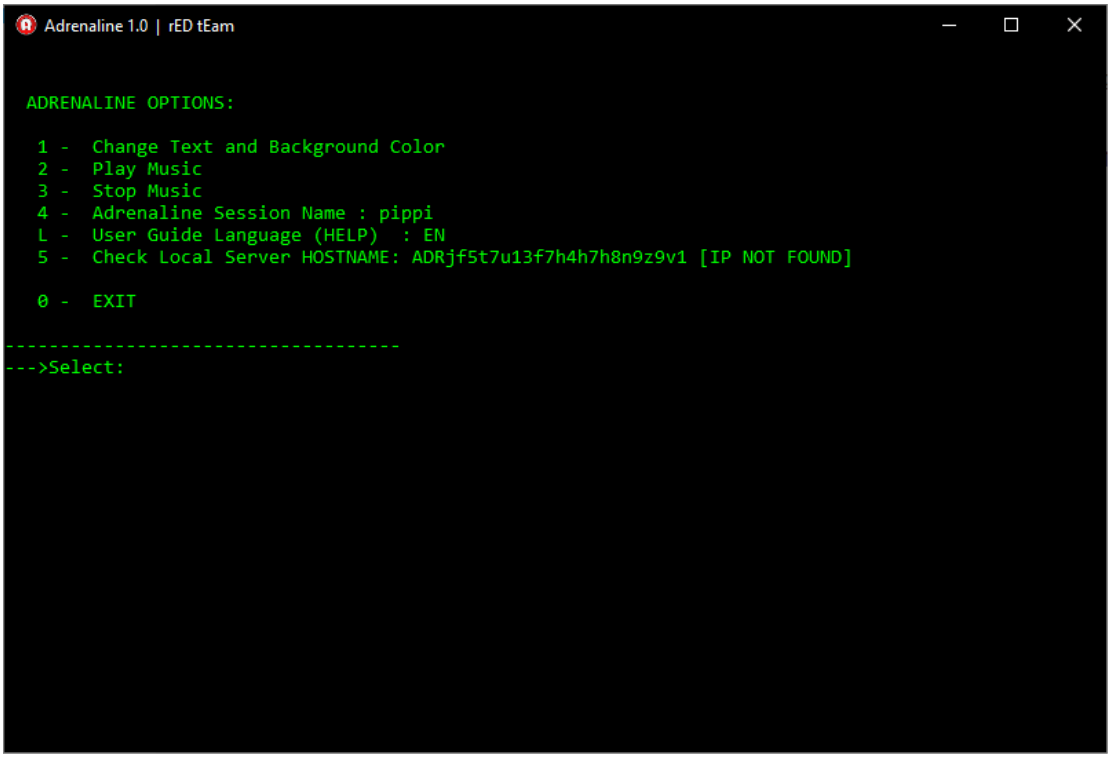
Insert the Tiny85 digispark and wait for it to finish.

!!YES, DUCKY RUBBER IS READY!!

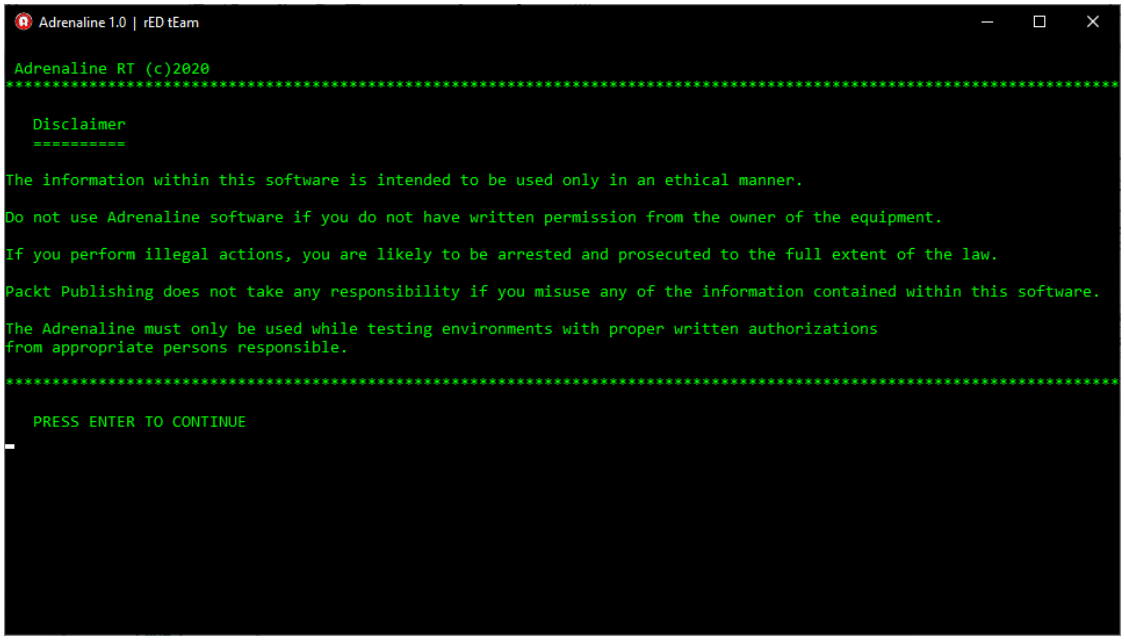
NOTICE!!: at the end of the operation, immediately remove the Ducky-Rubber key from the housing or USB cable

Or, to cancel the programming process: Press CTRL + C to terminate the program…

Config Adrenaline options:

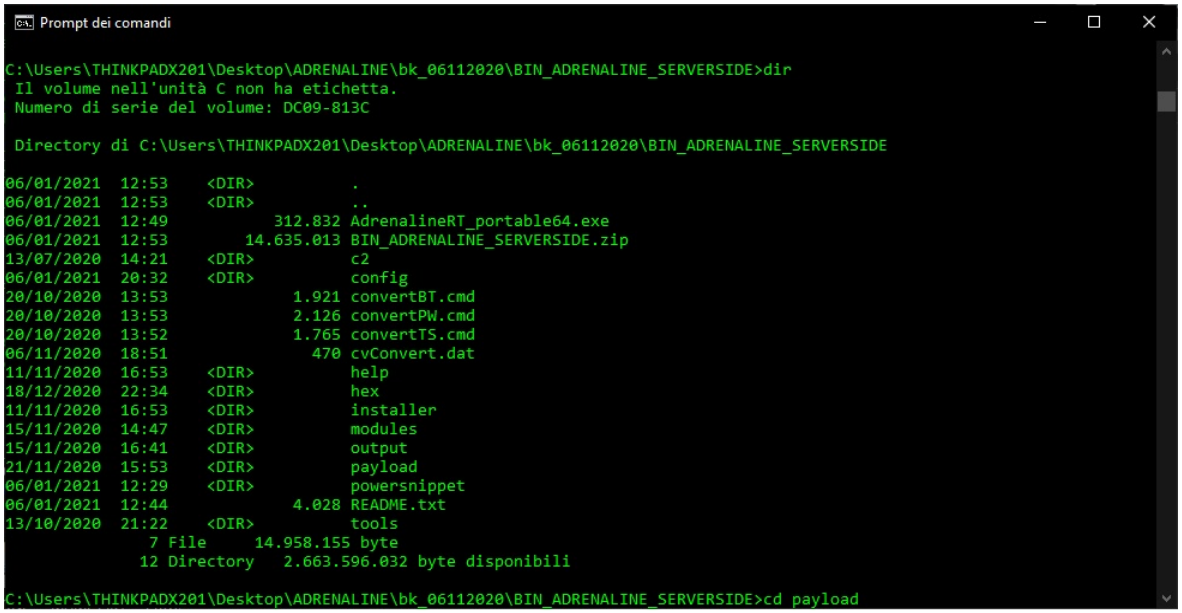


Disclaimer:

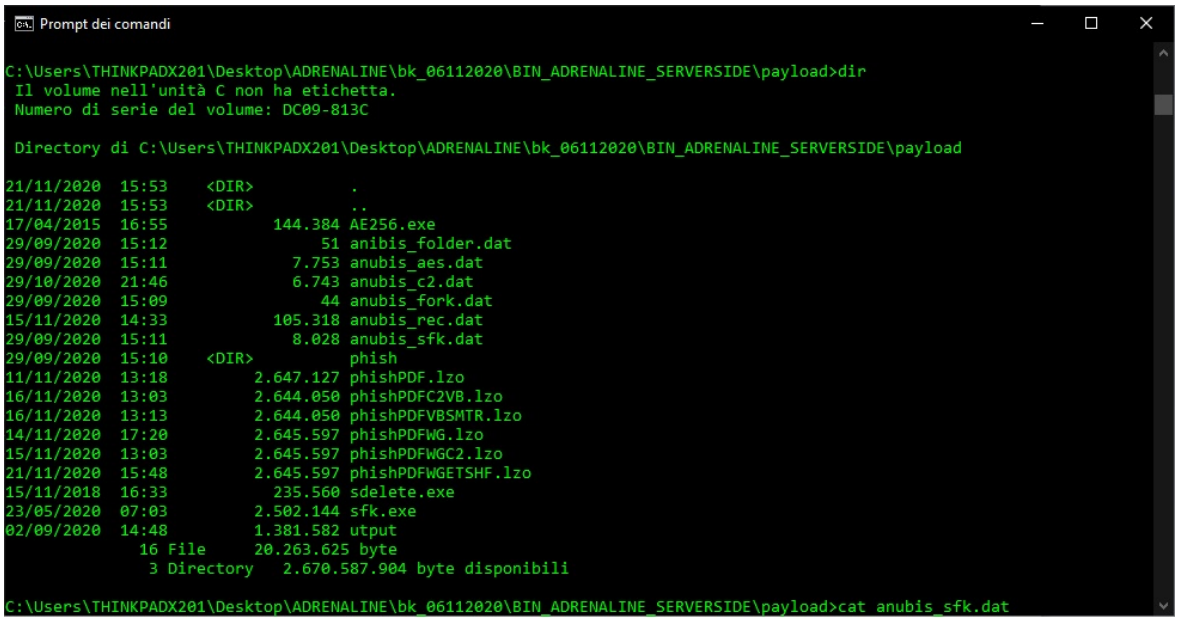


Read the source code of payload:

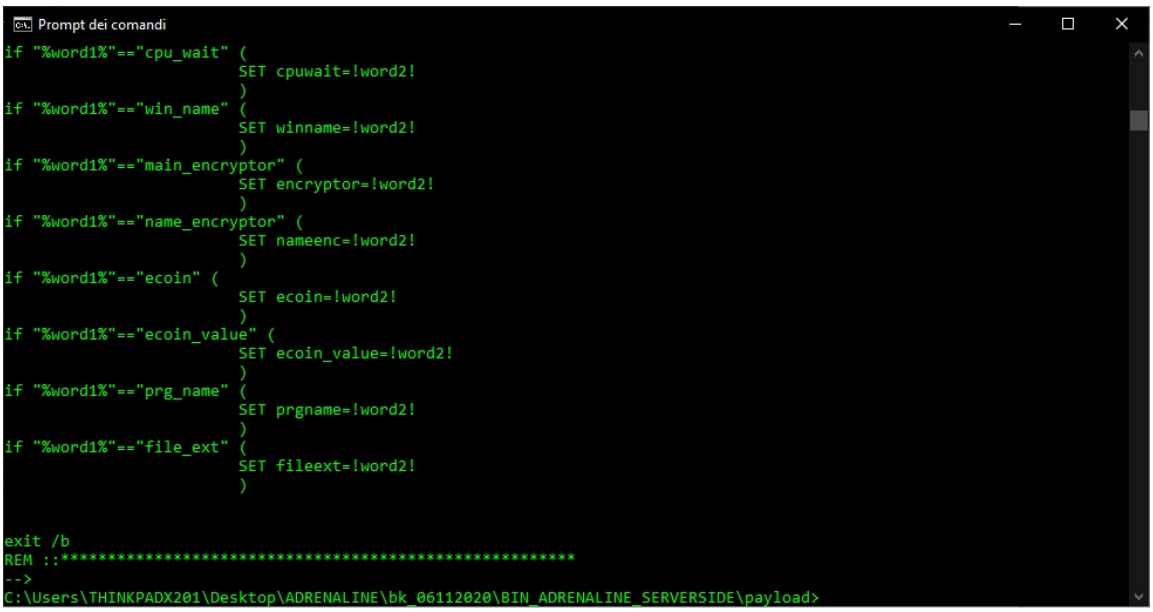
Open .dat file with cat



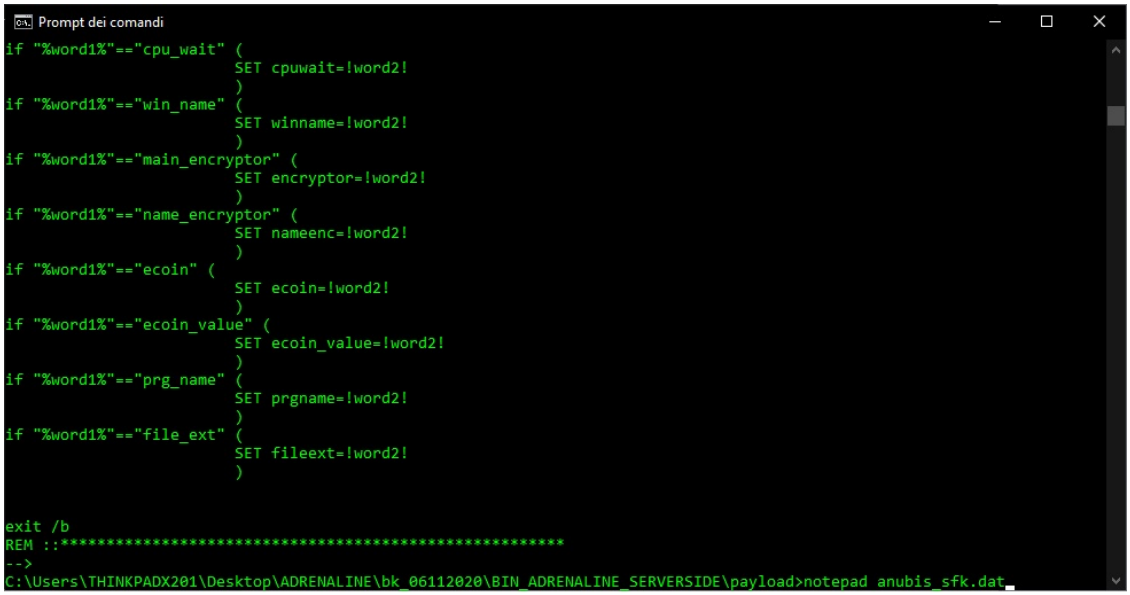
cat Anubis_sfk.dat



Output with cat:



Open .dat file with notepad.exe :



Notepad.exe results:

Glossary:

Cyber Awareness: Refers to how much end users know about the cybersecurity threats their networks face and the risks they introduce. End users are considered the weakest link and the main vulnerability within a network. Organizations allocate funding to protect their networks from external threats and reduce vulnerabilities. With end users as a major vulnerability, the technical means to improve security are not enough: organizations must also provide training for personal cybersecurity awareness. They should educate employees about current threats and how to avoid them.

Information security: is the set of means and technologies aimed at protecting information systems in terms of availability, confidentiality and integrity of IT assets or assets.

Penetration test: (or informally pen test) is the operational process of analyzing or evaluating the security of a computer system or network.

Phishing: is a type of scam carried out on the Internet through which an attacker tries to deceive the victim by convincing them to provide personal information, financial data or access codes, pretending to be a reliable entity in a digital communication.

Malware: in computer security, indicates any computer program used to disturb the operations performed by a user of a computer.

Exploit: is a term used in computer science to identify a type of script, virus, worm, piece of data or binary that exploits a bug or vulnerability to create unexpected behavior in software, hardware, or in electronic systems (usually computerized), eg. obtain access to computer systems, allow the acquisition of administrative privileges, or denial of service attacks (DoS or the related DDoS).

Trojan or trojan horse : in the context of computer security, indicates a type of malware. The trojan hides its functioning inside another apparently useful and harmless program: the user, by running or installing this latter program, in effect also activates the code of the hidden Trojan.

Ransomware: is a type of malware that restricts access to the device it infects, requiring a ransom (ransom in English) to be paid to remove the restriction. For example, some forms of ransomware lock the system and order the user to pay to unlock the system, while others encrypt the user's files by asking to pay to return the encrypted files in the clear.

Script: in computer science, designates a particular type of program, written in a particular class of programming languages, called scripting languages. A specific class of such programs are so-called shell scripts, that is, scripts designed to be executed within an operating system shell.

Social engineering: in the field of information security, is the study of the individual behavior of a person in order to steal useful information.

Command and Control, C & C: Once communication is established, the infected machine sends a signal to the attacker's server looking for the next instruction. The infected computer will execute commands from the attacker's C2 server and may install additional software. The attacker now has complete control of the victim's computer and can execute any code. Malicious code typically spreads to multiple computers, creating a botnet - a network of infected machines. In this way, an

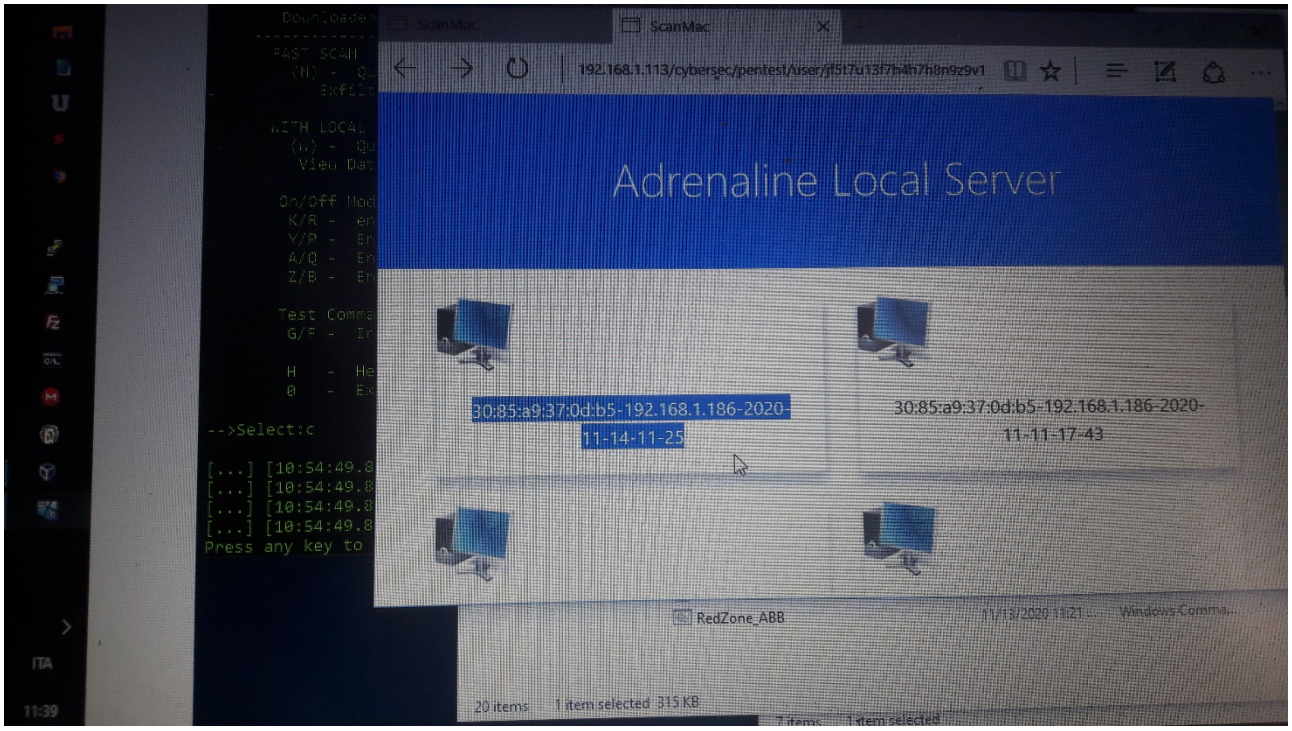
attacker who is not authorized to access a company's network can gain full control of that network.

Fork Bomb: (fork bomb) is a denial of service attack against a computer that uses the fork function. The action is based on the assumption that the number of programs and processes that can run concurrently on a computer has a limit.

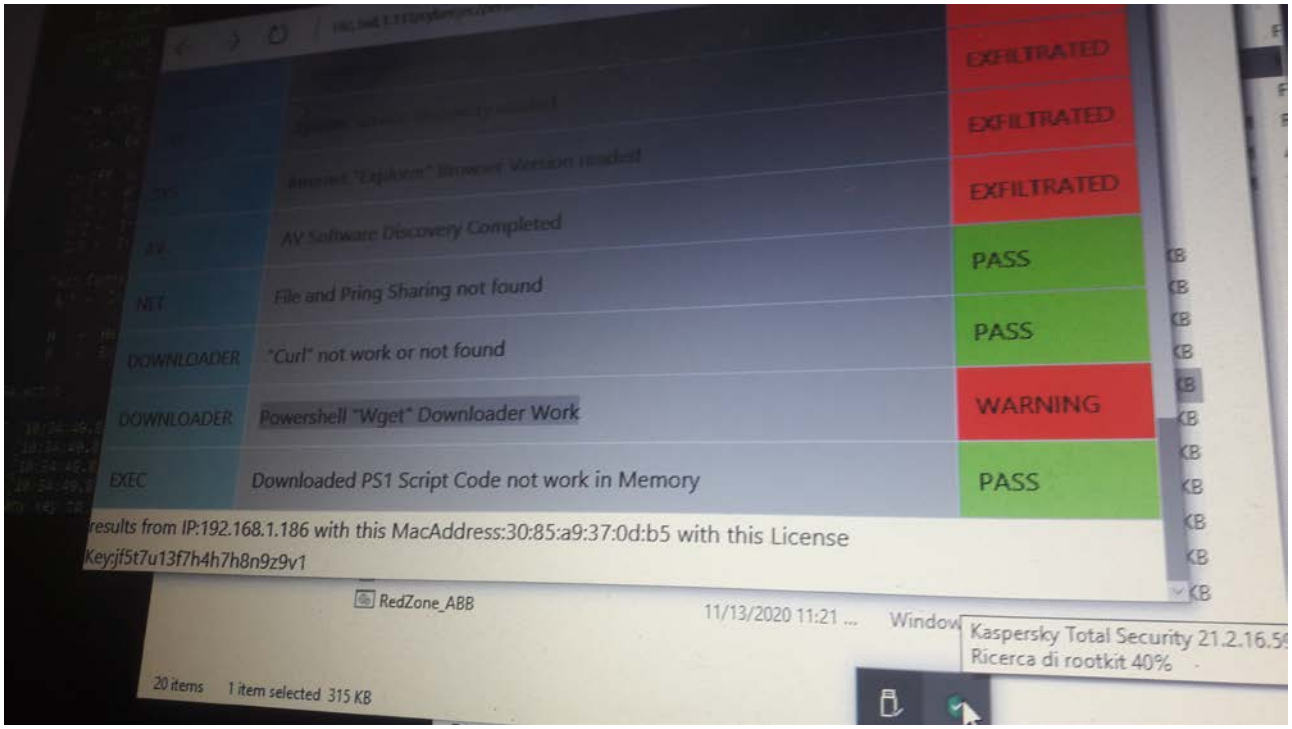
Privilege escalation: (intended as overrun of authorizations) the exploitation of a flaw, of a project or configuration error of an application software or of an operating system in order to acquire control of machine resources normally closed to a user or a 'application. An application with more permissions than those provided by the origin development

Read Local Server Log with the default Browser:

!! ATTENTION !!, you can read the log files only at the end of the Reconnaissance Payload operation launched by "QuickScan" or by the Adrenaline Matrioska payload.



[MAC ADDRESS][IP][DATE-TIME]:



View Data(C): for open Local Server Log

```
Adrenaline 1.0 | rED tEam

                ADRENALINE MATRIOSKA ATTACK SIMULATOR
        ############################################################
            updatelist : 28/10/2020 , optimized for Windows 10
        ############################################################

              Script Code : command Line / Powershell / exe
     Downloader |  UAC Bypass  |  C2 Test  |  AV Evasion | Exfiltration
   ------------------------------------------------------------------------------
     FAST SCAN
       (N) -  Quick Test / Store Data in Local Drive :.\output\myScan\
          Exfiltered data:(V)   HTML_result:(I)   LOG:(L)

     WITH LOCAL SERVER ( require Adrenaline Local Server )
       (W) -  Quick Test / Store Data in Local Server (IP_API: 192.168.1.113)
        View Data:(C)    Update ip from IP_API:(J)

      On/Off Mode:
       K/R -  enable WMIC Downloader   :DISABLED
       Y/P -  Enable UAC Bypass        :OFF  LOG:(U) AV_Evasion: mode4
       A/Q -  Enable Ransomware Test   :OFF
       Z/B -  Enable Fork-Bomb  Test   :OFF   [DOS Limiter=3]

      Test Command & Control:
       G/F -  Install C2               :UNINSTALLED  LOG:(T)

       H   -  Help
       0   -  Exit

-->Select:
```

Note:

This user manual is the property of Sgneep.com.

Disclosure without the prior consent of Sgneep.com and its respective owners is strictly prohibited.

Sgneep.com and its respective authors and owners have no responsibility for the improper use of the "Adrenaline-RT" and "Adrenaline-Server" software.

The modification of the code, license evasion, and the improper use of the Adrenaline RT software will be prosecuted by law.

All payloads used are for training and simulation purposes only.

Author: Mazzoni Roberto (CEO)

Federico Bombardi (CEO))


Windows 10
ARDUINO
MICROCHIP
APACHE
HTTP SERVER
ATMEL