Vryus works for Viss @Phobos

@vyrus001's Pages from a Sword-Maker's Notebook

<https://www.youtube.com/watch?time_continue=2395&v=2-zos1EAvNY>

<https://www.youtube.com/watch?v=mLg29dSOA0U&t=9s>

* Initial Access
  + Phishing
    - Loud and inelegant but it works
    - Microsoft Office
      * Macros
        + Laughting\_Mantis
      * DDEAuto
    - PDF?
  + Fake Update
    - BDF Proxy/Sig Thief
      * Code Caves, backdoors binaries and replaces with old sig
    - Evilgrade
      * Mitm backdoor update
      * BDF does this
    - BEEF
    - Manual Packet Spoof
      * Send packets pretending to be an update, when they get an update yours go first and get absorbed (INTERESTING)
  + Backdoor Warez
  + Backdoor Porn
  + 0 Day
  + Old Day
    - Gdlib popping profile pictures
    - Libpurple
    - Look Em Up
  + In Browser Malware
  + Beef Keylogger
* Persistence
  + Boot
    - MBR (512 byte malware) binary
    - UEFI
      * Doable
  + Daemonize
    - Sysv
    - Init.d
    - Rc.d
    - System.d service
    - Backdoor startup file
    - Cronjob
      * Dynamically pull down malware
  + Userspace
    - Windows
      * Startup registry keys
      * Bootexecute
      * Userinit, appinitdll
      * Services
      * Browser helper dlls
        + “Recall”
      * Appcert dllls
      * File associations (change .\_\_ to open with our program
      * Wmi persistence
        + Scheduled task
        + Run after reboot
        + Blackhat Graeber talk
      * Powershell
      * Shortcut hijack
      * Dll Hijacking
      * Pe Backdoor
        + Code caves
        + The backdoor factory
    - Linux
      * LD preload
        + Matt bostock go backdoor
      * Kernal module
        + Icco backdoor
      * Kernal modification
      * Syscall factory
      * PatchPam
        + beat\_gammit/simple pam
      * setuidRoot
        + Dergachew
      * Elf backdoor
  + Keylogging
    - Everyone does it the same way
    - Build your own baby
  + Screen capture
    - Create device context and store image bitmap in it
  + Webcam
    - Use OpenCv
  + Microphone
    - PortAudio
  + Browser Data
    - Pull all the data immediately
    - Nirsoft Utility
    - \
  + Steal Email
    - Proxy through their machine
    - Download everything through backup
    - Delete email
  + Steal Wifi Keys
  + Password managers
  + Geolocate
    - Pull all their wifi access points
    - Pull their IP
  + Compiling w/ different compilers ;)
  + Search
    - email/social media grab
    - Get all files on a computer, convert to text, index in Apache Nutch
    - Download all messages from fb
  + Background process -> libudev
  + Memdump + dfir
    - Chrome\_ragamuffin
    - Dumpit
    - Rekal
  + Whitelist Evasion
    - pcalua
  + Packing
    - Virus go mimikatz
      * Have your own mimikatz
      * Ebowla
  + Dynamic execution
    - Vmdetect
    - Opcode jumping
    - Domainsinkhole

How to Shot Web: PenTester Methodology

<https://www.youtube.com/watch?v=VPAz5heLcZY>

Vysec Tips

<https://github.com/vysec/RedTips>

What is autoruns?

**Intel Techniques**

https://twitter.com/CryptoCypher/status/973237866297004034

http://osintframework.com/

Mattifestation and all of Spectre Ops

Vysec https://github.com/vysec/Aggressor-VYSEC AngryPuppy

Sigint On a Budget

<https://www.youtube.com/watch?v=y4UJOdBRMa4>

<https://www.youtube.com/watch?v=7awwG9aaR4c>

Budget NSA

<https://www.youtube.com/watch?v=rDJ5I_Bh65Y>

Inveigh to steal hashes and creds by sniffing shares and other places

**Wireless** https://medium.com/@adam.toscher/top-5-ways-i-gained-access-to-your-corporate-wireless-network-lo0tbo0ty-karma-edition-f72e7995aef2

1. RADIUS Impersonation Vulnerabilities

Lo0tBo0ty KARMA

<https://github.com/sensepost/mana>

2. Open and Captive Network Evil Twin

4. WEP & WPA2-PSK Cracking

3. Guest Networks

5. Rogue Access Points

Why is no one using MANA and every example I come across is still KARMA?

Has anyone had success with the wifiphisher's "known beacon" attack -https://github.com/wifiphisher/wifiphisher

Local phone capture text intercept

**Hardware**

Chipwhisperer <https://twitter.com/colinoflynn/status/972443710972624896>

Professor Plum does hackacks