Mudge:

<https://blog.cobaltstrike.com/2016/10/03/cobalt-strike-3-5-1-important-security-update/>

<https://www.rapid7.com/db/modules/exploit/linux/http/empire_skywalker>

<http://www.harmj0y.net/blog/empire/empire-fails/>

<https://media.blackhat.com/bh-dc-11/Weeks/BlackHat_DC_2011_Weeks_Counterattack-Slides.pdf>

<https://media.blackhat.com/bh-dc-11/Weeks/BlackHat_DC_2011_Weeks_Counterattack-wp.pdf>

<https://github.com/justinsteven/advisories/blob/master/2017_metasploit_meterpreter_dir_traversal_bugs.md>

<https://github.com/justinsteven/advisories/blob/master/2017_metasploit_meterpreter_dir_traversal_bugs.md>

* Scene
  + <http://www.skidlist.com/>
  + <https://gist.github.com/Xyl2k>

“a botnet upon which the sun never sets”

**What if you man-in-the-middled malware command and control and were able to scan a C2 server for vulnerabilities or fuzz inputs using its internal, obfuscated mechanisms?**

**Omarax Implementation Steps**

[**Omarax Notes**](https://docs.google.com/document/d/19oYz82_7QDcaHh6WRTb-0f7ENXy9zynJQywoLOeRGVY/edit)

[**Function Hooking Notes**](https://docs.google.com/document/d/1Dorb6dUk0XKo15fs95wfRF92beJOU7w9m-HbCNiEqAE/edit?pli=1)

[**Function Hooking, Functionally**](https://docs.google.com/document/d/1y_45bWup_yREkcJIq62o2OEGCw6pnS9EbeQ8gAVMaSI/edit?pli=1)

[**Hacking Implementation Steps**](https://docs.google.com/document/d/1Pw0TlZ1bqpJluiv_aLa5nwZ7otkQVzrLyG_bgzoqNrQ/edit)

**Hacking Back Notes**

**Hacking Back Functionality**

<http://0x27.me/HackBack/0x00.txt>

<https://ghostbin.com/paste/6kho7>

* Uncategorized
  + <https://recon.cx/2016/training/trainingbotnet.html>
  + <https://samvartaka.github.io/exploitation/2016/06/03/dead-rats-exploiting-malware>
  + <https://www.blackhat.com/docs/us-14/materials/us-14-Sood-What-Goes-Around-Comes-Back-Around-Exploiting-Fundamental-Weaknesses-In-Botnet-C&C-Panels-WP.pdf>
* Automated Scanners
  + Priority
    - <https://github.com/zaproxy>
    - <https://github.com/andresriancho/w3af>
    - <http://wapiti.sourceforge.net/>
    - <http://rgaucher.info/beta/grabber/>
  + Other
    - <https://github.com/zigoo0/webpwn3r>
    - <https://github.com/faizann24/XssPy>
    - <https://www.nccgroup.trust/us/about-us/resources/wsbang/>
    - <https://ironwasp.org/>
  + sqlMap
* Fuzzing
  + <https://github.com/xmendez/wfuzz>
  + <http://www.powerfuzzer.com/>
  + <http://peachfuzz.sourceforge.net/>
* Vulnerabilities
  + Reversing Malware to Extract Cryptographic Keys and File Uploading
    - File Upload
      * How
      * Malware (bots) binaries are reversed to extract cryptographic keys used for authentication at the gates
      * Using the cryptographic keys, remote management shells (such as C-22,PHP-Spy, etc.) are uploaded on the compromised servers.
      * Paths to remote management shells and configurations files are traversed for executing commands and extracting configuration parameters
      * Database credentials are extracted from the configuration files for obtaining access to the backend databases (MySQL etc.) for additional information
      * MD5 hashes are obtained from tables present in the databases used for C&C operations. The hashes are transferred to the cracking engines to obtain passwords for the C&C panels.
    - Resources
      * <https://blogs.forcepoint.com/security-labs/putting-cyber-criminals-notice-watch-your-flank>
      * <https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/PEST-CONTROL.pdf>
      * <https://malware.lu/articles/2012/05/21/analysis-and-pownage-of-herpesnet-botnet.html>
      * <https://www.youtube.com/watch?v=KeGaXXfISY0>
  + Finding Design and Deployment Flaws including Vulnerabilities
    - <https://bitrot.sh/post/11-12-2017-hunting-thundershell/>
    - [https://gist.github.com/Xyl2k](https://gist.github.com/Xyl2k?page=2)
    - Buffer overflow
      * <https://www.rapid7.com/db/modules/exploit/windows/misc/poisonivy_bof>
      * <https://samvartaka.github.io/malware/2015/09/07/poison-ivy-reliable-exploitation>
    - serialization vulnerability
      * Metasploit
      * <https://github.com/justinsteven/advisories/blob/master/2016_metasploit_rce_static_key_deserialization.md>
    - Input Inject
      * + <https://malware.lu/articles/2012/05/21/analysis-and-pownage-of-herpesnet-botnet.html>
        + [SQL Injection in DarkComet](https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/PEST-CONTROL.pdf)
        + <https://secniche.blogspot.com/2011/08/blasting-spyeye-c-sql-injection-wins.html>
    - Panel Exploit
      * Blind Sql
        + <https://github.com/MalwareTech/PhaseHack/blob/master/hax.py>
        + <https://github.com/MalwareTech/NeutrinoBotHack/blob/master/neutrino.py>
    - File Download
      * [Arbitrary File Read from the Client’s File System in DarkComet](https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/PEST-CONTROL.pdf)
      * <https://github.com/samvartaka/exploits/blob/master/darkcomet_filedownloader.rb>
    - Brute Force Directories
    - Brute Force Logins
      * <https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf>
  + DNS Sinkhole
    - <https://pdfs.semanticscholar.org/5c0a/546093b332c5e011fa29f26c8bd467a52117.pdf>
    - <https://web.archive.org/web/20160304231035/http://dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration>
    - <https://web.archive.org/web/20160304030247/http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies>
    - <https://seclab.cs.ucsb.edu/media/uploads/papers/torpig.pdf>
    - <https://www.usenix.org/conference/leet12/workshop-program/presentation/dittrich>
  + Backdoor
  + Webshell
    - <http://community.websense.com/blogs/securitylabs/archive/2014/06/12/zeus-c-amp-c-vulnerability.aspx>
    - <https://www.owasp.org/index.php/Unrestricted_File_Upload>

HiddenSalamander

DefiantWarrior

Quantam Bot

* Enhanced Attribution Program
  + Technical POC: Dr. Angelos Keromytis, Program Manager, DARPA/I2O
  + BAA Email: enhanced-attribution@darpa.mil
  + **The goal of the Enhanced Attribution program is to develop technologies for generating operationally and tactically relevant information about multiple concurrent independent malicious cyber campaigns. The objective is to not only collect and validate this pertinent information, but to create the means to share such information with any of a number of interested parties without  
    putting at risk the sources and methods used for collection. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems.**
  + **technologies to extract behavioral and physical biometrics from a range of devices andvantage points to consistently identify virtual personas and individual malicious cyberoperators ovtwer time and across different endpoint devices and C2 infrastructures;**
  + **techniques to decompose the software tools and actions of malicious cyber operators into semantically rich and compressed knowledge representations;**
  + **scalable techniques to fuse, manage, and project such ground-truth information over time, toward developing a full historical and current picture of malicious activity;**
  + **algorithms for developing predictive behavioral profiles within the context of cyber Campaigns;**
  + **technologies for validating and perhaps enriching this knowledge base with other sources  
    of data, including public and commercial sources of information.**
  + [**https://www.fbo.gov/index?id=d3ff4bd4107aac47348776f0594595cc**](https://www.fbo.gov/index?id=d3ff4bd4107aac47348776f0594595cc)