

Vault 7: CIA Hacking Tools Revealed



Releases ▼ (../index.html) **Documents** ▼ (index.html)

Navigation: » [Directory \(index.html\)](#) » [AED Development Tradecraft \(space_3506177.html\)](#) » [AED Development Tradecraft Home \(page_3375113.html\)](#)

Owner: User #2064619 ([user_2064619.html](#))

Development Tradecraft DOs and DON'Ts

SECRET//NOFORN

(U) General (e.g. all PE/Mach-O/ELF or other binary files)

Directive

Rationale

(S//NF) DO obfuscate or encrypt all strings and configuration data that directly relate to tool functionality. Consideration should be made to also only de-obfuscating strings in-memory at the moment the data is needed. When a previously de-obfuscated value is no longer needed, it should be wiped from memory.

(S//NF) DO NOT decrypt or de-obfuscate all string data or configuration data immediately upon execution.

(S//NF) DO explicitly remove sensitive data (encryption keys, raw collection data, shellcode, uploaded modules, etc) from memory as soon as the data is no longer needed in plain-text form.

DO NOT RELY ON THE OPERATING SYSTEM TO DO THIS UPON TERMINATION OF EXECUTION.

(S//NF) DO utilize a deployment-time unique key for obfuscation/de-obfuscation of sensitive strings and configuration data.

(S//NF) DO strip all debug symbol information, manifests(MSVC artifact), build paths, developer usernames from the final build of a binary.

(U//FOUO) DO strip all debugging output (e.g. calls to printf(), OutputDebugString(), etc) from the final build of a tool.

(S//NF) String data and/or configuration data is very useful to analysts and reverse-engineers.

(S//NF) Raises the difficulty for automated dynamic analysis of the binary to find sensitive data.

(S//NF) Raises the difficulty for incident response and forensics review.

(S//NF) Raises the difficulty of analysis of multiple deployments of the same tool.

(S//NF) Raises the difficulty for analysis and reverse-engineering, and removes artifacts used for attribution/origination.

(S//NF) Raises the difficulty for analysis and reverse-engineering.

(S//NF) DO NOT explicitly import/call functions that is not consistent with a tool's overt functionality (i.e. WriteProcessMemory, VirtualAlloc, CreateRemoteThread, etc - for binary that is supposed to be a notepad replacement).

(S//NF) DO NOT export sensitive function names; if having exports are required for the binary, utilize an ordinal or a benign function name.

(S//NF) DO NOT generate crashdump files, coredump files, "Blue" screens, Dr Watson or other dialog pop-ups and/or other artifacts in the event of a program crash.

DO attempt to force a program crash during unit testing in order to properly verify this.

(S//NF) DO NOT perform operations that will cause the target computer to be unresponsive to the user (e.g. CPU spikes, screen flashes, screen "freezing", etc).

(S//NF) DO make all reasonable efforts to minimize binary file size for all binaries that will be uploaded to a remote target (without the use of packers or compression). Ideal binary file sizes should be under 150KB for a fully featured tool.

(S//NF) Lowers potential scrutiny of binary and slightly raises the difficulty for static analysis and reverse-engineering.

(S//NF) Raises the difficulty for analysis and reverse-engineering.

(S//NF) Avoids suspicion by the end user and system admins, and raises the difficulty for incident response and reverse-engineering.

(S//NF) Avoids unwanted attention from the user or system administrator to tool's existence and behavior.

(S//NF) Shortens overall "time on air" not only to get the tool on target, but to time to execute functionality and clean-up.

(S//NF) DO provide a means to completely "uninstall"/"remove" implants, function hooks, injected threads, dropped files, registry keys, services, forked processes, etc whenever possible. Explicitly document (even if the documentation is "There is no uninstall for this <feature>") the procedures, permissions required and side effects of removal.

(S//NF) DO NOT leave dates/times such as compile timestamps, linker timestamps, build times, access times, etc. that correlate to general US core working hours (i.e. 8am-6pm Eastern time)

(S//NF) DO NOT leave data in a binary file that demonstrates CIA, USG, or its witting partner companies involvement in the creation or use of the binary/tool.

(S//NF) DO NOT have data that contains CIA and USG cover terms, compartments, operation code names or other CIA and USG specific terminology in the binary.

(S//NF) DO NOT have "dirty words" (see dirty word list – TBD) in the binary.

(S//NF) Avoids unwanted data left on target. Also, proper documentation allows operators to make better operational risk assessment and fully understand the implications of using a tool or specific feature of a tool.

(S//NF) Avoids direct correlation to origination in the United States.

(S//NF) Attribution of binary/tool/etc by an adversary can cause irreversible impacts to past, present and future USG operations and equities.

(S//NF) Attribution of binary/tool/etc by an adversary can cause irreversible impacts to past, present and future USG operations and equities.

(S//NF) Dirty words, such as hacker terms, may cause unwarranted scrutiny of the binary file in question.

(U) Networking

Directive

Rationale

(U//FOUO) DO use end-to-end encryption for all network communications.

NEVER use networking protocols which break the end-to-end principle with respect to encryption of payloads.

(S//NF) DO NOT solely rely on SSL/TLS to secure data in transit.

(S//NF) DO NOT allow network traffic, such as C2 packets, to be re-playable.

(S//NF) DO use IETF RFC compliant network protocols as a blending layer. The actual data, which must be encrypted in transit across the network, should be tunneled through a well known and standardized protocol (e.g. HTTPS)

(S//NF) DO NOT break compliance of an RFC protocol that is being used as a blending layer.

(i.e. Wireshark should not flag the traffic as being broken or mangled)

(S//NF) DO use variable size and timing (aka jitter) of beacons/network communications. DO NOT predicatively send packets with a fixed size and timing.

(S//NF) Stifles network traffic analysis and avoids exposing operational/collection data.

(S//NF) Numerous man-in-middle attack vectors and publicly disclosed flaws in the protocol.

(S//NF) Protects the integrity of operational equities.

(S//NF) Custom protocols can stand-out to network analysts and IDS filters.

(S//NF) Broken network protocols can easily stand-out in IDS filters and network analysis.

(S//NF) Raises the difficulty of network analysis and correlation of network activity.

(S//NF) DO proper cleanup of network connections.
DO NOT leave around stale network connections.

(S//NF) Raises the difficulty of network analysis and incident response.

(U)Disk I/O

Directive

(S//NF) DO explicitly document the "disk forensic footprint" that could be potentially created by various features of a binary/tool on a remote target.

(S//NF) DO NOT read, write and/or cache data to disk unnecessarily. Be cognizant of 3rd party code that may implicitly write/cache data to disk.

(S//NF) DO NOT write plain-text collection data to disk.

(S//NF) DO encrypt all data written to disk.

Rationale

(S//NF) Enables better operational risk assessments with knowledge of potential file system forensic artifacts.

(S//NF) Lowers potential for forensic artifacts and potential signatures.

(S//NF) Raises difficulty of incident response and forensic analysis.

(S//NF) Disguises intent of file (collection, sensitive code, etc) and raises difficulty of forensic analysis and incident response.

(S//NF) DO utilize a secure erase when removing a file from disk that wipes at a minimum the file's filename, datetime stamps (create, modify and access) and its content.

(Note: The definition of "secure erase" varies from filesystem to filesystem, but at least a single pass of zeros of the data should be performed. The emphasis here is on removing all filesystem artifacts that could be useful during forensic analysis)

(S//NF) DO NOT perform Disk I/O operations that will cause the system to become unresponsive to the user or alerting to a System Administrator.

(S//NF) DO NOT use a "magic header/footer" for encrypted files written to disk. All encrypted files should be completely opaque data files.

(S//NF) DO NOT use hard-coded filenames or filepaths when writing files to disk. This must be configurable at deployment time by the operator.

(S//NF) DO have a configurable maximum size limit and/or output file count for writing encrypted output files.

(S//NF) Raises difficulty of incident response and forensic analysis.

(S//NF) Avoids unwanted attention from the user or system administrator to tool's existence and behavior.

(S//NF) Avoids signature of custom file format's magic values.

(S//NF) Allows operator to choose the proper filename that fits with in the operational target.

(S//NF) Avoids situations where a collection task can get out of control and fills the target's disk; which will draw unwanted attention to the tool and/or the operation.

(U) Dates/Time

Directive

Rationale

(U//FOUO) DO use GMT/UTC/Zulu as the time zone when comparing date/time.

(S//NF) Provides consistent behavior and helps ensure "triggers/beacons/etc" fire when expected.

(S//NF) DO NOT use US-centric timestamp formats such as MM-DD-YYYY. YYYYMMDD is generally preferred.

(S//NF) Maintains consistency across tools, and avoids associations with the United States.

(S//NF) PSP/AV

Directive

(S//NF) DO NOT assume a "free" PSP product is the same as a "retail" copy. Test on all SKUs where possible.

(S//NF) DO test PSPs with live (or recently live) internet connection where possible.

NOTE: This can be a risk vs gain balance that requires careful consideration and should not be haphazardly done with in-development software. It is well known that PSP/AV products with a live internet connection can and do upload samples software based varying criteria.

Rationale

(S//NF) While the PSP/AV product may come from the same vendor and appear to have the same features despite having different SKUs, they are not. Test on all SKUs where possible.

(S//NF) PSP/AV products exhibit significant differences in behavior and detection when connected to the internet vice not.

(S//NF) Encryption

(S//NF) NOD publishes a Cryptography standard: "NOD Cryptographic Requirements v1.1

TOP SECRET.pdf

(files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf)". Besides the guidance provided here, the requirements in that document should also be met.

Directive Rationale

SECRET//NOFORN

Comments:

2015-03-13 10:50 [User #2064619 (user_2064619.html)]:

I believe the spirit of what you're saying is covered in the NOD Cryptographic Requirements doc listed above (See section 2.4). TL;DR – You must use one the approved crypto suites or get an explicit wavier from NOD.

However, if you still feel strongly about having the guidance of "DO NOT write your own crypto, unless you must?" you are welcome to add it. However, I'd recommend against the "unless you must" part. *Do. Or Do Not. There is no try.*

2015-03-09 16:50 [User #3375388 (user_3375388.html)]:

How about: DO NOT write your own crypto, unless you must?

2014-11-21 12:22 [User #3375388 (user_524344.html)]:

May want to have a section to talk about how to check some of these things. While most of us know how to check for strings, debug info, and such new people may not know how to look for them.

May want to consider removing the Manifest data from your binary depending on what data gets put in their as it can sometimes contain revealing information.

Attachments:

NOD Cryptographic Requirements v1.1 TOP SECRET.pdf

(files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf)

Previous versions:

| 1 (page_14587111.html) *SECRET* | 2 (page_14587113.html) *SECRET* | 3 (page_14587121.html) *SECRET* | 4 (page_14587131.html) *SECRET* | 5 (page_14587133.html) *SECRET* | 6 (page_14587134.html) *SECRET* | 7 (page_14587135.html) *SECRET* | 8 (page_14587136.html) *SECRET* | 9 (page_14587141.html) *SECRET* | 10 (page_14587142.html) *SECRET* | 11 (page_14587144.html) *SECRET* | 12 (page_14587145.html) *SECRET* | 13 (page_14587146.html) *SECRET* | 14 (page_14587147.html) *SECRET* | 15 (page_14587148.html) *SECRET* | 16 (page_14587149.html) *SECRET* | 17 (page_14587151.html) *SECRET* | 18 (page_14587153.html) *SECRET* | 19 (page_14587155.html) *SECRET* | 20 (page_14587243.html) *SECRET* | 21 (page_14587247.html) *SECRET* | 22 (page_14587249.html) *SECRET* | 23 (page_14587251.html) *SECRET* | 24 (page_14587379.html) *SECRET* | 25 (page_14587381.html) *SECRET* | 26 (page_14587386.html) *SECRET* | 27 (page_14587387.html) *SECRET* | 28 (page_14587450.html) *SECRET* | 29 (page_14587452.html) *SECRET* | 30 (page_14587454.html) *SECRET* | 31 (page_14587461.html) *SECRET* | 32 (page_14587463.html) *SECRET* | 33 (page_14587467.html) *SECRET* | 34 (page_14587471.html) *SECRET* | 35 (page_14587476.html) *SECRET* | 36 (page_14587478.html) *SECRET* | 37 (page_14587480.html) *SECRET* | 38 (page_14587481.html) *SECRET* | 39 (page_14587482.html) *SECRET* | 40 (page_14587484.html) *SECRET* | 41 (page_14587628.html) *SECRET* | 42 (page_14587629.html) *SECRET* | 43 (page_14587630.html) *SECRET* | 44 (page_14587632.html) *SECRET* | 45 (page_14587865.html) *SECRET* | 46 (page_14587867.html)

SECRET | 47 (page_14588097.html) SECRET | 48 (page_23592994.html) TOP SECRET | 49
(page_23592996.html) TOP SECRET | 50 (page_23592998.html) TOP SECRET | 51
(page_23592999.html) TOP SECRET | 52 (page_23593000.html) TOP SECRET |



WL Research Community - user contributed research based on documents published by WikiLeaks.

(<https://our.wikileaks.org>)

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

(<https://www.torproject.org/>)

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity.


(<https://tails.boum.org/>)

The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record.

(<https://www.couragefound.org/>)

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.

(<https://www.bitcoin.org/>)

 (<https://www.facebook.com/wikileaks>)

 (<https://twitter.com/wikileaks>)