Πανόπτης 2019

Διαχείριση συμβάντων-συλλογή-ανάλυση πληροφοριών:
Προτεινόμενα εργαλεία

Πχος (Μ) Σ. Παπαγεωργίου ΠΝ
spapageorgiou@mil.gr

Περίγραμμα

- Γενικά
- Νόμος 4577/2018
- Ιστοσελίδα Εθνικής Αρχής & CSIRT, διαδικασία αναφοράς
- Επεισόδια “ΠΑΝΟΠΤΗ 2019”

ΠΑΝΟΠΤΗΣ 19

Ημερομηνία:**10 – 14 Ιουνίου 2019**
Προάσκηση: **10 Ιουνίου**
Άσκηση: 11 – 14 Ιουνίου
Απενημέρωση εσωτερική: **14 Ιουνίου 2019**

Συμμετοχή στα emails:
grammateia@cd.mil.gr
panoptis@cd.mil.gr

Επεισόδια ΠΑΝΟΠΤΗ 19

- Challenges (windows)
- Windows forensics (Browser, memory forensics, log file analysis)
- Linux forensics
- Network forensics
- Drone forensics
- IOT-Router forensics
- SCADA
- Network CTF
- Hunting the threat **-IOC's**
- Διαδικασίες αναφοράς (**Ιδιαίτερη έμφαση**)

Προτεινόμενα εργαλεία:

Διαχείριση συμβάντων-συλλογή πληροφοριών:

- https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape
  - KAPE is a multi-function program that primarily: 1) collects files and 2) processes collected files with one or more programs.
- https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip
  - Συλλέγει μνήμη, registry και λαμβάνει ακριβές αντίγραφο ενός σκληρού δίσκου σε windows λειτουργικά.
  - Συλλέγει αντίστοιχες πληροφορίες σε Linux and MacOs.
  - Αντικατάσταση του forecopy.
  - Σύνδεσμος για να δημιουργήσουμε το δικό μας module
    - http://www.brimorlabsblog.com/2015_09_01_archive.html
- https://github.com/proneer/Tools/tree/master/FPLive_win
- Για ανάπτυξη: https://pithos.okeanos.grnet.gr/public/EPF5AtuXfbZmgPlmyRQVE6

Συλλογή Πληροφοριών σε Linux

- https://github.com/SekoiaLab/Fastir_Collector_Linux/blob/master/fastIR_collector_linux.py
- https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip

Διαχείριση συμβάντων-εντοπισμός παραβίασης

- Εργαλείο ανεπτυγμένο από ΓΕΕΘΑ/Ε6, συνδυασμός information sharing (MISP) and incident response
  - **https://github.com/DimChris0/LoRa**
- Επόμενο βήμα, συνεργασία με
  - https://github.com/google/grr

LoRa
Collecting & Hunting for Indicators of Compromise (IOC) The two specialiced scanners LOKI and Rastrea2r have been merged into a new generic IOC scanner called LoRa. By using a client/server RESTful API, it can also hunt for IOCs on disk and memory across multiple systems using YARA rules. The server is the one responsible for finding, downloading the IOCs and then serving them as yara rules to the clients. The clients recieve the data and proceeds to scan its system and produce the reports of the result. The server side is inside the server folder(lora_server.py) and the client side inside win32 folder(lora_win32.py).

Διαχείριση συμβάντων-εντοπισμός παραβίασης rastrea2r

https://github.com/rastrea2r/rastrea2r

- Fast Triaging: Execute Sysinternals tools, or any other 3rd party batch scripts (including custom scripts) to perform basic triaging ** Windows Only
- Forensic Artifact Collection: Capabilities to Create snapshots quickly (Implements a wrapper for CyLR tool, which collects forensic artifacts from hosts with NTFS file systems quickly, securely and minimizes impact to the host.) **Windows Only
- Web History: Collect the Browser History (Currently supports IE, Chrome, Firefox only) **
- Prefetch Tool: Collect the prefetch data in Windows as they are great artifacts for forensic investigations to analyze applications that have been run on a system. ** Windows only
- Memory Dump: Acquires a memory dump from the endpoint ** Windows only
- Yara Disk: Yara scan for file/directory objects on disk
- Yara Mem: Yara scan for running processes in memory

Διαχείριση συμβάντων-εντοπισμός παραβίασης Loki

https://github.com/Neo23x0/Loki

Scanner for Simple Indicators of Compromise

Detection is based on four detection methods:

- File Name IOC
- Regex match on full file path/name
- Yara Rule Check
- Yara signature match on file data and process memory
- Hash check
- Compares known malicious hashes (MD5, SHA1, SHA256) with scanned files
- C2 Back Connect Check
- Compares process connection endpoints with C2 IOCs (new since version v.10)

Additional Checks:

- Regin filesystem check (via --reginfs)
- Process anomaly check (based on Sysforensics)
- SWF decompressed scan (new since version v0.8)
- SAM dump check
- DoublePulsar check - tries to detect DoublePulsar backdoor on port 445/tcp and 3389/tcp
- PE-Sieve process check

Συλλογή μνήμης (windows)

Winpmem

- https://github.com/google/rekall/releases/download/v1.5.1/winpmem-2.1.post4.exe

Dumpit

- http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

Fireeye Memoryze

- https://www.fireeye.com/services/freeware/memoryze.html

Fireeye Redline

https://www.fireeye.com/services/freeware/redline.html

Συλλογή μνήμης (Linux)

Lime

- https://github.com/504ensicslabs/lime

Ανάλυση μνήμης

Volatility (windows+linux)

- http://www.volatilityfoundation.org/#!25/c1f29

Fireeye redline (windows)

- https://www.fireeye.com/services/freeware/redline.html

Rekall (windows+linux)

- https://github.com/google/rekall/releases/tag/v1.5.0

Συλλογή της Registry

FTK Imager

- http://www.accessdata.com/support/product-downloads#

Windows_Live_Response

- https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip

Forecopy

- https://github.com/proneer/Tools/tree/master/forecopy

Rawcopy

- https://github.com/jschicht/RawCopy

Ανάλυση της Registry

Regripper

- https://code.google.com/p/regripper/

Registry Explorer

- https://github.com/EricZimmerman/RECmd/releases/download/0.7.0.0/RegistryExplorer_RECmd.zip

Registryviewer

- http://www.accessdata.com/support/product-downloads#

Regviewer

- http://sourceforge.net/projects/regviewer/

Registry Browser

- https://lockandcode.com/software/registry_browser

Disk Forensics

Sleuthkit autopsy (windows version)

- http://www.sleuthkit.org/autopsy/download.php

FTK Imager

- http://www.accessdata.com/support/product-downloads#

Sleuthkit

- http://www.sleuthkit.org/sleuthkit/download.php

bulk_extractor

- https://github.com/simsong/bulk_extractor

Last activity view

- http://www.nirsoft.net/utils/computer_activity_view.html

χρονική ανάλυση

- https://github.com/log2timeline/plaso

Raw Disk Image to Virtual Machine

- VBoxManage convertfromraw <filename> <outputfile> [--format VDI|VMDK|VHD]

File system recovery forensics

Scalpel

- https://github.com/sleuthkit/scalpel

Foremost

- http://foremost.sourceforge.net/

Web Browser Forensics

Nirsoft forensics tools

- http://www.nirsoft.net/utils/#browser_tools

Browser History Viewer

- https://www.foxtonforensics.com/browser-history-viewer/download

Email headers
ανάλυση

- https://toolbox.googleapps.com/apps/messageheader/analyzeheader

Malware forensics

remnux

- https://remnux.org/#distro

Ida pro

- https://www.hex-rays.com/products/ida/support/download_freeware.shtml

Immunity debugger

- https://www.immunityinc.com/products/debugger/

Olly debugger

- http://www.ollydbg.de/version2.html

Malware forensics

sysinternals tools

- https://live.sysinternals.com/

buatapa

- http://www.brimorlabsblog.com/2015/08/publicly-announcing-buatapa.html

Didier Stevens virus total tools

- https://blog.didierstevens.com/programs/virustotal-tools/

Didier Stevens Authenticode tools

- https://blog.didierstevens.com/programs/authenticode-tools/

National Software Reference Library

- http://www.nsrl.nist.gov/Downloads.htm#isos
- http://rjhansen.github.io/nsrllookup/

Malware forensics

Cuckoo

- **http://www.cuckoosandbox.org/**

Pyew

- https://github.com/joxeankoret/pyew

Online tools

- https://malwr.com/submission/

Network forensics

Tcpdump

- http://www.tcpdump.org/#latest-release

Wireshark

- http://www.wireshark.org/download.html

Xplico

- http://www.xplico.org/download
- http://www.forensicswiki.org/wiki/Network_forensics

Command-Line Log Analysis

- https://pastebin.com/WEDwpcz9
- https://www.youtube.com/watch?v=Sb747MCVYB8

Mobile forensics

mobile analysis framework - live cd

- Androl4b (https://github.com/sh4hin/Androl4b)
  - https://github.com/sh4hin/MobileApp-Pentest-Cheatsheet
- Santoku (https://santoku-linux.com/)
- MobSF (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF)

Live forensics CD’s

SIFT

- http://digital-forensics.sans.org/community/downloads

Kali

- http://www.kali.org/downloads/

Santoku

- https://viaforensics.com/resources/tools/santoku/

CAINE

- http://www.caine-live.net/page5/page5.html

Τεχνικά εγχειρίδια

- http://certcoop.eu/index.php/tutorials/

Τεχνικά Εγχειρίδια

- Συλλογή Αποδεικτικών Στοιχείων σε Linux Λειτουργικά Συστήματα
- Συλλογή Αποδεικτικών Στοιχείων σε Windows Λειτουργικά Συστήματα
- Εγχειρίδιο ασφαλούς ρύθμισης και χρήσης για το λειτουργικό σύστημα Windows 10

links

- http://en.wikipedia.org/wiki/List_of_digital_forensics_tools
- https://uk.sans.org/posters/windows_artifact_analysis.pdf
- https://digital-forensics.sans.org/media/Poster_SIFT_REMnux_2016_FINAL.pdf
- https://digital-forensics.sans.org/media/rekall-memory-forensics-cheatsheet.pdf
- https://digital-forensics.sans.org/media/Poster-2015-Memory-Forensics2.pdf
- https://digital-forensics.sans.org/media/DFIR-Smartphone-Forensics-Poster.pdf
- https://digital-forensics.sans.org/media/Poster_2016_Find_Evil.pdf
- https://digital-forensics.sans.org/media/evidence_collection_cheat_sheet.pdf
- https://digital-forensics.sans.org/media/linux-shell-survival-guide.pdf
- https://digital-forensics.sans.org/media/windows_to_unix_cheatsheet.pdf
- https://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdf
- https://digital-forensics.sans.org/media/hex_file_and_regex_cheat_sheet.pdf
- https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf
- https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf
- http://dfir.to/Find-Evil-Poster
- https://pen-testing.sans.org/retrieve/windows-cheat-sheet.pdf
- https://pen-testing.sans.org/retrieve/linux-cheat-sheet.pdf
- https://digital-forensics.sans.org/media/memory-forensics-cheat-sheet.pdf
- http://cryptome.org/isp-spy/access-data-spy1.pdf
- http://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/
- http://www.sleuthkit.org/autopsy/docs/quic
- http://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdfk/index.html
- http://digital-forensics.sans.org/media/sift_cheat_sheet.pdf
- http://www.nirsoft.net/utils/

links

- https://ericzimmerman.github.io/