The Armadito antivirus project

RMLL 2017

François Déchelle (fdechelle@teclib.com)

Proprietary antivirus: privacy

- most antivirus rely on a cloud infrastructure:
  - for advanced file scans
  - to improve detection
- every instance of the antivirus contribute to the global knowledge base
- but…
  - what files are uploaded to *.com?
  - what guarantee of privacy do you have?
  - what control do you have on this process?

Proprietary antivirus: privacy (2)

- may be you would like to run the cloud on **your** own infrastructure:
  - you are very concerned about privacy (private data, industrial secret...)
  - you may be the target of dedicated attacks and want to have your own knowledge base
  - you want to control the antivirus updates from A to Z
- the answer is (very likely): you can’t

Proprietary antivirus: confidence

- no third-party code audit
- to be discovered, nice vulnerabilities need Tavis Ormandy
- an example: CVE-2016-2208 (“Unpackers in the Kernel: Maybe not the best idea?”)
- free software is not a 100% guarantee
- but it helps a lot
- for instance http://seclists.org/fulldisclosure/2016/Jun/69

  :/

Armadito antivirus project

- a free software antivirus
  - mix of GPL v3, LGPL v3 and MS-PL
- modular...
- multi-platforms
  - GNU/Linux
  - MS-Windows
- supported by Teclib’ (GLPI)
- started mid 2015
- sources on github since May 2016

Functionalities

- classical:
  - on-demand scan
  - quarantine
  - alerts
  - journal
- real-time protection
  - GNU/Linux: with fanotify
  - MS-Windows: with its own driver (file system filter)

Modular

- scanning a file descriptor is done by **modules**:
  - plugins
  - simple API (load, configure, scan, unload)
- current modules:
  - ClamAV
  - YARA
  - heuristic for PE/ELF (deprecated, false positives)
  - heuristic for PDF
- modules written in C and … Python!

User interface

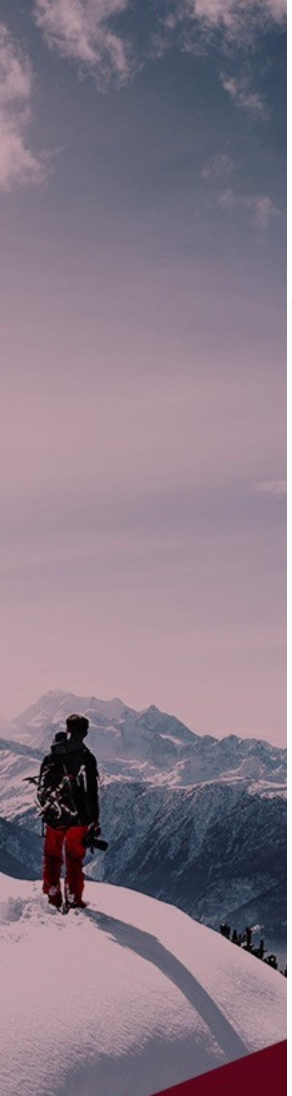
- an antivirus needs a user interface???
  - apparently yes
  - as lightweight as possible
- systray
  - only notifications
  - developed with native toolkit
- web interface… angular, http server… deprecated!

Antivirus administration

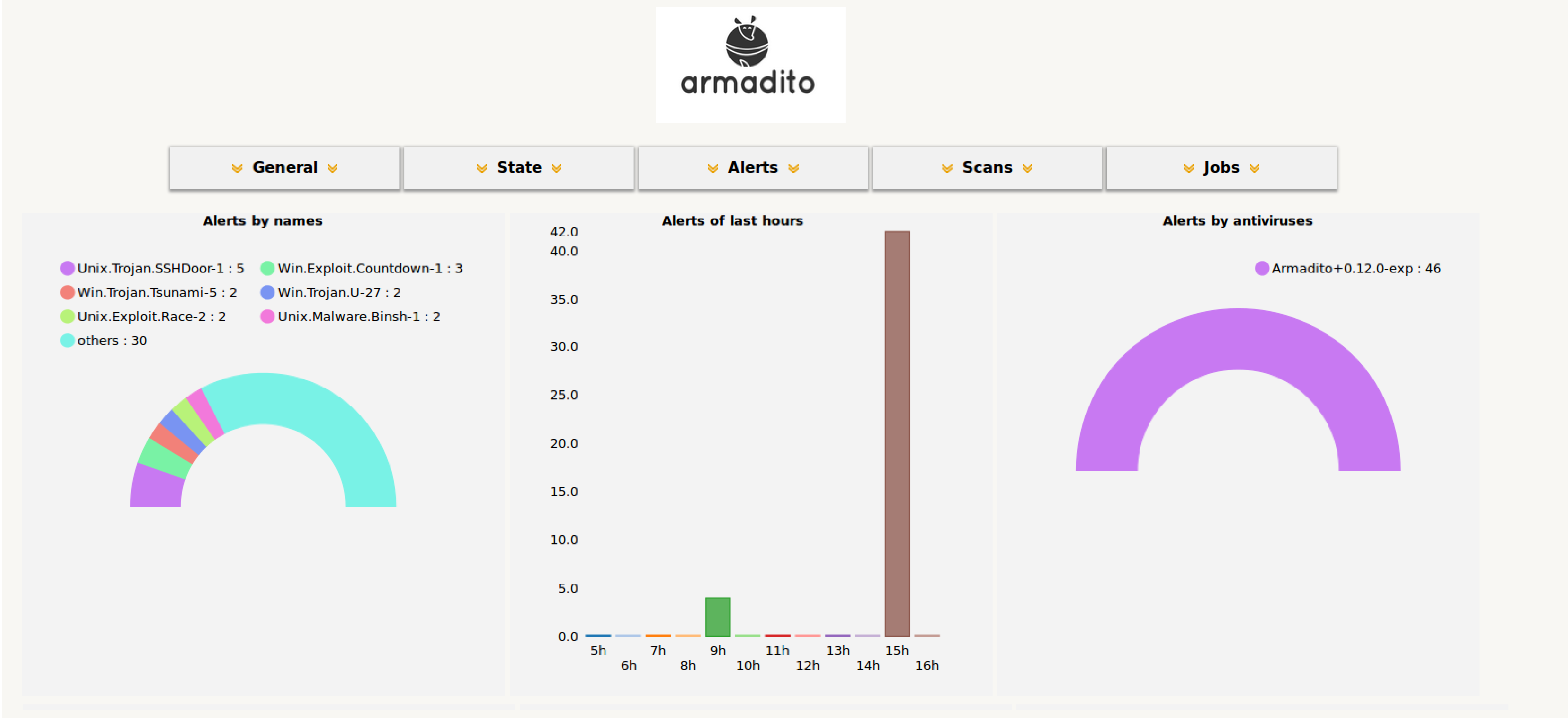
- antivirus deployment needs a centralized administration tool
  - monitoring (alerts, updates)
  - forced updates
  - remote scans
- provided by most proprietary antivirus
- need free software alternatives
- armadito: GLPI plugin, Prelude SIEM interface

Armadito GLPI plugin

- GLPI: Gestion Libre de Parc Informatique
- provides: inventory, tickets (and much more)
- Armadito GLPI plugin:
  - alerts, updates
  - deploy config or bases
  - journal
  - remote scan
- generic w.r.t. antivirus: supports Armadito, Kaspersky, ESET NOD32 (and possibly more)



Armadito GLPI plugin



Sandboxing

- https://googleprojectzero.blogspot.fr/2016/06/how-to-compromise-enterprise-endpoint.html
- CVE-2016-2208
- “Unpackers in the Kernel: Maybe not the best idea?”
- unpackers in a privileged process: …
- unpackers in a non-isolated process: …
- scanning complex file format in a non-isolated process: …
- so: sandbox/jail

Sandboxing (2)

- current solution on GNU/Linux uses nsjail
- http://github.com/google/nsjail
- syscalls:
  - 38 authorized
  - 1 controlled: socket(AF_UNIX, SOCK_STREAM,)
  - others kill
- limited and read-only mounts, no chroot yet
- worked with YARA out of the box, ClamAV with some tweaking

ClamAV vs. YARA

- ClamAV:
  - legacy
  - automatic bases update
  - unpackers
  - many archive formats
- but
  - high memory footprint (450 Mo), ok for servers, unusable for desktop
  - detection rate: could be better (see virustotal)

ClamAV vs. YARA (2)

- YARA:
  - a de facto standard for rules exchange
  - supported by many vendors and organizations
  - nice text format for rules
  - extensible by modules (PE...)
- but
  - standard rules set? http://github.com/Yara-Rules/rules.git
  - archives/unpacker (yextend)

ClamAV vs. YARA (3)

- translating ClamAV signatures to YARA rules is feasible
- several implementations (python, go)
- none fully functional
  - not all ClamAV signature formats are supported
  - generated YARA rules may be invalid
- some tests: 17% detection rate with ClamAV, 10% with YARA rules translated from ClamAV bases

ClamAV vs. YARA (4)

- another path: generate YARA rules automatically
- some free software projects:
  - YARA Rule Generator https://yaragenerator.com/
  - yarGen https://github.com/Neo23x0/yarGen by Florian Roth
- need a big base of cleanwares to avoid false positives
- a promising path

Where is it?

- Code: github.com/armadito
- Documentation: armadito-av.readthedocs.io
- Talk:

  gitter.im/armadito/armadito-av

  irc.freenode.net #armadito (very low activity)
- Ubuntu PPA: launchpad.net/~armadito

- sizeof(team) is an issue… may be you’re interested?