Schädlingsbekämpfung im Netzwerk mit Desinfec’t und opsi

Eric Esser

- Seit 2007 Systemadministrator im Wissenschaftszentrum Berlin
- Seit 2015 bei o4i
- Seit 2022 bei Sea-Watch
- 2022-2023 bei der Meldestelle Antiziganismus
- Im Herzen eigentlich Bartender in der KollektivBar ES (Berlin-Neukölln)
- Kontakt: eric.esser@wzb.eu | hello@ericesser.wtf

YARA

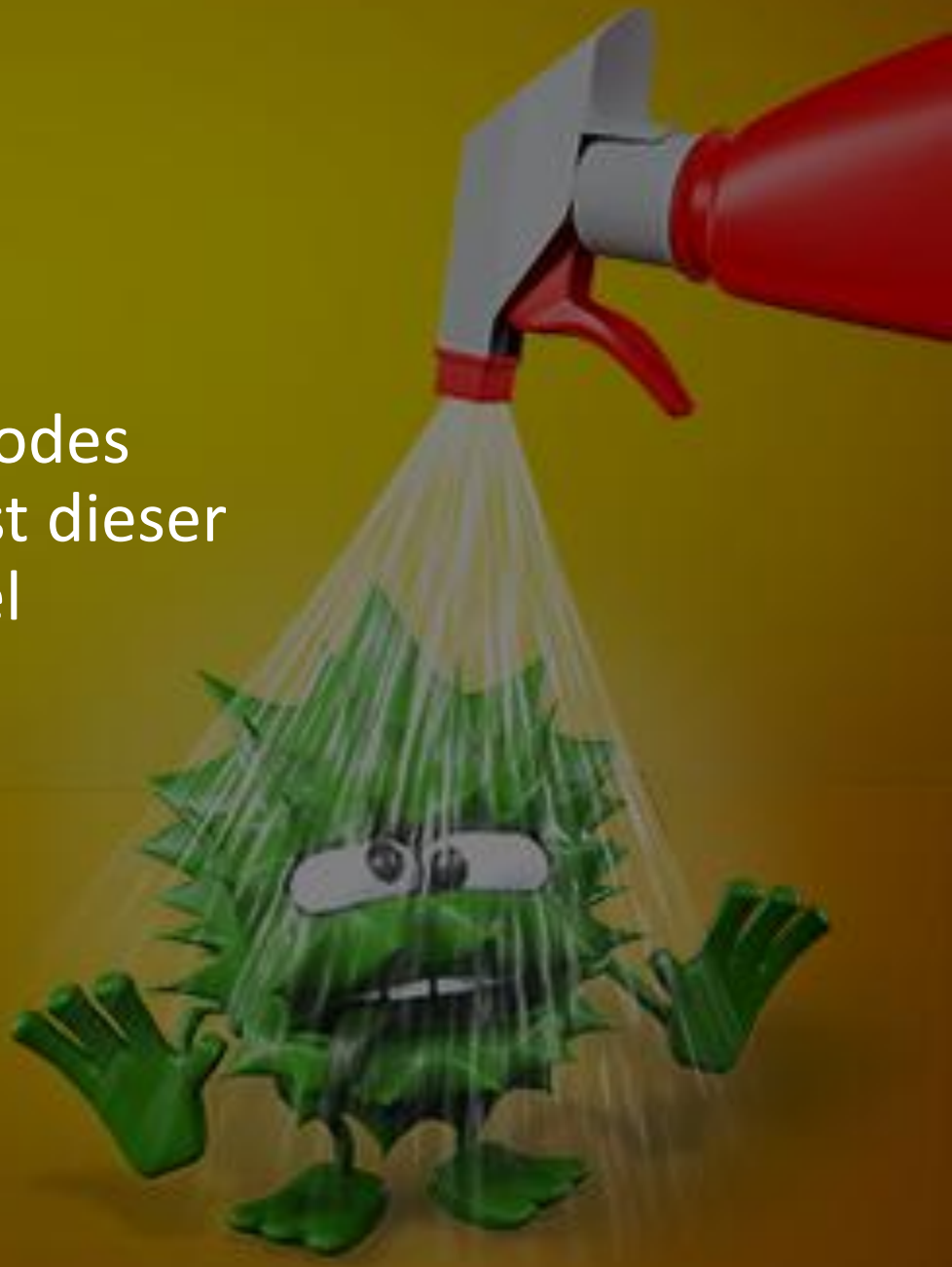
- „Yet Another Ridiculous Acronym“
- Von VirusTotal entwickeltes quelloffenes Framework zur Mustererkennung

Desinfec‘t

- Ubuntu-basiertes Live-System aus dem Heise-Verlag mit 5-6 Malwarescannern
- Kann Entschlüsselung mit Bitlocker & VeraCrypt
- Forensik-Tools
- Software für Datenrettung und -evakuierung
- Tools zur Systemreparatur
- Spiele für die Wartezeit

Desinfec‘t

- Lokales System startet nicht und eventueller Schadcode wird somit nicht ausgeführt
- Selbst bei versehentlicher Ausführung des Codes bei Untersuchung eines Windows-Systems ist dieser höchstwahrscheinlich nicht Linux-kompatibel



Desinfec‘t

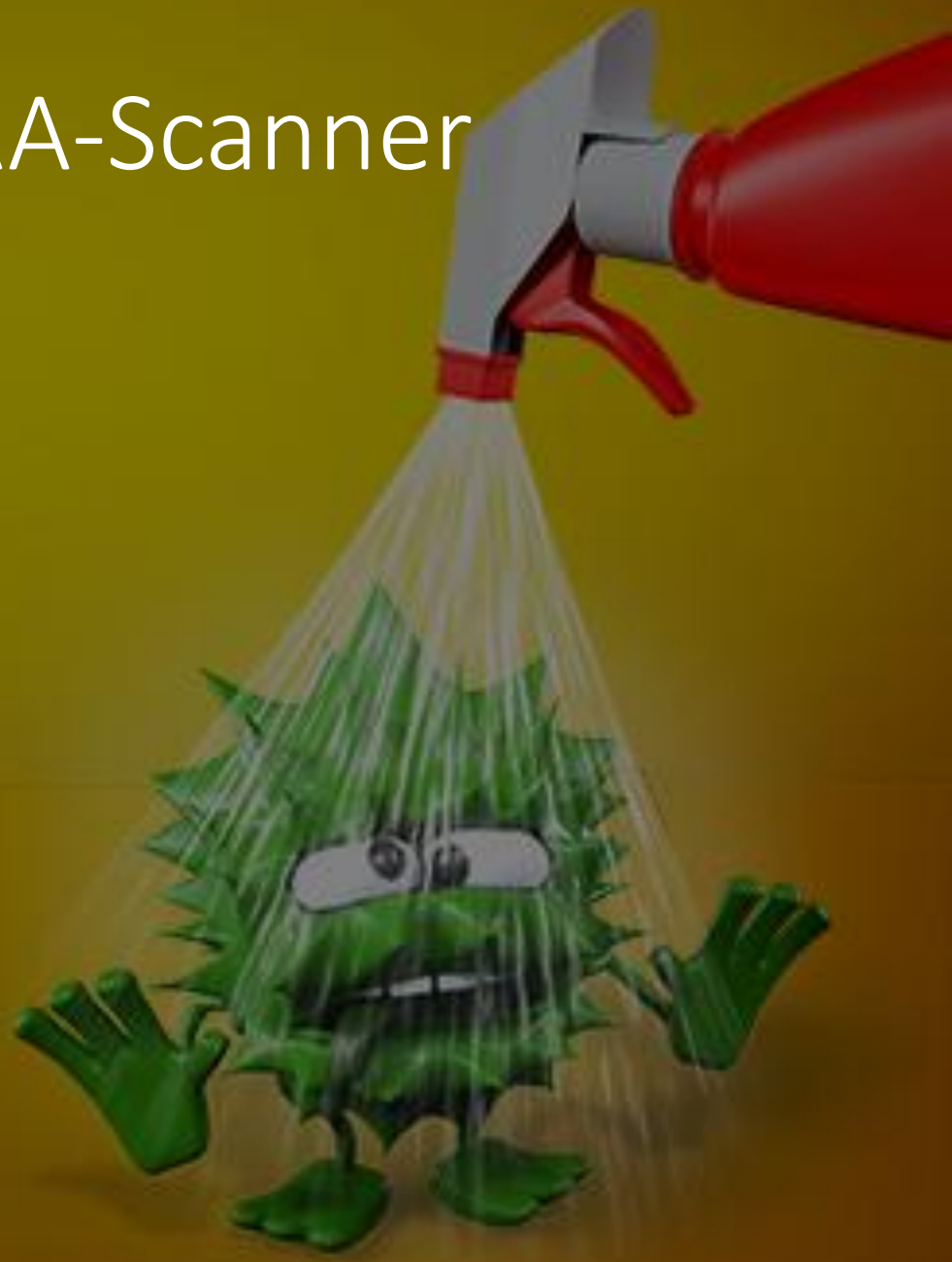
- Seit 2004, bis 2009 „Knoppicillin“
- Aktuell (202526) auf Ubuntu 24.4 LTS-Basis
- Erscheint zweimal im Jahr:
  - Mai-Ausgabe mit ct, Version z.B. 202500
  - September: Sonderheft, Version z.B. 202526
- Virendefinitions-Abos immer ein Jahr gültig
- Lizenzmodell verschieden
- Virenupdates vor jedem Lauf

Desinfec’t

Das Antivirus-Boot-System

1. Desinfec‘t – Viren- und YARA-Scanner

- ESET
- Withsecure (ehem. F-Secure) (202425)
- Ikarus (202500)
- ClamAV
- Nextron Thor Lite
- Open Thread Scanner



Desinfec’t

Das Antivirus-Boot-System

YARA-Scanner

- Wenn das Forensik-Team noch Ursachen erforscht und Lagebild erstellt: Thor Lite (oder Thor)
- Wenn die Schadsoftware erkannt wurde: Open Thread Scanner gezielt mit custom Yara-Regeln
- Auch ClamAV kann custom YARA-Regeln

o4i_desinfect

- Netboot-Produkt
- Desinfec't: DHCP, TFTP, NFS
- opsi 4.2: DHCP, TFTP, NFS, Samba
- 4 mal gebaut: 2015, 2020, 2023, 2025
- opsi-Bootimage nochmal neu

o4i_desinfect-Startpfad

1. PXE
2. TFTP
3. opsi-Boot-Image
4. Depot-mount
5. Lädt Desinfect Boot-Images vom opsi-Depot
6. Desinfec‘t-squashfs-Boot über NFS/Samba

o4i_desinfect 4.3.x

- ISOLINUX wurde von grub abgelöst
- Raus sind:
  - NFS Boot aus /var/lib/opsi/depot/opsi_nfs_share
  - SERVER_DATA
  - Properties als %Platzhalter% im Template
- Alles anders, daher neue Versionierung: 4.3.202425
- Dafür gibt‘s jetzt ein Python-Skript (o4i_desinfect.py)
  - bei Netboot endlich Properties validieren können
  - Möglichkeit, Python Libs zu nutzen

Autoscan-Ablauf

1. Desinfec‘t bootet
2. Liest ggf. custom YARA aus custom-Ordner
3. Übernimmt ggf. konkreten Pfad aus opsi-Property
4. Entschlüsselt Bitlocker-verschlüsselte Systemplatte
5. Scan mit YARA-Regeln auf Datenträgern
6. Schreibt das Log über den opsi-Service zurück
7. Fährt ggf. System wieder herunter
8. Steuerung durch Properties oder komplettes Shell-Autoscript

Features

- SMB-Boot (unverschlüsselt)
- Handling von Bitlocker-Keys
- Depot-Boot-Images anstatt nochmal TFTP
- Eingeschränkte zentrale Signaturverwaltung
- Beispielskripte für geskripteten Autoscan

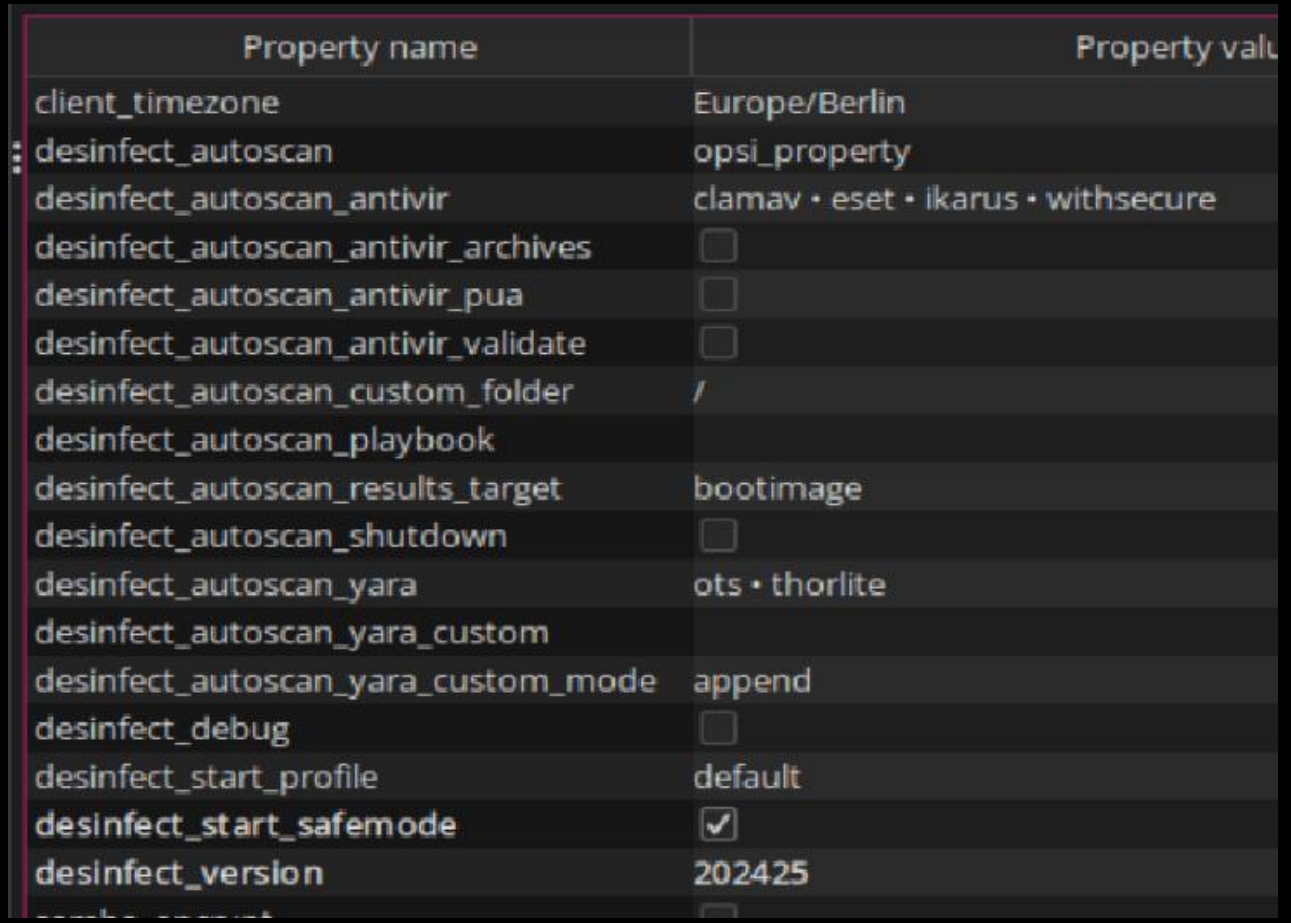
opsi-Properties: Boot

Property name	Property value
askbeforeinst	☐
boot_initrd	**initrd.55**
boot_kernel	**vmlinuz.55**
boot_misc_parameters	
boot_server	**192.168.56.10**
boot_server_type	**nfs**
boot_share	**/opt/o4i_desinfect/isocontent**
client_drive_bitlocker_password	*****
client_hostname	desinfect
client_hostname_by	opsi_database
client_hostname_postfix	
client_hostname_prefix	
client_ip_config	dhcp
client_keyboard_model	pc105

opsi-Properties: Client

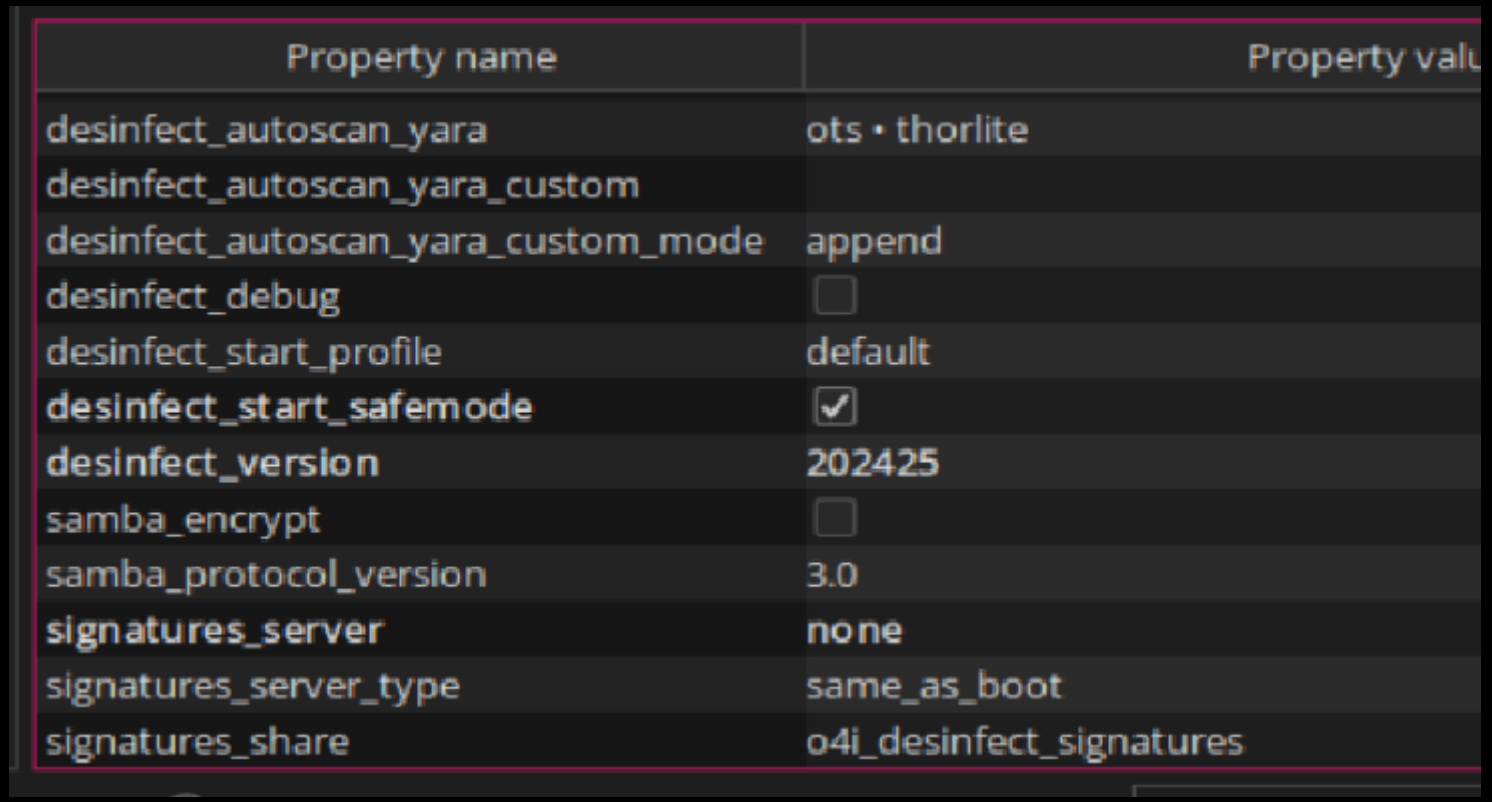
Property name	Property value
boot_share	/opt/o4i_desinfect/isocontent
client_drive_bitlocker_password	*****
client_hostname	desinfect
client_hostname_by	opsi_database
client_hostname_postfix	
client_hostname_prefix	
client_ip_config	dhcp
client_keyboard_model	pc105
client_language_keyboard	de
client_language_locale	de_DE
client_language_system	de
client_timezone	Europe/Berlin
desinfect_autoscan	opsi_property
desinfect_autoscan_antivir	clamav • eset • ikarus • withsecure

opsi-Properties: Desinfec‘t



Property name	Property valu
client_timezone	Europe/Berlin
desinfect_autoscan	opsi_property
desinfect_autoscan_antivir	clamav • eset • ikarus • withsecure
desinfect_autoscan_antivir_archives	☐
desinfect_autoscan_antivir_pua	☐
desinfect_autoscan_antivir_validate	☐
desinfect_autoscan_custom_folder	/
desinfect_autoscan_playbook	
desinfect_autoscan_results_target	bootimage
desinfect_autoscan_shutdown	☐
desinfect_autoscan_yara	ots • thorlite
desinfect_autoscan_yara_custom	
desinfect_autoscan_yara_custom_mode	append
desinfect_debug	☐
desinfect_start_profile	default
desinfect_start_safemode	☑
desinfect_version	202425

opsi-Properties: Signaturen & Samba



Property name	Property valu
desinfect_autoscan_yara	ots • thorlite
desinfect_autoscan_yara_custom	
desinfect_autoscan_yara_custom_mode	append
desinfect_debug	☐
desinfect_start_profile	default
desinfect_start_safemode	☑
desinfect_version	**202425**
samba_encrypt	☐
samba_protocol_version	3.0
signatures_server	**none**
signatures_server_type	same_as_boot
signatures_share	o4i_desinfect_signatures

Installation

- *opsi-cli package install o4i_desinfect*
- Ordnerstruktur anlegen unter */opt/o4i_desinfect*
- Ablegen der ISO-Dateien von Desinfec‘t
- Ggf. zusätzlicher NFS-Server
- Ggf. zusätzliches Samba-Shares
- Installations-Skripte in CLIENT_DATA/tools
  - *first-run.sh* (Setup-Skript)
  - *install-desinfect-binaries.sh* (ISO-Dateien installieren)

Sicherheit

- One-Time-Password bei Netboot mit *netboot.use_host_onetime_password* sehr empfohlen
- NFS/Samba-Boot ist unverschlüsselt
- Signature-Share ist suboptimalerweise rw

Ausblick

- Veröffentlichung auf o4i-public Repository: https://repo.o4i.org/public
- Verschlüsselter SMB-Boot
- Verbesserte zentrale Signaturverwaltung
- Sicherere Übergabe von Credentials
- VeraCrypt-Unterstützung
- Managen mehrerer Bitlocker-Keys
- Eventuell Netboot-OTP Unterstützung
- Auswertung des Massenscans per Grafana

Weiterführende Informationen

- Desinfec‘t Forum
  https://www.heise.de/forum/heise-Security/Themen-Hilfe/Desinfect/forum-33383/
- Desinfec‘t FAQ
  https://www.heise.de/ratgeber/FAQ-zum-c-t-Sicherheitstool-Desinfec-t-2025-10336138.html
- Heise ct Sonderheft Desinfec‘t
  https://www.heise.de/thema/Desinfect
- YARA-Regeln
  https://www.heise.de/select/ct/2018/20/153775554918252
  https://github.com/Neo23x0/YARA-Style-Guide
- readme.md des Pakets
  https://git.o4i.org/eric.esser/o4i_desinfect

Danke an

Dennis Schirrmacher vom Heise-Verlag
Den uib-Support, vor allem Mathias Radtke
Meine Kollegis von o4i

Fragen?

Danke!