Who we are

- Olaf Schwarz
  - Austrian Energy CERT
  - Incident Handling, Forensics
  - Member of BSidesVienna Crew

- Christian Wojner
  - CERT.at / GovCERT Austria
  - Malware Analysis, Reverse Engineering, Forensics
  - Author of ProcDOT, Densityscout, Bytehist, and Minibis
The vision

Build a DFIR package for the "Casual Incident Responder"

- Not your every days duty
- 0 - 5 cases/year
- Frequent re-familiarization
- Error-prone
- Inefficient/unstructured
- Missing/unsufficient notes
The vision

SIRF is not ...

- ... a mystic "Forensicator-Pro-Button"
- ... yet another blackboxed, module-driven money-shredder
- ... a SIFT replacement
Motivation

First-Aid-Kit

Maintenance/Training/Exercises
- Own team
- Constituency

Solid data pool for starting IR

Consider GDPR
Major aspects

- Knowledge database
- Templates
- Documentation of temporary work-arounds
  - Tool versions/builds
  - Microsofts "Feature-Updates"
- Encryption
- Portable
- Affordable
The concept

SIRF-Kit

ESXi

VM

Wiki "Know-How"

Wiki "Case"

VM

SIFT + Tools

HD

Write-Blocker

Evidence

Analyst

Analyst
GDPR and IR – An untold story

DISK IMAGES
MEMORY DUMPS
LOGS, PCAPS, FILES
CASE CORRESPONDENCE
DISCLAIMER
WE ARE NO LAWYERS!
The GDPR challenge
- Discard all relevant case data
- At a certain point in time

Our viewpoint
- Destroy access to data == Destroy data
- Encryption leads to cascading delete
Encrypt all case data

- Generate new key per case
- Encrypt data at rest
- Case correspondence (i.e. e-mails), too
- Delete key for final clean-up
Encrypt all case data
- Generate new key per case
- Encrypt data at rest
- Case correspondence (i.e.
- Delete key for final clean-up)

Mission accomplished?
Pitfalls

- LUKS key vs. master-key
- Re-Encryption necessary
- Encryption adds overhead to communication start-up
- Encryption absorbs IR time
Pitfalls

- LUKS key vs. master-key
- Re-Encryption necessary
- Encryption adds overhead to communication start-up
- Encryption absorbs IR time
SIRF and GDPR – Return to workbench
dd if=/dev/zero of=$volume
dd if=/dev/zero of=$volume

Introduce new channel
SIRF and GDPR – The new channel

Fully fledged chat service
- Text messages
- File exchange
- Transport layer encryption
- Multiple user accounts
- Browser-based
- Client/Server (≠ Pear2Pear)

Hosting
- Low-profile public IP address
- Encapsulated in VM (simple removal)

Potential candidates
- Mattermost, ...
SIRF and GDPR – The new channel

- Fully fledged chat
  - Text messages
  - File exchange
  - Transport layer encryption
  - Multiple user accounts
  - Browser-based
  - Client/Server (≠ Peer2Peer)

- Hosting
  - Low-profile public IP address
  - Encapsulated in VM (simple removal)

- Potential candidates
  - Mattermost, …
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny
The components

**Hardware candidates/evaluation**
- Intel Nuc Skull
- MSI Nightblade
- **Lenovo P320 Tiny**

**Write-Blocker candidates/evaluation**
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- Logicube WriteProtect Portable
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny

Write-Blocker candidates/evaluation
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- Logicube WriteProtect Portable
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny

Write-Blocker candidates/evaluation
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- Logicube WriteProtect Portable

Virtualization software
- VirtualBox
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny

Write-Blocker candidates/evaluation
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- Logicube WriteProtect Portable

Virtualization software
- VirtualBox ............. but .............
The components

VirtualBox Licensing: Frequently Asked Questions

This page deals with questions you may have about VirtualBox and its licensing. This information is accurate for VirtualBox 5.2 and later. You may want to look at the User FAQ and Developer FAQ for additional topics.

1. How is VirtualBox licensed?

The VirtualBox base package contains the full VirtualBox source code and platform binaries and is licensed under the GNU General Public License, version 2. You can distribute and modify the base package, provided that you distribute all modifications under the GPLv2 as well.

The VirtualBox Extension Pack is available under the VirtualBox Extension Pack Personal Use and Evaluation License, which is a free license for personal, educational or evaluation use, or an Enterprise License, which is a for-fee license that allows most commercial, non-distribution uses restricted by the PUEL.

More information about the Oracle VM VirtualBox Enterprise License for...
The VirtualBox Extension Pack is available under the VirtualBox Extension Pack Personal Use and Evaluation License, which is a free license for personal, educational or evaluation use, or an Enterprise License, which is a for-fee license that allows most commercial, non-distribution uses restricted by the PUEL.
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- Lenovo P320 Tiny

Write-Blocker candidates/evaluation
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- Logicube WriteProtect Portable

Virtualization software
- VirtualBox
- ESXi
The components

Hardware candidates/evaluation
- Intel Nuc Skull
- MSI Nightblade
- **Lenovo P320 Tiny**

Write-Blocker candidates/evaluation
- Tableau USB Writeblocker
- CRU WiebeTech Forensic Ultradock + USB 3.0 Writeblocker
- **Logicube WriteProtect Portable**

Virtualization software
- VirtualBox
- **ESXi**
Data is the fuel that powers IR!
Constituency SIRFification

Get in touch with your constituency ... beforehand!

- Clear decision- and escalation path
- Involve working council
- Prepared press statement(s)
- Analysis data pool checklist
- Start collecting now!
- Get familiar with your environment (What is normal?)
- Disk-Encryption in use?
- Identify your IR key-players
- Things they shouldn't do
- Communication channel
- Practice!
- ...

...
Analysis data pool

Logs
- DNS, Proxy, Firewall, Eventlog/Syslog, ...
- Centralized & time-synchronized
- Sufficient time coverage
- Content configuration

Network
- Diagram
- Flowdata
- PCAPs (on demand)

Baselines, Golden Images, Configuration Files

...
Did u know Chuck Norris had a role in Star Wars. He was the force.