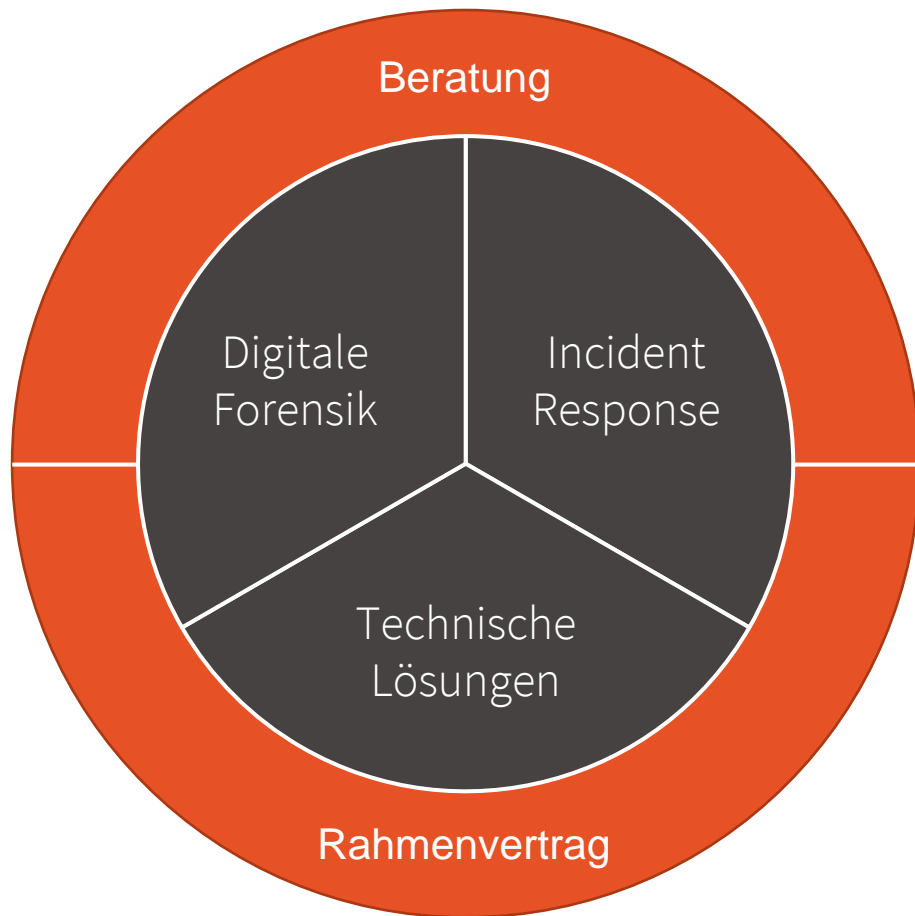


Incident Response & Forensics





Wir sind Ihr **Spezialist** für die Erkennung, Abwehr und Behandlung digitaler Angriffe.



	Digitale Forensik	Incident Response	Technische Lösungen
Ausführung	Durchführung technisch forensischer Analysen zur Klärung der Sachlage	Analyse, Kommunikation und Koordination im Bedrohungs- oder Sicherheitsvorfall	Konfiguration und Implementierung relevanter Sicherheitslösungen
Rahmenverträge	Vereinbarung von Rahmenverträgen oder kontinuierlichen Dienstleistungen in den drei Bereichen		
Beratung	Unterstützung in und Durchführung von Projekten im Sicherheitsbetrieb; speziell Auditierung, Ausführung von Übungen, Erstellung von Prozeduren und Richtlinien		

Who are we?

Aurélien Thierry

- Malware Analysis (automated detection) in academia (PhD)
- Worked for Airbus CyberSecurity: Malware Analysis + Forensics + Incident Response

@QuoSec:

- Forensics + Incident Response + Malware Analysis
- Security Engineering
- Banking sector
- French
- a.thierry@quosec.net (@yaps8)

Security in a corporate environment

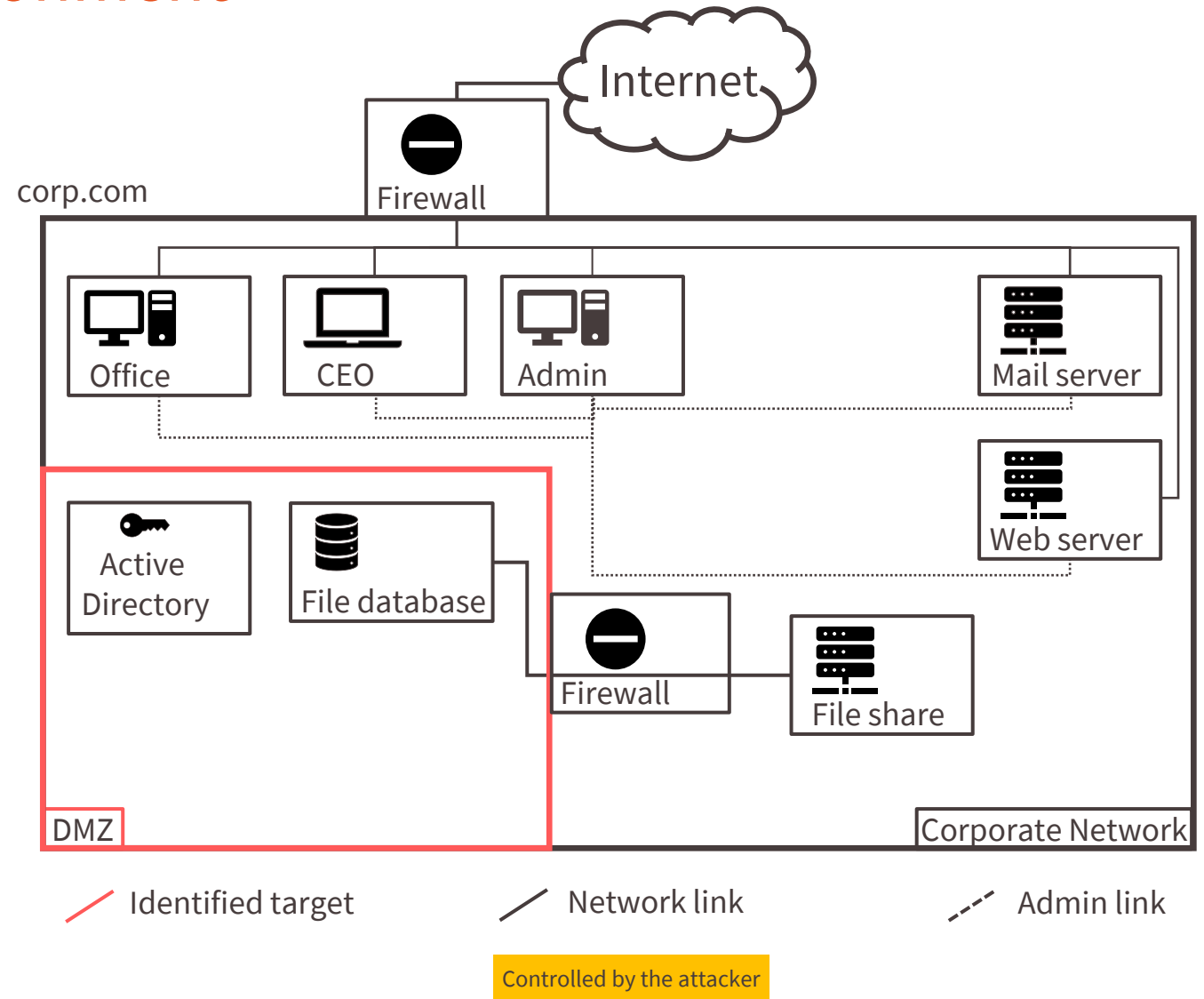
What is IT Security ?

What do you want to secure ?

- Information (data including personal data)
- Systems (machines)
- Business
- Employees
- Users
- ...

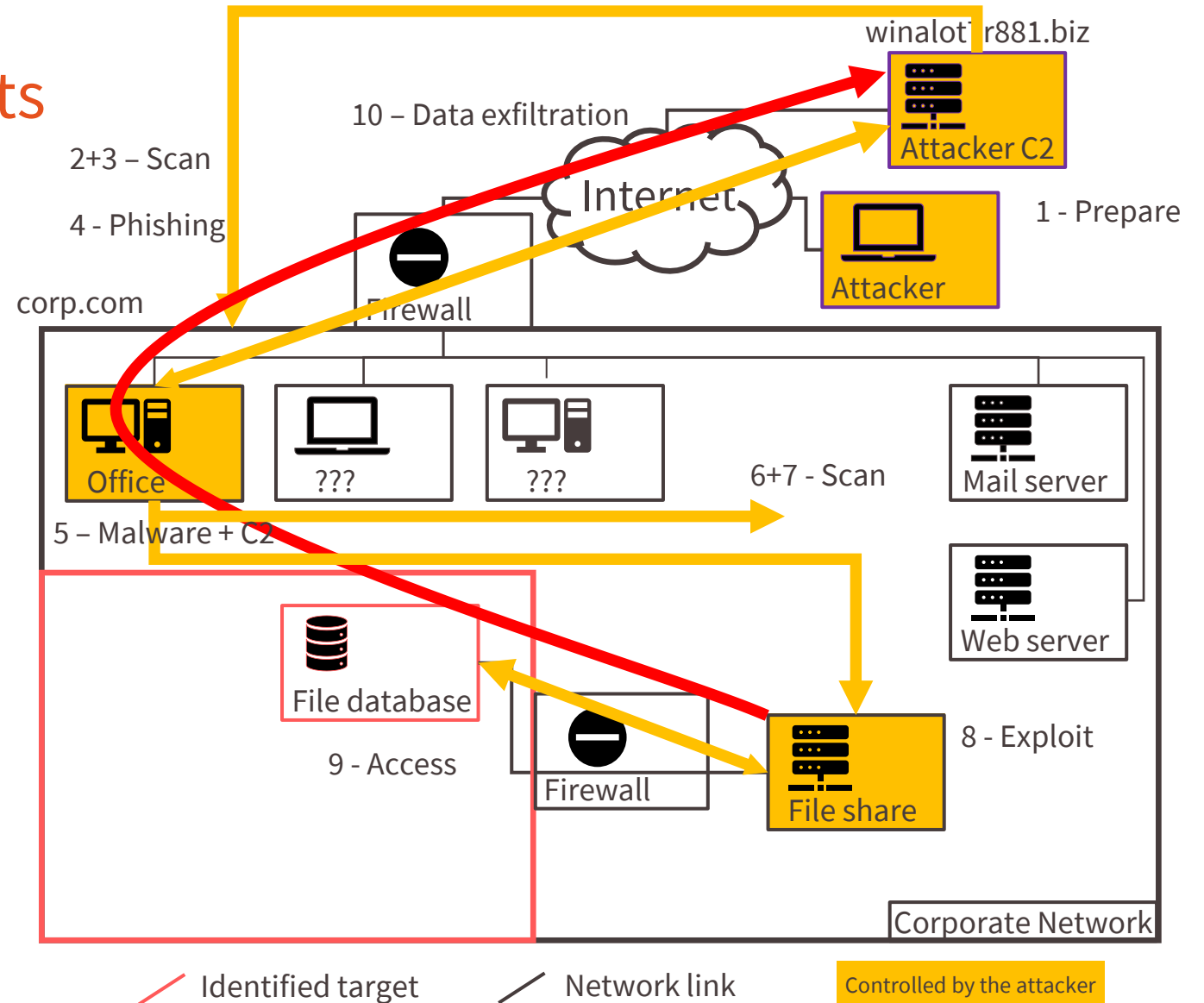
Fundamental security properties:

- Confidentiality
- Integrity
- Availability



Attack: exfiltrate trade secrets

1. Prepare your C2 infrastructure
2. Network scan (outside)
3. Vulnerability scan
4. Phishing:
 1. Find names of some employees (Google, LinkedIn...)
 2. Prepare malicious document + mail
 3. Sending to multiple surname.name@corp.com
5. Malware installation and connection to C2 (persistence)
6. Network scan (inside)
7. Vulnerability scan: **File share is vulnerable**
8. Vulnerability exploit
9. Access the documents
10. Exfiltrate data to C2



Defense strategy

Prepare:

- Network segregation
- Patch and harden systems

Monitor:

- Know your network
- Collect log and alerts from network
 - ▶ IDS / IPS: Intrusion Detection System
- & from hosts:
 - ▶ Antivirus / Endpoint Protection
 - ▶ SIEM: Log management

Detect:

- Have a team looking into logs and alerts
- Escalate attacks

Respond:

- Analyze / Understand the attack(er)
- Block the attacker
- Enhance your security

Monitoring challenges

SOC (Security Operations Center):

- Receives logs and alerts
- Escalates attacks to the incident response team
- Ticket-based workflow

False negative:

- Attack that is not detected

False positive:

- Legitimate action that is detected as an attack
- Risk of “drowning” the analysts with garbage

Triage effectively ?

- Not every alert is an attack
- Not every attack needs incident response



Monitoring challenges



SOC (Security Operations Center):

- Receives logs and alerts
- Escalates attacks to the incident response team
- Ticket-based workflow

False negative:

- Attack that is not detected

False positive:

- Legitimate action that is detected as an attack
- Risk of “drowning” the analysts with garbage

Triage effectively ?

- Not every alert is an attack
- Not every attack needs incident response

L1 – First contact – 24/24 7/7

- Point of contact for employees/customers
- Sees many false positives
- Triage to L2 with explicit guidance (example: ignore this IDS rule that makes mostly false positives)

L2 – Analyst – office hours + on call

- Investigates and triages with public and private data
- Asks the customer further information (what is this machine ?)
- Reports directly or raises incidents to L3

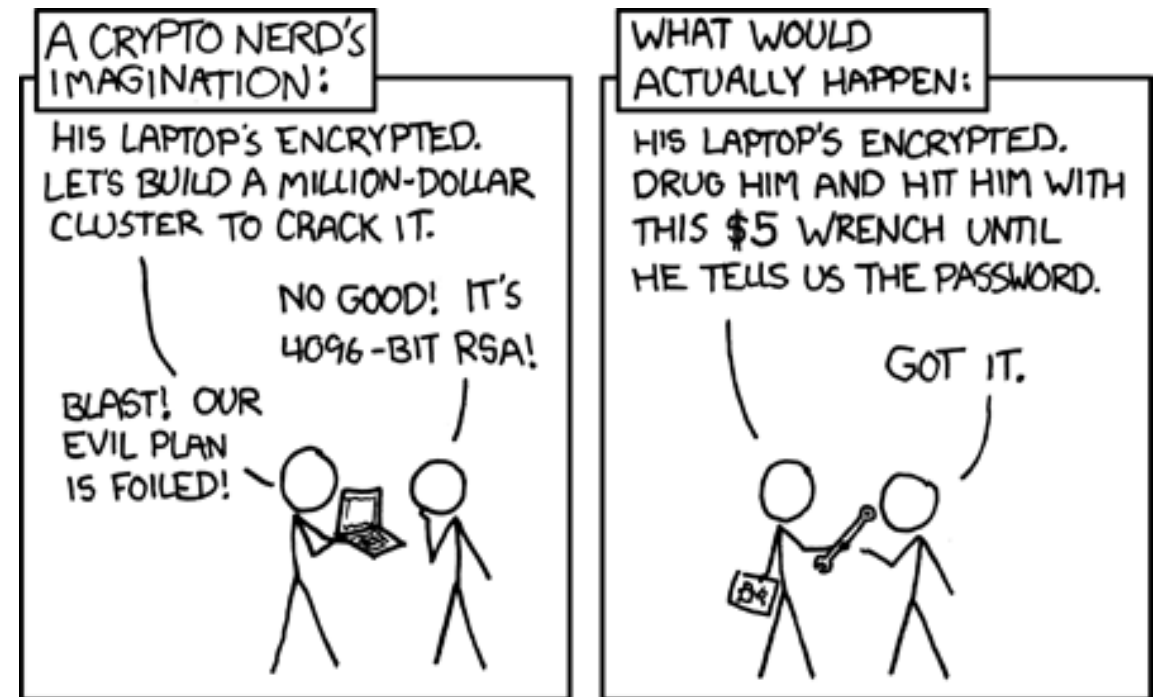
L3 – Incident Response – office hours + on call

- Reviews previous data
- Asks for technical data (drive / memory images, files, Event logs, firewall logs...)
- Does deep technical analysis
- Drives the response with the customer

Attackers and defenders (adversarial field)

Technical security is extremely difficult.

- Arms race
(new attack → new defense → new attack ...)
- Attackers need to find one way in
 - ▶ Technical and human vulnerabilities (Phishing, social engineering...)
- Defenders need to **defend them all**
 - ▶ Comply with laws (can't attack back)
- Attackers have the initiative
- Defenders (should) know their assets, network, company ...
 - Control their infrastructure (disconnect, poweroff ...)
 - Take back initiative & control



xkcd.com

Threat Intelligence

Know Your Enemies



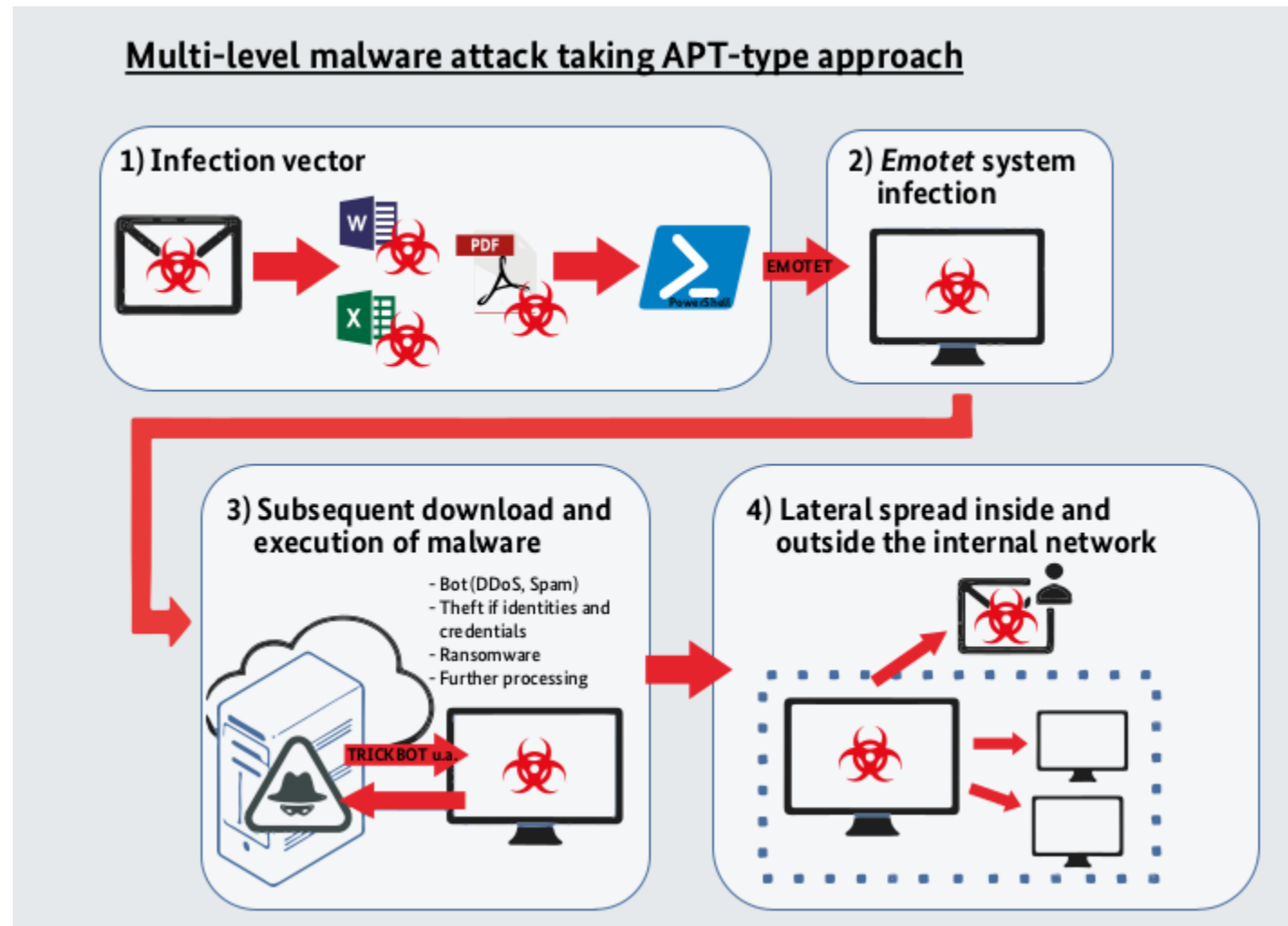
Type of attackers: <https://www.recordedfuture.com/cyber-attack-kill-chain/>

APT (Advanced Persistent Threat):

- Sophisticated threat actor
- Political or economical objectives
- Nation states (NSA...)

Threat Intelligence

Know Your Enemies: Emotet + TrickBot + SamSam



Attack complexity

“You get the attackers you deserve”

Common point in:

- Metasploit
 - Mimikatz
 - Empire
 - QuasarRAT
 - ...?
-
- Open-source offensive tools, maintained on GitHub
 - Ready to use “out-of-the-box”
 - Used by attackers in real attacks, including advanced attackers

Why?

- Cheaper
- Harder to attribute

APT attackers don't like to burn their fancy 0-days.

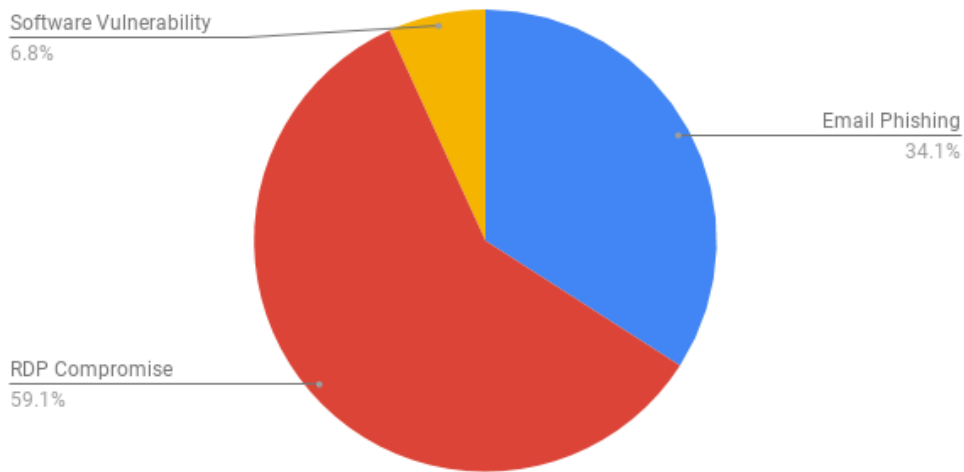
- Use phishing
- Exploit weak passwords
- Exploit unpatched systems
- Exploit weak security policy
- ...have the same kind of 3-Tier support system as SOC's ?...

Technically:

- Use open-source offensive projects
- Use open-source malware
- Use existing commercial malware
- Use custom malware
- Use custom exploit/payload for known vulnerabilities
- Find and use 0-days

Initial Access

Attack Vectors Commonly Used in Ransomware Incidents: Q2 2019

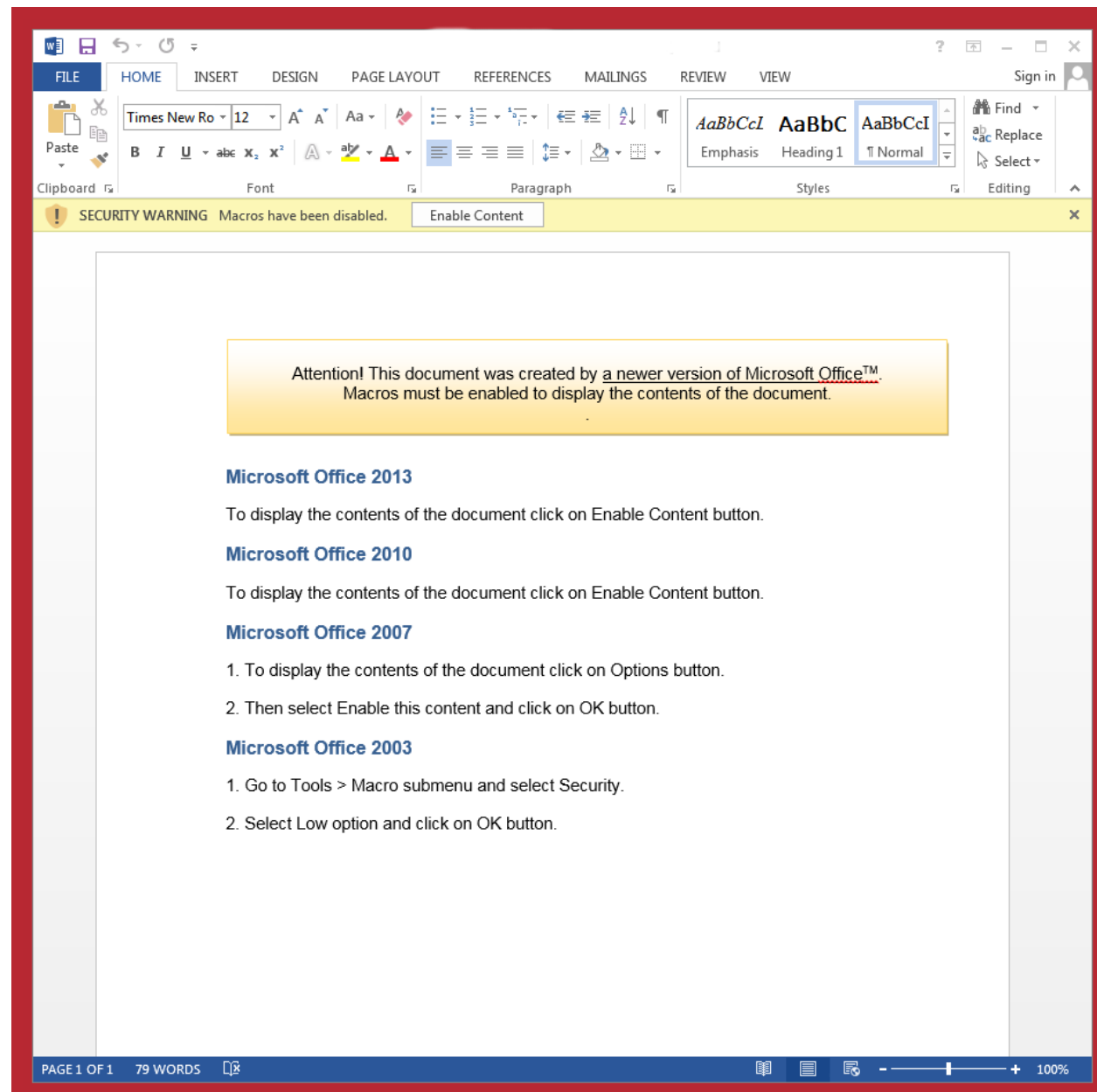
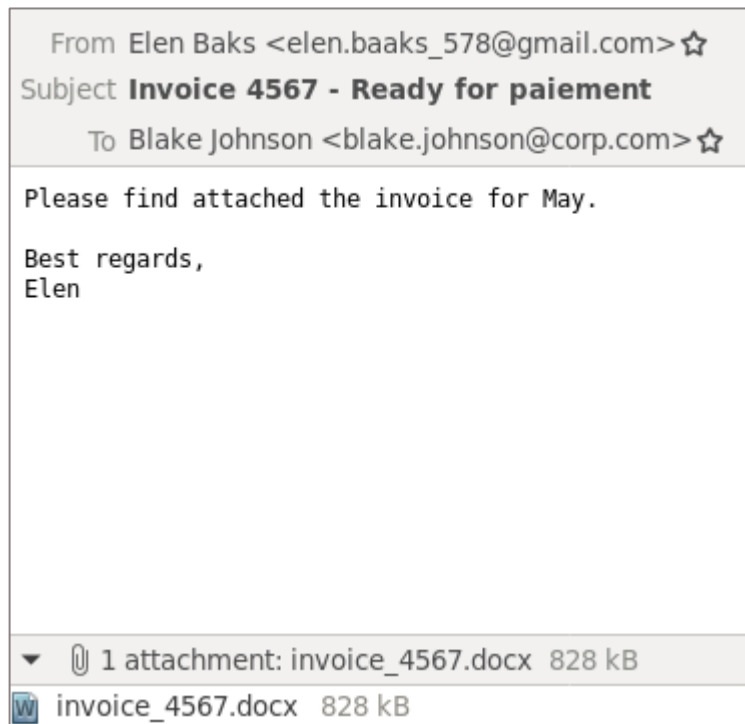


<https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread>

Personal experience:

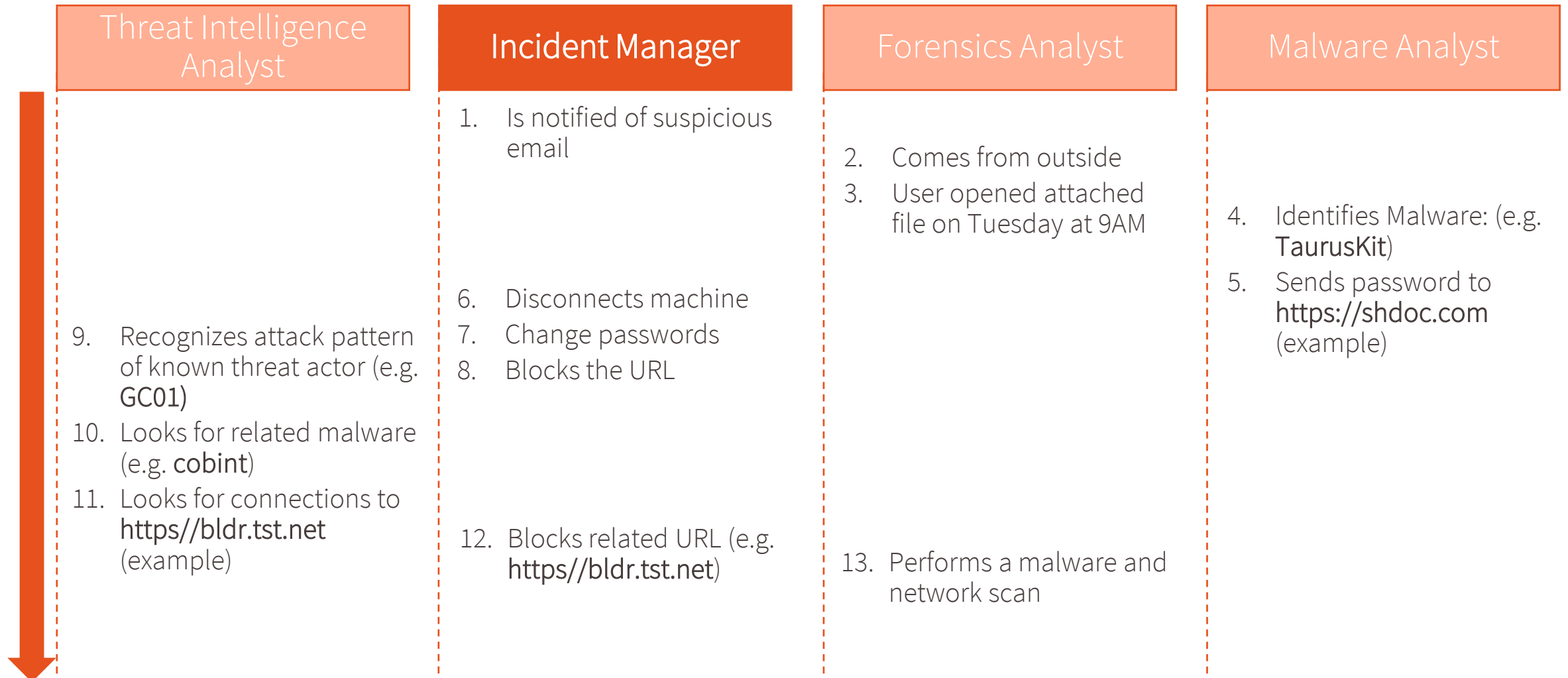
- Email Phishing
- Bad password policy (SSH / RDP):
 - ▶ Weak passwords
 - ▶ Password reuse
- Unpatched software:
 - ▶ A bit behind on updates
 - ▶ OS unsupported for years... (Windows XP, RHEL 6...)
- 0-day vulnerability in custom software (web-app)

Incident Response Phishing Campaign



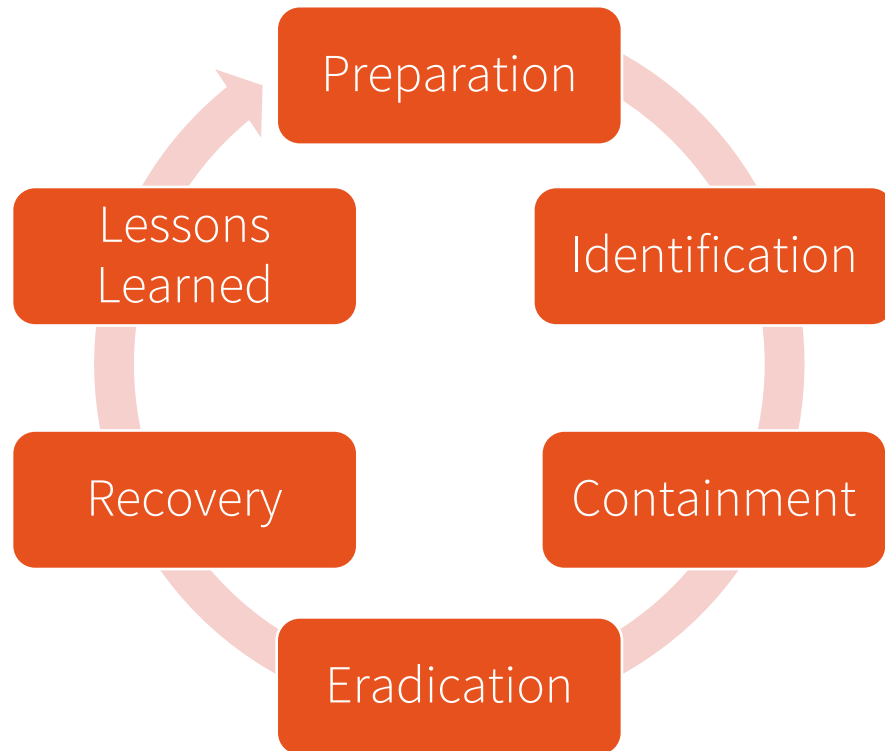
Incident Response

Roles: Who does what ?



Incident Response

Incident lifecycle (SANS, NIST)



Forensics ?

1. Preparation
 1. Define and know your assets / network / people / processes
 2. Prepare your technical defenses
2. Identification
 1. Detect the attack and initiate IR
 2. Identify compromised assets
3. Containment
 1. Collect technical evidence
 2. Mitigate impact (disconnect machines...)
4. Eradication
 1. Disinfect / re-image machines
 2. Block relevant artifacts (hostnames, malware...)
5. Recovery
 1. Ensure re-infection is not possible (patch systems...)
 2. Regain operational capabilities (reconnect machines...)
6. Lessons Learned
 1. Update techniques and processes

Phishing Campaign Forensics

Many people had the same phishing email

- One user reported that he clicked...

Forensics Analysis of his machine

- Collect volatile artifacts (RAM image)
- Power off and remove the hard drive
- Take an image with a write-blocker:
 - ▶ Do not overwrite the disk
 - ▶ Use `dcfldd` to compute hash while copying

Two options:

- Hardware write blocker (Tableau) + any Linux + `dcfldd`
- Linux with software write blocker (DEFT Zero) + `dcfldd`

```
dcfldd if=/dev/sdb of=/mnt/image.raw bs=4M hash=md5,sha1,sha256
```

Always work on images to preserve evidence.
May be crucial if there is a legal case.



In the Tableau Devices – world:

Yellow is a **WRITE** Module

Black is Write **BLOCKER**



Forensics

Useful artifacts

Forensics goals on one machine:

- What is the attack entrypoint ?
- What other machines / accounts are compromised ?
- What did the attacker do ?

RAM image analysis with **volatility**:

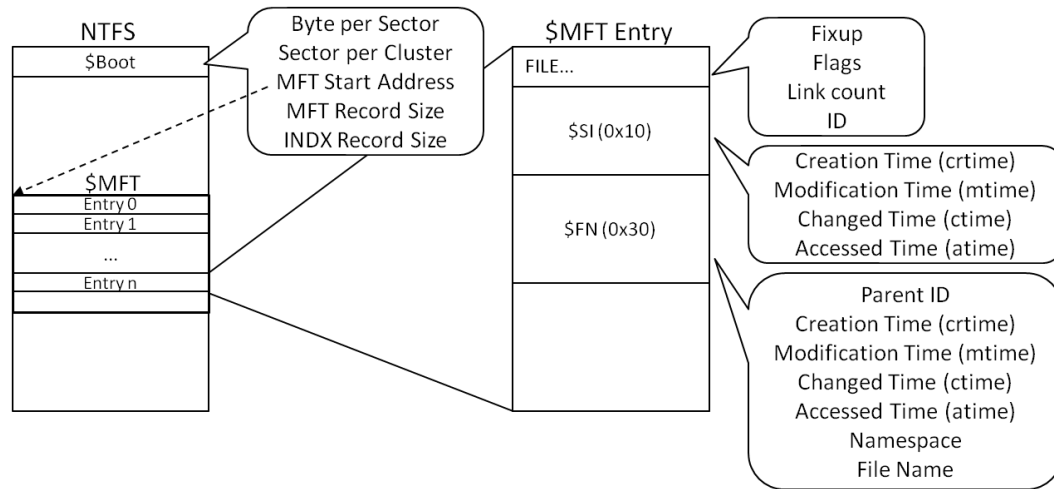
- Running processes
- Suspicious processes/DLL/drivers
- Commands from cmd.exe, powershell...
- Processes memory
- Opened files (handles)
- Network connections

Hard drive analysis:

- MFT: file system forensics + timestamp forensics
- Windows Registry: malware persistence...
- Event logs: login/logoff...
- Scheduled tasks: malware persistence...
- Prefetch, ShimCache, AmCache: which application was launched / when ?
- Shadow Copy Volumes: system backups
- Application logs
- Files: Malware detection (yara), Malware Analysis...

Master File Table (NTFS)

Timestamp Forensics



<http://www.kazamiya.net/en/fte/MFT>

Reference on file systems forensics:

- File System Forensic Analysis (Brian Carrier)

MACB:

- M: Modification (Data) Time
- A: Access (Data) Time
- C: Change (Metadata) Time
- B: Birth

Standard Information:

- Can be read and modified with API
- Can be faked by regular user

File Name:

- Only parsed and written by kernel, no API access
- Needs Admin rights + code to fake

Windows® Time Rules

\$ STANDARD_INFORMATION

	File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
M	Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
A	Access – Time of File Creation	Access – Time of Access (No Change only on NTFS Win7+)	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
C	Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
B	Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

\$ FILENAME

	File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
M	Modified – Time of File Creation	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Time of File Copy	Modified – No Change	Modified – Time of Move via CLI	Modified – Time of Cut/Paste	Modified – No Change
A	Access – Time of File Creation	Access – No Change	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of Move via CLI	Access – Time of Cut/Paste	Access – No Change
C	Metadata – Time of File Creation	Metadata – No Change	Metadata – No Change	Metadata – No Change	Metadata – Time of File Copy	Metadata – No Change	Metadata – Time of Move via CLI	Metadata – Time of Cut/Paste	Metadata – No Change
B	Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of Move via CLI	Creation – Time of Cut/Paste	Creation – No Change

Windows

NTFS

MACB updates

Starting your forensics analysis

- You are part of a chain of people working on the case
- Incident detected:
 - ▶ Security Monitoring (“suspicious attachment”)
 - ▶ Symptoms (“machine blocked”)
- You should already have some context:
 - ▶ What has already been observed?
 - ▶ When did it happen?
 - ▶ What has already been done?

Timestamp Forensics

“User opened suspicious email on 21/11/2019”

```
Thu Nov 21 2019 13:09:17 3834,mac., "C:/.../AppData/Local/Microsoft/Outlook/16/AutoD...aurelien.thierry.perso@outlook.com.xml"
Thu Nov 21 2019 13:09:17 4083,mac., "C:/.../AppData/Local/Microsoft/Outlook/16/AutoD...eab82e5a99a0e/4d9015f60282b0acba - Autodiscover.xml"
[...]
Thu Nov 21 2019 13:09:30 48,...b, "C:/.../AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/60L7E37R'
Thu Nov 21 2019 13:09:30 82,macb, "C:/.../AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/60L7E37R ($FILE_NAME)"
[...]
Thu Nov 21 2019 13:09:51 144,...b, "C:/.../AppData/Local/Mozilla/Firefox/Profiles/wux47sc7.default/cache2/trash29259"
Thu Nov 21 2019 13:09:51 86,...b, "C:/.../AppData/Local/Mozilla/Firefox/Profiles/wux47sc7.default/cache2/trash29259 ($FILE_NAME)"
[...]
Thu Nov 21 2019 13:09:53 360,macb, "C:/.../AppData/Roaming/Mozilla/Firefox/Profiles/wux47sc7.default/storage/default/https+++send.firefox.com'
Thu Nov 21 2019 13:09:53 114,macb, "C:/.../AppData/Roaming/Mozilla/Firefox/Profiles/wux47sc7.default/storage/default/https+++send.firefox.com ($FILE_NAME)"
[...]
Thu Nov 21 2019 13:09:55 280064,...b, "C:/.../Downloads/update_installer.exe"
Thu Nov 21 2019 13:09:55 106,macb, "C:/.../Downloads/update_installer.exe ($FILE_NAME)"
[...]
Thu Nov 21 2019 13:10:01 392,mac., "C:/.../Downloads"
Thu Nov 21 2019 13:10:01 280064,ma., "C:/.../Downloads/update_installer.exe"
[...]
Thu Nov 21 2019 13:10:23 280064,...c., "C:/.../Downloads/update_installer.exe"
Thu Nov 21 2019 13:10:31 3103,ma.b, r/rrwxrwxrwx,0,0,78120-128-4, "C:/Windows/Prefetch/UPDATE_INSTALLER.EXE-013895E1.pf'
Thu Nov 21 2019 13:10:31 130,macb, r/rrwxrwxrwx,0,0,78120-48-2, "C:/Windows/Prefetch/UPDATE_INSTALLER.EXE-013895E1.pf ($FILE_NAME)"
```

The Sleuth Kit - <https://www.sleuthkit.org/>

```
fls -r -m C: /dev/sdb2 > fls.out
```

```
mactime -b fls.out -d > mactime_d.out
```

1. Email received through Outlook
2. ...with document attached (INetCache)
3. Link clicked on document preview
4. Executable downloaded through Firefox (probably on send.firefox.com)
5. Executable launched (Prefetch .pf file)

Timestamp Forensics

External hard drive data

Windows® Time Rules									
\$ STANDARD_INFORMATION									
	File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion
M	Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
A	Access – Time of File Creation	Access – Time of Access <small>(No Change only on NTFS Win7+)</small>	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
C	Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
B	Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

Analysis of a NTFS-formatted USB stick

invoice.docx:

- Modified on another machine then copied to the stick (File Copy)

```
invoice.docx
M: Thu Nov 14 12:26:11 2019
A: Fri Nov 22 07:55:06 2019
C: Fri Nov 22 07:55:06 2019
B: Fri Nov 22 07:55:06 2019
```

Timestamp Forensics

POSIX: Linux, OpenBSD, FreeBSD

- POSIX specifies MAC timestamps
- Linux, OpenBSD, FreeBSD are “reasonably” compliant
- Some differences

Directory listing:

- `readdir()` shall mark for update the last data access (A) timestamp

ls dir/

- Linux, OpenBSD: A updated
- FreeBSD: A not updated

Access/Read timestamp (A) is not always updated for performance reasons:

- Win7+: A is not updated on File Access (read)
- Linux: with **relatime** (default) A is updated only if M or C is earlier or if A is at least 1 day old
- FreeBSD: A is always updated (default)
- OpenBSD: A is always updated (default), or with **noatime** A is only updated if the operation also updates M or C

MACB Timestamps

Profile Linux, OpenBSD, FreeBSD

```
$ ./profile_os

File Creation (PROFILE.OS.FILE.NEW):
dir/
  M.C.
newfile
  MACB

File Rename (PROFILE.OS.FILE.RENAME):
src
  !!!!
dst
  >>C>
dir/
  M.C.
```

On-going project to automatically profile OSes

>	M/A/C/B is same as src file/dir
M/A/C/B	M/A/C/B is updated to current time
.	M/A/C/B is not modified
!	Error (mostly: the file did not exist anymore)

https://github.com/QuoSecGmbH/os_timestamps

MACB Timestamps

Profile Linux, OpenBSD, FreeBSD

Linux MACB Timestamps

M	Last data Modification
A	Last data Access
C	Last file status Change
B	Birth
Resolution	1 nanosecond
M/A/C/B	M/A/C/B is updated to current time
m/a/c/b	M/A/C/B is inherited from m/a/c/b of source file/dir
.	M/A/C/B is not modified

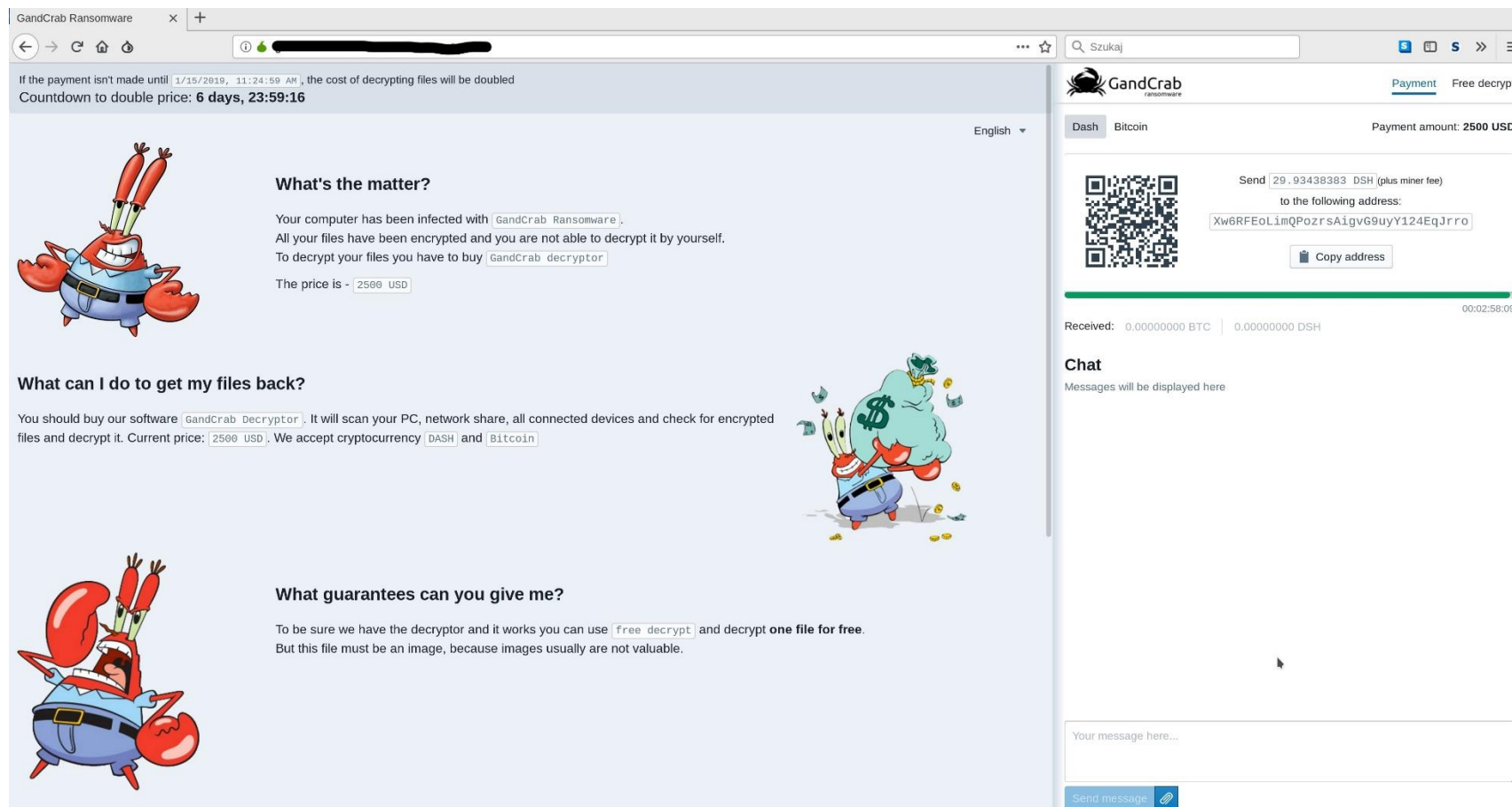
Mount Option	Description
(default)	MCB updates are all performed
relatime (default)	A updates are performed if A was earlier or equal to M or C, or at least 1 day old
noatime	A updates are never performed
nodiratime	A updates are never performed for directories
strictatime	A updates are always performed

	New File/Dir touch, mkdir	File Read /Execute cat, exec()	Symlink Read/Follow readlink	File Write >, >>	File/Dir Change chmod, chown	New/Delete Hardlink ln, rm	Local File/Dir Move mv	Volume File/Dir Move mv	File/Dir Copy (new) cp	File Copy (existing) cp
M	M	.	.	M	.	.	.	m	M	M
A	A	A	A	a	A	.
C	C	.	.	C	C	C	C	C	C	C
B	B	B	B	.

	Dir Traversal cd	Dir Listing ls	Dir: New/Rename Child (File/Dir/Hardlink) touch, mkdir, ln, mv, cp	Dir: Delete Child (File/Dir/Hardlink) rm, mv	Dir: Child Read/Exec/Write/Change cat, readlink, >>...
M	.	.	M	M	.
A	.	A	.	.	.
C	.	.	C	C	.
B

Ransomware quality

GandCrab



Malware Analysis:

- Malware family?
- Malware type? (RAT, Ransomware, cryptostealer...)
- What does it do?
- Is it persistent? How?

Constraints:

- Quick Analysis (1 day max)
- ~~Manual Reverse Engineering~~
- Antivirus
- Sandbox
- ~~Online Submission~~
- Virus Total (hash only)

Indicators Of Compromise (IOC)

Forensics:

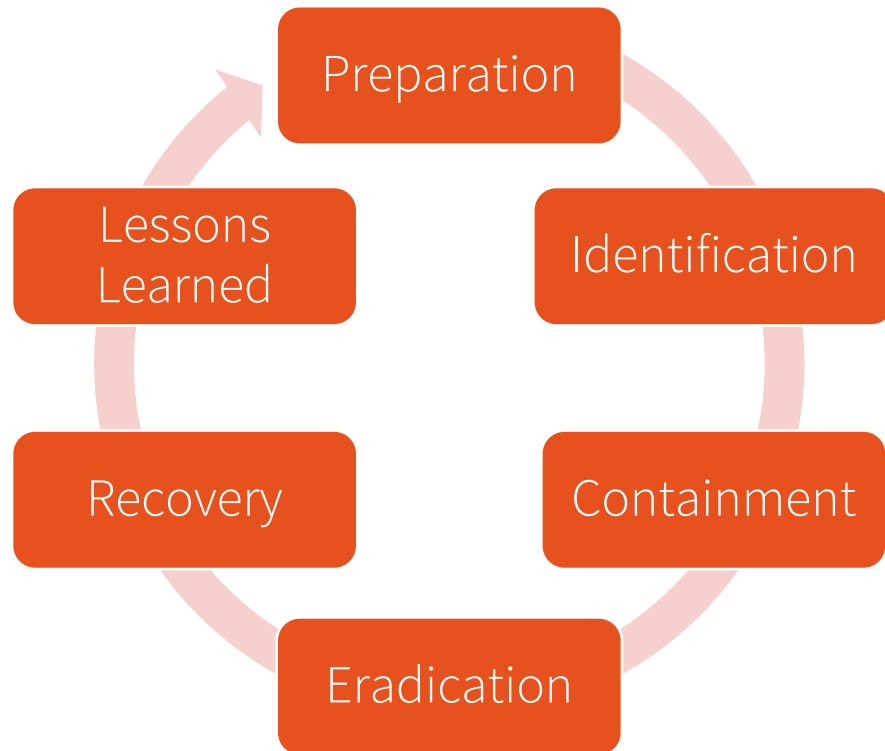
- Hostnames: kjfske-office.co.ru
- Email addresses: hello_motto_cot@gmail.com
- URL: https://dropbox.com/pages/mal_43_page/
- IP: 45.23.43.12
- File (malware):
 - ▶ Name: reg32_b.exe
 - ▶ Path: C:\\Windows\\iexplore.exe
 - ▶ SHA256:
15d67cf44f20acaed6ddd655bb95c4766df77859f
aef95abcbdb2a3aeb4cf9b0
- Registry value
- ...

Incident Response: What to do now?

- Detect them (IDS, AV...)
- Block them (Firewall, IPS, AV...)
- Find other compromised machines/accounts
- Clean machines?
- Disconnect infected machines?
- Find related attacks
- Share IOC with partners

Incident Response

Incident lifecycle (SANS, NIST)



1. Preparation
 1. Define and know your assets / network / people / processes
 2. Prepare your technical defenses
2. Identification
 1. Detect the attack and initiate IR
 2. Identify compromised assets
3. Containment
 1. Collect technical evidence
 2. Mitigate impact (disconnect machines...)
4. Eradication
 1. Disinfect / re-image machines
 2. Block relevant artifacts (hostnames, malware...)
5. Recovery
 1. Ensure re-infection is not possible (patch systems...)
 2. Regain operational capabilities (reconnect machines...)
6. Lessons Learned
 1. Update techniques and processes

Traditional forensics applied to IT-Security

Traditional Digital Forensics (full-drive imaging, police work):

- Preserving evidence is priority #1



Chain of
Custody is
filled

Evidence is
handed over

Write
Blocker
attached

Hard Disk is
mounted

Hard Disk is
imaged
(cloned)



500GB drive =
up to 500GB image size =
analysis of 500GB data !

- Need to image volatile data (RAM...)
- Encryption ?
- Can you physically remove/image the drive ?

Critical server:

- Critical to business: website, production line...
- Needs to stay up and connected

Multiple employees' machines are infected:

- How long does imaging + analysis + disinfection take ?

What about personal information ?

Rob Lee (SANS, 2018):

- "... less than 1% of the total data of a hard drive is all the data you will need to solve a case as that is all your tools forensicate and parse – the rest is “data” and mostly junk.”
- “we aren’t seizing the entire “kitchen” if a body is found in it – just the evidence that is usable.”
- You only need a forensics data (<1% of the drive) + some malicious files (<1% of the drive)

Traditional forensics applied to IT-Security

Traditional Digital Forensics (full-drive imaging, police work):

- Preserving evidence is priority #1



Chain of
Custody is
filled

Evidence is
handed over

Write
Blocker
attached

Hard Disk is
mounted

Hard Disk is
imaged
(cloned)



500GB drive =
up to 500GB image size =
analysis of 500GB data !

🔲 Cyber Forensics (selective imaging):



Volatile Data is
collected

Targeted data is
collected

(Original evidence is
preserved)



500GB drive =
~ 1% of size + Memory size

- Quicker collection
- Can be done remotely (cheaper)
- Machine is still usable
- Good for large-scale incident response and triaging
- Less forensically-safe

Issues:

- User / IT has touched/turned off the device
- You may still need full images after triaging

Traditional forensics applied to IT-Security

Traditional Digital Forensics (full-drive imaging, police work):

- Preserving evidence is priority #1



Chain of
Custody is
filled

Evidence is
handed over

Write
Blocker
attached

Hard Disk is
mounted

Hard Disk is
imaged
(cloned)



500GB drive =
up to 500GB image size =
analysis of 500GB data !

📦 Cyber Forensics (selective imaging):



Volatile Data is
collected

Targeted data is
collected

(Original evidence is
preserved)



500GB drive =
~ 1% of size + Memory size

📦 A combination:



Volatile
Data is
collected

Targeted
data is
collected

Write
Blocker
attached

Hard Disk is
mounted

HDD is
cloned



Selective imaging / Live forensics

Run an application on the compromised machine to collect relevant artifacts only

- No need to remove the drive
- Quicker imaging
- Remote imaging
- Large scale imaging

Selective Imaging Revisited (2013):

- Johannes Stüttgen, Andreas Dewald and Felix C. Freiling
- Formal definition of **selective imaging** and **partial images**
- Implementation using AFF4 storage

- FTK Imager - <https://accessdata.com/product-download>
- FastIR – https://github.com/Fast-IR/Fastir_Collector
- DFIR-ORC – <https://github.com/DFIR-ORC/dfir-orc>
- GRR - <https://github.com/google/grr>

Assess:

- What artifacts are collected ?
- What artifacts/data is modified by the imaging ?
- Forensically sound ?

DFIR-ORC

- Selective imaging tool by ANSSI (French agency for IT-Sec)
- Windows only
- Open-Source: <https://dfir-orc.github.io>

Modular framework:

- Possible to add binaries (other tools)
- Configuration with XML files
- Config files included as PE resources



DFIR ORC

ANSSI

DFIR-ORC: Usage

```
PS C:\Users\xach\Desktop\bin\dfir-orc-config\output> .\DFIR-Orc.exe /keys
Mothership v10.0.11
DFIR-Orc v10.0.11
Start time           : 06/09/2020 05:21:40.171 (UTC)
Computer             : XACH-PC
Full Computer        : xach-PC
User                 : xach-PC\xach (elevated)
System type          : WorkStation
System tags           : OSBuild#7601,SP1,Windows7,WorkStation,x64
Operating System      : Microsoft Windows 7 Professional Service Pack 1 (build 7601), 64-bit
Output directory     : C:\Users\xach\Desktop\bin\dfir-orc-config\output (encoding=UTF8)
Temp directory        : C:\Users\xach\AppData\Local\Temp\WorkingTemp (encoding=UTF8)
Log file              : DFIR-ORC_WorkStation_xach-PC_20200609_052140.log
Repeat Behavior       : No global override set (config behavior used)
Priority              : Low

[X] Archive: Main (file is DFIR-ORC_WorkStation_xach-PC_Main.7z)
    [X] Command SystemInfo
    [X] Command Processes
    [X] Command GetEvents
    [X] Command Autoruns
    [X] Command NTFSInfo
    [ ] Command NTFSInfoHashPE
    [X] Command FatInfo
    [ ] Command FatInfoHashPE
    [X] Command USNInfo
    [X] Command GetArtefacts

[X] Archive: Hives (file is DFIR-ORC_WorkStation_xach-PC_Hives.7z)
    [X] Command GetSystemHives
    [X] Command GetUserHives
    [X] Command GetSamHive

[ ] Archive: Yara (file is DFIR-ORC_WorkStation_xach-PC_Yara.7z)
    [X] Command GetYara

[X] Archive: CollectedFiles (file is DFIR-ORC_WorkStation_xach-PC_CollectedFiles.7z)
    [X] Command CollectFiles
```

DFIR-ORC: Reconfigurable through PE resources

CFF Explorer VIII - [DFIR-Orc.exe]

File Settings ?

File: DFIR-Orc.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Relocation Directory
- Debug Directory
- TLS Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor

DFIR-Orc.exe

- BINARY
 - "COLLECTFILES_CONFIG.XML" - [lang:0]
 - "DD_SQLSCHEMA" - [lang:0]
 - "EXTRACTDATA_REPORT_SQLSCHEMA" - [lang:0]
 - "FATINFOHASHPE_CONFIG.XML" - [lang:0]
 - "FATINFO_CONFIG.XML" - [lang:0]
 - "FATINFO_SQLSCHEMA" - [lang:0]
 - "GETARTEFACTS_CONFIG.XML" - [lang:0]
 - "GETCOMOBJECTS_SQLSCHEMA" - [lang:0]
 - "GETEVENTS_CONFIG.XML" - [lang:0]
 - "GETSAMHIVE_CONFIG.XML" - [lang:0]
 - "GETSAMPLES_SQLSCHEMA" - [lang:0]
 - "GETSECTORS_SQLSCHEMA" - [lang:0]
 - "GETSYSTEMHIVES_CONFIG.XML" - [lang:0]
 - "GETTHIS_SQLSCHEMA" - [lang:0]
 - "GETUSERHIVES_CONFIG.XML" - [lang:0]
 - "GETYARASAMPLES_CONFIG.XML" - [lang:0]
 - "IMPORTDATA_SQLSCHEMA" - [lang:0]
 - "NTFSINFOHASHPE_CONFIG.XML" - [lang:0]
 - "NTFSINFO_CONFIG.XML" - [lang:0]
 - "NTFSINFO_SQLSCHEMA" - [lang:0]
 - "NTFSUTIL_SQLSCHEMA" - [lang:0]
 - "OBJINFO_SQLSCHEMA" - [lang:0]

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	72	75	6C	65	20	64	66	69	72	5F	6F	72	63	20	7B	0A	rule.dfir_orc.{
00000010	20	20	20	20	73	74	72	69	6E	67	73	3A	0A	20	20	20strings:....
00000020	20	20	20	20	24	64	75	6D	6D	79	20	3D	20	22	54	\$dummy.="T
00000030	68	69	73	20	69	73	20	61	20	64	75	6D	6D	79	20	72	his.is.a.dummy.r
00000040	75	6C	65	20	6E	6F	74	20	73	75	70	70	6F	73	65	64	ule.not.supposed
00000050	20	74	6F	20	6D	61	74	63	68	20	61	6E	79	74	68	69	.to.match.anythi
00000060	6E	67	20	62	75	74	20	74	68	65	20	62	69	6E	61	72	ng.but.the.binar
00000070	79	20	65	6D	62	65	64	64	69	6E	67	20	69	74	21	22	y.embedding.it!"
00000080	0A	20	20	20	20	63	6F	6E	64	69	74	69	6F	6E	3A	0Acondition:.
00000090	20	20	20	20	20	20	20	24	64	75	6D	6D	79	0A	7D	\$dummy.}
000000A0	0A																.

Ongoing Project

Selective imaging: ORC improvements

Forensics soundness:

- Enforce integrity of collected evidence
- Evaluate impact of imaging on the system

Improvement of ORC output:

- Currently a bunch of .7z files
- Provide a single AFF4 archive

Full-drive imaging VS selective imaging

Useful artifacts (Windows):

- RAM
- Machine name, version, user, harddrive info...
- File timestamps (MFT)
- Targeted files (paths or YARA rule)
- Registry hives
- Windows Events (EVTX)
- Prefetch files
- AmCache, BITS
- Files

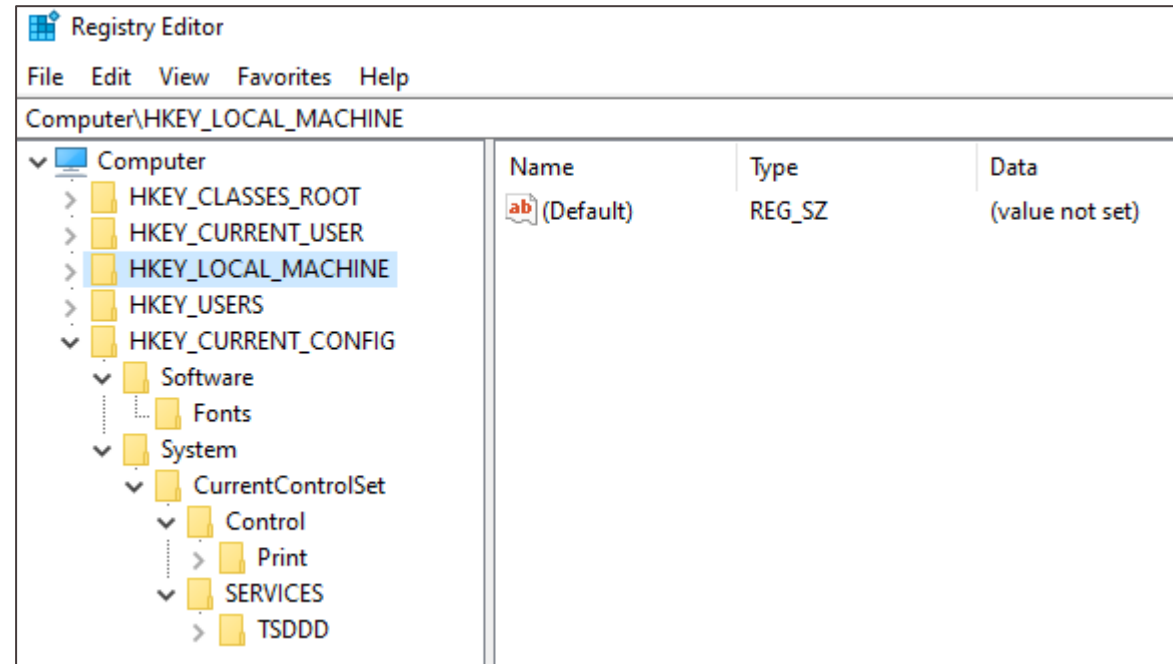
Memory Analysis (volatility)

Selective imaging (ORC)

Full-drive imaging

Windows Registry

- Hierarchical database (tree)
- Stores settings
- Are stored in registry files:
 - ▶ C:\System32\Config\SAM
 - ▶ ...
 - ▶ C:\Users\John\Ntuser.dat
 - ▶ ...



- Run keys:
 - ▶ Are executed when windows launches (persistence)

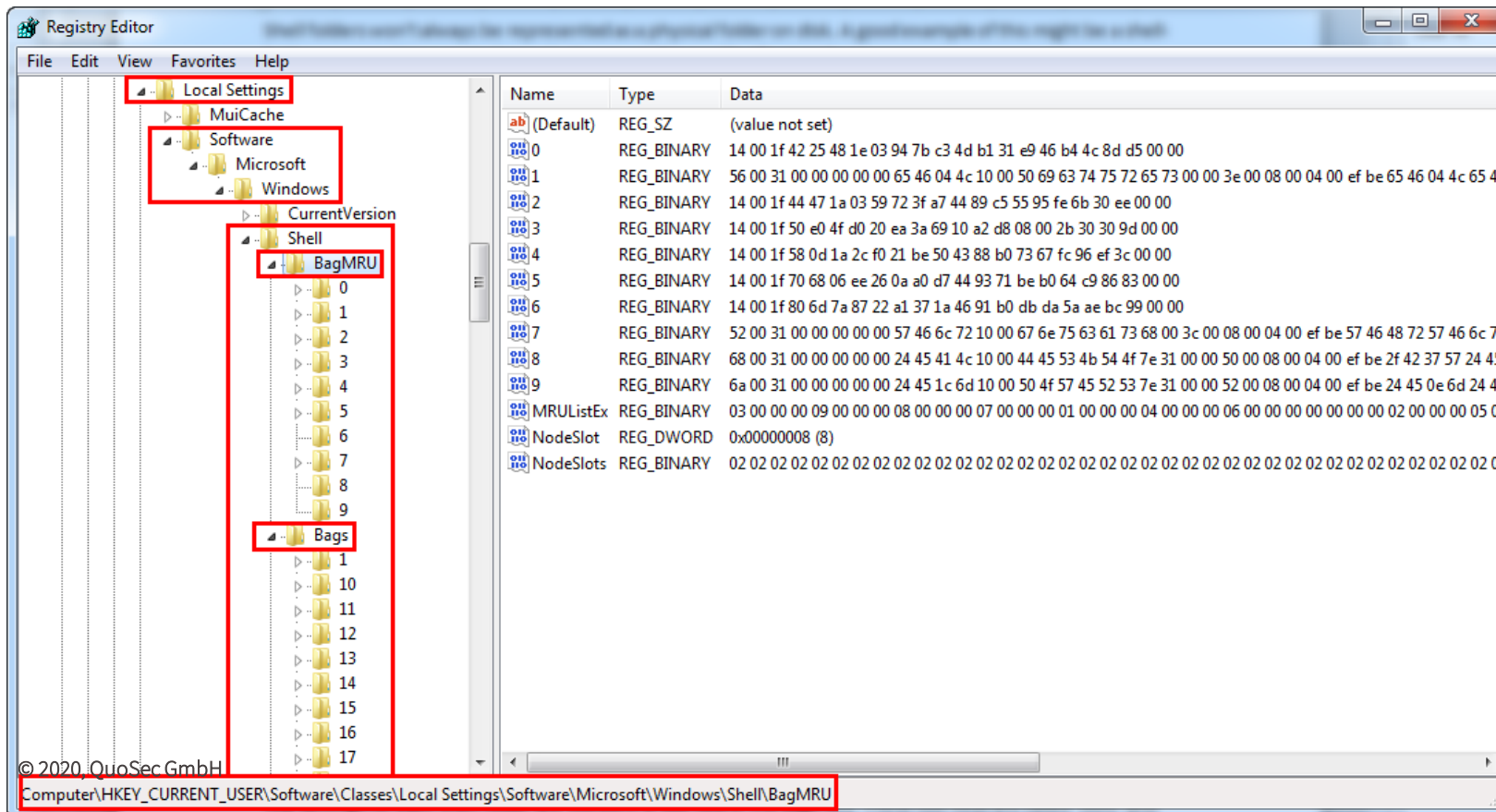
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
>	ReserveManagi	Name	Type	Data
>	RetailDemo	(Default)	REG_SZ	(value not set)
	Run	SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
	RunOnce	VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe
	Search			

Shell bags:

- Windows remembers folders browsed through Windows Explorer (GUI)
- It is used to know the user preference (icons type, window position...)
- Gives some forensics artifacts (timestamps)
- Need specific parser

Shell bags:

- Windows remembers folders browsed through Windows Explorer (GUI)
- It is used to know the user preference (icons type, window position...)
- Gives some forensics artifacts (timestamps)
- Need specific parser



Windows Registry: Shell bags (EnCase)

The screenshot displays the EnCase Enterprise Training software interface. The left pane shows a file tree with 'Desktop' selected. The center pane shows a table of registry entries. The bottom pane shows a detailed view of the selected entry, '48'.

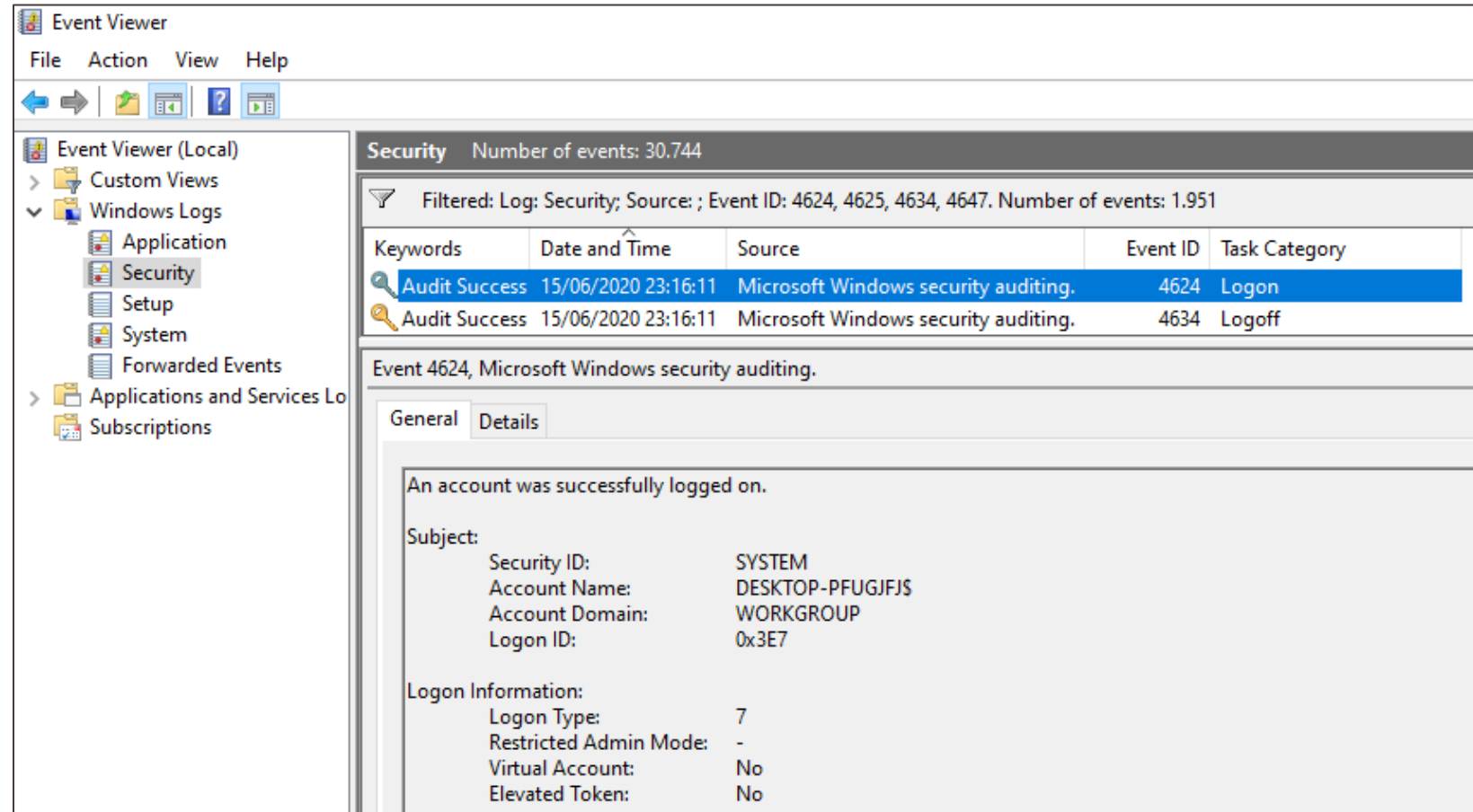
	Target Name	Shell-Item Type	Shell-Item Sub-Type	ShellBag Path	MRU Index	Node Slot	View Mode	Icon Size	Registry Created
1	2010-08-18 Antigua	File/Folder Entry	None	Desktop\4\1\0	0	56	Icons	96	19/08/10 03:54:57
2	48	File/Folder Entry	None	Desktop\4\1\1	1	70	Icons	96	24/08/10 22:50:36

Target Name	48
Shell-Item Type	File/Folder Entry
Shell-Item Sub-Type	None
ShellBag Path	Desktop\4\1\1
MRU Index	1
Node Slot	70
View Mode	Icons
Icon Size	96
Registry Created	24/08/10 22:50:36
Target Created	05/07/10 22:36:52
Target Last-Accessed	05/07/10 22:37:12
Target Last-Modified	05/07/10 22:37:12
Target MFT Record Number	51853
Target MFT Record Sequence Number	2

ShellBags

Windows Events (EVTX)

- Windows stores many events (logs)
- Stored into .evtx files
- Login (4246)/Logoff, type gives details:
 - ▶ 2: console (keyboard)
 - ▶ 3: network
 - ▶ 7: unlock
 - ▶ 10: RDP
 - ▶ ...
- Network share access
- Virus detected
- ...



Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 30.744

Filtered: Log: Security; Source: ; Event ID: 4624, 4625, 4634, 4647. Number of events: 1.951

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	15/06/2020 23:16:11	Microsoft Windows security auditing.	4624	Logon
Audit Success	15/06/2020 23:16:11	Microsoft Windows security auditing.	4634	Logoff

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: SYSTEM
- Account Name: DESKTOP-PFUGJFJS
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:

- Logon Type: 7
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

“Malware can hide, but it must run” (SANS)

Malware running:

- Found in RAM
- Leaves traces on drive:
 - ▶ Prefetch file is created for each running .exe
 - ▶ ...

Persistent malware:

- Run keys (Registry)
- Windows services
- Scheduled tasks
- Modified/patched binary
- ...

Rootkit hiding from the system:

- Full-drive image necessary
- May hide in rare locations (MBR...)
- May hide elsewhere (device firmware...)

```
$ python2 prefetch.py -f WMIPRVSE.EXE-1628051C.pf

=====
WMIPRVSE.EXE-1628051C.pf
=====

Executable Name: WMIPRVSE.EXE

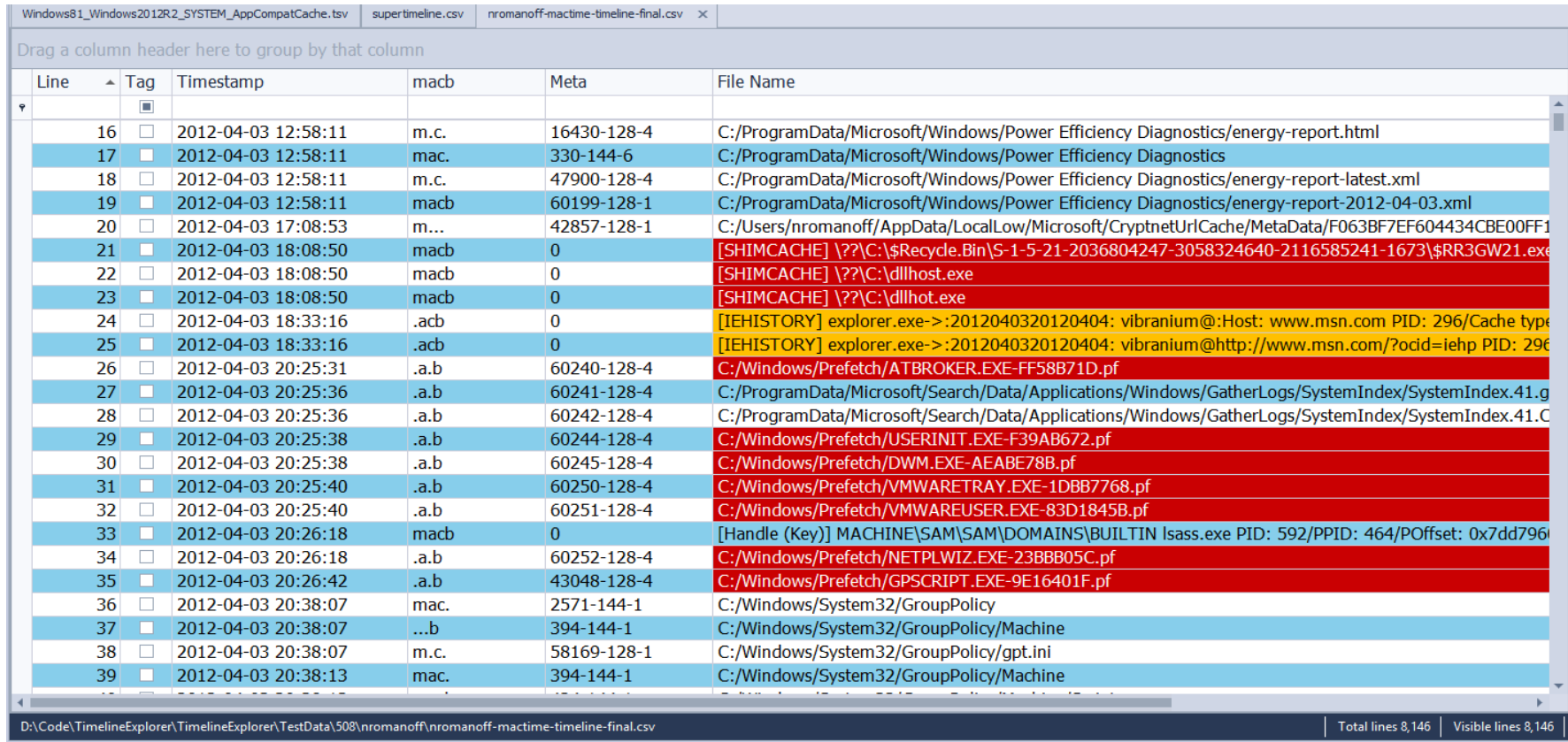
Run count: 4
Last Executed: 2018-08-02 10:05:25.389374

Volume Information:
  Volume Name: \DEVICE\HARDDISKVOLUME2
  Creation Date: 2018-08-02 18:32:47.390626
  Serial Number: 943611ce
```

Supertimeline (N artifacts -> 1 merged timeline)

Plaso and log2timeline:

- <https://github.com/log2timeline/plaso>
- Timeline generation and analysis (visualization / filtering...)
- Merge all (timestamps) logs and forensics artifacts into a single timeline



Drag a column header here to group by that column					
Line	Tag	Timestamp	macb	Meta	File Name
16	<input type="checkbox"/>	2012-04-03 12:58:11	m.c.	16430-128-4	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report.html
17	<input checked="" type="checkbox"/>	2012-04-03 12:58:11	mac.	330-144-6	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics
18	<input type="checkbox"/>	2012-04-03 12:58:11	m.c.	47900-128-4	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-latest.xml
19	<input checked="" type="checkbox"/>	2012-04-03 12:58:11	macb	60199-128-1	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-2012-04-03.xml
20	<input type="checkbox"/>	2012-04-03 17:08:53	m...	42857-128-1	C:/Users/nromanoff/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/F063BF7EF604434CBE00FF1
21	<input checked="" type="checkbox"/>	2012-04-03 18:08:50	macb	0	[SHIMCACHE] \\?\C:\\$Recycle.Bin\S-1-5-21-2036804247-3058324640-2116585241-1673\\$_RR3GW21.exe
22	<input type="checkbox"/>	2012-04-03 18:08:50	macb	0	[SHIMCACHE] \\?\C:\dllhost.exe
23	<input checked="" type="checkbox"/>	2012-04-03 18:08:50	macb	0	[SHIMCACHE] \\?\C:\dllhot.exe
24	<input type="checkbox"/>	2012-04-03 18:33:16	.acb	0	[IEHISTORY] explorer.exe->:2012040320120404: vibranium@:Host: www.msn.com PID: 296/Cache type
25	<input checked="" type="checkbox"/>	2012-04-03 18:33:16	.acb	0	[IEHISTORY] explorer.exe->:2012040320120404: vibranium@http://www.msn.com/?ocid=iehp PID: 296
26	<input type="checkbox"/>	2012-04-03 20:25:31	.a.b	60240-128-4	C:/Windows/Prefetch/ATBROKER.EXE-FF58B71D.pf
27	<input checked="" type="checkbox"/>	2012-04-03 20:25:36	.a.b	60241-128-4	C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.41.g
28	<input type="checkbox"/>	2012-04-03 20:25:36	.a.b	60242-128-4	C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.41.C
29	<input checked="" type="checkbox"/>	2012-04-03 20:25:38	.a.b	60244-128-4	C:/Windows/Prefetch/USERINIT.EXE-F39AB672.pf
30	<input type="checkbox"/>	2012-04-03 20:25:38	.a.b	60245-128-4	C:/Windows/Prefetch/DWM.EXE-AEABE78B.pf
31	<input checked="" type="checkbox"/>	2012-04-03 20:25:40	.a.b	60250-128-4	C:/Windows/Prefetch/VMWARETRAY.EXE-1DBB7768.pf
32	<input type="checkbox"/>	2012-04-03 20:25:40	.a.b	60251-128-4	C:/Windows/Prefetch/VMWAREUSER.EXE-83D1845B.pf
33	<input checked="" type="checkbox"/>	2012-04-03 20:26:18	macb	0	[Handle (Key)] MACHINE\SAM\SAM\DOMAINS\BUILTIN lsass.exe PID: 592/PPID: 464/POffset: 0x7dd796
34	<input type="checkbox"/>	2012-04-03 20:26:18	.a.b	60252-128-4	C:/Windows/Prefetch/NETPLWIZ.EXE-23BBB05C.pf
35	<input checked="" type="checkbox"/>	2012-04-03 20:26:42	.a.b	43048-128-4	C:/Windows/Prefetch/GPSCRIPT.EXE-9E16401F.pf
36	<input type="checkbox"/>	2012-04-03 20:38:07	mac.	2571-144-1	C:/Windows/System32/GroupPolicy
37	<input checked="" type="checkbox"/>	2012-04-03 20:38:07	...b	394-144-1	C:/Windows/System32/GroupPolicy/Machine
38	<input type="checkbox"/>	2012-04-03 20:38:07	m.c.	58169-128-1	C:/Windows/System32/GroupPolicy/gpt.ini
39	<input checked="" type="checkbox"/>	2012-04-03 20:38:13	mac.	394-144-1	C:/Windows/System32/GroupPolicy/Machine

D:\Code\TimelineExplorer\TimelineExplorer\TestData\508\nromanoff\nromanoff-mactime-timeline-final.csv | Total lines 8,146 | Visible lines 8,146

Forensics imaging at scale (1 machine -> N machines)

For IT departments:

- Possible to prepare (install solution on perimeter)
 - ▶ Endpoint security solutions from AV vendors
 - ▶ Open-source solutions (custom GRR configuration)
- Train security team

For customers:

- No previous installation
- “Fire and forget”
- ORC: 1 binary to run, only need to fetch output
- Deployment:
 - ▶ Manually (a few machines)
 - ▶ GPO
 - ▶ PsExec
 - ▶ Asset Management solution
 - ▶ ...
- Selective imaging: lower risk of personal information leak
- Analysis at scale?

Incident Response + Forensics

Security:

- Attackers vs Defenders
- **Absolute security is not possible**
- Techniques + Process + People

Defend:

- Identify critical assets
- Prepare your defense
- **Monitor + Detect + Respond**

Incident Response Issues:

- Time
- Do not impact business
- Many infected machines at the same time
- Lots of data
- User or IT compromised the evidence

Forensics:

- Start from the context (**Detect**)
- Lots of different artifacts
- **Timestamp forensics** works on all OSes
- Malware analysis must be quick
- **Selective imaging:**
 - ▶ Quicker than full-disk imaging
 - ▶ Remote
 - ▶ How to make it forensically sound ?



QuoSec

Radilostr. 43
60489 Frankfurt am Main
curious@quosec.net