Remote Forensic Investigations
(In the Context of COVID-19)

Xavier Mertens | TF-CSIRT #62 | January 2021
[TLP:White]
Who’s Talking?

- Xavier Mertens (@xme)
- Freelance based in Belgium
- Blueteam
- SANS ISC Senior Handler
- SANS Instructor
- BruCON Co-Organizer
20(20|21)...

... will definitively change our behaviour at all levels. From a business point of view, most of us are working remotely and this should remain a standard...
This implies our tools and process have to fulfil new requirements...
Friday, 10PM
Your Phone Rings…

You’re on duty… A customer suspects some malicious activity on a computer. The customer is located 500KM away and asks you to perform investigations as soon as possible.

Many incidents occur at the wrong time.

“Everything takes longer than you think.”
(Murphy’s law)
Forensic 101

“The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.” (Wikipedia)

• Collect relevant data from the “suspicious” host in safe way

• Basic artefacts
  • Filesystem
  • Memory
  • Registry

• Useful
  • Application data (browsing history, …)
Forensic 101

Toolbox

• Agent-based
  • Encase
  • GRR (Google Rapid Response)
  • MIG (Mozilla InvestiGator)
  • OSQuery, OSSEC
• On-demand
  • SIFT Workstation
SIFT Workstation

The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings.
Requirements

• Easy and quick to deploy
• « Forensically » aware
• Lot of tools preinstalled
• Disk management
• Interaction with users
• Compatible with many systems/networks
• Customers keep control (grant/deny access)
• Low bandwidth usage: process data remotely (just grab evidences)
Bitscout
“A customizable Live OS constructor tool almost entirely written in Bash”

- Live Linux OS
- Simple & customizable at build time
- Extendable at run time
- Minimal system requirements
- Low bandwidth / VPN
- Unprivileged isolated access
- Two roles: “Expert” and “Owner”
Bitscout

Key Points

• The “Expert” is root in his/her restricted environment

• Multiple layers

• Access only to authorised resources

• To prevent tampering of evidences

<table>
<thead>
<tr>
<th>QEmu (VM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot (QCOW2)</td>
</tr>
<tr>
<td>Evidence</td>
</tr>
<tr>
<td>Root FS (Container)</td>
</tr>
<tr>
<td>Bind FS</td>
</tr>
<tr>
<td>Overlay FS</td>
</tr>
<tr>
<td>Live CD</td>
</tr>
</tbody>
</table>
Bitscout Architecture

"Expert"

VPN/LAN/WiFi

Chat

"Owner"

Container

RO Mapping

RW Mapping
Bitscout
Configuration & Customisation

• Prepare your personal ISO
• OpenVPN setup
• SSH setup (keys)
• IRC (will never die 😛)

Note: The Expert needs to deploy some servers (VPN, IRC, Syslog, …)
Bitscout
Configuration & Customisation

• Create new Bash scripts (Ex: to install your own tools)

• Regenerate the ISO image (.automake.sh)

• Make the ISO image available to download for your customers
Bitscout

Boot

• Burn a CD

• Or generate a USB stick

• Or add to a datastore and boot a VM (create a temporary VM and assigned the suspicious .vmdk)

• Internet access required! (DNS & UDP/1194)
Bitscout

Network Setup

ssh -i .ssh/csirt user@bitscout.vpn.company.com

"Expert"

OpenVPN automatic phone home
Bitscout
Disk Management

/dev/sda
Bitscout
Disk Management

/dev/sda
/dev/host/evidence0
Investigation
Classic Disk Tools

- Mount your filesystems
- Use classic tools
  - Loki
  - BulkExtractor
  - Log2Timeline
  - ...(*)

(*) Install and use your preferred tools
Investigation

Working with a Live System

- Sometimes, working on a live system is easier
- Again, evidences must be preserved
- QEmu (available on the Live CD) to the rescue!
- Let’s boot the infected/suspicious system in two steps:
  1. Create a snapshot of the mapped disk
  2. Boot the VM using the snapshot as main storage
Investigation
Memory Analysis

• Memory analysis is a key location for artefacts

• Performing memory acquisition is a pain because
  
  • Memory size is bigger (32GB is common even for a laptop)

• Tools not user friendly

(Memory acquisition as seen by end-users)
Need for More Tools?
Installation of Extra Tools

- Sometimes, Windows tools are required (ex: Sysinternals)
- QEmu to the rescue again!
- Boot the VM with a SMB share emulated through QEmu
- Copy files on the mount directory
- Enjoy!
Other Features
Chat between Owner & Expert

- Communication is key!
- Safe channel through the VPN
- IRC server operated by the Expert (Docker)
Other Features

Sensitive Command Approval

The following command was requested to be executed as root on host. It may be a good idea to take a photo or write it down before approval:

```
scp evidences.tgz xavier@server:/tmp
```

Your command is being reviewed. Once review is complete, you shall see output here.
Data Transfer

The Power of SSH

• Transfert data to Expert’s system

On Expert’s system:
# nc -l -p 5555 >evidence0.dd.gz
# ssh -i .ssh/csirt -R 5555:127.0.0.1:5555 user@bitscout.vpn.rootshell.be

On BitScout:
# cat /dev/host/evidence0 | gzip -9 -c | nc 127.0.0.1:5555

• Define a proxy to download through the VPN

On Expert's system:
# ssh -i .ssh/csirt -R 3128:192.168.254.8:3128 user@bitscout.vpn.rootshell.be

On BitScout:
# export http_proxy=http://127.0.01:3128
Bitscout

Credits

• Bitscout is developed and maintained by Vitaly Kamluk (@vkamluk)

• I’m a simple contributor to the project

• Want to try it / use it? https://github.com/vitaly-kamluk/bitscout
Thank You!

Q&A

! or ?