MUNI
FI

Data backup system with integrated active protection against ransomware

vSafe Agent development

Pavel Novák

Malware Attack Loop

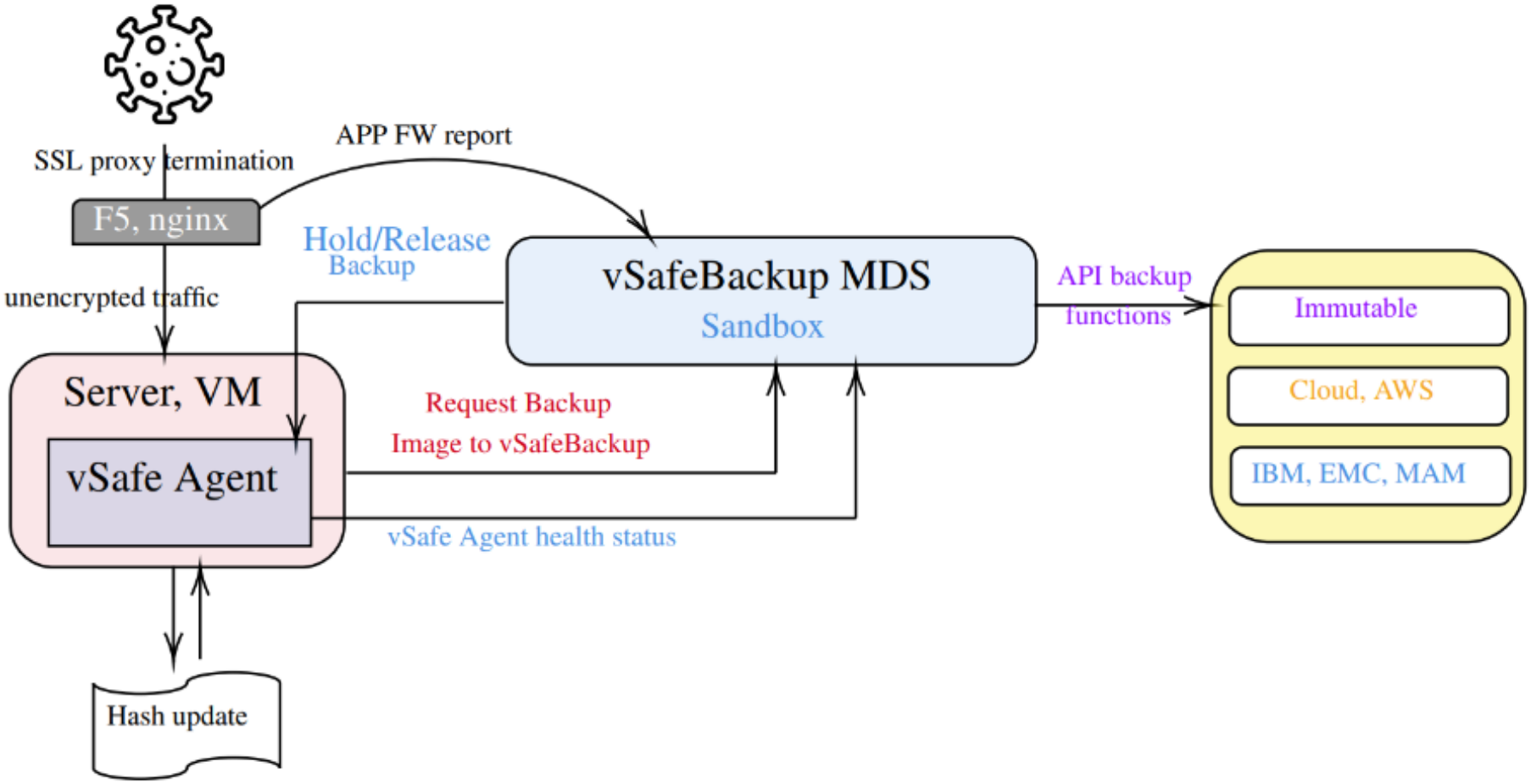
- Robust backup system → protection against ransomware attack
  - Backup diversification
  - Backup testing
- Robust backup system is not a bulletproof solution
- What if the backup is already infected with “sleeping malware”?
  - Malware can infect the system and then “sleep” for several weeks or months before detonating
  - Recovered copy is already infected and full recovery might not be possible at all
  - This technique is commonly used also to avoid dynamic inspection

vSafe Project

- Cooperation with Agora plus a.s. company
- Goal – create “intelligent” and complex system to detect ransomware in backups and avoid attack loops
- Leverages machine learning (Faiss) and hash analysis

- Similar projects:
  - Kaspersky Security for Virtualization

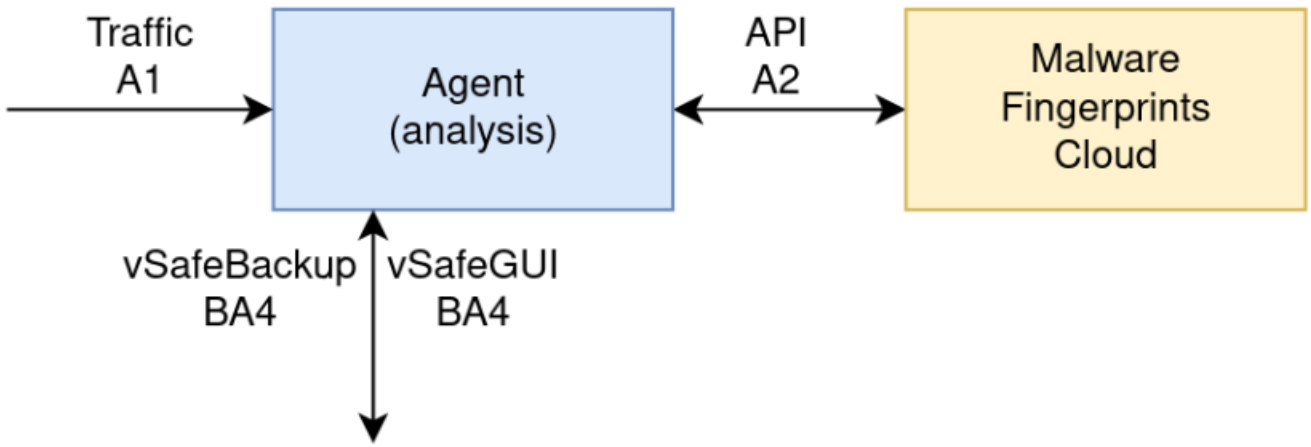
Solution Overview



MUNI FI

vSafe Agent High Level Solution

- The agent stands on the edge of the VM and monitors network traffic in real time
- Analysis of the traffic (meta)data
- The main responsibility of an agent is to extract interesting metadata in real time and look for suspicious patterns



MUNI FI

Agent vs. Agentless Solution

- Agentless solution
  - Original idea
  - Agent was supposed to be implemented as a VMware plugin
  - No need to install additional SW on the VM
  - Problems with network traffic monitoring in the VMware environment
  - Vendor specific solution

- Agent solution
  - Currently being implemented (C++ language)
  - An additional SW must be installed and run on the VM
  - Security concerns
  - Performance concerns

MUNI
FI

Agent Components

JA3

- JA3 → lightweight method to quickly detect malicious communication based on TLS handshake
- JA3s → for the server-side communication
- vSafe Agent performs real-time JA3 computation and compares it against the DB of known JA3 signatures
- Faiss model is used to quickly determine exact match of the fingerprint

C2 Communication

- Monitoring of **outgoing** traffic
- Two phases
  - Learning phase – building local DB of whitelisted IPs and processes that initiates the communication
  - Monitoring phase
- Looking for suspicious communication with potential C2 servers
- Looking for unknown processes initiating the outgoing communication

Data Scanner

- Compare hashes of incoming data against known malicious samples
- Lightweight AV solution
- OPSWAT
- CIRCL.lu
- VirusTotal


```
{
 "md5": "6A5C19D9FFE8804586E8F4C0DFCC66DE",
 "sha1":
"016CD548A5BA78015F85E2591BF6189658ACA066",
 "sha256":
"BE41E36233DD8DB2B28A109E7FC7C409E1353BF2D1710
158BBE267280E163353",
 "scan_result_history": [
  {
   "total_detected_avs": 15,
   "total_avs": 37,
   "scan_all_result_i": 1,
   "start_time": "2019-02-26T21:53:32.770Z",
   "data_id":
"ZTE3MDgyMkh5UmZGTl94cV9aUzFsSWU3aGtVNA"
  },
  {
   "total_detected_avs": 15,
   "total_avs": 37,
   "scan_all_result_i": 1,
   "start_time": "2019-02-25T23:05:26.628Z",
   "data_id":
"ZTE3MDgyMkh5UmZGTl94cV9aQnlPR2RaUFJIRQ"
  },
  {
   "total_detected_avs": 15,
   "total_avs": 37,
   "scan_all_result_i": 1,
   "start_time": "2019-02-24T09:10:11.792Z",
   "data_id":
"ZTE3MDgyMkh5UmZGTl94cV9aSHlneFNneHphQlY"
  }
 ]
}
```

Suricata/Static Analyzer

- Add Suricata module and scan incoming traffic with static rules
- Freely available Suricata rulesets
- Possibility to detect
  - Known malware C2 communication patterns
  - CVE exploits
  - Exploit scans
  - etc.
- Potential performance issues

Next Steps

- Implementation of JA3 arbiter is already finished
- Implementation of the rest of vSafe Agent components
- Integration with the rest of the vSafe project
- Performance tests
- Quality tests on infected machines

Thank you for your attention

This presentation is based upon the grant of the Ministry of the Interior of the Czech Republic, Open challenges in security research, VK01030030, Data backup and storage system with integrated active protection against cyber threats.