Contact

Alexandre GONZALVEZ

- Post-doc CNRS/IRISA
- EMSEC/CAPSULE Team
- Working on Ransomware Detection and Prevention
- *Mail*: alexandre.gonzalvez@irisa.fr

Subject

- **Title** : Ransomware and keys recovering
- **Resume** : We are looking to reverse a Ransomware's keygen from a Windows Ransomware. The goals are to build and to analyze different use cases to make an automatic recover of the cryptographic keys:
  - Simple memory analysis
  - Memory acquisition when process are running (API calls analysis)
  - After a simulated ColdBoot attack
    (Simulation of decayed keys + key recovering)
- **Tools** (Free version) : VM Windows (XP+), Python, Angr, PEStudio, x64dbg, HxD, gmpy2, IDA, CryptominiSAT, ...

References

1. Bajpai, P., & Enbody, R. (2020, June). *Memory forensics against ransomware*. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.
2. Halderman, J. A., et al. (2009). *Lest we remember: cold-boot attacks on encryption keys.* Communications of the ACM, 52(5), 91-98.
3. De Micheli, G., & Heninger, N. (2020). *Recovering cryptographic keys from partial information, by example.*
4. Kamal, A. A., & Youssef, A. M. (2010, July). *Applications of SAT solvers to AES key recovery from decayed key schedule images.* In 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies (pp. 216-220). IEEE.

Main steps

Please be careful with Ransomware: you must do all the work, all the time, at least, in a Virtual Machine ! You may be responsible for any damage suffered.

- From the MalShare website[1], download a Ransomware[2].
- Summarizing the overall functionality of this ransomware based on the overall disassembly and decompilation.
- With the help of Angr, automate the acquisition of the memory and the extraction of the keys.
- Simulate ColdBoot attack consequences over the binary.
- Recovering all the keys with different levels of corrupted memory made by a ColdBoot attack, and with the help of gmpy2 and/or CryptominiSAT.
- BONUS: Repeat all steps with different Ransomware[3]

---

[1] https://malshare.com

[2] MD5: 3cf87e475a67977ab96dff95230f8146

[3] To be defined