Jérémy BEAUME

Freelance Security Researcher, Reverse engineer, Malware Analyst,
Senior Cybersecurity Pentester and Auditor

Certifications:

BADGE RE: Reverse engineering training, partnership between Quackslab & ESIEA (2020)
OSCE: Offensive Security Certified Expert (2018)
OSCP: Offensive Security Certified Professional (2018)

Publications:

Gatewatcher blog:

- AgentTesla : https://www.gatewatcher.com/en/malware-analysis-agent-tesla/
- RecordBreaker : https://www.gatewatcher.com/en/malware-analysis-recordbreaker/
- Lyceum : https://www.gatewatcher.com/en/malware-analysis-lyceum/

Blog: https://bidouillesecurity.com (some personal research on reverse engineering)
CVE-2017-7177: Vulnerability on Suricata IPS detection (full bypass possible)

Experience:

Oct 2021-Dec 2022 (1 year): Security Researcher and Malware Analyst, Gatewatcher, Paris

- Reverse engineering of malware samples, redaction of reports and blog articles with Yara and Suricata rules.
- Development of a x86 disassembler and code analysis tool for malware detection purpose.

2016-2021 (5 years): Cybersecurity Consultant and Reverse Engineer, OPPIDA, Montigny-le-Bretonneux

Activities for clients:

- Reverse engineering: malware (APT), products (black box)
- Binary analysis software development (LLVM)
- Intrusion testing: web applications, Android, infrastructure, workstations
- Phishing campaigns (Red Team)
- CSPN evaluations (subset of Common Criteria): network probe, card reader access control, network gateway
- Code audit: JAVA
- Configuration audit: Windows, Linux, Apache, Tomcat, firewalls, switches, based on CIS and ANSSI hardening guides.
- Architecture audits
- Project manager for audits (several consultants)
- CISO assistance, vulnerability monitoring
- Courses in engineering school

Internal activities:

- Internal tool development (python), several tools created and maintained
- Management of the company's internal network (twenty servers, 2 firewalls, 6 networks)
- Internal training courses, on technical subjects
- Proofreading and technical validation of audits reports
- Recruitment: creation of challenges, technical interview of candidates
- Supervision of trainees, work-study students, junior auditors
- Pre-sales: costing, help in writing proposals, defenses
- Organization of internal events

2015-2016 (1 year): Study Engineer in Cybersecurity, Thales Services, Palaiseau

- European project concerning social engineering attacks (DOGANA)
- Network analysis of the communications of a network probe.
- Work on event correlation for attack pattern detection

Contact:

☎ +33 (0)6 41 22 15 72

✉ jeremy.beaume@protonmail.com

Personal blog and research:
https://wirediver.com

http://www.root-me.org/Jeremy-BEAUME

github.com/jeremybeaume

www.linkedin.com/in/beaumejeremy/

French nationality

Skills:

Reverse engineering:

- Malware analysis (APT)
- Manual unpacking
- Heavy client audits
- Products audits (black box)
- IDA, debuggers, intel pintools, …

Technical audits:

- Intrusion testing (web, mobile, …)
- Code
- Configuration
- Architecture
- CSPN evaluations

Programming:

- C/C++, x86-64
- LLVM
- Python
- JAVA, PHP

Embedded and electronics:

- Simple personal projects (LEDs cube),

Language:

- French (mother tongue)
- English (fluent)

Other:

- Certified Paragliding pilot
- First level of scuba diving

2015: final internship, Thales Communication and Security, Gennevilliers

- USB attack tool using a Raspberry Pi
- Encrypted traffic analysis
- IPS detection evasion (discovery of a 0-day vulnerability in Suricata)

Training:

2015: M2 SeCReTS (cryptography and network security) at Université de Versailles Saint-Quentin-En-Yvelines (UVSQ, www.master-secrets.uvsq.fr), at the same time as the 3rd year of engineering school.

2012-2015: ENSIIE engineering school (École Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise, www.ensiie.fr).