

Federico Maggi, Ph.D

Ricercatore

@ fede@maggi.cc

Italia

<https://maggi.cc>

<https://twitter.com/phretor>

Mi occupo di ricerca in ITC e cybersecurity da oltre 15 anni, con esperienza nel pubblico e nel privato, sia in veste di consulente per piccole realtà, sia nella gestione e implementazione di progetti di ricerca di rilevanza internazionale.

Attività di ricerca

Ho svolto attività di ricerca sulla sicurezza di applicazioni web, protocolli di rete, dispositivi embedded, sistemi di controllo remoto a radiofrequenza, robot industriali, autoveicoli e dispositivi mobili. Cerco sempre di seguire approcci di ricerca basati su raccolta e analisi di dati, che ho applicato con successo ad esempio all'analisi del traffico di botnet, rilevazione di ransomware, rilevazione di frodi finanziarie, rilevazione di anomalie nel traffico di rete.

Il mio lavoro è stato riconosciuto da diversi gruppi di ricerca, con cui collaboro o ho collaborato in passato. Alcune delle mie ricerche sono state riprese da media mainstream come Wired, Reuters, Forbes, Hackread, ZDNet, Bloomberg e MIT Technology Review.

Cultura ed esperienza professionale

Durante la mia carriera ho accumulato esperienza industriale e accademica, come dipendente, professore e consulente. Pertanto ho avuto moltissime occasioni di interfacciarmi con realtà molto eterogenee tra di loro: grandi multinazionali, laboratori di ricerca, piccole aziende e liberi professionisti.

La mia esperienza spazia dallo sviluppo alla ricerca applicata e teorica, comprese attività tecniche, divulgative e di revisione di prodotti scientifici. Ho esperienza nella ricerca e nell'analisi di vulnerabilità di sicurezza e ho svolto perizie sia di parte sia per i tribunali per l'analisi di evidenze di reati informatici.

Università e ricerca

Oltre al lavoro svolto in diversi gruppi di ricerca internazionali, sono stato Professore di ruolo e a contratto per diversi corsi universitari presso il Politecnico di Milano, dove gestivo un piccolo gruppo di ricerca in cybersecurity (ora famoso perché alcuni membri sono parte della squadra nazionale di hacking, i mHackeroni).

Durante questi anni ho avuto modo di interagire e gestire centinaia di studenti della laurea specialistica e di dottorato con oltre 35 lavori di tesi dal 2009 al 2016.

Strumenti e Abilità Tecniche

Attività di R&D richiedono altissima flessibilità. Di seguito alcuni degli strumenti e ambienti di sviluppo che uso spesso.

- **ML** Pandas, NumPy, SciPy, Scikit-Learn, R.
- **Dati**: MongoDB, Elastic Search, Kibana, Splunk, Hadoop.
- **Sviluppo**: Python, Bash, C/C++, Arduino, x86, LaTeX.
- **Reverse engineering**: Apktool, GDB, Ghidra, IDA Pro, Smali, ALF.
- **Web**: Flux, React, FastAPI, Flask, Django, Bootstrap.
- **Systemi operativi**: OS X, Linux, FreeBSD, Windows, Docker, AWS.
- **Hardware**: Universal Radio Hacker, GNU Radio, RFCat, KiCad.

Esperienza lavorativa

Senior Threat Researcher

Trend Micro, Inc.

07/2016–Present Italia

Professore a Contratto, Cybersecurity

Politecnico di Milano (POLIMI)

2016–2017 Italia

Visiting Professor

UC Santa Barbara (UCSB)

10/2015–03/2016 Stati Uniti

Ricercatore di Ruolo A

Politecnico di Milano (POLIMI)

2014–2016 Italia

Ricercatore

Politecnico di Milano (POLIMI)

2010–2014 Italia

Consulente

Secure Network S.r.l.

2005–2016 Italia

Consulente

B.M.S. S.r.l.

2002–2006 Italia

Educazione

Scienze e Tecniche Psicologiche

Università degli Studi di Padova (UNIPD)

10/2020 (part time) Italia

Visiting Research Scholar

UC Santa Barbara (UCSB)

2008–2009 Stati Uniti

Dottorato in Ing. Informatica

Politecnico di Milano (POLIMI)

2007–2010 Italia

Laurea in Ing. Informatica

Politecnico di Milano (POLIMI)

2001–2006 Italia

Selezione di Progetti e Pubblicazioni

Sicurezza di robot industriali

📅 2017-2020

Dal 2017 ho lavorato in collaborazione con il Politecnico di Milano sull'analisi della superficie di attacco di robot industriali, creando strumenti per la ricerca e l'analisi di vulnerabilità logiche nei programmi di automazione.

Pubblicazione: Marcello Pogliani et al. (ott. 2020). "Detecting Insecure Code Patterns in Industrial Robot Programs". In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*. Taipei, TW

Analisi su larga scala di web defacement

📅 2017-2018

Ho tracciato e analizzato il modus operandi di diverse campagne di web defacement nel corso di circa un vent'ennio, dal 1999 al 2016, individuando e classificando automaticamente l'attività di diversi gruppi cybercrime.

Pubblicazione: Federico Maggi et al. (4 giu. 2018). "Investigating Web Defacement Campaigns at Large". In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security. AsiaCCS '18*. Incheon, Republic of Korea: ACM, pp. 443-456. ISBN: 978-1-4503-5576-6. DOI: 10.1145/3196494.3196542

Analisi di malware per frodi finanziarie

📅 2017

Ho collaborato al design di uno strumento di analisi forense per l'estrazione di artefatti lasciati dai più comuni malware usati per rubare fondi da conti bancari privati, al fine di costruire automaticamente delle signature di rilevazione.

Pubblicazione: Andrea Continella et al. (2 mag. 2017). "Prometheus: Analyzing WebInject-based information stealers". In: *Journal of Computer Security Preprint*, pp. 1-21

EyePyramid

📅 2016

Basandomi su una copia dell'ordine di custodia cautelare spiccato nei confronti dei fratelli Occhionero, nel 2016 ho tracciato e analizzato l'attività di un malware noto come "EyePyramid," impiegato per attività di spionaggio negli ambienti politici e industriali italiani.

Pubblicazione: <https://github.com/eyepyrmaid/eyepyrmaid/>

Altri lavori di ricerca

- Lista completa delle pubblicazioni: <https://maggi.cc/publication>
- Interventi a convegni (inter)nazionali: <https://maggi.cc/talk>
- Advisory di sicurezza: <https://maggi.cc/advisories>

Attività di revisione scientifica

- 2020: Black Hat Europe, APWG eCrime
- 2019: EuroSec, DIMVA, APWG eCrime
- 2018: AsiaCCS, ACSAC
- 2017: ACSAC, DIMVA, AsiaCCS, AppSec EU, APWG eCrime, IMPs
- 2016: ACSAC, DIMVA
- 2015: DIMVA, TRUST, MALWARE, WISTP, EUC, AppSecEU, PPREW, ESSoS.
- 2014: PPREW, MCSoc, TRUST, DPMPC, WISTP, IJCNN.
- 2013: CyCon, ICISS,
- 2011: EC2ND, BADGERS
- 2010: COMPENG
- 2008: DIMVA

Pubblicazioni (dal 2007)

- 49 peer-reviewed conference papers
- 10 peer-reviewed journal papers
- 17 technical reports
- 36 public conference talks

Premi e riconoscimenti

- Dimitri N. Chorafas PhD Thesis Award (USD 4,000), 2010
- Best M.Sc. Thesis Nominee at Premio tesi ClusIT, 2007

Volontariato


- Blood donor.
- Mentore per LeadTheFuture.tech.
- Supporto informatico alle comunità locali.


Lingue


Italiano ●●●●●

Inglese ●●●●●

Altre informazioni

 **Contributi open source**
<https://github.com/phretor>

 **CV**
<https://maggi.cc/cv>

 **Blog personale**
<https://maggi.cc/diary>