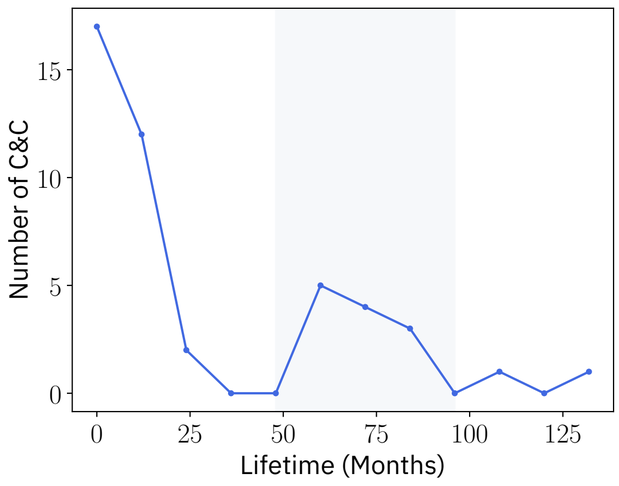
# Empirical Analysis of Lifespan Increase of IoT C&C Domains

*Daniel Uroz* [1] Ricardo J. Rodríguez [1] Carlos H. Gañán [2]

[1]Universidad de Zaragoza, Spain [2]Delft University of Technology, The Netherlands

## Preliminary Insights

- IoT C&C domains are becoming more resilient
- Significantly longer C&C lifetime than previously observed [2]




## Methodology

1049 IoT Malware Samples (2022 Q4–2023 Q1)

IoTPOT Honeypot [3]

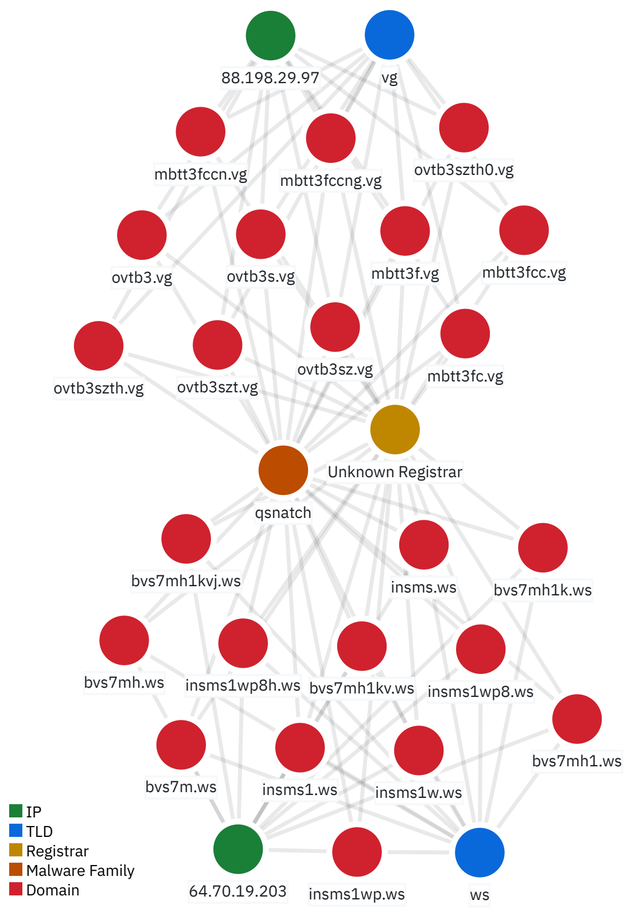
- Malware classification (AVClass) [4]
- Dynamic analysis

Contacted Domains

- Malicious (VirusTotal & DGA pattern)
- Registration (Whois & WhoisXMLAPI)
- Passive DNS (DNSDB Scout)
- Sinkholes discarded [1]

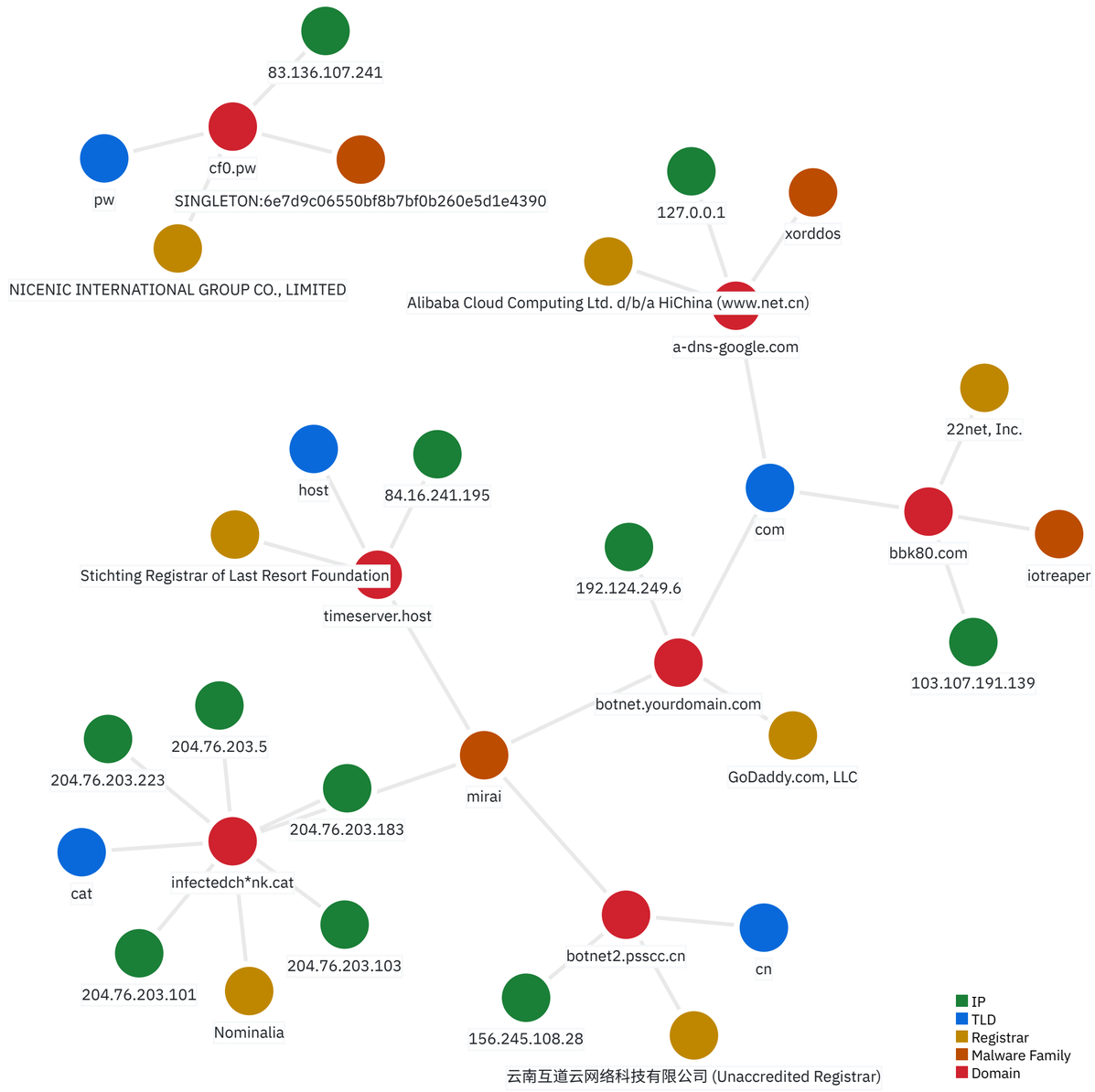
549 C&C Domains

## Active Domains Without Information




- 23 domains under `.vg` and `.ws` TLD resolve, but **registration info is missing**
  - Current and historical lack of Whois information
- No records of passive DNS but for a domain
  - `insms.ws` is **active since at least 2016 Q1**

## Active Domains




- Active domains with an **average lifetime of 5.7 years**
- The **`.com` TLD has three active domains** with different lifetimes:
  - `botnet.yourdomain.com`: 1.7 years
  - `a-dns-google.com`: 7.7 years (60% of its lifetime resolves to `127.0.0.1`)
  - `bbk80.com`: 10.9 years
- **`cf0.pw` has a lifetime of 9.4 years**:
  - Registered through the privacy provider Njalla
  - Using a privacy provider is not bulletproof; `ozxxb.eu` was also under one but lasted about a year
- `botnet2.psscc.cn` and `botnet.yourdomain.com` last 1.7 years:
  - Both have passive DNS information on the same day
  - Similar subdomain naming convention

## Cross-Information with Inactive Domains

- Common IPs in passive DNS information for three domains related to Mirai, but registered through different registrars:
  - `sdfsd.xyz`: registered through Epik LLC (IANA ID: 617)
  - `dogeatingch*nk.uno`: registered through eNom, Inc. (IANA ID: 48)
  - `infectedch*nk.cat`: registered through Nominalia (IANA ID: 76), lifetime of 1.5 years and suspended for 162 days
- Qsnatch malware samples queried a large number of domains under 130 different TLDs, but the 95% are currently unresolved
- Two domains related to IotReaper with different lifetimes:
  - `bbk80.com`: active after 10.9 years
  - `cbk99.com`: inactive domain that lasted 5.8 years and registered through Gname.com Pte. Ltd. (IANA ID: 1923)

## Future Work

- Complete this empirical study with a larger dataset
- Identify common patterns and preferences in domain selection in IoT malware
- Clarify the causes of this observed increasing C&C lifetime trend

## References

[1] Eihal Alowaisheq, Peng Wang, Sumayah A. Alrwais, Xiaojing Liao, XiaoFeng Wang, Tasneem Alowaisheq, Xianghang Mi, Siyuan Tang, and Baojun Liu. Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs. In *NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[2] Carlos Gañán, Orcun Cetin, and Michel van Eeten. An Empirical Analysis of ZeuS C&C Lifetime. In *Proceedings of the 10th Asia CCS '15*, pages 97–108, New York, NY, USA, 2015. Association for Computing Machinery.

[3] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. IoTPOT: A Novel Honeypot for Revealing Current IoT Threats. *Journal of Information Processing*, 24(3):522–533, 2016.

[4] Silvia Sebastián and Juan Caballero. AVclass2: Massive Malware Tag Extraction from AV Labels. In *Proceedings of the 36th Annual Computer Security Applications Conference*, ACSAC '20, pages 42–53. Association for Computing Machinery, 2020.

## Acknowledgments

The authors would like to thank Prof. Katsunari Yoshioka and his team for providing the experimental dataset used in this paper. The research of D. Uroz and R. J. Rodríguez was supported in part by the Spanish National Cybersecurity Institute (INCIBE) under *Proyectos Estratégicos de Ciberseguridad – CIBERSEGURIDAD EINA UNIZAR* financed by the European Union (Next Generation) through the Recovery, Transformation and Resilience Plan funds, and by the University, Industry and Innovation Department of the Government of Aragón under "Programa de Proyectos Estratégicos de Grupos de Investigación" (DisCo research group, ref. T21-23R). The research of D. Uroz was also supported by the Government of Aragón under a DGA Predoctoral Grant (period 2019–2023). The research of R. J. Rodríguez was also supported by the Spanish Ministry of Science, Innovation and Universities under "*Ayudas para la Recualificación del Sistema Universitario Español*," financed by the European Union (Next Generation) through the Recovery, Transformation and Resilience Plan funds. The research of C. H. Gañán was supported in part by the RAPID project (Grant No. CS.007) financed by the Dutch Research Council (NWO).

[1]https://reversea.me
[2]https://www.tudelft.nl/tbm/cybersecurity

2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain