Poster

Empirical Analysis of Lifespan Increase of IoT C&C Domains

Uroz, Daniel; Rodríguez, Ricardo J.; Gañán, Carlos H.

DOI
10.1145/3646547.3689670

Publication date
2024

Document Version
Final published version

Published in
IMC 2024 - Proceedings of the 2024 ACM Internet Measurement Conference

Poster: Empirical Analysis of Lifespan Increase of IoT C&C Domains

Daniel Uroz
Universidad de Zaragoza
Zaragoza, Spain

Ricardo J. Rodríguez
Universidad de Zaragoza
Zaragoza, Spain

Carlos H. Gañán
Delft University of Technology
Delft, The Netherlands

ABSTRACT

The increasing prevalence of Internet of Things (IoT) devices have made them attractive targets for malware, highlighting the critical need to understand the dynamics of IoT Command and Control (C&C). While previous research observed short-lived C&Cs, recent observations indicate that the lifespan of domain names linked to IoT botnets is extending, deviating from previously recorded survival rates. To understand and characterize this emerging trend, we collected and examined 1049 IoT malware samples from late 2022 to early 2023, identifying 549 unique domains contacted by these samples. Domains were classified as malicious if detected by VirusTotal or followed a Domain Generation Algorithm pattern. Using data from `WhoisXMLAPI` and `DNSDB Scout`, we analyzed registration information and historical DNS resolutions, and identified relationships. Our findings reveal that the majority of C&C domains belong to `Qsnatch` and `Mirai` malware families, with an average lifespan of 2.7 years. Notably, seven active domains had an average lifespan of 5.7 years. We also observed a significant number of domains under the `.vg` and `.ws` TLDs, but with lack of passive DNS and registration information.

ACM Reference Format:
Daniel Uroz, Ricardo J. Rodríguez, and Carlos H. Gañán. 2024. Poster: Empirical Analysis of Lifespan Increase of IoT C&C Domains. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3646547.3689670

1 MOTIVATION

Since the inception of the most notorious IoT botnet, `Mirai` [3], in 2016, botnet masters have continually evolved their malware. While previous research characterized IoT botnets infrastructure as disposable and short-lived [4], current IoT malware families have developed methods to improve their persistence and stability. To determine to what extend this trend of increasing lifespan is common, we conduct an empirical analysis of IoT Command and Control (C&C) domains. We find an anomalous increase in the lifespan of several IoT C&C domains, which does not follow the domain survival rates discussed in previous research [4].

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689670

2 METHODOLOGY

To identify IoT C&C domains, we first collected 1049 IoT malware samples actively distributed during 2022 Q4 to 2023 Q1 (a total of 85 days) through the IoTPOT honeypot [5]. Each malware sample was dynamically run and classified using AVClass [6]. We then conducted an empirical study of 549 unique domains for which DNS traffic was present in the traces.

We consider a domain to be a *true C&C domain* if at least one security vendor on VirusTotal [1] has detected it as malicious. When a domain has not been seen in VirusTotal, we consider it to be malicious if it follows a Domain Generation Algorithm (DGA) pattern. Specifically, a domain is tagged as malicious if two or more domain names are requested in sequence very quickly (in particular, in less than 1 second) and the domain names are very similar (i.e., they only change in a few characters between them).

For each C&C domain, we obtain its registry information through whois, and complemented this information with historical registration information provided by `WhoisXMLAPI`[1]. For historical resolution of IPs and name servers associated with the domain, we collect the information through `DNSDB Scout`'s passive DNS service[2]. All collected data was collected as of 2024/05/14, and we request all available information provided by `DNSDB Scout` through 2024/06/04.

With all the data collected, we analyze related graphs through `Neo4J`[3] to see relationships between C&C domains contacted by different malware families, registrar preferences and TLD choice, and shared IPs between different domains. The information on the name servers associated with the domain allows us to discard sinkhole domains thanks to the list given in [2], along with the name servers of `ns[1-3].sinkhole.caad.fkie.fraunhofer.de`.

3 DISCUSSION OF RESULTS

3.1 Domain Lifetime

The majority of the 549 domains contacted belong to `Qsnatch` (91%) and `Mirai` (7%) malware families. Only 45 of the 549 domains contained passive DNS information, with an average lifespan of 2.7 years. The lifetime of domains that have resolved at least once is shown in Figure 1.

3.2 Active Domains

There are currently seven active C&C domains, and all of them with very long lifetimes, averaging 5.7 years. As for the `.com` TLD, there are three domains that are still alive: `botnet.yourdomain.com`, `a-dns-google.com`, and `bbk80.com`, with lifetimes of 1.6, 7.7, and 10.9 years, respectively. The second domain currently resolves to

[1] https://whois.whoisxmlapi.com (accessed on July 12, 2024).
[2] https://scout.dnsdb.info (accessed on July 12, 2024).
[3] https://neo4j.com (accessed on July 12, 2024).

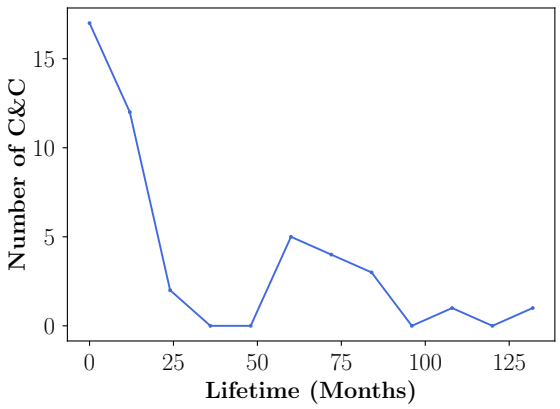

Figure 1: Uptime of analyzed domains that have resolved at least once in their lifetime.

`127.0.0.1`. In particular, 60% of its lifetime is resolving to `localhost` address.

Eleven domains under the `.vg` TLD and twelve under the `.ws` TLD do not provide registration information, although all are currently resolving. Similarly, WhoisXMLAPI has no records. DNSDB Scout returns data for only one of these twenty-three domains, meaning that the `insms.ws` domain has been active since at least the first quarter of 2016. All domains appear to follow a DGA naming convention. More research is needed to find out the reason for the lack of passive DNS and registration information for domains under these TLDs.

Another example of long lifespan is `cf0.pw`, which currently lasts 9.4 years. In this case, the domain is registered through the privacy provider Njalla. However, using a privacy provider is not bulletproof, as we found that the `ozxxb.eu` domain was also under the same provider, but it lasted for about a year (specifically from 2022 Q3 to 2023 Q3).

Two of the still active domains belong to the Mirai malware family and began to have passive DNS information on the same day and with similar subdomain naming convention: `botnet2.psscc.cn` and `botnet.yourdomain.com`, both last approximately 1.7 years. The first domain is registered with a registrar without an ICANN-accredited registrar ID, and the second is registered with a subdomain service provider.

3.3 Cross-information with Inactive Domains

There are common IPs in the passive DNS information for the domains `sdfsd.xyz`, `dogeatingchink.uno`, and `infectedchink.cat`, all related to `Mirai` but registered through different registrars. The `infectedchink.cat` is still active after 1.5 years under the registrar `Nominalia` (IANA ID: 76), although it suffered a suspension of 162 days from 2023 Q4 to 2024 Q1, when it resumed its activity according to its historical name server information.

In the case of the `Qsnatch` malware family, we found that the malware samples were querying a large number of domains under 130 different TLDs, but the 95% are currently unresolved. In fact, the only domains currently being resolved are those previously discussed under `.vg` and `.ws` TLDs. There is also information for less durable domains under other TLD (such as `.com`, `.org`, or `.mx`, to name a few), with an average lifespan of 7 months and 4 out of 8 being sinkholed.

Finally, the `Iotreaper` malware family has two domains that share common IPs. Specifically, the active domain `bbk80.com` discussed above and the inactive domain `cbk99.com`, which lasted 5.8 years and was registered through the registrar `Gname.com Pte. Ltd.` (IANA ID 1923).

4 PRELIMINARY INSIGHT & FUTURE WORK

This study shows that IoT C&C domains are becoming more resilient, with a significantly longer lifetime than previously observed. Notably, domains under the `.com`, `.vg`, and `.ws` TLDs remain active for several years, challenging previous research on their typically ephemeral nature. Our goal is to complete this empirical study with a larger dataset of contacted domains to identify other common patterns and preferences in domain selection in IoT malware and clarify the causes of this observed increasing C&C lifetime trend.

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).

REFERENCES

[1] [n. d.]. VirusTotal. [Online; https://www.virustotal.com/]. Accessed on July 11, 2024..

[2] Eihal Alowaisheq, Peng Wang, Sumayah A. Alrwais, Xiaojing Liao, XiaoFeng Wang, Tasneem Alowaisheq, Xianghang Mi, Siyuan Tang, and Baojun Liu. 2019. 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.

[3] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*. 1093–1110.

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

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

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