LIÈGE université Library

https://lib.uliege.be

https://matheo.uliege.be

Master thesis : Honeypot Evolution: Creation Guidelines and Implementation for Third-Party Application Behavior Study Using Cisco SecureX as Monitoring Toolkit

Auteur : Deflandre, Guilian
Promoteur(s) : Donnet, Benoît; 6116
Faculté : Faculté des Sciences appliquées
Diplôme : Master : ingénieur civil en informatique, à finalité spécialisée en "computer systems security"
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/14580

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Honeypot Evolution: Creation Guidelines and Implementation for Third-Party Application Behavior Study Using Cisco SecureX as Monitoring Toolkit - Appendices

University of Liège

School of Engineering and Computer Science

Academic Supervisor: Prof. Benoît DONNET

Co-Supervisor: Hugues DE PRA

Master's thesis carried out to obtain
the degree of Master of Science in
Computer Science and Engineering

DEFLANDRE Guilian

G.Deflandre@student.uliege.be

Acknowledgements

First, I would like to thank my academic supervisor, Professor Benoît Donnet, for his availability, his advices and his support during this thesis, my university training and even beyond these scopes. I also express my gratitude to my co-supervisor, Hugues de Pra, for his expertise and his trust. I am grateful as well to the entire Cisco team that allowed me to live this exceptional professional experience within this unique company. In particular, many thanks to Senad Aruc who makes this work possible, to Evgeny Mirolyubov and Christopher Van Der Made for their technical advices regarding Cisco's solutions and the rest of the Cisco Amsterdam team for their warm welcome. I want to personally thank Chris Sanders too, who did not hesitate to share his broad experience about honeypots.

Further, I would like to take this opportunity to express my special thanks to my elder brother, without whom I would probably never have got where I am today. His wise advices and constant encouragements have been changing me into a better person every day, for a long time now.

Many thanks also to my girlfriend for her unwavering support and her patience during this process. To all my friends, who have not hesitated to spend time for proofreading or to share their honest opinions regarding my approaches, I also want to convey my deep gratitude. I am aware of being rich in those around me and I will never be grateful enough for their presence in my life.

I am finally very thankful to all the people who directly or indirectly contributed to the completion of this thesis, which is also somehow theirs. To all of them, my sincere thanks.

Abstract

In a world where the cyber threat has never been higher[1, 2], getting to know the adversary is more important than ever. While traditional computer security technologies strive to keep insiders outside the perimeter they defend, honeypots try at all cost to be the primary targets of cyber attacks. They attempt not only to detect these last but also to collect useful information about the black hat community. This thesis aims at defining strong frameworks to create and monitor efficiently the limitless technology that honeypots represent. Through two practical implementations, these frameworks will be used to create two different type of these devices. A first low interaction honeypot will simulate Microsoft's remote desktop protocol for both detection and research. The second is a medium interaction research one feigning an Elastic stack deployment. Relying on the elaborated powerful monitoring framework, efficient strategies will be elaborated using industry IT toolkit to ensure the proper monitoring of these security tools, thus drastically reducing the risk which is too often unfairly associated with them. The data accumulated by these two deployments will show that in a short amount of time, a significant quantity of valuable information, not only for the research community but also for the corporate world, can already be collected by these devices, pointing to their promising future.

Contents

List of Acronyms and Abbreviations

API	Application Programming Interface
ARP	Address Resolution Protocol
ASN	Autonomous System Number
AS	Autonomous System
AV	Antivirus
BYOD	Bring your own Device
CAIDA	Center for Applied Internet Data Analysis
CA	Certificate Authority
CEST	Central European Summer Time
CLI	Command-Line Interface
CSP	Cloud Service Provider
DNS	Domain Name System
DoS	Denial-of-Service
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
HaaS	Honeypot as a Service
IC3	Internet Crime Complaint Center
IDS	Intrusion Detection System
IP	Internet Protocol
IQR	Interquartile Range
ISP	Internet Service Provider
ITU-T	ITU Telecommunication Standardization Sector
ITU	International Telecommunication Union
IT	Information Technology
IaaS	Infrastructure as a Service
IoT	Internet of Things
L&M	Logging and Monitoring
MFA	Multi-Factor Authentication

NIB	National Internet Backbone
NIST	National Institute of Standards and Technology
OS	Operating System
PDF	Portable Document Format
PNG	Portable Network Graphics
RDP	Remote Desktop Protocol
REST	Representational State Transfer
SME	Small and Medium-Sized Enterprise
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TPDU	Transport Protocol Data Units
TPKT	Transport Packet
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
XDR	Extended Detection and Response

Appendices

A.1 Cisco Laboratory Network Architecture

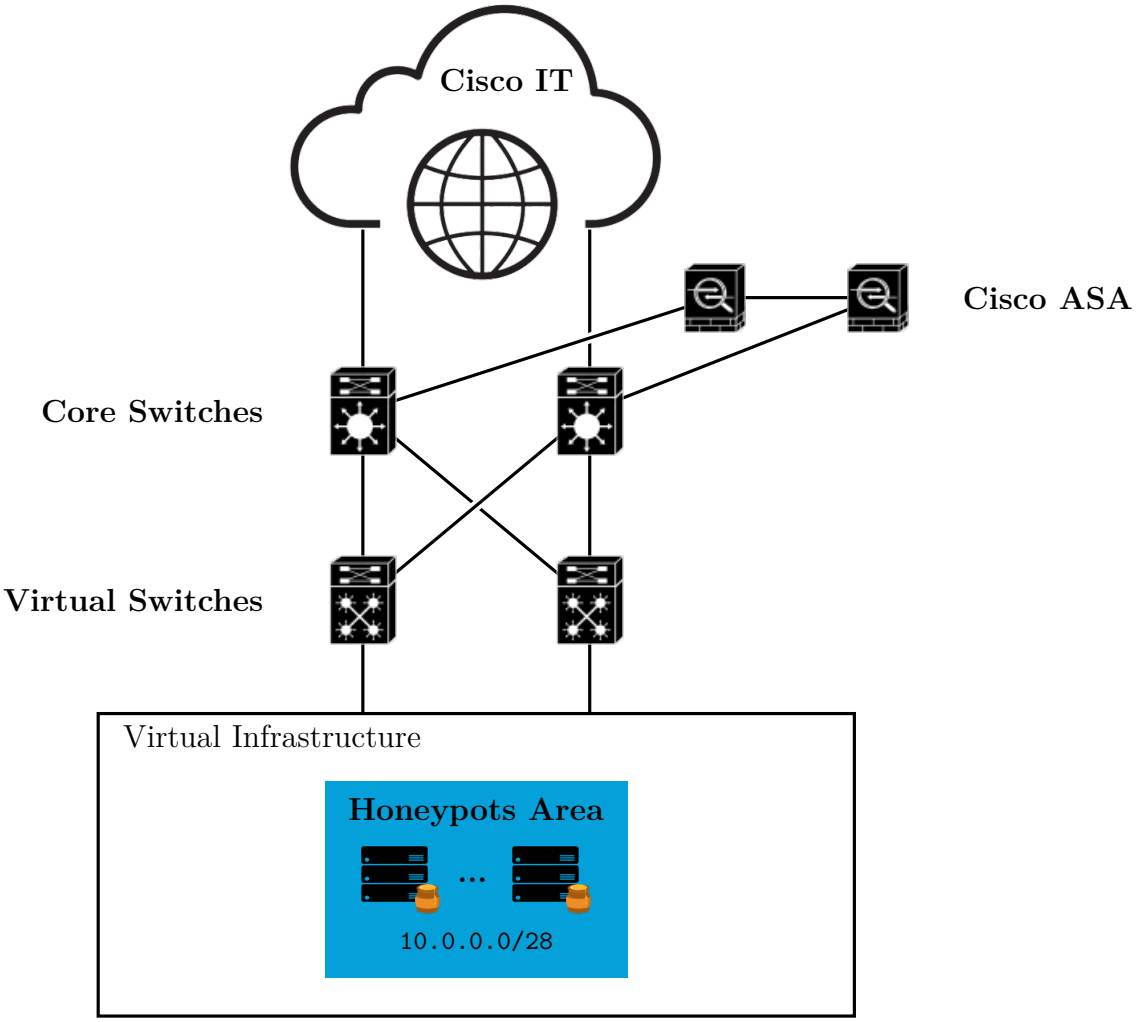

FIGURE A.1.1
Global overview of the Cisco laboratory from Diegem and the placement of the honeypots deployed for this thesis (blue zone). Cisco is its own network provider, managed by Cisco IT which handles most of the network security. Two Cisco Adaptive Security Appliance (ASA) are however also present in the lab infrastructure for this purpose.

A.2 University of Liège Network Architecture

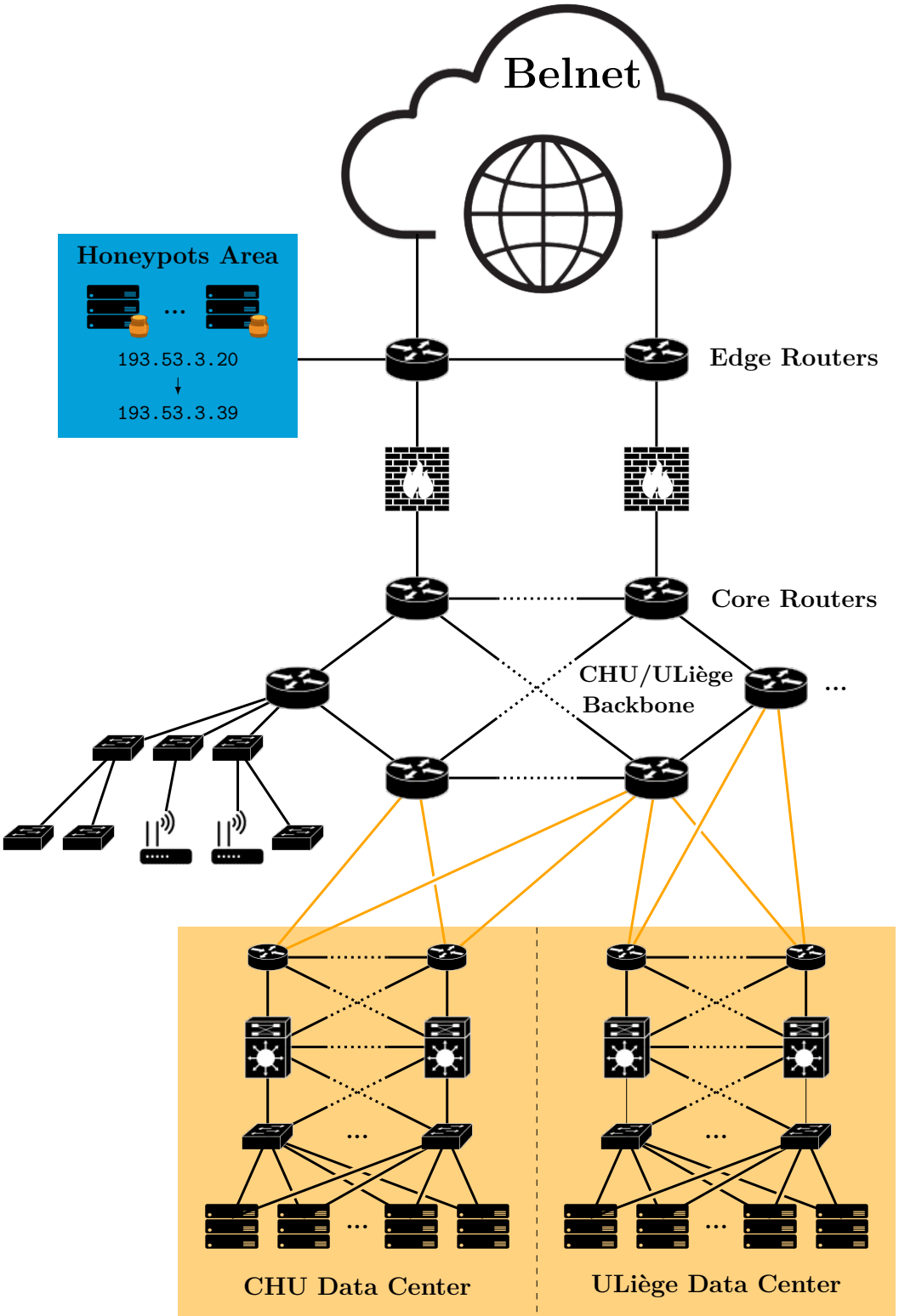

FIGURE A.2.1

Global overview of the university of Liège network and the placement of the honeypots deployed for this thesis (blue zone). Only one LAN has been illustrated here but each of the router in the backbone can be attached to several of them. The dotted lines illustrate that the exact number of devices is not represented on this diagram. In orange are voluntarily depicted ULiège's data center area and their interconnections in the university network.

A.3 University of Liège's Centralized Log Management Infrastructure

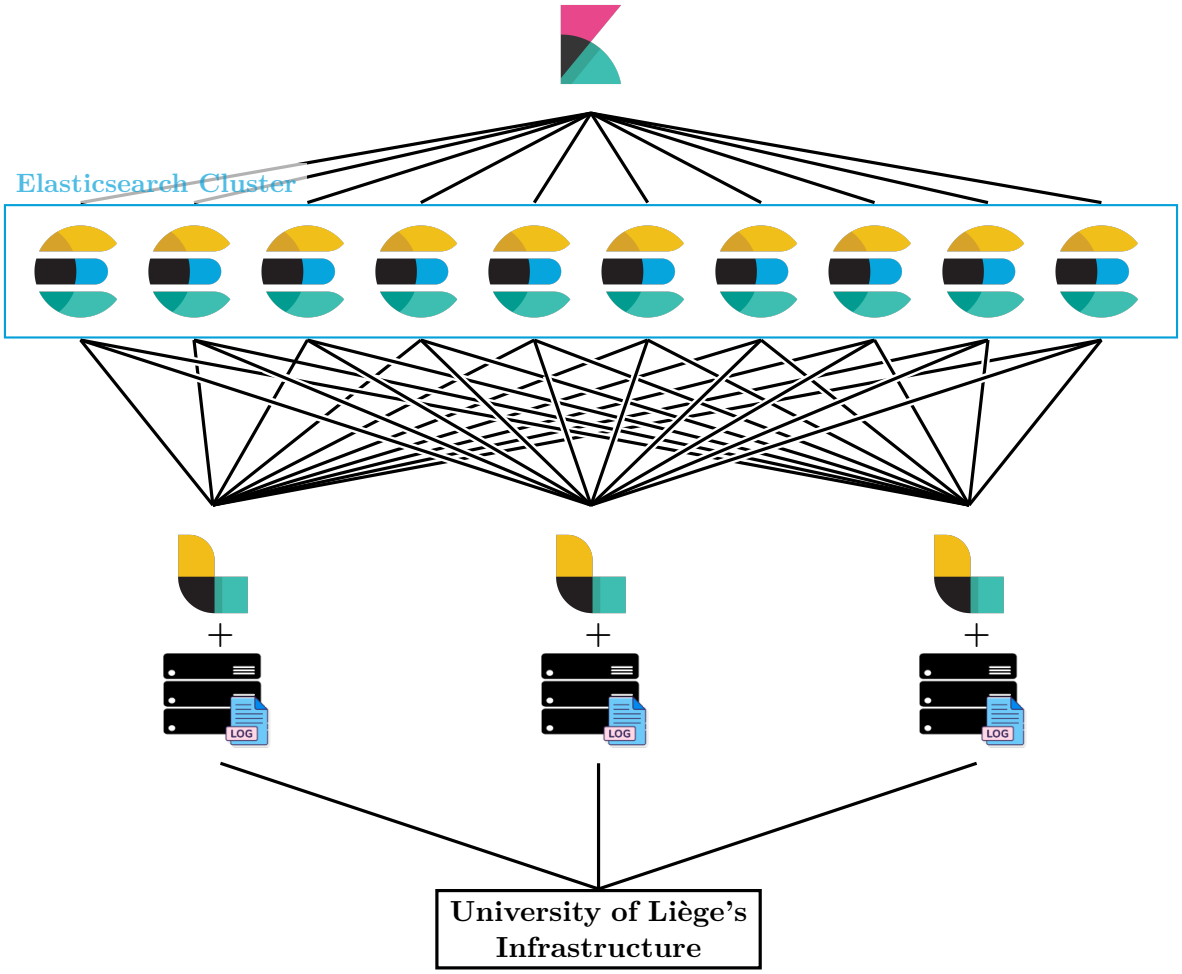

FIGURE A.3.1

Global overview of the university of Liège ELK stack deployments. Each of the syslog servers (using Rsyslog, ***a.k.a.*** the rocket-fast system for log processing) is fed with logs coming from devices and applications of the university of Liège's infrastructure. Logstash crawl the logs in these servers, collecting the ones matching its configured rules, reformatting them and sending them to the Elasticsearch cluster (framed in blue). This cluster is made of 10 Elasticsearch nodes storing the collected infrastructure logs, 5 placed in ULiège's data center and the 5 other in the CHU one (***cf.*** FIGURE A.2.1). Finally, the single Kibana node connects to each node of the Elasticsearch cluster, offering the user friendly interface of the centralized log management infrastructure.

B.1 Identified IP Sub-networks

Subnets	IP Address	Proportion of IP Addresses
5.253.204.0/24	5.253.204.105, 5.253.204.139	2.19%
103.128.0.0/9	103.197.196.238, 103.136.83.233	1.46%
181.214.206.0/24	181.214.206.102, 181.214.206.113, 181.214.206.131, 181.214.206.155, 181.214.206.163, 181.214.206.174, 181.214.206.185, 181.214.206.186, 181.214.206.187, 181.214.206.191, 181.214.206.200, 181.214.206.204, 181.214.206.212, 181.214.206.236, 181.214.206.243, 181.214.206.70, 181.214.206.93	12.409%
192.241.208.0/20	192.241.211.225, 192.241.212.173, 192.241.220.232, 192.241.221.151, 192.241.222.113, 192.241.222.195, 192.241.223.182, 192.241.213.94, 192.241.222.69, 192.241.223.13	7.299%
104.152.52.96/27	104.152.52.101, 104.152.52.124	1.46%
212.102.32.0/19	212.102.34.247, 212.102.35.12, 212.102.35.135, 212.102.35.139, 212.102.35.142, 212.102.35.146, 212.102.35.152, 212.102.35.153, 212.102.35.29, 212.102.35.30, 212.102.57.214	8.029%
36.93.18.216/29	36.93.18.219, 36.93.18.220	1.46%
45.144.0.0/12	45.146.164.28, 45.155.204.28	1.46%
45.93.201.0/24	45.93.201.224, 45.93.201.29	1.46%
91.128.0.0/9	91.188.10.146, 91.222.246.75	1.46%

117.224.0.0/11	117.239.226.89, 117.254.110.10, 117.254.110.11, 117.254.110.12, 117.254.110.13, 117.254.110.14, 117.254.110.15, 117.254.110.16, 117.254.110.17, 117.254.110.18, 117.254.110.19, 117.254.110.20, 117.254.110.21, 117.254.110.22, 117.254.110.23, 117.254.110.24, 117.254.110.25, 117.254.110.26, 117.254.110.27, 117.254.110.28, 117.254.110.29, 117.254.110.30, 117.254.110.31, 117.254.110.32, 117.254.110.33, 117.254.110.34, 117.254.110.35, 117.254.110.36, 117.254.110.37, 117.254.110.38, 117.254.110.39, 117.254.110.40, 117.254.110.41, 117.254.110.42, 117.254.110.43, 117.254.110.44, 117.254.110.45, 117.254.110.46, 117.254.110.47, 117.254.110.48, 117.254.110.49, 117.254.110.50, 117.254.110.51, 117.254.110.52, 117.254.110.53, 117.254.110.7, 117.254.110.8, 117.254.110.9	35.036%
185.192.0.0/11	185.193.56.25, 185.222.56.78	1.46%
191.96.168.0/24	191.96.168.176, 191.96.168.192, 191.96.168.197, 191.96.168.226, 191.96.168.254, 191.96.168.87, 191.96.168.90, 191.96.168.99	6.569%
195.78.54.0/24	195.78.54.185, 195.78.54.223, 195.78.54.225, 195.78.54.252, 195.78.54.88	4.38%

TABLE B.1.1

Identified sub-networks in the data set collected by the RDP honeypot placed in the public Internet and the respective list of IP addresses used to identify them. These sub-networks has been derived from the IP addresses having initiated a connection with the honeypot.

Subnets	IP Address	Proportion of IP Addresses
192.241.192.0/18	192.241.213.19, 192.241.222.143, 192.241.214.115, 192.241.212.81, 192.241.225.67, 192.241.225.180, 192.241.222.155, 192.241.222.91, 192.241.214.251, 192.241.213.83, 192.241.214.25, 192.241.215.230, 192.241.213.56, 192.241.212.70, 192.241.224.90, 192.241.225.82, 192.241.214.10, 192.241.226.93, 192.241.226.127, 192.241.212.191, 192.241.223.144, 192.241.202.128, 192.241.217.171, 192.241.218.80, 192.241.218.109, 192.241.216.216, 192.241.211.140, 192.241.216.163, 192.241.213.107, 192.241.223.56, 192.241.214.247, 192.241.219.60, 192.241.213.115, 192.241.219.83, 192.241.220.48, 192.241.219.66	92.308%
104.152.52.0/24	104.152.52.101, 104.152.52.153	5.128%

TABLE B.1.2

Identified sub-networks in the data set collected by the Elasticsearch node 1 of the Elastic honeypot placed in the public Internet and the respective list of IP addresses used to identify them. These sub-networks has been derived from the IP addresses having initiated a connection with the honeypot.

Subnets	IP Address	Proportion of IP Addresses
5.128.0.0/9	5.253.204.105, 5.187.49.188	2.439%
104.152.52.0/24	104.152.52.101, 104.152.52.153	2.439%
35.192.0.0/10	35.195.93.98, 35.233.62.116	2.439%

192.241.192.0/18	192.241.202.128, 192.241.207.140, 192.241.211.140, 192.241.211.188, 192.241.212.191, 192.241.212.219, 192.241.212.220, 192.241.213.107, 192.241.213.115, 192.241.213.194, 192.241.213.196, 192.241.214.115, 192.241.214.186, 192.241.214.247, 192.241.214.251, 192.241.215.106, 192.241.215.230, 192.241.216.163, 192.241.216.216, 192.241.217.104, 192.241.217.118, 192.241.217.133, 192.241.217.171, 192.241.218.109, 192.241.220.132, 192.241.220.201, 192.241.220.225, 192.241.221.137, 192.241.221.149, 192.241.222.155, 192.241.222.177, 192.241.222.231, 192.241.222.234, 192.241.223.144, 192.241.224.156, 192.241.224.198, 192.241.225.142, 192.241.225.146, 192.241.225.163, 192.241.225.180, 192.241.226.127, 192.241.212.70, 192.241.212.76, 192.241.212.81, 192.241.213.19, 192.241.213.35, 192.241.213.56, 192.241.213.83, 192.241.214.10, 192.241.214.25, 192.241.216.53, 192.241.216.55, 192.241.216.76, 192.241.218.16, 192.241.218.80, 192.241.219.60, 192.241.219.66, 192.241.219.83, 192.241.220.4, 192.241.220.48, 192.241.221.54, 192.241.222.91, 192.241.223.44, 192.241.223.56, 192.241.223.96, 192.241.224.53, 192.241.224.90, 192.241.225.67, 192.241.225.82, 192.241.226.24, 192.241.226.52, 192.241.226.93	87.805%

TABLE B.1.3

Identified sub-networks in the data set collected by the Elasticsearch node 2 of the Elastic honeypot placed in the public Internet and the respective list of IP addresses used to identify them. These sub-networks has been derived from the IP addresses having initiated a connection with the honeypot.

Subnets	IP Address	Proportion of IP Addresses
5.184.0.0/13	5.187.189.246, 5.188.210.227	2.632%

192.241.192.0/18	192.241.207.235, 192.241.208.242, 192.241.211.133, 192.241.212.102, 192.241.212.113, 192.241.212.134, 192.241.212.160, 192.241.212.219, 192.241.212.227, 192.241.212.230, 192.241.213.143, 192.241.214.222, 192.241.214.239, 192.241.216.128, 192.241.217.154, 192.241.217.227, 192.241.219.213, 192.241.222.113, 192.241.222.195, 192.241.223.101, 192.241.223.202, 192.241.223.207, 192.241.224.191, 192.241.225.100, 192.241.225.224, 192.241.225.240, 192.241.192.34, 192.241.196.83, 192.241.209.85, 192.241.212.70, 192.241.212.75, 192.241.212.97, 192.241.213.19, 192.241.213.80, 192.241.214.40, 192.241.214.50, 192.241.214.65, 192.241.215.35, 192.241.216.32, 192.241.220.12, 192.241.221.43, 192.241.222.4, 192.241.222.90, 192.241.223.11, 192.241.223.55, 192.241.223.66, 192.241.223.72, 192.241.224.61, 192.241.224.67, 192.241.225.16, 192.241.225.29, 192.241.225.56, 192.241.225.67, 192.241.226.62, 192.241.226.77	72.368%

TABLE B.1.4

Identified sub-networks in the data set collected by the Kibana node of the Elastic honeypot placed in the public Internet and the respective list of IP addresses used to identify them. These sub-networks has been derived from the IP addresses having initiated a connection with the honeypot.

B.2 Identified Autonomous Systems

AS Number	IP Addresses	IP Address Count	Proportion of IP Addresses
174	191.96.168.176, 191.96.168.192, 191.96.168.197, 191.96.168.226, 191.96.168.254, 191.96.168.87, 191.96.168.90, 191.96.168.99, 191.96.185.224, 195.78.54.185, 195.78.54.223, 195.78.54.225, 195.78.54.252, 195.78.54.88	14	10.219%

3257	181.214.206.102, 181.214.206.113, 181.214.206.131, 181.214.206.155, 181.214.206.163, 181.214.206.174, 181.214.206.185, 181.214.206.186, 181.214.206.187, 181.214.206.191, 181.214.206.200, 181.214.206.204, 181.214.206.212, 181.214.206.236, 181.214.206.243, 181.214.206.70, 181.214.206.93	17	12.409%
3269	80.21.180.50	1	0.73%
3462	220.128.240.221	1	0.73%
4192	129.150.99.216	1	0.73%
5384	2.50.147.164	1	0.73%
7713	36.93.18.219, 36.93.18.220	2	1.46%
7922	50.215.30.198	1	0.73%
8151	187.195.37.141, 201.103.58.1	2	1.46%
8452	41.41.117.44	1	0.73%
9009	5.253.204.105, 5.253.204.139	2	1.46%
14987	104.152.52.101, 104.152.52.124	2	1.46%
15924	195.87.254.102	1	0.73%
17623	112.91.139.237	1	0.73%
24560	106.214.116.85	1	0.73%
36352	107.172.13.161, 198.23.149.111, 23.94.255.80	3	2.19%
42398	185.193.56.25	1	0.73%
43279	91.188.10.146	1	0.73%
45102	8.214.18.137	1	0.73%
45769	114.79.151.170	1	0.73%
49505	45.146.164.28, 45.155.204.28	2	1.46%
50340	45.93.201.224, 45.93.201.29	2	1.46%
51167	207.180.210.75	1	0.73%
51447	185.222.56.78	1	0.73%
52180	91.222.246.75	1	0.73%
60068	212.102.34.247	1	0.73%
134714	103.197.196.238	1	0.73%
137678	103.136.83.233	1	0.73%
208091	87.251.75.64, 94.232.42.169	2	1.46%
211632	5.181.86.17	1	0.73%

9829	117.239.226.89, 117.254.110.10, 117.254.110.11, 117.254.110.12, 117.254.110.13, 117.254.110.14, 117.254.110.15, 117.254.110.16, 117.254.110.17, 117.254.110.18, 117.254.110.19, 117.254.110.20, 117.254.110.21, 117.254.110.22, 117.254.110.23, 117.254.110.24, 117.254.110.25, 117.254.110.26, 117.254.110.27, 117.254.110.28, 117.254.110.29, 117.254.110.30, 117.254.110.31, 117.254.110.32, 117.254.110.33, 117.254.110.34, 117.254.110.35, 117.254.110.36, 117.254.110.37, 117.254.110.38, 117.254.110.39, 117.254.110.40, 117.254.110.41, 117.254.110.42, 117.254.110.43, 117.254.110.44, 117.254.110.45, 117.254.110.46, 117.254.110.47, 117.254.110.48, 117.254.110.49, 117.254.110.50, 117.254.110.51, 117.254.110.52, 117.254.110.53, 117.254.110.7, 117.254.110.8, 117.254.110.9	48	35.036%
14061	192.241.211.225, 192.241.212.173, 192.241.220.232, 192.241.221.151, 192.241.222.113, 192.241.222.195, 192.241.223.182, 164.92.202.31, 192.241.213.94, 192.241.222.69, 192.241.223.13	11	8.029%
212238	212.102.35.12, 212.102.35.135, 212.102.35.139, 212.102.35.142, 212.102.35.146, 212.102.35.152, 212.102.35.153, 212.102.35.29, 212.102.35.30, 212.102.57.214	10	7.299%

TABLE B.2.1

Identified autonomous system numbers for the IP addresses in the data set collected by the RDP honeypot placed in the public Internet.

AS Number	IP Addresses	IP Address Count	Proportion of IP Addresses
14061	192.241.213.19, 192.241.222.143, 192.241.214.115, 192.241.212.81, 192.241.225.67, 192.241.225.180, 192.241.222.155, 192.241.222.91, 192.241.214.251, 192.241.213.83, 192.241.214.25, 192.241.215.230, 192.241.213.56, 192.241.212.70, 192.241.224.90, 192.241.225.82, 192.241.214.10, 192.241.226.93, 192.241.226.127, 192.241.212.191, 192.241.223.144, 192.241.202.128, 192.241.217.171, 192.241.218.80, 198.199.114.60, 192.241.218.109, 192.241.216.216, 192.241.211.140, 192.241.216.163, 192.241.213.107, 192.241.223.56, 192.241.214.247, 192.241.219.60, 192.241.213.115, 192.241.219.83, 192.241.220.48, 192.241.219.66	37	94.872%
14987	104.152.52.101, 104.152.52.153	2	5.128%

TABLE B.2.2

Identified autonomous system numbers for the IP addresses in the data set collected by the Elasticsearch node 1 of the Elastic honeypot placed in the public Internet.

AS Number	IP Addresses	IP Address Count	Proportion of IP Addresses
9009	5.253.204.105	1	1.22%
10439	66.240.192.138	1	1.22%
14987	104.152.52.101, 104.152.52.153	2	2.439%
15169	34.140.248.32, 35.233.62.116	2	2.439%
56048	223.71.167.163	1	1.22%
197155	5.187.49.188	1	1.22%
396982	35.195.93.98	1	1.22%

14061	192.241.202.128, 192.241.207.140, 192.241.211.140, 192.241.211.188, 192.241.212.191, 192.241.212.219, 192.241.212.220, 192.241.213.107, 192.241.213.115, 192.241.213.194, 192.241.213.196, 192.241.214.115, 192.241.214.186, 192.241.214.247, 192.241.214.251, 192.241.215.106, 192.241.215.230, 192.241.216.163, 192.241.216.216, 192.241.217.104, 192.241.217.118, 192.241.217.133, 192.241.217.171, 192.241.218.109, 192.241.220.132, 192.241.220.201, 192.241.220.225, 192.241.221.137, 192.241.221.149, 192.241.222.155, 192.241.222.177, 192.241.222.231, 192.241.222.234, 192.241.223.144, 192.241.224.156, 192.241.224.198, 192.241.225.142, 192.241.225.146, 192.241.225.163, 192.241.225.180, 192.241.226.127, 192.241.212.70, 192.241.212.76, 192.241.212.81, 192.241.213.19, 192.241.213.35, 192.241.213.56, 192.241.213.83, 192.241.214.10, 192.241.214.25, 192.241.216.53, 192.241.216.55, 192.241.216.76, 192.241.218.16, 192.241.218.80, 192.241.219.60, 192.241.219.66, 192.241.219.83, 192.241.220.4, 192.241.220.48, 192.241.221.54, 192.241.222.91, 192.241.223.44, 192.241.223.56, 192.241.223.96, 192.241.224.53, 192.241.224.90, 192.241.225.67, 192.241.225.82, 192.241.226.24, 192.241.226.52, 192.241.226.93, 198.199.114.60	73	89.024%

TABLE B.2.3

Identified autonomous system numbers for the IP addresses in the data set collected by the Elasticsearch node 2 of the Elastic honeypot placed in the public Internet.

AS Number	IP Addresses	IP Address Count	Proportion of IP Addresses
4134	113.103.80.48, 123.52.172.151, 171.13.39.193	3	3.947%
5466	86.42.233.73	1	1.316%

5483	5.187.189.246	1	1.316%
6939	184.105.139.67	1	1.316%
9121	194.54.56.42	1	1.316%
10292	208.138.25.30	1	1.316%
14061	192.241.207.235, 192.241.208.242, 192.241.211.133, 192.241.212.102, 192.241.212.113, 192.241.212.134, 192.241.212.160, 192.241.212.219, 192.241.212.227, 192.241.212.230, 192.241.213.143, 192.241.214.222, 192.241.214.239, 192.241.216.128, 192.241.217.154, 192.241.217.227, 192.241.219.213, 192.241.222.113, 192.241.222.195, 192.241.223.101, 192.241.223.202, 192.241.223.207, 192.241.224.191, 192.241.225.100, 192.241.225.224, 192.241.225.240, 198.199.113.212, 192.241.192.34, 192.241.196.83, 192.241.209.85, 192.241.212.70, 192.241.212.75, 192.241.212.97, 192.241.213.19, 192.241.213.80, 192.241.214.40, 192.241.214.50, 192.241.214.65, 192.241.215.35, 192.241.216.32, 192.241.220.12, 192.241.221.43, 192.241.222.4, 192.241.222.90, 192.241.223.11, 192.241.223.55, 192.241.223.66, 192.241.223.72, 192.241.224.61, 192.241.224.67, 192.241.225.16, 192.241.225.29, 192.241.225.56, 192.241.225.67, 192.241.226.62, 192.241.226.77	56	73.684%
14618	44.202.76.90	1	1.316%
14987	104.152.52.124	1	1.316%
34665	5.188.210.227	1	1.316%
40913	208.93.152.31	1	1.316%
49505	45.155.204.146	1	1.316%
49544	185.189.182.234	1	1.316%
50113	185.40.4.96	1	1.316%
56040	120.239.150.213	1	1.316%
63949	172.104.15.201	1	1.316%
202425	94.102.61.8	1	1.316%
213220	109.248.6.5	1	1.316%

394695	103.76.228.216	1	1.316%

TABLE B.2.4

Identified autonomous system numbers for the IP addresses in the data set collected by the Kibana node of the Elastic honeypot placed in the public Internet.

Bibliography

[1] Proximus. (Oct. 2021). "Research report cybersecurity - cybersecurity research report 2021," [Online]. Available: https://cybersecurity.proximus.be/survey-2021/research-report-cybersecurity (visited on May 21, 2022).

[2] Federal Bureau of Investigation, "Internet crime report," Internet Crime Complaint Center division of the Federal Bureau of Investigation, Tech. Rep., 2021. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (visited on Nov. 18, 2021).

[3] L. Spitzner, *Honeypots: Tracking Hackers*. USA: Addison-Wesley Longman Publishing Co., Inc., 2002, ISBN: 978-0321108951.

[4] ENISA, "Cybersecurity for smes - challenges and recommendations," European Union Agency for Cybersecurity (ENISA), Tech. Rep., Jun. 2021. DOI: 10.2824/770352. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (visited on Nov. 18, 2021).

[5] C. Sanders, *Intrusion Detection Honeypots: Detection Through Deception*. Applied Network Defense, 2020, ISBN: 978-1735188300. [Online]. Available: https://books.google.nl/books?id=suubzQEACAAJ.

[6] L. Spitzner, "Honeypots: Catching the insider threat," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, 2003, pp. 170–179. DOI: 10.1109/CSAC.2003.1254322.

[7] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, "Byod policy compliance: Risks and strategies in organizations," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 61–72, 2022. DOI: 10.1080/08874417.2019.1703225.

[8] S. François, *Digitalisation de la société: Quid de la cybersécurité?* Conference Presentation, 2022. [Online]. Available: https://seclists.org/honeypots/2003/q1/128 (visited on Apr. 22, 2022).

[9] C. Stoll, *The cuckoo's egg: Tracking a spy through the maze of computer espionage*. Doubleday, 1989, pp. 1–399, ISBN: 978-0-3852-4946-1.

[10] C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, and W. J. Buchanan, "A comparative analysis of honeypots on different cloud platforms," *Sensors*, vol. 21, no. 7, 2021, ISSN: 1424-8220. DOI: 10.3390/s21072433. [Online]. Available: https://www.mdpi.com/1424-8220/21/7/2433.

[11] Y. Sun, Z. Tian, M. Li, S. Su, X. Du, and M. Guizani, "Honeypot identification in softwarized industrial cyber–physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5542–5551, 2021. DOI: 10.1109/TII.2020.3044576.

[12] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *Journal of Information Security and Applications*, vol. 41, pp. 103–116, 2018, ISSN: 2214-2126. DOI: 10.1016/j.jisa.2018.06.004.

[13] P. Lackner, "How to mock a bear: Honeypot, honeynet, honeywall & honeytoken: A survey," in *Proceedings of the 23rd International Conference on Enterprise Information Systems*, INSTICC, vol. 2, SciTePress, 2021, pp. 181–188, ISBN: 978-989-758-509-8. DOI: 10.5220/0010400001810188.

[14] U. J. C. Pramodya, K. T. Y. U. De Silva Wijesiriwardhana, K. T. D. Dharmakeerthi, E. A. K. V. Athukorala, A. N. Senarathne, and D. Tharindu, "Agenthunt: Honeypot and ids based network monitoring device to secure home networks," in *Proceedings of the Future Technologies Conference (FTC) 2021, Volume 3*, K. Arai, Ed., Cham: Springer International Publishing, 2022, pp. 194–207, ISBN: 978-3-030-89912-7.

[15] X. Wei and D. Yang, "Study on active defense of honeypot-based industrial control network," in *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, 2021, pp. 2019–2022. DOI: 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00301.

[16] K. D. Singh, "Securing of cloud infrastructure using enterprise honeypot," in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2021, pp. 1388–1393. DOI: 10.1109/ICAC3N53548.2021.9725389.

[17] J. Jafarian and A. Niakanlahiji, "Delivering honeypots as a service," Jan. 2020. DOI: 10.24251/HICSS.2020.227.

[18] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in iot smart factory using honeypot combined with machine learning," *PeerJ Computer Science*, vol. 7, e350, 2021. DOI: 10.7717/peerj-cs.350.

[19] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021.

[20] E. D. Saputro, Y. Purwanto, and M. F. Ruriawan, "Medium interaction honeypot infrastructure on the internet of things," in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, IEEE, 2021, pp. 98–102, ISBN: 978-1-7281-9448-6.

[21] CyberSRC. (Jul. 2021). "Honeypot as service - CyberSRC," [Online]. Available: https://cybersrcc.com/cybersrc-honeypot-service/ (visited on Jun. 5, 2022).

[22] Blumira. (Mar. 2021). "Virtual honeypot software | honeypot software - Blumira," [Online]. Available: https://www.blumira.com/product/honeypots/ (visited on Jun. 5, 2022).

[23] J. Cândido, M. Aniche, and A. van Deursen, "Log-based software monitoring: A systematic mapping study," *PeerJ Computer Science*, vol. 7, e489, 2021. [Online]. Available: http://arxiv.org/abs/1912.05878.

[24] E. Mendes and F. Petrillo, "Towards logging noisiness theory: Quality aspects to characterize unwanted log entries," *CoRR*, vol. abs/2106.03018, 2021. arXiv: 2106.03018. [Online]. Available: https://arxiv.org/abs/2106.03018.

[25] Q. Fu, J. Zhu, W. Hu, J.-G. Lou, R. Ding, Q. Lin, D. Zhang, and T. Xie, "Where do developers log? an empirical study on logging practices in industry.," in *ICSE 2014*, Jul. 2014. DOI: 10.1145/2591062.2591175. [Online]. Available: https://www.microsoft.com/en-us/research/publication/developers-log-empirical-study-logging-practices-industry-2/.

[26] B. Chen, "Improving the software logging practices in devops," in *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, 2019, pp. 194–197. DOI: 10.1109/ICSE-Companion.2019.00080.

[27] R. A. Grimes, *Honeypots for Windows*, 1st ed. Apress, 2005, pp. 1–424, ISBN: 978-1-59059-335-6.

[28] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu, and H. Bao, "Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 250–261, 2020. DOI: 10.1109/OJCS.2020.3030825.

[29] O. Hayatle, A. Youssef, and H. Otrok, "Dempster-shafer evidence combining for (anti)-honeypot technologies," *Information Security Journal: A Global Perspective*, vol. 21, no. 6, pp. 306–316, 2012, ISSN: 1939-3555. DOI: 10.1080/19393555.2012.738375.

[30] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "Towards systematic honeytoken fingerprinting," in *13th International Conference on Security of Information and Networks*, Association for Computing Machinery, Nov. 2020, pp. 1–5, ISBN: 9781450387514. DOI: 10.1145/3433174.3433599.

[31] J. Uitto, S. Rauti, S. Laurén, and V. Leppänen, "A survey on anti-honeypot and anti-introspection methods," in *Recent Advances in Information Systems and Technologies*, vol. 570, 2017, ISBN: 978-3-319-56537-8. DOI: 10.1007/978-3-319-56538-5_13.

[32] R. Joshi and A. Sardana, *Honeypots: a new paradigm to information security*. CRC Press, 2011.

[33] N. Kambow and L. K. Passi, "Honeypots: The need of network security," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 5, pp. 6098–6101, 2014.

[34] L. Spitzner, "Honeypots: Catching the insider threat," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, 2003, pp. 170–179. DOI: 10.1109/CSAC.2003.1254322.

[35] ——, "Honeypots: Catching the insider threat," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, IEEE, 2003, pp. 170–179.

[36] G. Bell and A. Elang, "Network malware laboratory based on honeypots technologies," *Journal of Cybersecurity Research (JCR)*, vol. 3, pp. 1–12, Dec. 2018. DOI: 10.19030/jcr.v3i1.10226.

[37] ENISA, "General report," European Union Agency for Cybersecurity (ENISA), Tech. Rep., 2012. DOI: 10.2824/16829. [Online]. Available: https://www.enisa.europa.eu/publications/corporate/general-report-2012 (visited on Nov. 18, 2021).

[38] Björn Bengtson. (Dec. 2021). "Bap - http basic authentication honeypot," [Online]. Available: https://github.com/bjeborn/basic-auth-pot (visited on Dec. 20, 2021).

[39] Cymmetria. (Dec. 2021). "Cisco asa honeypot," [Online]. Available: https://github.com/cymmetria/ciscoasa_honeypot (visited on Dec. 20, 2021).

[40] Niels Provos. (Dec. 2021). "Developments of the honeyd virtual honeypot," [Online]. Available: http://www.honeyd.org/index.php (visited on Dec. 20, 2021).

[41] NETSEC. (Dec. 2021). "Specter - intrusion detection system," [Online]. Available: http://www.specter.com/ (visited on Dec. 20, 2021).

[42] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating System Concepts*, 9th. Wiley Publishing, 2012, ISBN: 1118063333.

[43] Cowrie. (Dec. 2021). "Cowrie," [Online]. Available: https://www.cowrie.org/ (visited on Dec. 20, 2021).

[44] D. Salmon. (Dec. 2021). "Miniprint," [Online]. Available: https://github.com/sa7mon/miniprint (visited on Dec. 20, 2021).

[45] Be the root. (Dec. 2021). "Sticky elephant," [Online]. Available: https://github.com/betheroot/sticky_elephant (visited on Dec. 20, 2021).

[46] R. Steenson and C. Seifert. (Jul. 2021). "Capture hpc," [Online]. Available: https://www.honeynet.org/projects/old/capture-hpc/ (visited on Dec. 1, 2021).

[47] The Honeynet Project. (Dec. 2021). "Sebek homepage," [Online]. Available: https://honeynet.onofri.org/tools/sebek/ (visited on Dec. 27, 2021).

[48] R. Vermeulen. (Dec. 2021). "Argos - an emulator for capturing zero-day attacks," [Online]. Available: https://www.few.vu.nl/argos/ (visited on Dec. 27, 2021).

[49] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Computer Security Incident Handling Guide*, en, 61. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, Aug. 2012, vol. 800, pp. 1–147. [Online]. Available: 10.6028/NIST.SP.800-61r2.

[50] Prometheus Authors. (Feb. 2022). "Prometheus - monitoring system & time series database," [Online]. Available: https://prometheus.io/ (visited on Feb. 5, 2022).

[51] I. Mokube and M. Adams, "Honeypots: Concepts, approaches, and challenges," in *Proceedings of the 45th annual southeast regional conference*, 2007, pp. 321–326.

[52] Wikipedia Community. (May 2022). "The boy who cried wolf," [Online]. Available: https://en.wikipedia.org/wiki/The_Boy_Who_Cried_Wolf (visited on May 3, 2022).

[53] J. Sullivan, *Extended Detection and Response (XDR) For Dummies, Cisco Special Edition*, en. John Wiley & Sons, Inc., 2022, pp. 1–46, ISBN: 978-1-119- 84557-7.

[54] Osquery. (Dec. 2021). "Osquery | easily ask questions about your linux, windows, and macos infrastructure," [Online]. Available: https://osquery.io/ (visited on Dec. 27, 2021).

[55] Cisco Systems, Inc. (Dec. 2021). "Orbital help," [Online]. Available: https://orbital.amp.cisco.com/help/ (visited on Dec. 21, 2021).

[56] S. Widup, A. Pinto, D. Hylender, G. Bassett, and p. langlois philippe, "Data breach investigations report," Verizon, Tech. Rep., May 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/ (visited on Apr. 18, 2022).

[57] CrowdStrike, "Global threat report," CrowdStrike Holdings, Inc., Tech. Rep., 2022. [Online]. Available: https://www.crowdstrike.com/global-threat-report/ (visited on Apr. 18, 2022).

[58] J. A. Sava. (Feb. 2022). "Total spending on global information security market by segment 2017-2021," [Online]. Available: https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/#:~:text=Spending%5C%20on%5C%20security%5C%20services%5C%20in,reach%5C%2072.5%5C%20billion%5C%20U.S.%5C%20dollars. (visited on May 3, 2022).

[59] A. Paes de Barros, *Res: Protocol anomaly detection ids - honeypots*, Email communication, 2003. [Online]. Available: https://seclists.org/honeypots/2003/q1/128 (visited on Apr. 22, 2022).

[60] L. Spitzner, "Honeytokens: The other honeypot," Jul. 2003. [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=74450cf5-2f11-48c5-8d92-4687f5978988&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (visited on Apr. 16, 2022).

[61] B. Bowen, S. Hershkop, A. Keromytis, and S. Stolfo, "Baiting inside attackers using decoy documents," in *Security and Privacy in Communication Networks*, Berlin, Heidelberg: Springer, Sep. 2009, pp. 51–70, ISBN: 978-3-642-05284-2. DOI: 10.1007/978-3-642-05284-2_4.

[62] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 1st ed. Chapman & Hall/CRC, Aug. 2007, ISBN: 978-1-58488-551-1. DOI: 10.1201/9781420010756.

[63] IBM Security, "Cost of a data breach report," IBM, Tech. Rep., 2012. [Online]. Available: https://www.ibm.com/security/data-breach (visited on Apr. 18, 2022).

[64] StatCounter. (Sep. 2021). "Desktop operating system market share worldwide," [Online]. Available: https://gs.statcounter.com/os-market-share/desktop/worldwide (visited on May 3, 2022).

[65] Security Space. (Mar. 2022). "Web server survey," [Online]. Available: https://secure1.securityspace.com/s_survey/data/202202/index.html (visited on Apr. 9, 2022).

[66] Cisco Systems, Inc. (Mar. 2022). "Secure endpoint user guide," [Online]. Available: https://docs.amp.cisco.com/en/SecureEndpoint/Secure%5C%20Endpoint%5C%20User%5C%20Guide.pdf (visited on Apr. 25, 2022).

[67] ——, (Jul. 2020). "Getting started — cisco securex integration workflows," [Online]. Available: https://ciscosecurity-sx-00-integration-workflows.readthedocs-hosted.com/en/latest/orchestration/getting_started.html (visited on Apr. 25, 2022).

[68] A. W. Conklin and G. White, *Principles of Computer Security: CompTIA Security+ and Beyond*, 5th ed. McGraw-Hill Education, Jun. 2018, ISBN: 978-1-260-02601-6.

[69] Wikipedia's Community. (Mar. 2022). "Black hat (computer security)," [Online]. Available: https://en.wikipedia.org/wiki/Black_hat_(computer_security) (visited on Apr. 11, 2022).

[70] D. Danchev. (Jun. 2010). "Study finds the average price for renting a botnet," [Online]. Available: https://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/ (visited on May 3, 2022).

[71] Telecommunication Standardization Sector, "T.128: Multipoint application sharing," International Telecommunication Union, Standard, Jun. 2008. [Online]. Available: https://www.itu.int/rec/T-REC-T.128 (visited on Apr. 9, 2022).

[72] ——, "T.122: Multipoint communication service - service definition," International Telecommunication Union, Standard, Feb. 1998. [Online]. Available: https://www.itu.int/rec/T-REC-T.122 (visited on Apr. 9, 2022).

[73] ——, "T.125: Multipoint communication service protocol specification," International Telecommunication Union, Standard, Feb. 1998. [Online]. Available: https://www.itu.int/rec/T-REC-T.125 (visited on Apr. 9, 2022).

[74] Y. Pouffary and A. Young, "Iso transport service on top of tcp (itot)," RFC Editor, RFC 2126, Mar. 1997. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2126 (visited on Apr. 9, 2022).

[75] Telecommunication Standardization Sector, "X.224 : Information technology - open systems interconnection - protocol for providing the connection-mode transport service," International Telecommunication Union, Standard, Nov. 1995. [Online]. Available: https://www.itu.int/rec/T-REC-X.224 (visited on Apr. 9, 2022).

[76] S. Reiner. (Jul. 2020). "Explain like i'm 5: Remote desktop protocol (rdp)," [Online]. Available: https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp (visited on Apr. 9, 2022).

[77] Thinkst Applied Research. (Mar. 2022). "Opencanary," [Online]. Available: https://github.com/thinkst/opencanary (visited on Apr. 8, 2022).

[78] G. Deflandre. (Sep. 2022). "Thesis honeypot data analizer," [Online]. Available: https://github.com/Guilian-Deflandre/honeypot-data-analizer (visited on Jun. 8, 2022).

[79] Elasticsearch B.V. (May 2022). "Our story | elastic," [Online]. Available: https://www.elastic.co/about/history-of-elasticsearch (visited on May 4, 2022).

[80] D. Horovits. (Jun. 2020). "The complete guide to the elk stack," [Online]. Available: https://logz.io/learn/complete-guide-elk-stack/ (visited on May 2, 2022).

[81] The Apache Software Foundation. (Mar. 2022). "Welcome to apache lucene," [Online]. Available: https://lucene.apache.org/ (visited on May 3, 2022).

[82] Elasticsearch B.V. (May 2022). "Welcome to elastic docs," [Online]. Available: https://www.elastic.co/guide/index.html (visited on May 3, 2022).

[83] C. Gormley and Z. Tong, *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*, 1st. O'Reilly Media, Inc., 2015, ISBN: 978-1-449-35854-9.

[84] Elasticsearch B.V. (May 2022). "Elastic," [Online]. Available: https://github.com/elastic (visited on May 3, 2022).

[85] G. Deflandre. (Sep. 2022). "Log generator," [Online]. Available: https://github.com/Guilian-Deflandre/thesis-log-generator (visited on Jun. 8, 2022).

[86] D. Faraglia. (May 2022). "Faker - pypi," [Online]. Available: https://pypi.org/project/Faker/ (visited on May 30, 2022).

[87] A. Robbins and D. MacKenzie. (2010). "Iftop(8) - linux man page," [Online]. Available: https://linux.die.net/man/1/id (visited on May 11, 2022).

[88] ISO Central Secretary, "Date and time - representations for information interchange - part 1: Basic rules," en, International Organization for Standardization, Geneva, CH, Standard ISO 8601-1:2019, 2019. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:8601:-1:ed-1:v1:en.

[89] Joda.org. (Sep. 2022). "Datetimeformat (joda-time 2.10.14 api)," [Online]. Available: https://www.joda.org/joda-time/apidocs/org/joda/time/format/DateTimeFormat.html (visited on May 3, 2022).

[90] P. Warren. (Nov. 2010). "Iftop(8) - linux man page," [Online]. Available: https://linux.die.net/man/8/iftop (visited on Apr. 11, 2022).

[91] J. C. Warner and C. Small. (Aug. 2021). "Top(1) - linux man page," [Online]. Available: https://linux.die.net/man/1/top (visited on Apr. 11, 2022).

[92] A. Barfar and S. Mohammadi, "Honeypots: Intrusion deception," *The Information Systems Security Association (ISSA) Journal*, pp. 28–31, Jan. 2007.

[93] C. Newman and G. Klyne, "Date and Time on the Internet: Timestamps," RFC Editor, RFC 3339, Jul. 2002, 18 pp. [Online]. Available: https://www.rfc-editor.org/info/rfc3339.

[94] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Boston, MA: Pearson Education Limited, 2017, ISBN: 978-1-292-15359-9.

[95] Team Cymru. (May 2022). "Ip to asn mapping service - team cymru," [Online]. Available: https://team-cymru.com/community-services/ip-asn-mapping/ (visited on May 28, 2022).

[96] CAIDA. (May 2022). "Index of /datasets," [Online]. Available: https://public-data.caida.org/datasets/ (visited on May 28, 2022).

[97] Center for Applied Internet Data Analysis. (Jun. 2022). "State of ip spoofing," [Online]. Available: https://spoofer.caida.org/summary.php (visited on Jun. 2, 2022).

[98] R. Dobbins and S. Bjarnason. (Jan. 2021). "Microsoft remote desktop protocol (rdp) reflection/amplification ddos attack mitigation recommendations," [Online]. Available: https://www.netscout.com/blog/asert/microsoft-remote-desktop-protocol-rdp-reflectionamplification (visited on May 21, 2022).

[99] Microsoft. (Dec. 2021). "Using the portqry command-line tool," [Online]. Available: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/portqry-command-line-port-scanner-v2 (visited on May 11, 2022).

[100] C. Hutin, "Les universités francophones victimes d'une cyberattaque," *Le Soir*, Mar. 2022. [Online]. Available: https://www.lesoir.be/431382/article/2022-03-21/les-universites-francophones-victimes-dune-cyberattaque (visited on Jun. 2, 2022).

[101] E. M. Hutchins, M. J. Cloppert, R. M. Amin, *et al.*, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," 1, vol. 1, Mar. 2011, p. 80. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (visited on Jun. 1, 2022).

[102] P. Pols, "The unified kill chain," Tech. Rep., 2017. [Online]. Available: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf (visited on Jun. 1, 2022).

[103] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," Tech. Rep., 2018. [Online]. Available: https://attack.mitre.org/docs/ATTACK%5C_Design%5C_and%5C_Philosophy%5C_March%5C_2020.pdf (visited on Jun. 1, 2022).

[104] D. Storey, "Catching flies with honey tokens," *Network Security*, no. 11, pp. 15–18, Nov. 2009.

[105] R. P. Jover, "Security analysis of SMS as a second factor of authentication," *Communications of the ACM*, vol. 63, no. 12, pp. 46–52, 2020.

[106] R. Karthikeyan, D. T. Geetha, S. Vijayalakshmi, and R. Sumitha, "Honeypots for network security," *International journal for Research & Development in Technology*, vol. 7, no. 2, pp. 62–66, 2017.

[107] Amazon Web Services, Inc. (May 2022). "The ELK stack," [Online]. Available: https://aws.amazon.com/opensearch-service/the-elk-stack/ (visited on May 3, 2022).

[108] Oxford University Press. (Dec. 2021). "Interactivity noun - definition," [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/interactivity?q=interactivity (visited on Dec. 18, 2021).

[109] Elasticsearch B.V. (Jan. 2022). "Free and open search: The creators of elasticsearch, elk & kibana | elastic," [Online]. Available: https://www.elastic.co/ (visited on Jan. 13, 2022).

[110] I. Goddijn and Cyber Risk Analytics Research Team, "2020 Year End Report - Data Breach QuickView," Risk Based Security, Tech. Rep., Jan. 2021.

[111] J. White, "Creating personally identifiable honeytokens," in *Innovations and Advances in Computer Sciences and Engineering*, T. Sobh, Ed., Dordrecht: Springer Netherlands, 2010, pp. 227–232, ISBN: 978-90-481-3658-2.

[112] E. Vasilomanolakis, S. Karuppayah, P. Kikiras, and M. Mühlhäuser, "A honeypot-driven cyber incident monitor: Lessons learned and steps ahead," in *8th International Conference on Security of Information and Networks*, Sochi, Russia, Sep. 2015. DOI: 10.1145/2799979.2799999.