Using a modern honeypot model to defend smart cities and provide early detection to APT and ransomware attacks

Guy Waizel
"Alexandru Ioan Cuza" University of Iasi, Romania
Guy.waizel@gmail.com

Abstract

Ransomware and advanced persistent threat (APT) attacks are proliferating on critical infrastructure in cities and nation-states. Holding a whole smart city for ransom using a combined cyberattack would, just a few years ago, have been the stuff of science fiction movies. Yet today sophisticated hacking techniques, the ease of use and availability of RaaS (Ransomware as a Service) and the vast vulnerabilities of computer systems, web applications, databases and various IoT-connected devices exposed in the wild are all creating a significant challenge for security teams. Such a movie may become reality.

Some security teams in various sectors use active defense technology and deception security to deceive, trick bait, and lure hackers towards fake assets. Regardless of vulnerabilities in the wild, it helps detect the breach at an early stage and allows faster threat remediation before it is too late.

In this study, we use a descriptive literature review to explore various real-life breach cases which occurred in smart cities. We use content analysis to detect similarities, patterns, significant correlations, and relationships between keywords. A synthesis analysis is conducted and the modern honeypot triangle model is suggested to reduce the risk of future similar breaches by deceiving cybercriminals and providing security teams with extensive early warning detection capabilities and intelligence about the attackers' techniques and tactics. Finally, we provide recommendations for further analysis.

Keywords: Ransomware, Deception Technology, Cybersecurity, IoT

1. Introduction

This paper explores real-life breach cases on smart cities reported in the media over recent years. Learning from real cases is essential, especially in understanding the impact of significant attacks on smart cities and how to detect such cyberattacks quickly and remediate the threats and risks.

Recently, the EU published the "Network and Information Security Directive" NIS2 and defined many new essential and important sectors that will be added to the original NIS directive. Reporting obligations and incident reporting are given special attention in the directive. Affected organizations will need to report any cyber incident within 72 hours. NIS2 will be applicable by 2024 after EU member states execute the legislation.[7], [22].

Early warning systems and active defense techniques are necessary to detect attackers and remediate the threat as early as possible, to reduce the potential damage from a breach. The

effectiveness of deception security has been researched in previous studies. For example, Ferguson-Walte [9], [10] concluded that the presence of deception, combined with knowledge of its existence, has the greatest effect on cyber attackers. A honeypot is a method to bait, deceive, and trick an attacker by placing fake computing assets in production or non-production networks. It looks real to attackers and provides alerts and intelligence as soon as the attacker communicates with the honeypot . The term honeypot for trapping attackers was used in the 1960s and 1970s when Clifford Stoll, an American astronomer, author, and teacher, set up a honeypot and tracked down a hacker who was later identified as KGB recruit Markus Hess. [16]. Over the last decade, a new technology industry has arisen, which Gartner also referred to as deception technology industry. [5]

Security operations centers use many tools for early warning of threats. However, not all of these tools utilize active defense technology, deception technology, or the modern honeypots that are discussed in this article. By implementing decoys and lures to deceive cybercriminals and distract them with fake assets, modern honeypots have the potential to reduce risk and improve service level agreements for early warning detection. This allows security teams to effectively remediate risks while the attackers are occupied and their efforts are wasted. The probability of harming real assets is reduced as soon as more decoys are added across the network and coverage is expanded or lures are used to divert the attackers to these decoys. This paper explores real-life breach cases on cities that have occurred already, synthesizing and suggesting a modern honeypot model as a deception strategy for smart cities.

This paper aims to equip the cyber community that defends smart cities with a toolset of deception ideas and best practices for leveraging existing active defense technologies to improve their early warning detection capabilities and meet necessary upcoming regulations such as NIS2. [7], [22]

Moreover, this paper identifies trends, relations, and common findings between various real-life breach cases that occurred and were reported in the news. The paper suggests insights and recommendations of how a suggested modern honeypot triangle model can help to defend smart cities and provide early detection to Advanced Persistent Threat (APT) and ransomware attacks. Finally, we also discuss suggestions for future research.

2. Methods

For this paper a descriptive literature review was conducted using three search engines: Google, Bing and Yahoo. The search engines were used to search for news reports of breach cases on cities.

The following search terms were used: "attack on cities", "attack on smart cities", "published attacks", "published breaches", "attack on government", "government breach", "attacks on IoT in cities", "attack on smart devices", "attack on connected devices", "attack on smart homes", " ransomware attack on cities", "APT attack on cities", "attack on emergency alarms", "attack on CCTV", "attack on transportation.", and "breaches in cities and government".

The criteria for inclusion in the literature review were: a published breach involving an official city or government office and a significant impact on the entity. This impact could take various forms, such as affecting many users, compromising safety or national security, interrupting online payment services or services offered to citizens, or impacting a large number of students. Additionally, significant operational disruptions in transportation, healthcare, finance, or other areas within a city or government were also considered.

The entry point, the impact of each breach, the type, and the sector were classified into categories. An in-depth review of all published cases was conducted, and the content of cases was compared between the various sources. In cases of ransomware, a search on which variants were used was also conducted.

Categories of business use case impact and technical use case impact were defined, and each case's business and technical impact were classified accordingly. Then analysis of key similarities and differences between these published breaches was conducted using content analysis, keyword frequency analysis, and Spearman correlation to search for significant correlations between certain keywords within the reported articles. The findings were then summarized for discussion in this paper; how we can minimize, reduce, and remediate the impact of similar cases in the future by using the modern honeypot model suggested in this paper to provide cities with outstanding early warning capabilities.

2. Results

2.1 Descriptive Literature Review and Synthetic Analysis

Following the articles search over three search engines, the initial query yielded eighty-six articles. Of these articles, twenty-one real-life breach cases met the criteria for inclusion in the literature review. These cases are outlined in Table 1. Even though all of the breach cases have already occurred and have been reported in the news, the researcher has chosen not to disclose the names of the affected organizations. Instead, the focus is on the impacted sectors and the nature of the breaches, as well as suggesting a future model to defend against similar incidents in the future.

When looking for similarities among the breach cases it was discovered that over 65% of the cases were in the government sector. Based on the published reports, ransomware attacks and data breaches were the main type of attacks. The ransomware variants used in the attacks were Ryuk, WannaCry, Trickbot, and Lockbit. When searching for common entry points, the following categories were defined: Computer systems were 44% of the cases, web applications were 33% of the cases, databases were 12% of cases, and IoT were 11% of cases.

Based on the published cases, most breaches resulted from weak or stolen credentials, unpatched or outdated software, a lack of authentication or authentication methods, and an insecure configuration or management interface. Based on the analysis conducted, the main

weaknesses used were divided into the following categories: 44% were unpatched servers, 33% were vulnerable web applications, 12% were exposed databases, and 11% were misconfigured firewalls.

Trellix reported similar findings [29] in Q3 2022, within the same time frame of these cases. Lockbit was one of the top ransomware families used in 2022. Additionally, they reported that Cobalt Strike and Mimikatz were the most malicious hacking tools used and attackers continue to leverage most Operating System (OS) binaries such as Command Prompt (CMD), PowerShell, Scheduled Tasks (Schtasks), and Windows Management Instrumentation (WMI) as well as third-party tools like remote access tools, red team tools, and file transfer tools.

The higher percentage of computer systems and web applications entry points in comparison to IoT and databases is related to the fact that computer systems and web applications have more potential entry points. For example, computer systems may have vulnerabilities in their operating system or open ports that attackers can exploit. Web applications may contain code or server vulnerabilities that allow malicious actors to inject malware or access sensitive information. By comparison, IoT systems and databases may have fewer entry points that can be targeted.

The attackers' main goal was to create as significant an impact as possible to increase the probability of getting their ransom request paid. In many cases, it was not reported whether the ransom was eventually paid or not.

Sophos's report also mentioned that in both state and governments, there were higher ransomware encryption rates 72% in 2022.[27]

Table 1. Examples for cyberattacks on cities which were reported in the news

Sector	Entry point category	Impact based on the source
Education	Computer Systems	Hundreds of thousands of students were affected.
Government	Computer Systems	A significant percentage of recorded storage devices
Government	Computer Systems	Hundreds of outside sirens activated.
Education	Computer Systems	School's data encrypted
Transportation	Web Applications	Online tickets, web and signals
Education	Web Applications	Tens of thousands of students were affected.
Education	Web Applications	Thousands of students were affected.
Government	Databases	Delayed rent payments
Legal	Web Applications	Tens of servers and workstations

Government	Web Applications	Servers/network and important city data were stolen.
Education	Computer Systems	Shut down of phone lines, locked and encrypted school system data.
Government	Web applications	Online payment utilities, traffic tickets and law enforcement operations.
Healthcare	Web applications	Health insurance/medical information.
Utilities	IoT	The hacker tried to poison the water supply.
Government	Computer Systems	Thousands of government computers The office moved to work with paper.
Government	Computer Systems	Email servers, fingerprinting and background checking system.
Government	Web applications	Hundreds of online computers during the holiday.
Government	Computer Systems	The city took all servers down as a precaution following the detection of the cyberattack.
Government	Web applications	Hundreds of computers were infected and all the city's files were locked.
Government	Databases	Telephones, online payments
Government	Computer Systems	911 and online payments were down and took weeks to recover as part of a simultaneous attack on many cities.

Sources: [4],[12],[14],[15],[18],[20],[21],[25],[26],[28],[30],[32],[33],[38],[39]

All twenty-one published breach case articles were analyzed using content analysis, keyword frequency analysis, and the Spearman correlation test between keywords using Voyant software [36]. When analyzing keyword frequency, the top fifty-five keywords met the expectation for this study (Fig. 3.) in which "ransomware" and "breach" appear among the top ten keywords which were: "city", "attack", "security"," incident"," government,"" data", "ransomware", "breach", "access", and "information" (Fig. 4.)

Fig. 3. Top 55 keywords frequency from published attacks

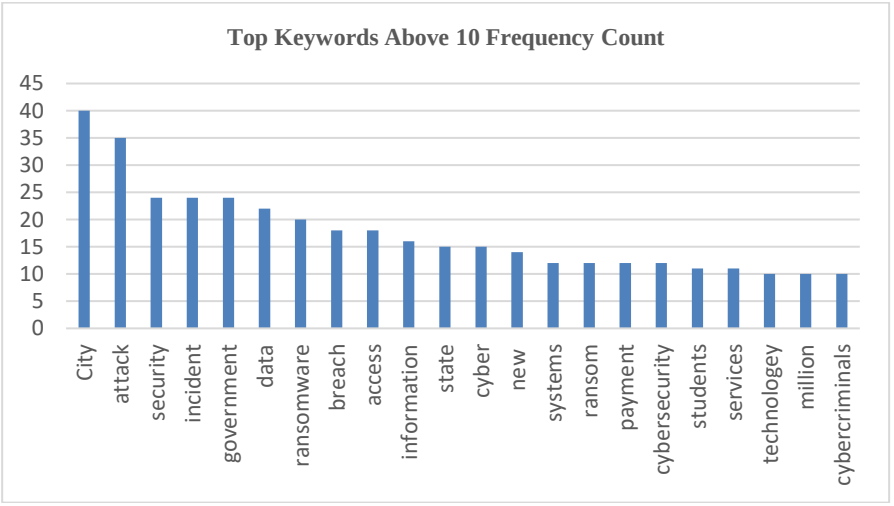
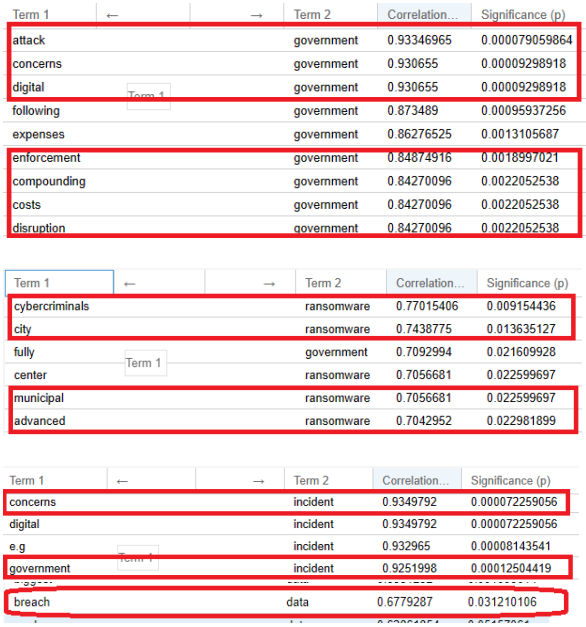


Fig. 4. Top Keywords Above 10 Frequency Count

When checking for Spearman correlations between keywords, interesting and significant findings were detected (Fig. 5.):
Between the keywords "attack", "concerns", "digital", "enforcement", "compufunding", "costs", and "disruption", and the keyword "government".

Between the keywords "cybercriminals", "city", "municipal", and "advanced", and the keyword: "ransomware".
Between the keywords: "concern" and "government", and the keyword "incident".
Between the keyword: "breach" and the keyword "data".



Term 1	←	→	Term 2	Correlation...	Significance (p)
attack			government	0.93346965	0.000079059864
concerns			government	0.930655	0.00009298918
digital			government	0.930655	0.00009298918
following			government	0.873489	0.00095937256
expenses			government	0.86276525	0.0013105687
enforcement			government	0.84874916	0.0018997021
compounding			government	0.84270096	0.0022052538
costs			government	0.84270096	0.0022052538
disruption			government	0.84270096	0.0022052538

Term 1	←	→	Term 2	Correlation...	Significance (p)
cybercriminals			ransomware	0.77015406	0.009154436
city			ransomware	0.7438775	0.013635127
fully			government	0.7092994	0.021609928
center			ransomware	0.7056681	0.022599697
municipal			ransomware	0.7056681	0.022599697
advanced			ransomware	0.7042952	0.022981899

Term 1	←	→	Term 2	Correlation...	Significance (p)
concerns			incident	0.9349792	0.000072259056
digital			incident	0.9349792	0.000072259056
e.g			incident	0.932965	0.00008143541
government			incident	0.9251998	0.00012504419
breach			data	0.6779287	0.031210106

Fig. 5. Significant keywords Correlations in published reports

The visual linkage between keywords clearly emphasizes that ransomware received a high level of attention in the breach cases reported in the news.

The relationship between the keywords: "attack" and "government"; "ransomware" and "government"; "attack" and "ransomware"; "ransomware", "access" and "data" were found to be significant, and this visual linkage is presented in Fig. 6.

These keywords' correlation seems obvious and makes sense. Most importantly, this ensures the reliability of the specific cases that are included in the literature review and allows a focused analysis of these cases for the purposes of this study in order to draw meaningful deductions regarding future potential implications and suggestions.

Since this paper recommends the use of active defense technology and modern honeypots for improving early warning capabilities, a keyword analysis was also conducted to assess whether deception technology, modern honeypots, or other keywords related to those topics exist in the articles. An interesting finding was that "active defense technology", "deception technology", "decoy", "lures", "honeypot", or "active defense" keywords did not appear in any of these published reports. There could be a few reasons for this. First, many published breaches do not mention which security tools the organization used and had in place during the attack. Second, if the attack or breach succeeds, the security tools in place are no longer an interesting topic to write about. However, if the breach was

made on a fake asset or decoys containing fake content and the fake data was leaked, stolen, or published by the attacker, then we would expect that a successful deception of an attacker at such a level would get published. A case of this sort was not found in the literature within this study, which may imply a gap in knowledge on this topic and highlights the potential importance and contribution of this paper to the cybersecurity community.

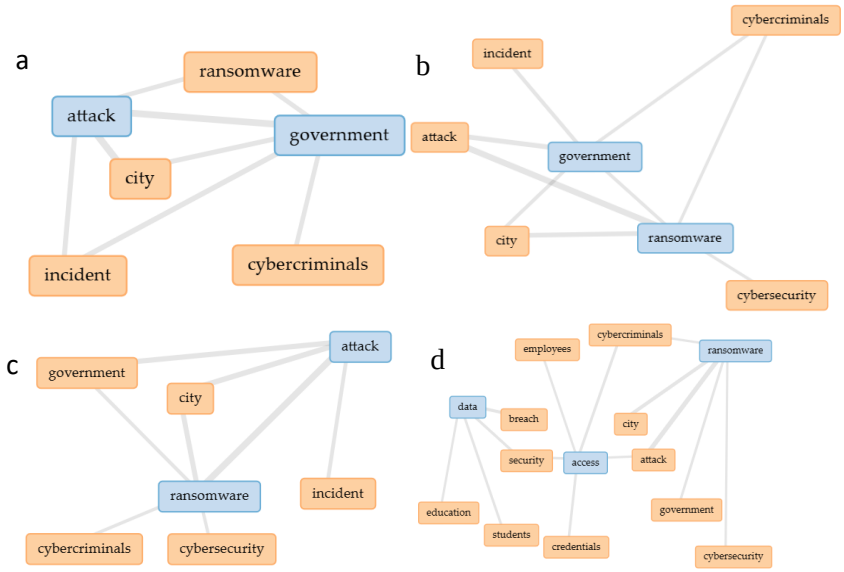


Fig. 6. (a) relationship between "attack" and "government" keywords; (b) relationship between "ransomware" and "government" keywords; (c) relationship between "ransomware" and "attack" keywords; (d) relationship between "ransomware", "access" and data keywords.

2.2 The Modern honeypot model for smart cities

Following the synthesis analysis of twenty-one published breach cases on smart cities, both business use case impact and technical use case impact were categorized for all these cases accordingly. The business use case categories that were defined were:

- Financial losses - expenses related to infrastructure damages and recovery costs;
- Loss of reputation - damage to public image and trust in businesses and government;
- Legal challenges - liability issues, regulations, and enforcement;
- Interruption of services - disruption to services and operations;
- Data loss - exposure or loss of confidential and sensitive data.

The technical impact use cases categories that were defined were:

- Encryption and access controls - includes items like locked files and encryption of computer systems;
- Network security - includes controlling and/or halting of IoT-CCTV, recording storage devices, VOIP, network devices, smart connected devices, and emergency alarms;

- Data loss - includes stolen data and controlling and/or halting of information systems;
- Online services - includes controlling and/or halting of online payment services, email server breaches, and signals;
- Critical infrastructure - includes controlling and/or halting of critical infrastructure and medical devices.

Deception technology includes high-level interaction decoys, medium-level interaction decoys, and low-level interaction lures. These can be purchased by business organizations and can be designed and customized as required [5].

Following the defined technical use case impact categories, we suggest the modern honeypot triangle model for smart cities by using deception technology and customization of decoys for any sector.

We define the full modern honeypot model as a unified main triangle consisting of four sub-triangles that must include the following components:

- The first component, a Full Operating System (OS) Windows decoy, which is a golden image of any version of Windows server decoy. Any software can be run on it, and it can monitor services such as Remote Desktop (RDP), Windows Management Instrumentation (WMI), Web, Microsoft SQL Server(MSSQL), Active Directory (AD), Domain Name Systems (DNS) and more. A Full OS of Linux is also an advantage to mimicking a Linux server and should contain high-interaction services such as Secure Shell (SSH) , Web service, MySQL service, and more;
- The second component is an emulated decoy that can easily be changed to any OS and can be adjusted to run multiple emulated services. It can be customized to look like a real server or workstation and can be deployed at scale across multiple VLANS;
- The third component is the lures, which are like bread crumbs distributed to endpoints. They deceive and bait attackers and refer them to the emulated decoys or the Full OS decoys;
- The fourth component of the full modern honeypot model is the remediation of the threat actor as soon as communication with one of the decoys occurs. There are various remediation measures that can be executed, such as blocking communication using a firewall, conducting network containment using endpoint protection and network access control systems, restoring an endpoint or server using backup systems, sending alerts to Security orchestration, automation and response (SOAR) or central management on the cloud, sending new signatures of zero-day to anti-virus, sending alerts through SMS and notifications, using the Security Information and Event Management (SIEM) or SOAR to perform advanced actions on endpoints, such as removal of files, and sending binaries to sandboxes for further analysis.

In Fig. 7 we associate the technical impact use case categories with the relevant component of the suggested modern honeypot model and in Fig. 8 we show a suggested example for implementing the model in the government sector.

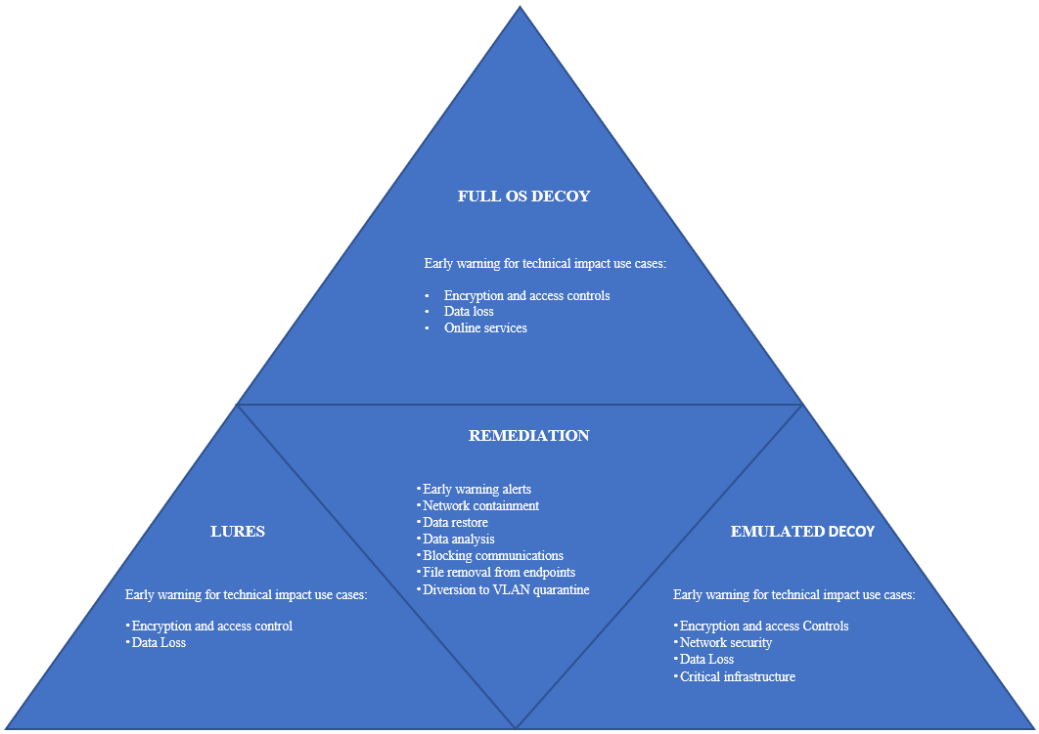


Fig. 7. The suggested modern honeypot triangle model for smart cities

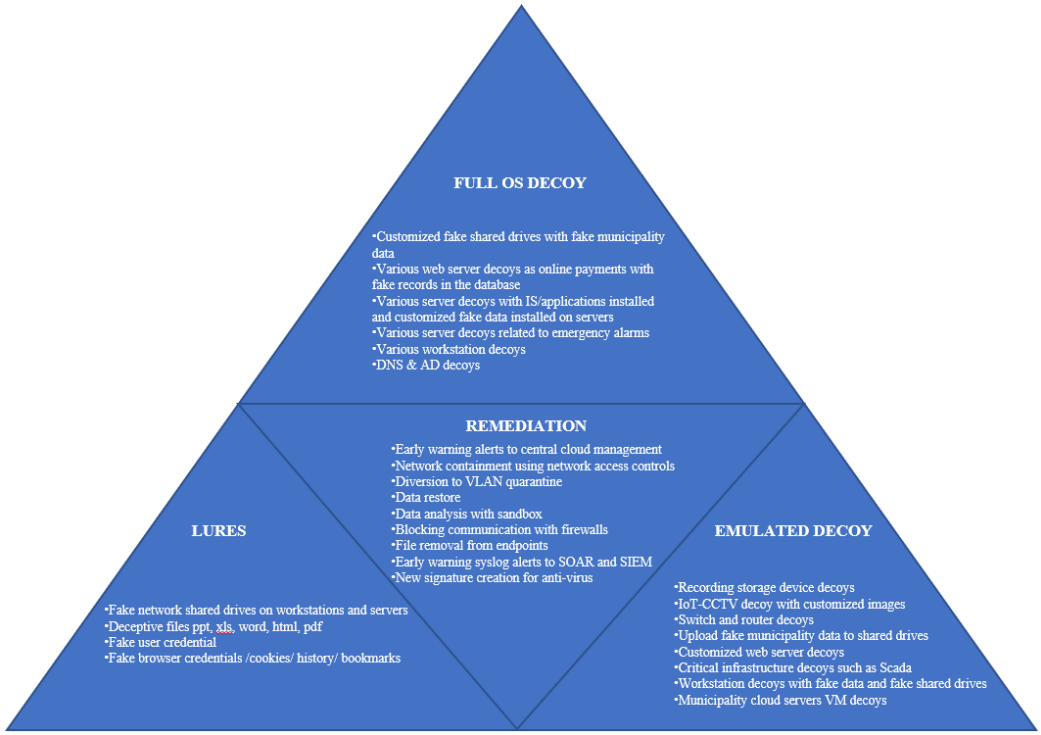


Fig. 8. Example of a modern honeypot triangle model implementation for a municipality

3. Discussion

This study used a descriptive literature review to explore various real-life attack cases on cities that occurred in recent years and were reported in the news. A synthesis analysis was conducted using content analysis, which revealed that significant keywords within the content of the published articles focused on and discussed ransomware and data breaches in cities and the government sector. This ensures that the selected cases share content that reflects the aim and purpose of this paper.

Although many vulnerabilities exist on IoT smart-connected devices which are distributed in smart cities, most of the attacks carried out over recent years and which are explored in this paper used ransomware variants, mainly targeting computer systems and web applications rather than IoT smart-connected devices. Computer systems and web applications have a large number of exposed vulnerabilities that are leveraged daily by attackers. These can be exploited even by unsophisticated technical hackers who use Ransomware as a Service (RaaS) [19]. Based on the cases reviewed in this paper, attackers' motivations were mostly financial. Their objective was to cause a significant financial loss, which would result in a high ransom payment and increase the likelihood of payment. This would create a heavy reliance on the attackers for system release. Whether or not the ransom was paid was not published for the selected cases. However, in 2022, Sophos published a survey of 965 respondents which revealed that the average global ransomware payment in 2021 was almost five times greater than in 2020. In their report for the state and local government sector, they reported an increase in the volume of cyberattacks of 59%, an increase in the complexity of cyberattacks of 59% and an increase in the impact of cyberattacks of 56% [27].

Smart cities should get prepared for the worst. A future combined cyberattack on a city could involve multiple groups of attackers encrypting key data such as financial and other critical infrastructure in cities, halting various essential services including healthcare, utilities, education, governmental, communication, transportation, and other systems by making them inaccessible. They may then threaten to release the stolen data publicly or keep it encrypted until the ransom amount is paid. To increase the chances of success, other attacks may be launched in tandem with ransomware attacks, such as distributed denial-of-service (DDoS) attacks to disrupt services and phishing campaigns to gain access to user credentials. A combined attack of this sort is a huge national security risk. It could disrupt essential online services, risk people's safety in hospitals or on roads, and affect the stock exchange, raw material prices, and essential food, gas and energy supply.

What do we learn from this study? We should not only ask how to prevent breaches from occurring in cities because the reality is that in today's digital world, it has become an impossible mission. The volume of attacks is increasing, and a future possible combined cyberattack on cities is becoming a huge risk. We should ask how we can delay attackers, get an early warning on breaches to minimize the effect, and how we can deceive the attackers and keep them busy while we remediate the threat. One day it will be interesting to see attackers publish fake data that they have stolen, believing that the locked shared

drives and files were all authentic. Such a phenomenon will symbolize a different approach to fighting cybercriminals and would potentially be a small win for organizations in their endless battle with attackers. We suggest the modern honeypot triangle model for smart cities. Deception technology as an early warning detection solution can be commercially achieved by any city, implemented and customized to fit its needs. The modern honeypot triangle model for smart cities will allow security operations to deceive, bait and trick attackers, reduce the time for detection, reduce risk, and improve remediation capabilities.

Future in-depth research on similar topics in smart cities is recommended to be done on breach cases where organizations used deception technology to research if the breach impact was minimized and at what level the attacker was deceived. Other future research is recommended on the effect of deception technology on attackers targeting IoT-connected devices in cities.

4. Disclosure and conflict of interest

The author of this article is a doctoral student researcher at "Alexandru Ioan Cuza" University of Iasi and was the former COO of TrapX Security (a global leader in deception security technology), which Commvault (a global data protection leader) acquired. Today he works at Commvault as Director, Business Operations-Metallic ThreatWise. Metallic ThreatWise solution offered by Commvault is an early warning cloud data protection solution based on TrapX deception technology. The author worked in the high-tech industry for 25 years and has 10 years of experience in deception technology solutions. The author has tried to remain unbiased in writing this research.

References

[1] AlDairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science, 109, 1086-1091. doi: 10.1016/j.procs.2017.05.391

[2] Baig, Z., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., & Chernyshev, M. et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13. doi: 10.1016/j.diin.2017.06.015

[3] Biggest Data Breaches in US History [Updated 2023] | UpGuard. (2023). Retrieved 18 March 2023, from https://www.upguard.com/blog/biggest-data-breaches-us

[4] Brewster, T. (2017, April 10). Hackers Turned On 156 Dallas Emergency Sirens And The City Got Noisy. Https://www.Forbes.com/. Retrieved April 16, 2023, from https://www.forbes.com/sites/thomasbrewster/2017/04/10/dallas-emergency-alarms-hacked/?sh=37d1e91f6683Hackers target cable TV alert system and send false messages. (2020, February 22). KIRO 7 News Seattle. https://www.kiro7.com/news/local/false-alert-indicating-radiological-incident-appeared-tv-jefferson-county/KJI2SNVTZBE6DAOMYWFOQK47SM/

[5] Deception related technology - its not just a "nice to have", its a new strategy of defense - Lawrence Pingree. (2016). Retrieved 22 April 2023, from https://blogs.gartner.com/lawrence-pingree/2016/09/28/deception-related-technology-its-not-just-a-nice-to-have-its-a-new-strategy-of-defense/

[6] Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences*, *13*(2), 790. https://doi.org/10.3390/app13020790

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.(2022) https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[8] Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A master attack methodology for an AI-based automated attack planner for smart cities. *IEEE Access*, *6*, 48360-48373.

[9] Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M.C.S., Nauer, K.S., Divis, K.M., Jones, A., Combs, A. and Abbott, R.G., (2018). The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception (No. SAND2018-5870C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[10] Ferguson-Walter, K.J., (2020). An empirical assessment of the effectiveness of deception for cyber defense.

[11] Fiscus, E. L., & Booker, F. L. (1995). Is increased UV-B a threat to crop photosynthesis and productivity?. *Photosynthesis Research*, *43*, 81-92.

[12] Freed, B. (2022, April 21). Illuminate education breach that affected NYC schools spreads to Connecticut. StateScoop. Retrieved March 19, 2023, from https://statescoop.com/illuminate-education-coventry-connecticut-breach/

[13] Golubchikov, O., & Thornbush, M. J. (2022). Smart Cities as Hybrid Spaces of Governance: Beyond the Hard/Soft Dichotomy in Cyber-Urbanization. *Sustainability*, *14*(16), 10080. https://doi.org/10.3390/su141610080

[14] Green, M. (2017). Romanian hackers infiltrated 65% of DC's outdoor surveillance cameras | CNN Politics. Retrieved 18 March 2023, from http://edition.cnn.com/2017/12/20/politics/romanian-hackers-dc-cameras/index.html

[15] Greig, J., Staff, T. R., Azhar, A., Branscombe, M., Hughes, O., Miles, B., & Greenberg, K. (2021, January 26). Governors hear about the dangers of a lackluster cybersecurity response, need for FBI coordination. TechRepublic. Retrieved March 19, 2023, from https://www.techrepublic.com/article/governors-hear-about-the-dangers-of-a-lackluster-cybersecurity-response-need-for-fbi-coordination/

[16] Honeypot (computing) - Wikipedia. (2021). Retrieved 22 April 2023, from https://en.wikipedia.org/wiki/Honeypot_(computing)

[17] Ijaz, S., Munam, A. S., Khan, A., & Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2)https://doi.org/10.14569/IJACSA.2016.070277

[18] Lardieri, A. (2019, August 20). Hackers Hold Computers of 23 Texas Towns For Ransom. Www.Usnews.com. Retrieved April 16, 2023, from https://www.usnews.com/news/national-news/articles/2019-08-20/hackers-hold-computers-of-23-texas-towns-for-ransom

[19] M. T. I. C. (. (2022, May 9). *Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself*. Www.Microsoft.com. Retrieved April 22, 2023, from https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

[20] Montalbano, E. (2021, February 9). *Hacker Tries to Poison Water Supply of Florida Town*. Https://Threatpost.com/. Retrieved April 16, 2023, from https://threatpost.com/hacker-tries-to-poison-water-supply-of-florida-town/163761/Cost of a data breach 2022. (2023). Retrieved 19 March 2023, from https://www.ibm.com/reports/data-breach

[21] New Orleans Declared A State of Emergency And Takes Down Servers After Cyber Attack. (2019). Retrieved 16 April 2023, from https://time.com/5750242/new-orleans-cyber-attack/

[22] NIS 2 Directive (2023). Available at: https://www.nis-2-directive.com/ (Accessed: 26 February 2023).

[23] Ogbodo, E. U., Abu-Mahfouz, A., & Kurien, A. M. (2022). A Survey on 5G and LPWAN-IoT for Improved Smart Cities and Remote Area Applications: From the Aspect of Architecture and Security. *Sensors*, *22*(16), 6313. https://doi.org/10.3390/s22166313

[24] Popescul, D., & Genete, L. D. (2016). Data security in smart cities: challenges and solutions. Informatica Economică, 20(1).

[25] Rani, A. (2022). Belarusian Railway experiences cyber breach. Retrieved 18 March 2023, from https://www.railway-technology.com/news/belarusian-railway-cyber-breach/
[26] Smart Cities: Threats and Countermeasures. (2023). Retrieved 18 March 2023, from https://www.rambus.com/iot/smart-cities/
[27] Sophos (2022, September 28). Nearly 75% of Local and State Government Organizations Attacked by Ransomware Had Their D*ata Encrypted, Sophos Survey Finds*. Https://www.Sophos.com/. Retrieved April 21, 2023, from https://www.sophos.com/en-us/press/press-releases/2022/09/local-and-state-government-organizations-attacked-by-ransomware
[28] Staff, S., Xiao, M., & Wang, C. (2022). Ransomware attack at La. city under investigation. Retrieved 19 March 2023, from https://www.scmagazine.com/brief/risk-management/ransomware-attack-at-la-city-under-investigation
[29] The Threat Report: Fall 2022 | Trellix. (2023). Retrieved 19 March 2023, from https://www.trellix.com/en-us/advanced-research-center/threat-reports/nov-2022.html
[30] Thomas, D., & Staff, S. (2022). State Bar of Georgia ransomware attack led to data breach. Retrieved 19 March 2023, from https://www.scmagazine.com/brief/ransomware/state-bar-of-georgia-ransomware-attack-led-to-data-breach
[31] Thomas, D., Thomas, D., Thomas, D., & Staff, S. (2022). The state of ransomware in state and local government. Retrieved 19 March 2023, from https://www.scmagazine.com/resource/ransomware/the-state-of-ransomware-in-state-and-local-government
[32] Thousands Exposed in Municipal Website Breaches. (2023). Retrieved 18 March 2023, from https://www.govtech.com/security/thousands-exposed-in-municipal-website-breaches.html
[33] TRUȚĂ, F. (2023). Two families sue Amazon over Ring security cam hacks. Retrieved 19 March 2023, from https://www.bitdefender.com/blog/hotforsecurity/two-families-sue-amazon-ring-security-cam-hacks/
[34] Ullo, S. L., & Sinha, G. R. (2020). Advances in smart environment monitoring systems using IoT and sensors. Sensors, 20(11), 3113.
[35] Vandercruysse, L., Buts, C., & Dooms, M. (2021). Public Procurement as a Safeguard for Competition: The Case of Smart City Services. CoRe, 5(2), 102-111. https://doi.org/10.21552/core/2021/2/5
[36] Varfolomeev, A. A., Alfarhani, L. H., & Oleiwi, Z. C. (2021). Overview of Five Techniques Used for Security and Privacy Insurance in Smart Cities. *Journal of Physics: Conference Series, 1897*(1)https://doi.org/10.1088/1742-6596/1897/1/012028
[37] Voyant Tools. (2023). Retrieved 22 April 2023, from https://voyant-tools.org/
[38] Williams, C. (2017, January 27). Hackers hit dc police closed circuit camera network city officials disclose. Www.Washingtonpost.com. Retrieved April 16, 2023, from https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html 63c4b4fb5a63_story.html?utm_term=.09d45f71c953&tid=a_inl_manual
[39] Young, K. (2021). Cyber Case Study: City of Atlanta Ransomware Incident - CoverLink Insurance - Ohio Insurance Agency. Retrieved 19 March 2023, from https://coverlink.com/case-study/city-of-atlanta-ransomware/