Security Evaluation

Tannaz Kalatian

23 June 2020

Table of Contents

Introduction

The COVID-19 pandemic has forced organisations and countries to embrace new practices such as social distancing and remote working. Businesses are reconsidering ways to ensure that their employees are safe by developing new solutions. However, while the world is focused on the health and economic threats posed by COVID-19, cyber threat actors are motivated to gain advantage of this crisis.

We are seeing both the likelihood and impact of cyber attacks increasing and cyber security good practices may fail as companies become more technology dependent and users working remotely. The current threat landscape is changing as attackers are exploiting uncertainty, unprecedented situations, and rapid IT and organisational change. Recent studies show that volumes of threats are increasing rapidly but threat actors are using the same Tactics, Techniques and Procedures (TTPs).

In this report, we will dig deeper into these concerns and explore several solutions.

The rest of this report is organized as follows:

Section 2 provides the background information. Section 3 explains the cyber threat landscape and how it is affected by bringing some examples. The proposed solutions and their evaluation will be expanded in Section 4. Finally, we will conclude the report in section 6 followed by references.

Background

Before going into details, there are some concepts used in section 3 and 4 which I will explain briefly.

Malware: Generally, people call a software a malware when the purpose of that software is exploiting a computer. It has various types such as computer viruses, trojan horses, ransomware, etc. This word is a combination of Malicious Software.[1]

Business Email Compromise (BEC): It is a type of cybercrime with targeting a specific company and organization. It mostly happens with spoofing an employee of the organization and trying to breach other colleagues.[2]

Security information and event management (SIEM): SIEM consists of various tools that have two main components: 1. keeping the log files with purpose of analysing the data and security events, 2. Real-time monitor and alert the

administrator of the system about various security issues and incidents. For example, the siem is logging all the personnels' activities. Then, if someone is logging in to the profile in a weird hour or any other suspicious act , the system will detect it and alert them. [3]

Use case: The rules and actions which are set previously in order to enhance the security of a system is a use case in cyber security. Generally, articles categorize it into three main groups: Real-Time Rule-Based Use Cases, Real-Time Security Analytics Use Cases, Batch Security. For example, if an employee attempts a wrong password more than 5 times, the system should give an alarm. Setting this rule is a use case.[4]

Blue team: Blue teamers are the security analysts working in a security operation system (SOC) defending against the cyber security attacks around the clock (24/7).[5]

Threat Landscapes

As the COVID-19 exacerbates into a worldwide pandemic, threat actors continue to manipulate the information flow to spread malware and exploit the panic for malicious gain.

There are several types of threats with consumption of Covid-19 such as:

1. **Spam emails:** researches show that since the users should work from home, they mainly use email and online software, which leads to increasing the number of spam emails, including malicious attachments. These emails encourage users to donate to health organizations, getting bank information for tax reduction, etc. [6]
2. **Malicious websites:** there are some websites with tempting domain addresses to visit such as antivirus-covid19[.]com and corona-antivirus[.]com. They appear when someone searches about COVID-19 on the Internet. Moreover, in some countries, due to lack of face mask, some website with a domain name such as buycoronavirusfacemasks[.]com .[6]
3. **Malicious social media messaging:** Since many entertainment websites such as HBO gave a free membership to encourage people to stay home, attackers use this opportunity and send some links throughout the Facebook messenger to offer people some free membership to Netflix or similar as a promotion. Another scenario was asking users to log in to their Facebook and giving them a survey to fill to offer the Netflix promotion.[6]
4. **Malware:** The spread of information stealing malware has been increased due to the COVID-19 crisis. We also can see many businesses are suffering from Ransomware attacks .[6]

5. **Business Email Compromise (BEC):** Adversaries are leveraging COVID-themed scam emails to trick victims to send payments to attacker-controlled accounts [7].
6. **Ransomware:** Two types of downloads for the malware are coronavirus ransomware and password stealing trojan. Attackers attacked one of the Czech Republic hospitals. [6]
7. **Mobile threats:** These kinds of attacks mainly on Android lock the user's phone and ask money from them, until they pay the money. Otherwise, the attackers will delete users' data. [6]
8. **Browser Apps:** Some apps are being downloaded when a user clicks on a title such as the COVID-19 Inform app. When this app has been downloaded, it steals all the browser history, payment information, cookies, etc. [6]

Figure 1 maps the recent notable security incidents to geographic location. Figure 2 shows the trend of the COVID-19 related newly registered domains over the past couple of months.

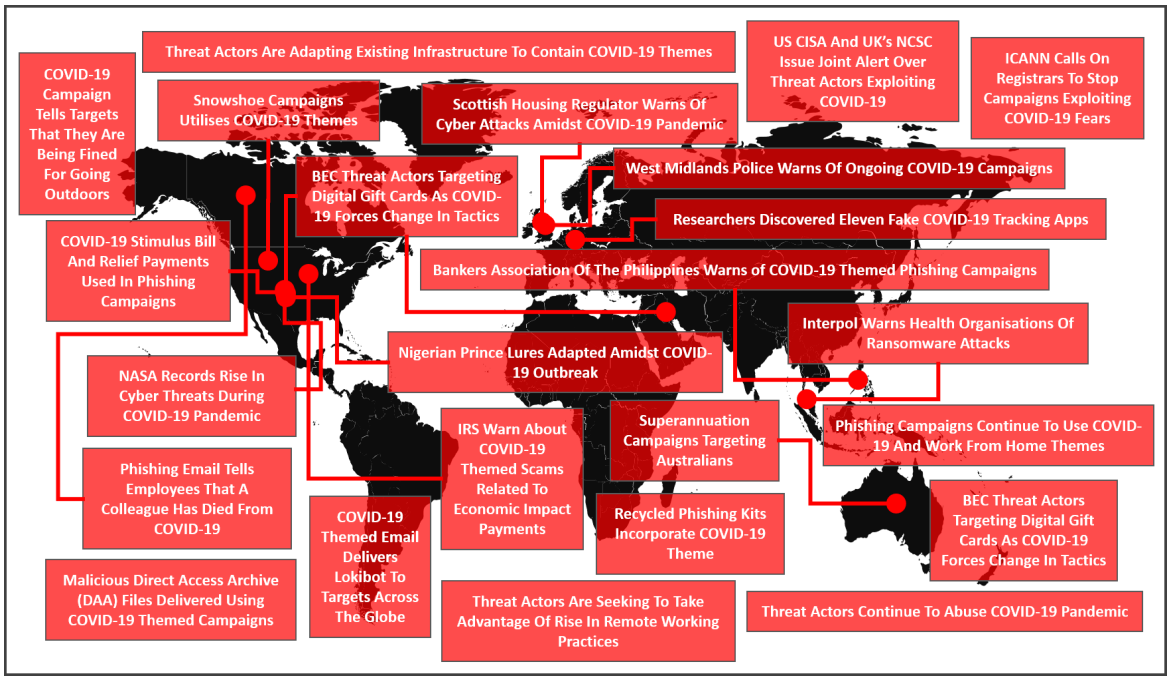

Figure 1: COVID-19 Themed Notable Events [9-15]

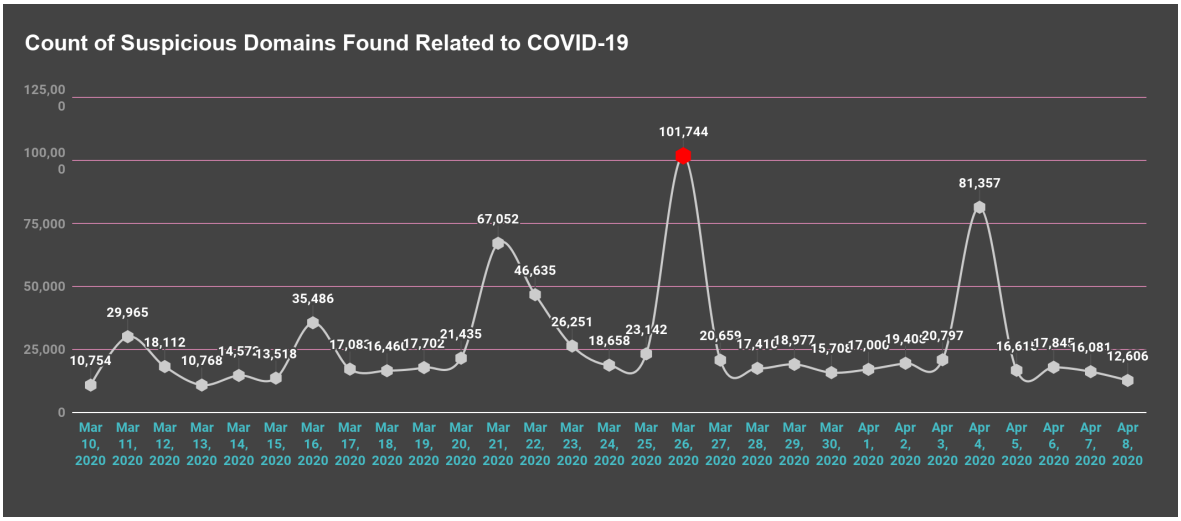

Figure 2: Significant increase in the suspicious Covid-19 related newly registered domains [8]

Proposed Solution

Most of the big organizations are leveraging SIEM products to collect data from various sources. This enables them to correlate security events and build detection rules (Use cases). Security analysts and network admins are expected to investigate these security alerts to detect security incidents (Blue team). It requires several detection rules to reduce the risk of Covid-19 cyber themed attacks. Here, we are exploring two solutions.

Solution 1	
Hypothesis	Threat actors are registering new domains with covid related keywords in it to trick users into opening an email or clicking on a link. This rule reduces the risk of end users getting phished. Goal of this solution is to detect malicious presence of newly registered domains in the organization.
Requirements	1. SIEM (or any other correlation engine) 2. Firewall or Proxy logs

	3. Email logs
Detection Logic	Compile the list of newly registered domains daily (It's free): • **Scenario 1:** Look for incoming emails from these domains daily (As a report). • **Scenario 2:** Look for any network traffic to the newly registered domains.
False positives	Based on the environment and users behaviour, these solutions might have high FPs. We can perform one or all of the following suggestions to reduce the noise: Scenario 1: 1. Exclude sender domains ending in ".com", ".ca", and "org". 2. Ignore emails if it was only sent to less than X recipients. 3. Search only for emails with an attachment or link in the body. Scenario 2: 1. Exclude sender domains ending in ".com", ".ca", and "org". 2. Only look for POST requests. 3. Only look for HTTP requests.
Performance	Network traffic files are very heavy and searching among them might take up to hours. Depending on the SIEM performance, we can compile the newly registered domains upto 2 weeks (age<2weeks).

Solution 2	
Hypothesis	Adversaries are leveraging the Covid-19 crisis to craft malicious emails and trick users based on Covid themed subjects. We are leveraging Machine Learning and Natural Language Processing (NLP) to Detect Malicious COVID themed phishing emails. High level

	process is shown in Appendix A.

Requirements	1. Email Security Logs
	2. Python Libraries:
	  a. Sickit Learn
	  b. Spacy
	  c. Pandas

Detection Logic	1. Compile a list of benign Email Subjects from the client environment. It is important to use the client data for training in order to get a better result.
	2. Compile a list of malicious Email Subjects.
	3. Note: 0 means benign and 1 means malicious
	4. Use NLP and Machine Learning to train the model.
	  a. Get a list of unique inbound emails
	  b. Use the train model to detect suspicious domains.
	  c. Investigate each malicious Email Subject
	  d. Retrain the model every X days with new data.

False positives	Evey machine learning solution has false positive problems by nature. We can reduce the false positive by: 1. Adding more features from email header 2. Label the data and retrain the model
Performance	• Training: this might take up to hours to train the model. But we only need to train once a week. • Testing: once the model has been trained, the testing would be fast. This is also dependent on the ML algorithm that we used.

Conclusion and Evaluations

Finally, for evaluating the solutions, both solutions have some drawbacks that lead to having false-positive results. To avoid false-positives, I brought some solutions as well. I also explained the requirement, which shows the **deployability** evaluation. Moreover, the **usability** evaluation has been shown in the performance explanation. As much as a system is usable, the performance should be better. Both solutions are working for the spam emails and software malicious and most of the links containing malware, therefore, the solutions will enhance the **security** of the system to avoid exploiting the computers and servers of enterprises and companies.

References

[1]:https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN

[2]:How to Recognize a Business Email Compromise Attack

[3]:What is SIEM | Security Information and Event Management Tools

[4]:5 Key Cloud Security Use Cases

[5]:https://en.wikipedia.org/wiki/Blue_team_(computer_security)#cite_note-ref1-1

[6]:Developing Story: COVID-19 Used in Malicious Campaigns - Security News

[7]:https://www.bleepingcomputer.com/news/security/ancient-tortoise-bec-scammers-launch-coronavirus-themed-attack/

[8]:https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

[9]:NASA Warns Employees of 'Exponential' Increase in Cyber Threats

[10]:COVID-19 Themed BEC Scams

[11]:IRS issues warning about Coronavirus-related scams; watch out for schemes tied to economic impact payments

[12]:Spearphishing Campaign Exploits COVID-19 To Spread Lokibot Infostealer

[13]:Cybercriminals targeting critical healthcare institutions with ransomware

[14]:Scottish Housing Regulator warns of cyber attacks as RSL targeted

[15]:Banks warn public vs new phishing method – The Manila Times