Analysis of the attack vectors used by threat actors during the pandemic

2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT) | 978-1-7281-7443-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/CSIT49958.2020.9321897

Vitalii Susukailo
Lviv Polytechnic National University
Department of Information Security
Lviv, Ukraine
Vitalii.A.Susukailo@lpnu.ua

Ivan Opirskyy
Lviv Polytechnic National University
Department of Information Security
Lviv, Ukraine
https://orcid.org/0000-0002-8461-8996

Sviatoslav Vasylyshyn
Lviv Polytechnic National University
Department of Information Security
Lviv, Ukraine
Sviatoslav.I.Vasylyshyn@lpnu.ua

***Abstract* — this article describes attacks methods, vectors and technics used by threat actors during pandemic situations in the world. Identifies common targets of threat actors and cyber-attack tactics. The article analyzes cybersecurity challenges and specifies possible solutions and improvements in cybersecurity. Defines cybersecurity controls, which should be taken against analyzed attack vectors.**

Keywords—threat actor, attack vector, malware, analysis, incident response, business continuity, Cyber Kill Chain.

I. INTRODUCTION

According to the World Health Organization, a pandemic is defined as the "worldwide spread of a new disease.". From a cybersecurity perspective, it means – disaster. During disasters, the quantity of cybercriminals is rapidly growing every day. As more specialists join their ranks, more malware is being launched daily, with approximately 230,000 new malware samples per day according to the information from PandaLabs security researchers statistics. The pandemic can be considered as an event, which can lead to business continuity plans execution or disaster recovery activities implementation. During this time growing quantity of cybersecurity threats should be analyzed, and applicable security measures should be defined. There are also plenty of administrative information security problems, which should also be taken into account. What to do with on-premise infrastructure monitoring? How to ensure high-level vulnerability management and incident response? Which management activities should be performed in Security Operations Centers? Answers on these questions provided in the following article, as well as in-depth analysis of attack vectors and security measures, which can be applied to prevent them.

II. CYBERSECURITY CHALLENGES CAUSED BY COVID-19

The COVID-19 pandemic situation changed work principles. People were concerned, and with this concern, they had a desire for information, a sense of security and support. At the same time, organized crime groups exploit the fear, insecurity and doubt associated with COVID-19, leaving individuals and entire companies vulnerable.[1] Due to that situation, private organizations and government institutions started to ensure operational activities remotely, which causes many security issues. At the same time, critical infrastructure objects, such as operational, infrastructure hospital assets and IoT's became to be prior targets for threat actors.

In-depth analysis of attack surface and cybersecurity state during COVID-19 defined four main cybersecurity challenges, described below.

Insufficient protection of critical infrastructure. The following challenge can lead to an increased quantity of private and government Security Operations Centres. Also, it can affect the quality of services which provides Security Operations Centres. Cybersecurity experts need to provide high-level security monitoring, vulnerability management and incident response to ensure that there will not be interruptions in critical infrastructure and personal patient data will be protected.

An insufficient number of Cyber Security specialists is an actual problem nowadays, and the pandemic situation shows how important it is to have qualified experts, which ensures the protection of information in government and private organizations. Following challenge can lead to improving the educational system in Cyber Security and increasing quantity institutions, which can prepare qualified specialists. [2]

Business continuity and disaster recovery processes must be improved. The situation with COVID-19 showed that a lot of operational security activities could not be performed remotely in organizations, which build their security solutions on on-premise infrastructure assets. It is expected that more cybersecurity solutions will be provided for end-users using Software as a Service model and use more agent-based approach.

Insufficient social engineering awareness level. Hackers weaponized COVID-19 map, manipulated information from WHO and other healthcare organizations, created many infected phishing websites, which jeopardized millions of users. Following challenge can lead to increasing of quantity of government social engineering awareness programs.

III. ANALYSIS OF ATTACK VECTORS

The most necessary part of attack vectors analysis is to understand the motivation of threat actors. The motivation during a pandemic is the financial gain which caused by the financial crisis in the world. Hackers can compromise organizational infrastructure or get unauthorized access to data or information, which can be used for financial gain. [3]

Also, hackers disrupt or sabotage manufacturing, electric power generation etc. to create chaos and anarchy. When motivation is defined, it is necessary to understand how the attack is performed. As the best practice, the Cyber Kill Chain, shown on Figure 2 can be used, analyze the attack vector at any point in the intruder's campaign [4] .

Cyber Kill Chain model was used to analyze attack vectors during a pandemic. Attack vectors were divided into three groups: social engineering attacks, attacks, which interrupts critical business functions, attacks on critical infrastructure.

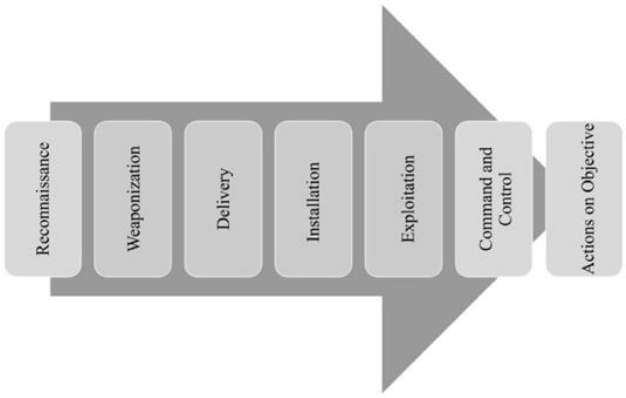

Fig. 1. Cyber Kill Chain

A. *Social engineering attacks*

The most common and popular attacks during a pandemic is a group of social engineering attacks, which uses people fears or compassion. For analysis were selected social engineering attacks during COVID-19, which used Alozurt malware.

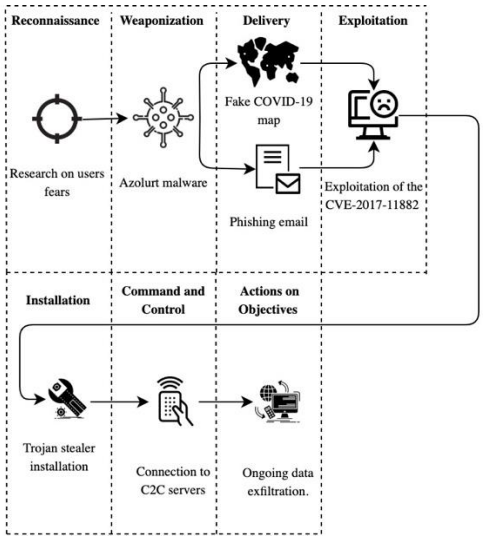

Fig. 2. The social engineering attack vector

During the reconnaissance phase, the attacker researched about most common end-user fears – the necessity of information about COVID-19. The most popular resources which users visited during pandemic were online interactive COVID-19 maps, which shared information about infection state in different countries. The second information source for people were newspapers. So the attackers used people fears and created thousands of fake COVID 19 Maps and fake news websites.

Then the attackers develop malware. The popular one was Azolurt, which is an information stealer malware that is targeted at stealing credentials and accounts.[5]

To deliver Azolurt, malware were used fake COVID-19 Online maps or phishing emails. The malware was delivered as a Microsoft Office document, which made it more simple for attackers to manipulate end-user fears. When the user opened file malware exploits the CVE-2017-11882 Microsoft Office Equation Editor vulnerability and downloads malicious executable. A malicious executable file then proceeds to make changes in the registry so that the system runs it at the system start.

At the final stage, the malware launches itself and then proceeds to steal the personal data and connect to the Command and Control servers. Then, a malicious executable file starts cmd.exe to delete itself after a 3-second timeout.

The first attack vector shows how threat actors exploit end-users fears. The second attack vector, which consists of social engineering techniques during the pandemic situation rely on human compassion. Attackers created multiple fake charity websites to deceive people and earn money or infect end-user assets by malware.

The third attack vector, which uses social engineering techniques is fake online shops, which sell medicine or medical supplies. The purpose of such websites is financial gain. To prevent this type of attacks information security controls must refer to defense in depth information assurance strategy. The first control which can be applied to avoid social engineering attacks is awareness sessions or trainings, which contains examples of fake pandemic resources such as *corona-virus-map[dot]com* and official resources, which is necessary to use, such as www.who.int. The results of awareness can be tested by execution of fake phishing attack on selected group of individuals, which attended training. The second control can be enabling of phishing detection modules and email malware scanning on endpoint security software and in electronic mail delivery system setting – GSuite, Office 365 already have phishing detection and prevention capabilities. Also, to avoid this type of attack VirusTotal browser extension can be installed, which will ensure websites filtering.

B. *Attacks, which interrupts critical business functions*

To ensure business continuity during a pandemic, commercial organizations need to provide high-level remote work capabilities, where possible. That's why most common services during remote work are VPN services, SaaS services, cloud technologies, conferencing software etc. For analysis of attack vectors on critical business, functions were selected attacks on Zoom conferencing software.

During March-April 2020, Zoom software was the primary target for attackers. Daily, threat intelligence sources informed about security and privacy issues in Zoom software, such as near 500,000 Zoom accounts sold on hacker forums, multiple critical vulnerabilities were found in Zoom desktop applications, cloud service, which stored recorded conferences was compromised. But the most widespread problem was Zoombombing, which allows attackers to join unprotected Zoom meetings. Following issue can lead from abusive content sharing, interruption of the business-critical meeting to end-users infection by malware.

The worst-case scenario, which can affect the organization is an infection of end-users by malware via sharing it in Zoom chat. When malware is shared under a legitimate user nickname, other users can download it and install on their assets. Fig 3. Attack via Zoom conferencing software describes a possible attack vector used by a threat actor to compromise organization via unprotected users.

As a first information security control to avoid attacks via Zoom conferencing software must be established password protection for meeting rooms. Ongoing malware signatures updates and deep file scanning activities could help detected malicious files shared via Zoom. Also, it is highly recommended to use endpoint detection and response software, such as Wazuh to detect anomalies on potentially infected asset.

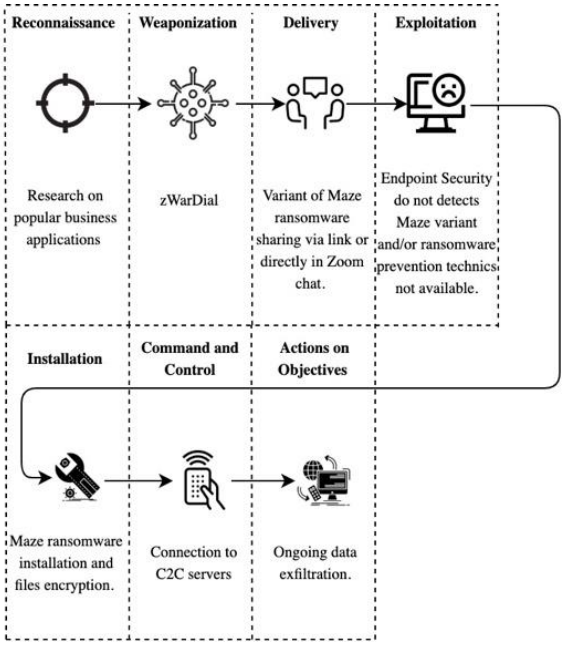

Fig. 3. Attack via Zoom conferencing software

C. Attacks on critical infrastructure

One more primary target for attackers during pandemic became to be hospitals and healthcare organizations. Attackers used standard techniques to compromise infrastructure and IoT devices through the vulnerabilities in software and services

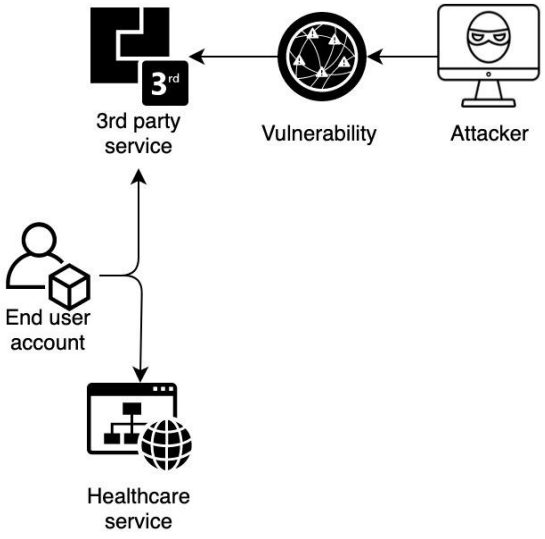

Fig. 4. Attack on healthcare services

The original attack vector was an attack through the 3rd party services. In April 2020 25,000 accounts from WHO, Gates Foundation, NIH were hacked. As informed following organizations, the attack was conducted on resources not related to healthcare organizations, but on services where those accounts were used for registration. To avoid attacks via 3rd party services supplier security verification process must be established by organizations, which integrate multiple services into one infrastructure.

IV. Preventive Measures

Pandemic complicates security operations activities. It gets harder for cybersecurity professionals to detect threats earlier and respond to them promptly. Security operations processes in organizations during a pandemic should be transformed. For Security Operations Centers, it became to be impossible to monitor network threats, which can affect their operational assets and end-users.

One more issue caused by the pandemic situation is controlled on end-user workstations. For organizations which use on-premise infrastructure, it becomes to be impossible to manage workstation without an active VPN connection.

Another issue is the vulnerability management process, which is built on central vulnerability scanning solution To prevent attacks and minimize information security risks during pandemic were defined information security controls, which should be applied to avoid analysed attacks and other pandemic threats.

A. Remote endpoint management

During an epidemic, it's necessary to ensure remote endpoint management. Cybersecurity specialists should be able to enforce security configurations remotely. Security policies, such as password policy, account lockout policy etc. should be applied. Operating system and services should be updated automatically. Also, the remote connection to end-user assets should be ensured to perform system troubleshooting activities.

B. Endpoints hardening

Endpoint hardening strategies need to be improved. To ensure secure work conditions for users, which performs their daily duties from home endpoint security software should be configured to be manageable from the cloud or through the Software as a Service management centre. Antimalware applications need to receive signatures directly from vendor threat intelligence sources. Endpoint detection and response software, with cloud-based management centre, should be installed on end-users endpoints. Endpoint firewall rules should be configured to allow remote connections to the workstations only from organizational IP's; unnecessary ports should be disabled. It's necessary to install web filtering and application control solutions, which can minimize risks of end-user compromisation from unknown resources. This will give an ability for cybersecurity professionals to perform ongoing security monitoring and detect anomalies on end-user workstations.

C. Remote vulnerability management

Network-based internal vulnerability scanning is a common approach nowadays. But in case, when users are not working from organizational facilities, it's impossible to detect security vulnerabilities on end-user workstations. Agent-based vulnerability scanning systems need to be used to replace network-based scanning software and detect vulnerabilities during remote work. Ongoing vulnerability monitoring should be ensured.

D. Business continuity management

Pandemic is a challenge for government and private organizations, which can lead to business continuity plan activation. Digital transformation and migration to the cloud should be considered by organizations, which rely on on-premise infrastructure.

E. Information security awareness

An important cybersecurity control during a pandemic is information security awareness. Social engineering awareness should focus users on fake pandemic news and informational resources, and available examples should be provided. Also, users should be informed about online shops and charity websites, created by threat actors.

F. Services Hardening

For each service used in the organization should be applied to additional hardening measures. Multi-factor authentication should be applied where possible for all user accounts. Additional alerting and logging capabilities should be configured. Administrator's accounts need to be under control, and anomalies from those accounts need to be analyzed more deeply.

The attack vector, which describes activities, which compromise critical business functions, shows how important it is to apply security configurations, provided by the vendor. In the case with Zoom application it was necessary to apply password protection for meetings, apply the configuration, which requires meeting participants to be accepted by the host, temporary do not store recorded videos in compromised Zoom cloud and apply MFA. Those simple hardening measures can be used to prevent users from been compromised.

Also, to protect organizational assets, secure connection to organizational on-premise services should be established via VPN services and approved remote management tools.

G. Legal issues prevention

To avoid legal issues, organizations should review their contractual agreement with customers, which contains information security requirements. That would allow the organization to prevent contractual agreement's violations.

H. Remote Incident Response

To ensure remote incident response during a pandemic, organizations must ensure ongoing remote connection to users endpoints and availability of communication channels which will be used by the incident response team.[6]

I. Remote Security Monitoring

Remote security monitoring should be focused on analyzing events from endpoints via host-based intrusion detection systems, endpoint detection and response solutions and endpoint security software, which allows remote management and events aggregation in the central console. Also, security analysts need to pay attention to events and logs from organizational services and cloud infrastructure assets.

It's a common approach to have distributed Security Information, and Event Management(SIEM) system, which is built on on-premise infrastructure But during the pandemic situation, it would be more useful to perform security monitoring using SaaS SIEM, or SIEM deployed in cloud infrastructure.

V. CYBERSECURITY TOOLKIT FOR THE PANDEMIC

Cybersecurity toolkit during a pandemic should be selected by each organization independently, depends on its type of organization and functions, which need to be archived.

Based on information security controls and attack vectors provided in the research, common cybersecurity toolkit open-source solutions were defined and specified in Table 1.

TABLE 1. CYBERSECURITY TOOLKIT FOR THE PANDEMIC

Security Control	Solution	Purpose
VPN	OpenVPN	Ensures secure remote connection to on-remise infrastructure
HIDS	OSSEC, Wazuh	Host-based intrusion detection system should be used to detect threats on endpoints.
Backup and Recovery	Bacula, Urbackup	Backup software is necessary to restore critical business infrastructure during the pandemic.
Infrastructure Monitoring	Zabbix, Nagios	Infrastructure monitoring software should be used to monitor the on-premise infrastructure state.
Endpoint Protection	Armadito, Clam Av	Endpoint protection software should be used to avoid malware infection.
IT Automation	Ansible	Ansible is useful to apply common security configurations for operational assets.
Vulnerability Management	Wazuh	Wazuh can be used to detect vulnerabilities on endpoints.
Patch Management	OPSI	Patch management tools must be used to update endpoints and infrastructure assets.
Security Orchestration	Patrowl Demisto	Security Orchestrations platforms need to be used to automate security operations activities during a pandemic.

The proposed toolkit should be used to initiate infrastructure and endpoints hardening and improve current cybersecurity controls.

ACKNOWLEDGEMENT

Pandemic forced organisations and individuals to embrace new practices such as remote working. It provides new challenges for cybersecurity area. New approaches, techniques and solutions, should be developed during the next years to ensure secure remote working conditions and more advance controls for critical infrastructure. The defined preventive measures in the following article can be applied to ensure appropriate security controls during a pandemic.

REFERENCES

[1] "Recommendations for enhancing cybersecurity contols during COVID -19", https://home.kpmg/ua/uk/home/insights/2020/04/covid-19-cyber-security.html

[2] D. Dubov, COVID-19: KEY CYBERSECURITY TRENDS, NSS 2019.

[3] John Wileym. Carbon Black Special Edition, "Threat Hunting For Dummies". Inc. 111 River St. Hoboken, 2017, pp 9.-10.

[4] O. Milov, A.Voitko, I. Husarova, I. Opirskyy, O. Fraze-Frazenko, et al., "Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems" Eastern-European Journal of Enterprise Technologies, 2019.

[5] "Alozurt - malware analysis", https://any.run/malware-trends/azorult

[6] "Incident Response and Remediation When Working Remotely", https://www.crowdstrike.com/resources/crowdcasts/conducting-incident-response-and-remediation-remotely/