BULLET: Jurnal Multidisiplin Ilmu
Volume 01, No. 02, April-Mei 2022
ISSN 2829-2049 (media online)
Hal 192-202

Surge of Cyber Scams during the COVID19 Pandemic: Analyzing the Shift in Tactics

Goutham Kacheru[1], Rohit Bajjuru[2], Nagaraju Arthan[3]

[1]Infostretch Corporation, United States

[2]Southern Illinois University Edwardsville

[3]University of Cumberlands, Williamsburg, Kentucky.

[1]Goutham.Kacheru@Infostretch.com, [2]rohitmyself17@gmail.com, [3]Narthan8486@Ucumberlands.edu

Abstract: The global society was majorly impacted due to the COVID19 pandemic, introduction of new normal and providing different opportunities for the cyber criminals. The paper looks into the impact of the pandemic on cybercrime, pointing out how attacks have become more commonplace and varied during a time when people are more fearful. It shows how careful examination of cyber-attacks in light of significant events in the real world reveals new techniques being applied by them. At first, there was a certain lag between the start of the pandemic and cyber-attacks related to it. However, they gradually went up until we were receiving multiple unique attacks per day. Based on data from the UK, it shows (and uses published studies where applicable) how cybercriminals took advantage of within these situations during a series of major events or government announcements to identify and create relevantly targeted campaigns. Certain recommendations are made which may be able to mitigate cybersecurity impact and help guides individuals as they deal with the changing challenge landscape.

Key words
COVID-19 pandemic, global society, cybercrime, cyber-attacks, cybercriminals, new normal, cybersecurity, cyber-attack techniques, cybersecurity impact, UK data, government announcements, targeted campaigns, mitigation recommendations,

INTRODUCTION

The life altering effects of the global COVID19 pandemic, fueled by the new strain of coronavirus SARSCoV2 virus have left entire populations isolated and many individuals dead. In addition to disrupting our society and economy, the pandemic has led to an explosion of visiting cyber-attacks and campaigns targeting cybercrime; a new risk hovering over the technology dependent world.

The spike ranges from scams impersonating public authorities and organizations to targeting platforms to launch attacks, perpetrating PPE fraud, and offering fake COVID19 cures. They take advantage of the unique stress and anxiety surrounding individuals, often working at home, while revealing weaknesses in the cybersecurity of software and other key infrastructures (e.g. healthcare services). The sudden transition to remote work on a massive scale has led to unparalleled cybersecurity issues for industry and the public, as cybercriminals have utilized both old tactics such as phishing and malware, augmented with new ones that take advantage of communication platforms.

Several technical advisories have been released on these threats by organizations such as the NCSC and CISA, but an overview of the broad spectrum of cyber-attacks related to the pandemic is yet to be compiled. Instead, information is spread out across multiple sources, and it has become very hard for organizations to leverage usable intelligence in order to devise appropriate protective as well response mechanisms against this evolving threat landscape. This paper seeks to analyze and detail how the cyber threat landscape during the COVID19 pandemic has been evolving in its tactics, and provides recommendations on how cybersecurity can improve to confront these threats better.

This work is complementary to ongoing research and presents a preliminary timeline of cyber-attacks tied to COVID19. This timeline and follow on analysis are intended to improve the understanding of these attacks, their evolution, and preparation efforts that can be made to address future events. We show that the emergence of targeted global cyber-attacks can be mapped to the spread of the virus and related events such as lockdowns, revealing patterns in which attack appearance often trails behind an announcement of a new wave of policy or other event. In this manner, we can measure the delay between the first reported cases of a pandemic in an area

and when cyber-attacks related to that pandemic begin, as well as whether attacks occurred before such reports were made.

We also give a detailed examination of some specific attacks relevant to the UK with regard to their evolution, execution, and overall impact. Outside the timeline, we talk about the extent of attacks and impact on worker vulnerability from examples reported — even risk ongoing. Our contributions include the chronological sequencing of attacks and representation of campaigns using a widely accepted attack taxonomy, facilitating work that is consistent with existing works while serving as a baseline for future attacks.

In the following sections, we conduct a review of literature on cyber-attacks and research in cybercrime, focusing on opportunities for opportunistic attacks during periods of crises (Section 2). Section 3 is the COVID19 cyber-attack timeline, in which a case study of UK is reviewed. However, Section 4 considers the effect of these attacks on remote workers and wider tech risks. In Section 5, the paper is concluded and future research directions are described.

LITERATURE REVIEW

Digital technologies have proliferated so widely that they have driven almost all areas of society online, from commerce to social interaction and business — the bad as well as good comes into our homes. Cybercrime is becoming more common and severe, with some estimates predicting cybercrime will cost $trillions annually and outnumber at least some traditional crime types. This makes cybercrime a low risk endeavor with high rewards, which is likely to ensure this pattern persists.

Perfect crime triangle similarly, our well known crime triangle can be used for cybercrime. According to this model, three factors need to come together in order for a criminal act to take place: The presence of a victim, means and opportunity. The target is the victim, the driver is the motive for a crime and the opportunity is exactly that: an opportunity to commit it such as a system weakness or sufficiently unprotected device. Other criminological models, such as Routine Activity Theory and the fraud triangle, incorporate similar elements albeit replacing the victim with means of the attacker.

Although the sophistication of modern cyber-attacks has seen a shift towards more specific and targeted attacks based on motivation whether financial gain, espionage, coercion or revenge it should be noted that opportunistic, untargeted attacks are here to stay. Opportunistic attacks are simply those that choose their victims in order to maximize chances of success against the attack. The attackers prey upon those who already have vulnerabilities, or use "hooks" an aspect of social engineering to create those vulnerabilities. So a hook is literally anything that can be used to lure an unsuspecting victim (tech, server or application) into a trap from where they will be unable to escape without being attacked. The hooks are designed to manipulate human elements of distraction, urgency and fear to make them more successful. Generally, a victim is suckered in by something of interest to lure them and is therefore an easy target for manipulation.

Cybercriminals have been quick to modify their tactics and exploit vulnerable individuals during times of crises such as the COVID19 pandemic. These attacks are designed to distract victims and take advantage of the confusion, uncertainty and emotional high that so often is involved when a person has experienced this kind of trauma. People panicking or pressed for time are more likely to fall for tricks and mess up, making them prime targets for scams and attacks. Things like having pressure at work, changes in personal life, health problems or macro stress events such as deaths and disasters only worsen this vulnerability. There are conditions to start targeting victims so, opportunistic attackers use this opportunity to target the victims when most natural disasters, crises at global level or a significant public event occurs. Thereby historically, a number of opportunistic attacks have made use of such incidents:

Natural Disasters: In the wake of Hurricane Katrina in 2005, a wealth of unscrupulous websites appeared asking for money, fraudulent emails sent local citizens seeking personal data to post to receive benefits or federal relief. And since then, we saw similar scams and attacks in the wake of numerous natural disasters such as earthquakes in Japan and Ecuador in 2016, Hurricane Harvey in 2017, and the Australian bushfires that ravaged the country back in 2020.

Significant Deaths or Events: Less than 24 hours after Michael Jackson died back in 2009, people received spam emails that allegedly provided details on the death. Later campaigns of spam emails claimed to feature private videos, photos or merchandise, but instead pointed victims toward malicious websites or had attachments with malware payloads. Cybercriminals also surf the wave of the hype linked to major public events, using scams with giveaways and ‘free tickets’ in order to commit fraud.

In 2012, hackers were able to get hold of millions of email addresses and passwords from LinkedIn in what was a monumental data breach that became opportunistically exploited as the years went on when that same data started appearing for sale on dark web marketplaces. They faced scams from blackmail and phishing, as well as accounts that had not changed caches since the breach being forgotten.

As such, the COVID19 pandemic has opened up an industry of new methods of opportunistic chumminess and attack vectors for cybercriminals looking to tap into fear, uncertainty and desperation. Cybercriminals also took advantage of the public's desire to help others during COVID19 as well, facing many phishing and scam campaigns pretending to be government agencies, healthcare groups, charities by triggering people's fears.

There are a multitude of reports showing that there has been an immense uptick in scams and malware attacks since the breakout of COVID19. Some key statistics include:

Share: Phishing Attacks – 600% increase in March 2020 alone

Global cybercrime: between December 31, 2019 and April 14 of this year a total of 30,000 new virtual attacks were registered that are related to COVID19 resulting in an increase of up to 50.1% as reported at the World Economic Forum.

COVID19 Related Cyber threats the surge of cyber threats linked to COVID19 was reported by CGI as up 30,000%.

Cybercrime in the Age of COVID19

Spam, Malware and Malicious URLs: Between January and April 2020 alone, Interpol reported nearly 907,000 spam messages along with 737 malware incidents and more than 48,000 malicious URLs on COVID19.

Ransom ware Payments: Average ransom ware payments jumped 60% in the second quarter of 2020 to $178,254; the increase could mean cybercriminals believe they have a better chance at getting paid because of pandemic circumstances.

Such attacks typically involve in demand items like PPE and COVID19 test kits, high yield investments in pandemic stocks or impersonation of public authorities like the WHO or welfare organizations.

But pinning down how much of the increase is directly linked to the pandemic, and across what types of attacks it occurred, is more difficult. Many researchers have noted a rise in cyber-attacks using COVID19related "hooks," but quantifying the extent to which these hooks replaced or supplemented preexisting forms during the pandemic would prove challenging. For instance, it is not clear how the 30,000 COVID19 related attacks reported by the WEF fits with their total 50.1% increase they report again as a single figure — nor whether other hooks were identified and their proportions. And much like CGI, they too added: "Due to the lack of data prior to the pandemic, this is based solely on [company experience]." The vagueness of these qualitative metrics makes it hard to quantify them precisely.

A TIMELINE OF CYBER-ATTACKS RELATED TO COVID19

In phases that we detail below, COVID19related cyber-attacks fall into three broad categories as they target different systems and employ increasingly sophisticated tactics:

Common cybercrime incidents due to the COVID19 pandemic are serious threats to the safety and economy of our world. The knowledge of how they work, spread and through which channels are important. Existing literature provides a range of analytical solutions, from formal definitions to systemic approaches that consider the nature of threats. But these methods, although helping to classify attacks, tend to fail when trying to map broadly distributed events like those related to the pandemic where multiple different but related events take place. Thus in this research a temporal visualization approach was selected. It enables the mapping of events without losing narrative cohesion. In cybersecurity, temporal visualizations of sequential cyber-attacks are prevalent.

Timeline creation methodology

Methods this section describes the methods used to generate a COVID19 cyber-attacks timeline. Search terms, data sources, and information sources used and types of attacks included It also points out any limitations it might have, and defines the terms used in that study.

In this particular case, "COVID19" is employed throughout in accordance with World Health Organization nomenclature.

Building the timeline required multiple searches for cyber-attacks associated with COVID19. These attacks were subsequently classified by the type of attack and method of delivery, before being ordered in chronological order. We present this information in the following sections.

This research compiles the cases of cyber-attacks, related with COVID19 using a variety of sources such as news articles from well-structured organizations and institutions, blog posts, security company reports and social media

posts. Blogs and social media is not often considered an academic source but many times provides good insight into emerging threat trends or attacks days ahead of mainstream press. While such news reports may be sensationalized, they do document genuine threats which the public faces.

This timeline summarizes attacks from mid-March to mid May 2020, and focuses on attacks that occurred before March 31st; after this date we reached what seems to be a saturation point of activity that appears representative. For further information on Kakak's attack dates, we've included the full timeline within a table that covers till May 13th, 2020; with the earliest reported attack being Jan.6,2020 and lastly March 31st, 2020 as noted in Figure (1).

Sources were collected with a similar criteria as established in literature reviews within the field of cybersecurity. We used various search engines:

- Google
- Baidu
- Qwant
- DuckDuckGo

Keywords were entered in English, Chinese, Japanese, French, Italian and Spanish and targeting the countries having considerable early COVID19 outbreaks.

Virus-related keywords included SARSCoV2, Covid, COVID19, Coronavirus and corresponding Chinese and Japanese names as confirmed by the WHO and national ministries of health. The keywords related to cyber-attacks were translated into Chinese, Japanese, French, Italian and Spanish and included words such as "Network attack", " Cyber Attack", " Hacking Attack" and " Computer attack".

To identify where we were seeing the first reports of cyber-attacks related to COVID19–we set an end date (midday 2020; last article encountered May 13th, 2020). We excluded results from behind paywalls, ones that required creating an account to view, duplicates and untranslatable.

To analyze the prominence of cyber-attacks, incidents were classified by type. There are many taxonomies of cybercrime but no general model [16]. This study employs the UK Crown Prosecution Service classification and defines cybercrime into two categories:

1Cyberdependent crimes: Crimes that can only be committed using computers or ICT

2) Cyber enabled crime: Traditional crimes that are transformed through computers or ICT in terms of scale or reach.

Table 1 – Descriptions of COVID-19 related cyber-attacks.

ID	Ref.	Country	Attack type	Description	Article date	Attack date
1	Henderson et al. (2020)	China	P.M	Vietnam accused of launching a METALJACK phishing campaign against the Wuhan district offices	22/04	06/01
2	AON (2020)	Global	P.M	International reports that both phishing and smishing campaigns are taking place	19/01	-
3	Forbes (2020)	China, Mongolia	P.M	Chinese hackers accused of distributing the Vicious Panda malware to Mongolia through emails purporting to come from the Mongolian ministry of affairs	12/03	20/01
4	F-Secure (2020)	Phillipines	P.M.F	REMCOS malware distributed to Phillipino citizens	13/03	23/01
5	Kaspersky (2020)	Singapore	P	Phishing campaign steals email log-in credentials	28/01	-
6	Walter (2020)	Japan	P.M.F	Safety measures phishing campaign distributes Emotet malware	28/01	28/01
7	smzdm.com (2020)	China	P.M.F	'Safety measure' email from a 'Singaporian specialist' distributes Emotet malware	06/02	29/01
8	Kaspersky (2020)	USA	P	Email purporting list of COVID-19 cases in victim's city takes user to website which steals credentials	11/02	31/01
9	CSDN (2020)	China	H	DoS on epidemic prevention units	09/02	02/02

10	CSDN (2020)	China	P	Phishing campaign steals email log-in credentials	09/02	02/02
11	TechRepublic (2020)	World	P.M.F	First cases of AZORult a data theft malware	10/02	-
12	cqgbxa.com (2020)	China	P.M	Email purporting specialist safety measures from WHO prompts malware download	12/02	-
13	F-Secure (2020)	Vietnam	P.M	LOKIBOT malware spread through email purporting incorrect invoice payment	13/03	03/02
14	Patranobis (2020)	China	P.Ph	Phishing attack on medical groups in China (from India)	06/02	06/02
15	freebuf.com (2020)	China	P.M.E	Distribution of CXK-NMSL ransom ware through COVID-19 themed emails	18/02	09/02
16	freebuf.com (2020)	China	P.M.E	Distribution of Dharma/Crysis ransom ware through COVID-19 themed emails	18/02	13/02
17	F-Secure (2020)	Italy	P.M	Trickbot malware distributed through email	13/03	02/03
18	Stonefly (2020)	Global	P.M.F	MBR wiper malware disguised as contact tracing information	04/03	-
19	F-Secure (2020)	USA	P.M	FORMBOOK malware distributed through email purporting parcel shipment advice	13/03	08/03
20	The Register (2020)	USA	M	Health systems in Champaign Urbana Public Health District (Illinois) affected by the netwalker ransomware	12/03	10/03
21	F-Secure (2020)	Spain	P.M	Email purports COVID-19 remedy as mooted by Israeli scientists days in advance	13/03	10/03
22	Millman (2020)	Czech	H	Cyber-attack on Czech hospital	14/03	14/03
23	Stein and Jacobs (2020)	USA	H	Denial of Service on U.S. Health Agency	16/03	-
24	Rosso (2020)	Libya	P.M	Corona live 1.1 is the SpyMax malware which in this case is a trojanised app which exfiltrates user data	18/03	-
25	Desai (2020)	World	P.M	Corona mask offer installs what appears to be a harmless malware which distributes an SMS to all contacts. Presumably an update to the app will mobilise the malware	19/03	-
26	FitzGerald (2020)	Global	P.E	Extortion campaign threatens to infect the recipient with COVID-19 unless a $4,000 bitcoin payment is made	17/04	20/03
27	Murica Today (2020)	Spain	P.M	Netwalker ransomware attack disguised as an email advising on restroom use	24/03	-
28	Koenig (2020)	USA	P.M	SMS asks recipient to take a mandatory COVID-19 'preparation' test, points to website which downloads malware	24/03	24/03
29	Glos Safe Cyber (2020)	UK	P.M	SMS informs recipient to stay at home with a link for more information. Link directs recipient to a malware ridden website	24/03	-

Often, one cyber-attack can fit within several of these categories. A combination of these malicious payloads can follow too; like, a phishing email might result in taking the user to a fake site and will try to capture personal data which uses at later stages for monetary fraud or only introducing malware that uses it at a further extortion level. The next section explains these sequential events.

In this section, we will define the types of cyber-attacks explored in this research and outline limitations of the table and timeline created.

Types of Cyber-attacks:

Phishing/Social Engineering: Individuals are deceived into taking certain actions (sharing information, visiting sites, etc.) under the impression that they are in contact with a legitimate entity. This is mostly through emails, SMS or WhatsApp messages (smishing).

Pharming: As with phishing but simply compromise systems (user system or DNS servers) and redirects user from the intended site to malicious sites. This needs slightly more tech savviness.

Technological Gestures for Financial Deception: tricking people or organizations with technology to earn money.

Extortion: When someone uses threats or force to make people do things, often financially.

Hacking: Breaching confidentiality or integrity of a system, with or without exploiting vulnerabilities.

Malware: Any software that is employed to cause a type of attack, such as interruption of service and retrieval of data. One of the more frequent versions is ransomware, malware and extortion bundled together.

Denial of service: Overwhelming services with bogus requests to interfere with genuine access and possibly take the server offline. A denial of service attack can also be used to divert people, or resources away during other attacks.

The following analysis through a timeline and discussion builds upon these forms of attack.

Limitations of the Table: There are two dates given in the table: Article Date (the actual date of publication), and Attack Date (if avail.). The table is sorted chronologically by Article Date. Both dates are listed because attacks may not always be reported right away. Disclaimer: The links to the webpages in the table may be updated after research was conducted.

Limitations of the Timeline: There are 2 kinds of cyberattack reports in timeline; some with fixed dates of attack and other without. This distinction matters for how we read the timeline of events put forward.

Furthermore, the timeline covers just the first 3.5 months of the pandemic, as the data indicated a saturation point was likely reached around mid-May 2020.

The timeline

In this section, COVID19 cyber-attacks are analyzed indepth using a timeline and details displayed in table form. Figure 2 shows, in a timeline format, the cyber-attacks reported previously, at the same time as when the first cases were identified and countries closed down [6]. The 44 cyber-attacks covered in the timeline are classified according to a taxonomy developed by the UK Crown Prosecution Service yn.

- P: Phishing (or smishing)
- M: Malware
- Ph: Pharming
- E: Extortion
- H: Hacking
- D: Denial of Service
- F: Financial Fraud

The COVID19 events on the timeline were cross referenced against the WHO timeline.

Cyber-attacks are organized by date (article date when attack date is unknown) in Table 1, which outlines the articles in greater detail. CPS Automated and Human In The Loop (HITL) Attack Surface Characterization Datasets Table. It includes the target country, attack method description, and attack type based on CPS taxonomy The figure and table investigate particular cyber-attacks and incidents. This excludes general advisories, discussions, attack summaries, and extended descriptions of attacker techniques.

CYBER ATTACKS RELATED TO COVID19 IN THE UK

This dedicates an example and focuses on COVID19related cybercrime in the UK as a case study to embrace its severe impact. Infra Gard Analysis This analysis does only analyses specific cybercrime incidents which are UK specific and does not include global attacks affecting the UK. This means that not global campaigns even if impacting UK citizens are considered.

The vast numbers of suspected suspect emails and fraud losses demonstrate the scale of this problem. The number of suspicious emails reported to the NCSC exceeded 160,000 by early May2020. As of the end of May, losses due to COVID19 scams were reported to be £4.6 million, with around 11,206 phishing/smishing victims. The NCSC removed 471 fake online shops in response, while HMRC took down a further 292 fraudulent websites.

The timeline as well as events specific to the UK and cybercrime incidents shown in Figure 3, expose both positive and negative relationships between announcements and when incidents occur. As represented by the solid colored arrows, direct correlations indicate that perpetrators used declarations or incidents to plan their attacks. Inverse correlation are events with no defined cause action correlation they can still be indirectly impacted by wider media coverage. This includes conversations about topics like personal protective equipment, or possible tax rebate programs before the formal government announcement, with phishing campaigns related to that sooner as well. But these correlations are not hard and fast rules.

March 11, 2020: UK government unveils budgetary measures such as £5 billion emergency response fund for public services, statutory sick pay for individuals who must self-isolate, support for selfemployed workers, hardship funds for councils and business interruption loan scheme; some firms have business rates abolished.

The government then went on to announce support measures on free school meal, hardship funds, extra funds for supermarkets helping vulnerable people, possible home test kits track and trace app and a job retention scheme.

Incidents like these play right into the hands of most cybercriminals who are well aware that the average would be more prone to distilling their guard down in such situations. However, if some of them seem related to certain events, other more or less classic scams like an offer to pay £250 in good will in exchange for receiving it and then refusing to do so a NHS donation request with fictitious companies or shops providing dubious supermarket vouchers through a link scam as well charitative donations have no evident strings back attached either towards the government's announcement nor some public speculations.

Cyber-attacks and related risk analysis

Taking stock of COVID19 related cybercrime, several conclusions emerge.

Cloud Security The focus on “postCOVID19” opportunistic Threat Overview: 1.Opportunistic attacks pop up to all new highs: There has been a spike of opportunistic cyber-attacks, especially phishing malware and fiscal fraud campaigns during the time of pandemic.

Attacks focusing on critical infrastructure: Cybercriminals accosting groups and types of services play a significant role in assisting COVID19 providers, exploration establishments, and vaccine masterminds.

This timeline provided in Figure 2 and the UK as an illustrative case study of pandemic based cyber-attacks The initial case report in China was followed by the first related cyber-attack 30 days later and within just 14 days, yet another assault was launched. The time between events and attacks gradually shrunk after that.

This provides the average distribution of attack types across the 43 cyber-attacks in our timeline:

- Phishing/Smishing : 37 (86%)
- Hacking: 2 attacks (5%)
- Denial of Service: 2 (5%) attacks
- Malware: 28 attacks (65%)
- Financial Fraud 15 attacks (34%)
- Pharming: 6 attacks (13%)
- Extortion: 6 attacks (15%)

Looking into the chronology of events in each attack reveals more. The timeline shows that the same sequence and patterns repeat, for example distributing malware (m) through phishing (p) to steal credentials for financial fraud (f), p,m,f. These sequences are very important because there can be many places where protective methods can be applied. Below, the attack sequences that were observed include:

- p,m: 8 attacks (19%)
- p,m,f: 10 attacks (23%)
- ph,m: 1 attack (2%)
- p,ph: 1 attack (2%)
- p,m,e: 5 attacks (12%)
- p,ph,m: 2 attacks (5%)
- p,ph,f: 1 attack (2%)
- p,e: 1 attack (2%)
- p,ph,m,f: 1 attack (2%)

The following analysis of the sequence is exclusive of the two hacks and two denial of service attacks. Although financial fraud is probably the main objective in most of the cases, it is only documented when specifically reported. Some p,m,f and p,ph,f attacks are not counted, so the real numbers are probably higher.

The early cyber-attacks by target country are shown in Figure 5 The original epicenters of the pandemic China and the USA were also leading targets, as evidenced by them accounting for a combined 39% of reported attacks. The attacks then became widespread in the UK and elsewhere. In March 2020, the majority of attacks were aimed at a worldwide audience; others continued to focus on country specific happenings such as COVID19 tax rebates.

None of the UK cyber-attacks we analyzed appeared to use malware in the way identified in the global analysis, despite search and discovery of an NHS malware distribution site on 23 April 2020, and its subsequent removal. There might be a few reasons for why that could happen:

Sophistication and Time: Malware campaigns are more sophisticated in their design and take longer to create than something simple like phishing.

Event/Announcement Connection: It may be harder to directly tie malware campaigns to specific events or announcements.

Low Time Lag between Announcement and Phishing Campaign: For some announcements, the time lag between them and a campaign is very low; such low time lags suggest that easier attacks like phishing are relatively easy to deploy in a short span of time. Notably, the "lockdown contravention fine" scam emerged merely two days after the announcement of the lockdown, similarly the job retention scam came only within two days after the unveiling of its scheme.

Phishing (smishing included) was the attack vector in 86% of global attacks seen in this analysis. Considering how affordable phishing is and decent success rates, this comes as no surprise. Phishing attacks related to COVID19 most often assumed the identity of government, WHO, NHS personnel as well as airlines, supermarkets and technology providers. Though the context of how this happened may differ, the techniques taken to get here and end objective will not.

For example, one false WHO email included a zip file that claimed to be an eBook about coronavirus origin and protective measures. The email misused WHO branding, provided helpful sounding instructions, and tugged at people with a slogan such as "your life count as everyone lives count". Other examples include a malware infested fake NHS website and fraudulent site mimicking the Johns Hopkins University COVID19 dashboard. These examples portray attackers leveraging trusted sources and weak emotional state to bypass their goals. However, the nonexistent WHO email contained spelling and grammar mistakes a hallmark of phishing attacks.

In order to increase the chances of exposures through phishing activity, cybercriminals have registered hundreds of domains that include "COVID" or "coronavirus." The domain names seem quite legitimate given they are followed by authentic organizations such as the WHO or CDC, or keywords like in Corona virusapps and many other examples. Com and anticovid19pharmacy.com. Popular communications platforms like Zoom, Microsoft, and Google have also fallen prey to similar scams via emails and domain names designed to mimic these commonly used services for work and individual use. Combined with effective social engineering in emails, SMS and hyperlinks, these tactics offer many attack vectors.

Pharming drugs often occur in conjunction with other types of attacks, though not as frequently (13% of cases). Fraud relating to COVID19 has been opportunistic by its very nature, taking advantage of governmental and scientific pronouncement and exploiting fears for monetary benefit. The top tactic used was phishing and email attacks. For instance, there was a scam email that pretended to be from the CDC asking people to donate Bitcoins for developing vaccines. Like other phishing emails, this one tried to exploit trust networks with requests for money and a plea to forward the message.

Some frauds threatened or appealed for its target, like threatening to infect someone with COVID19; offers to invest in companies promising only ways to prevent, detect or cure COVID19; as well as fraudulent schemes regarding the purported economic hardships related to and caused by the pandemic. There were also many offers of cures, vaccines and advice about treatment. Due to the abundant availability of fake products, regulatory bodies such as the FDA, OLAF and MHRA have responded by issuing warnings across searching sites related to sales of no genuine medical devices, while also opening inquiries and launching investigations.

Twelve percent of the incidents were extortion type attacks, but these are still less common. One notable abuse included an extortive email that claimed the sender would spread COVID19 to the recipient and their loved ones if they did not pay a ransom in Bit coin. To make the email seem more credible, they inserted the recipient's name and a password that could be from an older data breach.

BULLET: Jurnal Multidisiplin Ilmu
Volume 01, No. 02, April-Mei 2022
ISSN 2829-2049 (media online)
Hal 192-202

IMPACT ON WORKFORCE

Employment levels and the interaction between people and cyber enabled assets were greatly disrupted by the COVID19 pandemic, associated lockdowns, and a move to remote working. Along with technology built around resilience, socioeconomic structures, and finally modes of (mass) communication. Risk conflicts, where stringent security standards that would otherwise block data sharing are more harmful than the risks of sharing, were new with the pandemic. But that could be counterproductive, as to give an example in the UK if GPs are stopped from accessing patients' data from home during quarantine and social distancing there may actually be more harm than good. Additionally, CONFIDENTIAL patient DATA would need a DPIA for additional NHS support which may affect timely medical interventions.

Cyber Threats on Traditional Risk Classifications: asset registration and asset valuation, frequency of threat occurrences, and the probability weakness test. As a result, the workforce is expected to demonstrate changes in how they access information assets and perform their strategic, tactical, and operational tasks. This requires evolving risk statements to be originated and tested from then through threat agents, vulnerabilities, policy/process violations as well as overall asset exposure across years of emerging threat landscapes. Given these changes, the threat landscape regarding remote (telework) capability is further impacted as are attack vectors weapon zed in support of the pandemic settlement coming into October 2021. Although the long-term implications on the workforce remains unclear, their importance has already been seen. Hence, information control (storage, processing, and transmission) becomes a priority in the context of increased cyber-attacks against critical infrastructure.

Measures for trying to alleviate the effects of pandemic on data architectures and on information governance frameworks are being evaluated by governments and public and private sectors across Europe. It specifically highlights the implications of personal data processing. According to EU GDPR, personal data must be collected for specified, legitimate purposes and not further processed in a manner that is incompatible with those purposes, and the Data subject shall have the right to be informed about processing activities such as its features, nature, retention period and purpose. Tension between being compliant (with law and regulation) on the one hand, and being able to quickly access or process data at all (or at a decent speed), on the other. Such situations can also be observed with regard to the tendency of public authorities to acquire personally identifiable information in order to curb the spread of the virus, e.g. contact tracing applications and aggregate data platforms online for post processing. Such initiatives bring those data custodians an extra burden from data privacy and security perspective, which perilously calls for best practice based data protection principles to be taken into consideration at the outset of every such initiative.

Technical issues regarding the precision of DE identified personal data, consent processes and secure data disposal presented challenges for researchers using de identification technologies in high risk epidemiological investigations. The citizens became distrustful and existing processes were found ineffective given the speed with which data is being acquired and processed, along with the urgency of the situation.

Therefore, extended lockdowns in the majority of the countries tried their capacity to execute business recuperation procedures amidst a proceeding with pandemic circumstance, an undeniably troublesome exercise. On the other hand, the unprecedented speed and scale of R&D response to COIVD19 has facilitated collaborations across organizations. And one of the big challenges we faced across Europe was coordinating with all stakeholders to pass information in an accurate and timeous manner, including addressing instances where mainstream media would have spread misinformation.

As the number and magnitude of cyber-attacks rise, we will continue to overtax existing monitoring, auditing, access control and authentication schemes. Traditional defense in depth principles will be confronted, as will enterprise risk management methods and techniques — incident reporting, media disposal requirements from the U.S. To preserve sensitive data and the public trust, robust and adaptive cybersecurity has become paramount as the pandemic demonstrates.

CONCLUSION

An analysis of previous active cyber-attack campaigns using major announcements or media stories as lures demonstrates a clear relationship. That goes along with the fact that the pandemic has an impact for working practices as well longer socialization times as well over the years more time spent especially on TikTok. Rising Jobless will also Increase Cybercrime as people look for other sources of income? These two phenomena, which

we term the Duo of Deteriorating Cybercrime Interventions, warrant higher law enforcement capacity to deal with them.

One common approach seen across numerous cyber-attacks in this timeframe is using phishing campaigns to infect victims by downloading files containing malware or locations with malicious URLs, which ultimately leads to financial fraud. Campaigns of this nature are frequently designed to take advantage of media or government announcements to act more effectively. This is not a completely original tactic, but this research shows the link between it and events in the real world.

The implication of this analysis is that governments, media outlets and other institutions should be aware that announcements and stories can be used for cyber-attacks. Disclaimer or some plan about how and when the official announcement will be made can reduce this inherent risk. All the events & their intervention have a connection of cyber-attacks, and more research is required to propose predictive models. A more wide-ranging examination of distinct global cyber-attack case studies would help corroborate these results and enhance the generalizability of this detail.

REFERENCES

1. Abrams, L., 2020. New coronavirus screenlocker malware is extremely annoying. https://www.bleepingcomputer.com/news/security/new-coronavirus-screenlocker-malware-is-extremely-annoying/ (Accessed 30 May 2020).
2. Ahn, N.-Y., Park, J. E., Lee, D. H., Hong, P. C., 2020. Balancing personal privacy and public safety in COVID-19: Case of Korea and France.
3. Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 2018;4(1):1–15.
4. Anderson R, Barton C, Bölme R, Clayton R, Ganán C, Grasso T, Levi M, Moore T, Vasek M. In: Workshop on the Economics of Information Security (WEIS). Measuring the changing cost of cybercrime; 2019.
5. AON, 2020. Social engineering attacks and COVID-19. https://www.aon.com/cyber-solutions/thinking/social-engineering-attacks-and-covid-19/ (Accessed 17 June 2020).
6. AstraZeneca, 2020. AstraZeneca Advances Response to Global COVID-19 Challenge as it Receives First Commitments for Oxford's Potential New Vaccine. https://www.astrazeneca.com/media-centre/press-releases/2020/astrazeneca-advances-response-to-global-covid19-challenge-as-it-receives-first-commitments-foroxfords-potential-new-vaccine.html (Accessed on 20 June 2020).
7. Bellekens X, Hamilton A, Seeam P, Nieradzinska K, Franssen Q, Seeam A. Pervasive eHealth services a security and privacy risk awareness survey. In: 2016 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). IEEE; 2016. p. 1–4.
8. Bellekens X, Jayasekara G, Hindy H, Bures M, Brosset D, Tachtatzis C, Atkinson R. From cyber-security deception to manipulation and gratification through gamification. In: International Conference on Human-Computer Interaction. Springer; 2019. p. 99–114.
9. Bellekens, X. J., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A. W., Seeam, A., 2016b. A study on situational awareness security and privacy of wearable health monitoring devices..
10. BleepingComputer, 2020. Ransomware Gangs to Stop Attacking Health Orgs During Pandemic. https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgsduring -pandemic/ (Accessed 15 June 2020).
11. CBS Netherlands, 2020. Less traditional crime, more cybercrime. https://www.cbs.nl/en-gb/news/2020/10/ less-traditional-crime-more-cybercrime (Accessed 9 May 2020)
12. Chadwick, J., 2020. Cyber criminals create a spoof copy of the nhs website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data. https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data . Html (Accessed 30 May 2020).
13. Check Point, 2020. Coronavirus Cyber-attacks Update: Beware of the Phish. https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/ (Accessed 17 May 2020).
14. Chockalingam S, Pieters W, Teixeira A, van Gelder P. Bayesian network models in cyber security: a systematic review. In: Nordic Conference on Secure ITS Systems. Springer; 2017. p. 105–22. Ciardhuáin SÓ. An extended model of cybercrime investigations. Int. J. Digit. Evid. 2004;3(1):1–22.

15. CNET, 2017. Watch Out For Hurricane Harvey Phishing Scams. https://www.cnet.com/news/ hurricaneharvey-charity-donations-scam-phishing -attack/ (Accessed 15 June 2020).
16. CNET, 2020. Fake Coronavirus Tracking Apps Are Really Malware That Stalks You. https://www.cnet.com/news/fake-coronavirus-tracking-apps-are-really-malware-that-stalks-its-users/ (Accessed 15 June 2020).
17. Collier B, Horgan S, Jones R, Shepherd L. In: Research Evidence in Policing: Pandemics. The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations. Scottish Institute for Policing Research; 2020. Number 1
18. Cook, A., 2020. COVID-19: Companies and verticals at risk for cyber-attacks. https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for cyber-attacks/ (Accessed 17 June 2020).
19. CPS. In: Technical Report. Cybercrime - Prosecution Guidance. The Crown Prosecution Service (CPS); 2019. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (Accessed 17 June 2020)
20. cqgbxa.com, 2020. Fighting the spread of coronaviruses who faces severe cybersecurity threats. www.cqgbxa.com/newshy/67936.html (Accessed 30 May 2020).
21. Cressey, D. R., 1953. Other people's money; a study of the social psychology of embezzlement..
22. Cross M, Shinder DL. Scene of the cybercrime.. Singers Pub.; 2008.
23. CSDN, 2020. Take advantage of the fire! "The epidemic is a bait" cyber-attack. https://blog.csdn.net/weixin_43634380/article/details/104237121 (Accessed 30 May 2020).
24. Cybersecurity Ventures, 2019. 2019 official annual cybercrime report. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report (Accessed 17 June 2020).
25. Daily Mail, 2020. Cyber Criminals Create a Spoof Copy of the NHS Website in the Midst of the Coronavirus Pandemic to Trick Users Into Downloading Dangerous Malware That Can Steal Their Passwords and Credit Card Data. https://www.dailymail.co.uk/sciencetech/article-8250737/ Kaspersky-detects-fake-NHS-site-steals-credit-card-data. Html (Accessed 15 June 2020).
26. Dark Reading, 2020. Docusign phishing campaign uses COVID-19 as bait. https://www.darkreading.com/attacks-breaches/docusign-phishing-campaign-uses-covid-19-as-bait/d/did/1337776 (Accessed 30 May 2020)