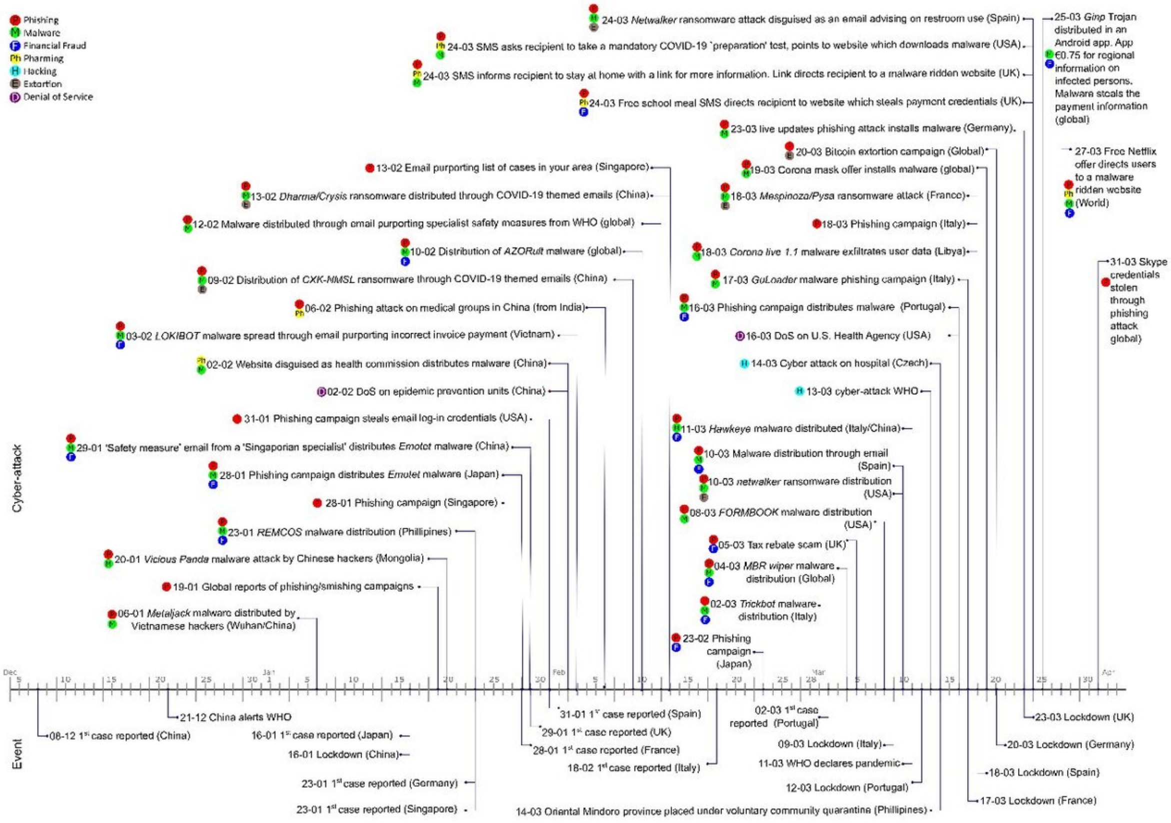
TechXplore

COVID-19-related cyberattacks leveraged government announcements

March 22 2021



Credit: University of Warwick

There has been a remarkable surge in cyber-security crime experienced during the global COVID-19 pandemic, with a particular significance between governmental policy announcements and cyber-crime campaigns. A consortium of researchers, including WMG, University of Warwick report that some days as many as 3 to 4 new cyber-attacks were being reported.

The COVID-19 pandemic created a new normal for billions of people around the world, with people working from home, ordering shopping and socializing online as shops and businesses were closed. However, with an increased amount of people being online, an increase in cyber-attacks has also been found.

Researchers from WMG, University of Warwick, Abertay University, University of Kent, University of Oxford and University of Strathclyde worked in collaboration in the study, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," published in the journal *Computers & Security*.

By using the UK as a case study, the paper reveals the explicit connection between governmental policy announcements and cyber-crime campaigns. Although this is a pattern that's been suspected for a while, this is the first analysis from 100s of cases around the world which makes this connection clear.

Since the outbreak of the pandemic in 2019 there have been reports of scams impersonating public authorities such as the World Health Organisation, and organizations such as supermarkets and airlines targeting support platforms such as PPE and offering COVID-19 cures. They often target the public, who are now socializing and spending more time online in general, as well as the increased population of people who are working from home.

Such scams can be sent by text or e-mail, and in most cases a URL pointed to a fake institutional website which requests debit/credit card details.

In order to support ongoing research, the researchers have proposed a novel timeline of 43 cyber-attacks related to the COVID-19 pandemic. This timeline and the subsequent analysis can assist in understanding those attacks and how they are crafted, and as a result, to better prepare to confront them if ever seen again.

They found that from the point that the first case was announced in China (8/12/19) the first reported cyber-attack was 14 days later. From this point onwards the timeframe between events and cyber-attacks reduced dramatically.

The cyber –attacks were categorised, and it was found:

- 86% involved phishing and/or smishing
- 65% involved malware,
- 34% involved financial fraud
- 15% involved extortion
- 13% involved pharming
- 5% involved hacking
- 5% involved denial of service

Dr. Harjinder Lallie, from WMG, University of Warwick said, "The analysis presented in this paper has highlighted a common modus-operandi of many cyber-attacks during the coronavirus period.

"Many of the cyber-attacks begin with a phishing campaign which directs victims to download a file or access a URL. The file or the URL act as the carrier of malware which, when installed, acts as the vehicle for financial fraud. The analysis has also shown that to increase the likelihood of success, the phishing campaign leverages media and governmental announcements. In fact some days we recorded as many as 3-4 new scams."

Dr. Xavier Bellekens from the University of Strathclyde, said: "Over the last year we have seen a surge in cyber-attacks targeting critical infrastructures, governments, organizations and end-users, influenced by governmental announcements. These have ranged from targeted attacks to selling counterfeited respirators to hospitals, denying of essential services through ransomware, selling fake online COVID-19 testing equipment as well as more recently, generating fake COVID travel tests. "These techniques, while common, had never been observed in relation to an event of this magnitude, making this study unique."

Dr. Lynsay Shepherd of Abertay's Division of Cybersecurity said, "Cybercrime is a highly sophisticated and organized activity and it did not come as a surprise to anyone in the cybersecurity industry that these individuals and groups used the COVID-19 pandemic as a vehicle to launch attacks.

"It is unlikely there will ever be a time when we can eradicate cybercrime. Therefore we must continue to educate everyone from as early a stage as possible, train our graduates to understand the mindset of cybercriminals as we do at Abertay, and to continue to invest in research, development, innovation and infrastructure."

Dr. Jason Nurse from the Institute of Cyber Security for Society (iCSS) at the University of Kent said, "COVID-19 has had a substantial negative impact on society, and this impact, as we show in our new research, has also meant a notable increase in cybercrime globally.

"There are several significant novel findings emerging from our analysis, but the one I found most salient was the targeted use of threats, scare tactics and fake incentives within attacks. Cybercriminals clearly understood that many people would be anxious, worried, distracted and away from their support networks (personal or work-related), and sought to exploit this as much as possible. I hope our research can provide a pathway for future work into faster reaction to these cyberattacks, and also increase society's awareness of their prevalence."

Dr. Arnau Erola, from the Department of Computer Science at the University of Oxford adds:

"Cybercriminals take any opportunity to their advantage. By getting insights on their modus operandi, polices to tackle cybercrime can become more effective. This is not only deterring cybercriminals from their unlawful activities but also educating the society about improper and unethical actions."

More information: Harjinder Singh Lallie et al. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, *Computers & Security* (2021). DOI: 10.1016/j.cose.2021.102248

Provided by University of Warwick

Citation: COVID-19-related cyberattacks leveraged government announcements (2021, March 22) retrieved 30 March 2023 from https://techxplore.com/news/2021-03-covid-related-cyberattacks-leveraged.html