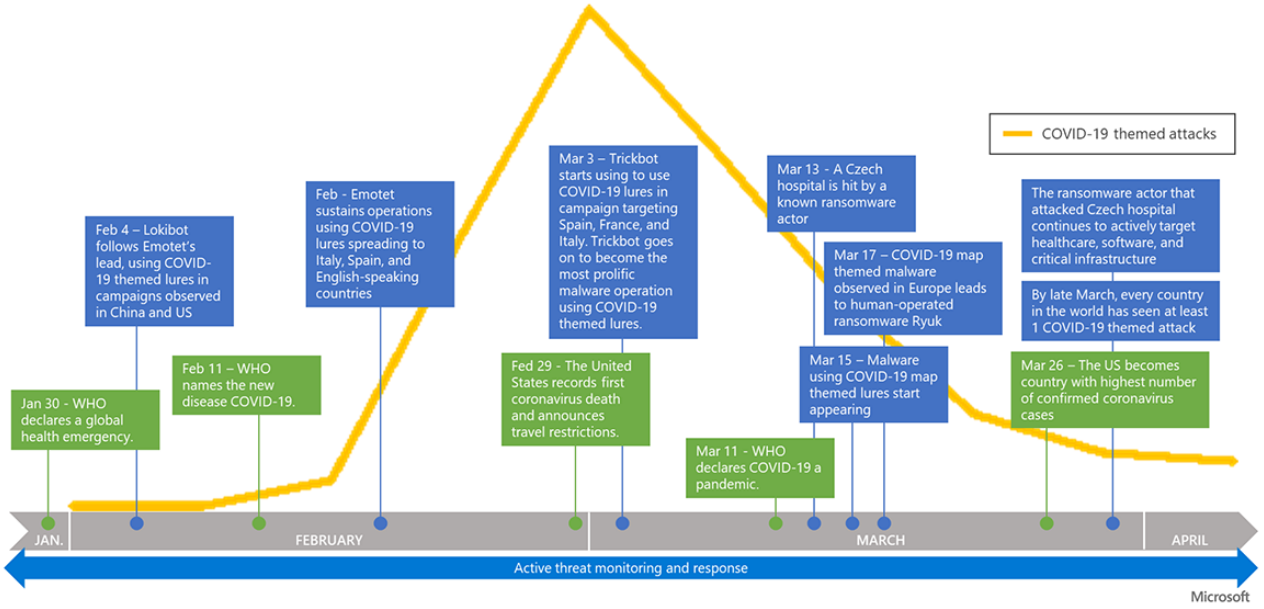
Exploiting a crisis: How cybercriminals behaved during the outbreak

microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

June 16, 2020



In the past several months, seemingly conflicting data has been published about cybercriminals taking advantage of the COVID-19 outbreak to attack consumers and enterprises alike. Big numbers can show shifts in attacker behavior and grab headlines. Cybercriminals did indeed adapt their tactics to match what was going on in the world, and what we saw in the threat environment was parallel to the uptick in COVID-19 headlines and the desire for more information.

If one backtracked to early February, COVID-19 news and themed attacks were relatively scarce. It wasn't until February 11, when the World Health Organization named the global health emergency as "COVID-19", that attackers started to actively deploy opportunistic campaigns. The week following that declaration saw these attacks increase eleven-fold. While this was below two percent of overall attacks Microsoft saw each month, it was clear that cybercriminals wanted to exploit the situation: people around the world were becoming aware of the outbreak and were actively seeking information and solutions to combat it.

Worldwide, we observed COVID-19 themed attacks peak in the first two weeks of March. That coincided with many nations beginning to take action to reduce the spread of the virus and travel restrictions coming into effect. By the end of March, every country in the world had seen at least one COVID-19 themed attack.

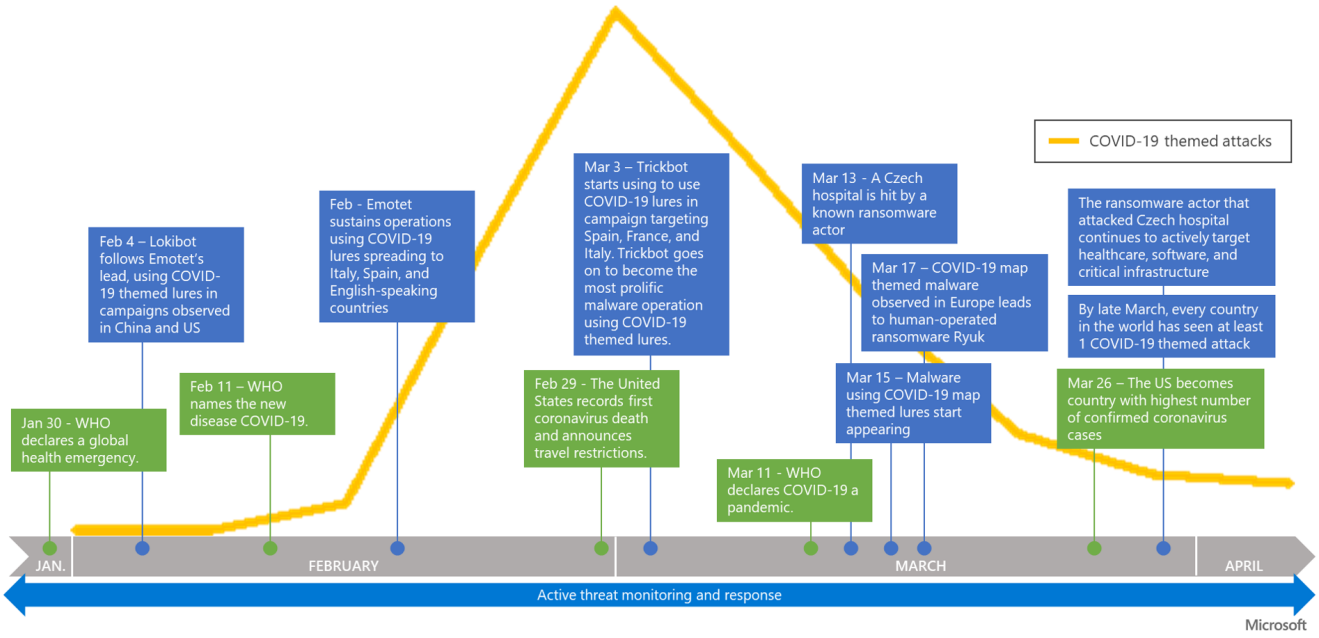


Figure 1. Trend of COVID-19 themed attacks

The rise in COVID-19 themed attacks closely mirrored the unfolding of the worldwide event. The point of contention was whether these attacks were new or repurposed threats. Looking through Microsoft's broad threat intelligence on endpoints, email and data, identities, and apps, we concluded that this surge of COVID-19 themed attacks was really a repurposing from known attackers using existing infrastructure and malware with new lures.

In fact, the overall trend of malware detections worldwide (orange line in Figure 2) did not vary significantly during this time. The spike of COVID-19 themed attacks you see above (yellow line in Figure 1) is barely a blip in the total volume of threats we typically see in a month. Malware campaigns, attack infrastructure, and phishing attacks all showed signs of this opportunistic behavior. As we documented previously, these cybercriminals even targeted key industries and individuals working to address the outbreak. These shifts were typical of the global threat landscape, but what was peculiar in this case was how the global nature and universal impact of the crisis made the cybercriminal's work easier. They preyed on our concern, confusion, and desire for resolution.

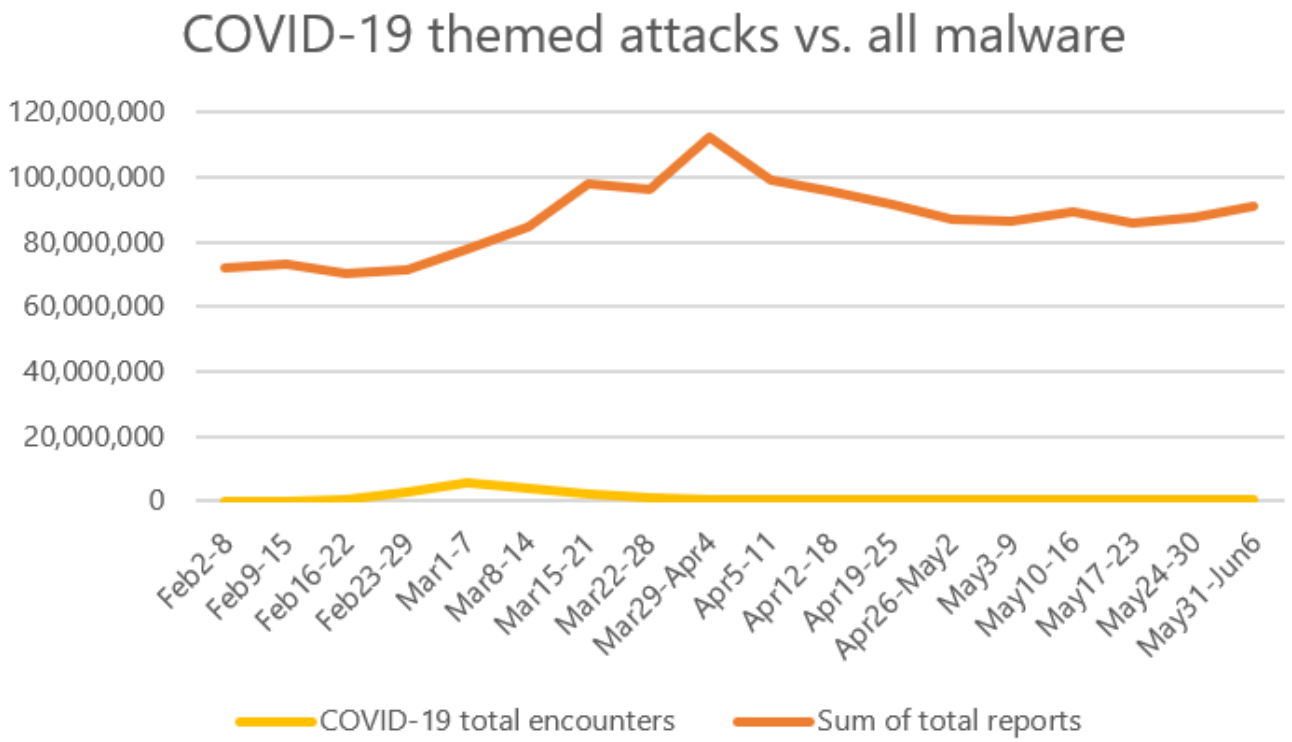


Figure 2. Trend of overall global attacks vs. COVID-19 themed attacks

After peaking in early March, COVID-19 themed attacks settled into a “new normal”. While these themed attacks are still higher than they were in early February and are likely to continue as long as COVID-19 persists, this pattern of changing lures prove to be outliers, and the vast majority of the threat landscape falls into typical phishing and identity compromise patterns.

Cybercriminals are adaptable and always looking for the best and easiest ways to gain new victims. Commodity malware attacks, in particular, are looking for the biggest risk-versus-reward payouts. The industry sometimes focuses heavily on advanced attacks that exploit zero-day vulnerabilities, but every day the bigger risk for more people is being tricked into running unknown programs or Trojanized documents. Likewise, defenders adapt and drive up the cost of successful attacks. Starting in April, we observed defenders greatly increasing phishing awareness and training for their enterprises, raising the cost and complexity barrier for cybercriminals targeting their employees. These dynamics behave very much like economic models if you turn “sellers” to “cybercriminals” and “customers” to “victims”.

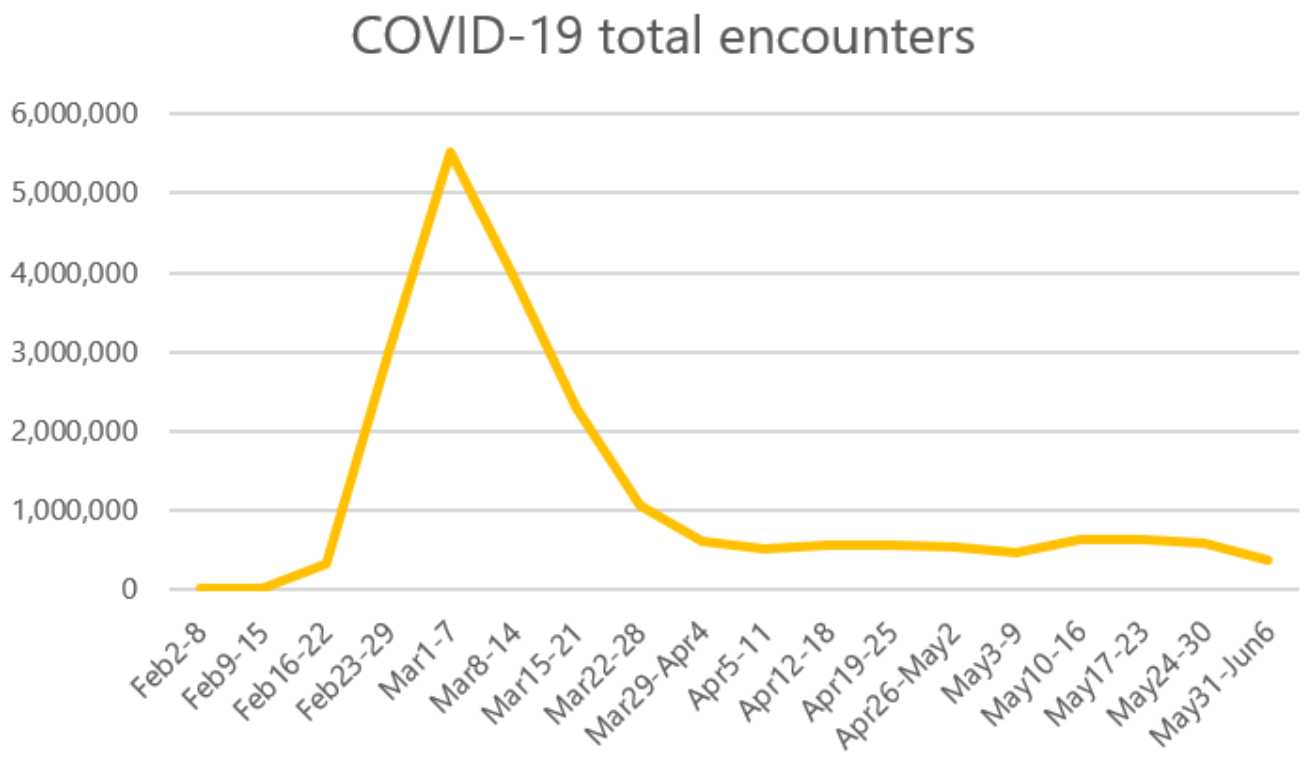


Figure 3. Trend of COVID-19 themed attacks

Lures, like news, are always local

Cybercriminals are looking for the easiest point of compromise or entry. One way they do this is by ripping lures from the headlines and tailoring these lures to geographies and locations of their intended victims. This is consistent with the plethora of phishing studies that show highly localized social engineering lures. In enterprise-focused phishing attacks this can look like expected documents arriving and asking the user to take action.

During the COVID-19 outbreak, cybercriminals closely mimicked the local developments of the crisis and the reactions to them. Here we can see the global trend of concern about the outbreak playing out with regional differences. Below we take a deeper look at three countries and how local events landed in relation to observed attacks.

FOCUS: United Kingdom

Attacks targeting the United Kingdom initially followed a trajectory similar to the global data, but spiked early, appearing to be influenced by the news and concerns in the nation. Data shows a first peak approximately at the first confirmed COVID-19 death in the UK, with growth beginning again with the FTSE 100 stock crash on March 9, and then ultimately peaking around the time the United States announced a travel ban to Europe.

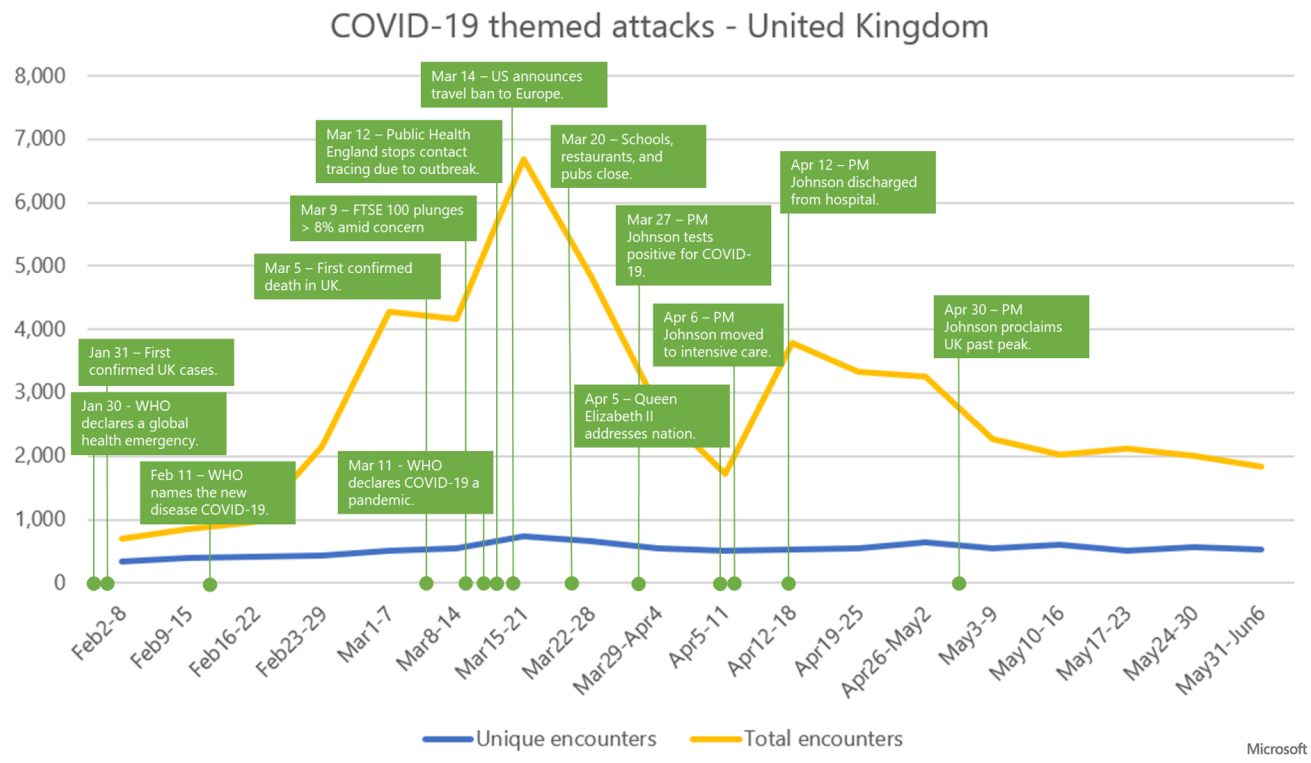


Figure 4. Trend of COVID-19 themed attacks in the United Kingdom showing unique encounters (distinct malware files) and total encounters (number of times the files are detected)

In the latter half of March, the United Kingdom increased transparency and information to the public as outbreak protocols were implemented, including the closure of schools. The attacks dropped considerably all the way to April 5, when Queen Elizabeth II made a rare televised address to the nation. The very next day, Prime Minister Boris Johnson, who was hospitalized on April 6 due to COVID-19, was moved to intensive care. Data shows a corresponding increase in attacks until April 12, the day the Prime Minister was discharged from the hospital. The level of themed attacks then plateaued at about 3,500 daily attacks until roughly the end of April. The UK government proclaimed the country had passed the peak of infections and began to restore a new normalcy. Attacks took a notable drop to around 2,000 daily attacks.

Figure 5. Sample COVID-19 themed lures in attacks seen in the UK

FOCUS: Republic of Korea

The Republic of Korea was one of the earliest countries hit by COVID-19 and one of the most active in combating the virus. We observed attacks in Korea increase and, like the global trend, peak in early March. However, the spike in attacks for this country is steeper than the worldwide average, coinciding with the earlier arrival of the virus here.

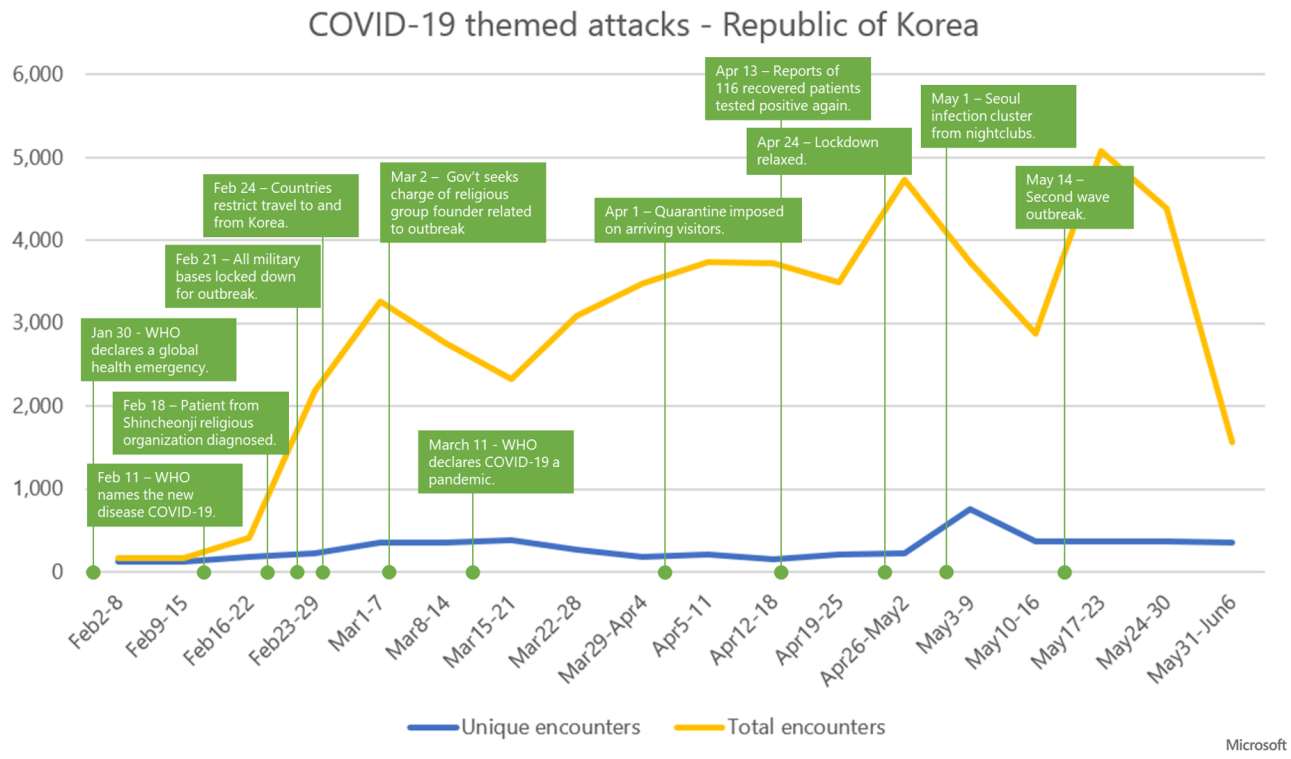


Figure 6. Trend of COVID-19 themed attacks in the Republic of Korea showing unique encounters (distinct malware files) and total encounters (number of times the files are detected)

Interestingly, themed attacks were minimal at the beginning of February despite the impact of the virus. Cybercriminals did not truly ramp up attacks until the middle of February, closely mapping key events like identifying patients from the Shincheonji religious organization, military base lock downs, and international travel restrictions. While these national news events did not create the attacks, it's clear cybercriminals saw an opening to compromise more victims.

Increased testing and transparency about the outbreak mapped to a downward trajectory of attacks in the first half of March. Looking forward through the end of May, the trend of themed attacks targeting Korean victims significantly departed from the global trajectory. We observed increasing attacks as the country restored some civic life. Attacks ultimately reached a peak around May 23. Analysis is still ongoing to understand the dynamics that drove this atypical increase.

FOCUS: United States

COVID-19 themed attacks in the United States largely followed the global attack trend. The initial ascent began mid-February after the World Health Organization officially named the virus. Attacks reached first peak at the end of February, coinciding with the first confirmed COVID-19 death in the country, and hit its highest point by mid-March, coinciding with the announced international travel ban. The last half of March saw a significant decrease in

themed attacks. Telemetry from April and May shows themed attacks leveling off between 20,000 and 30,000 daily attacks. The same pattern of themed attacks mirroring the development of the outbreak and local concern likely played out at the state level, too.

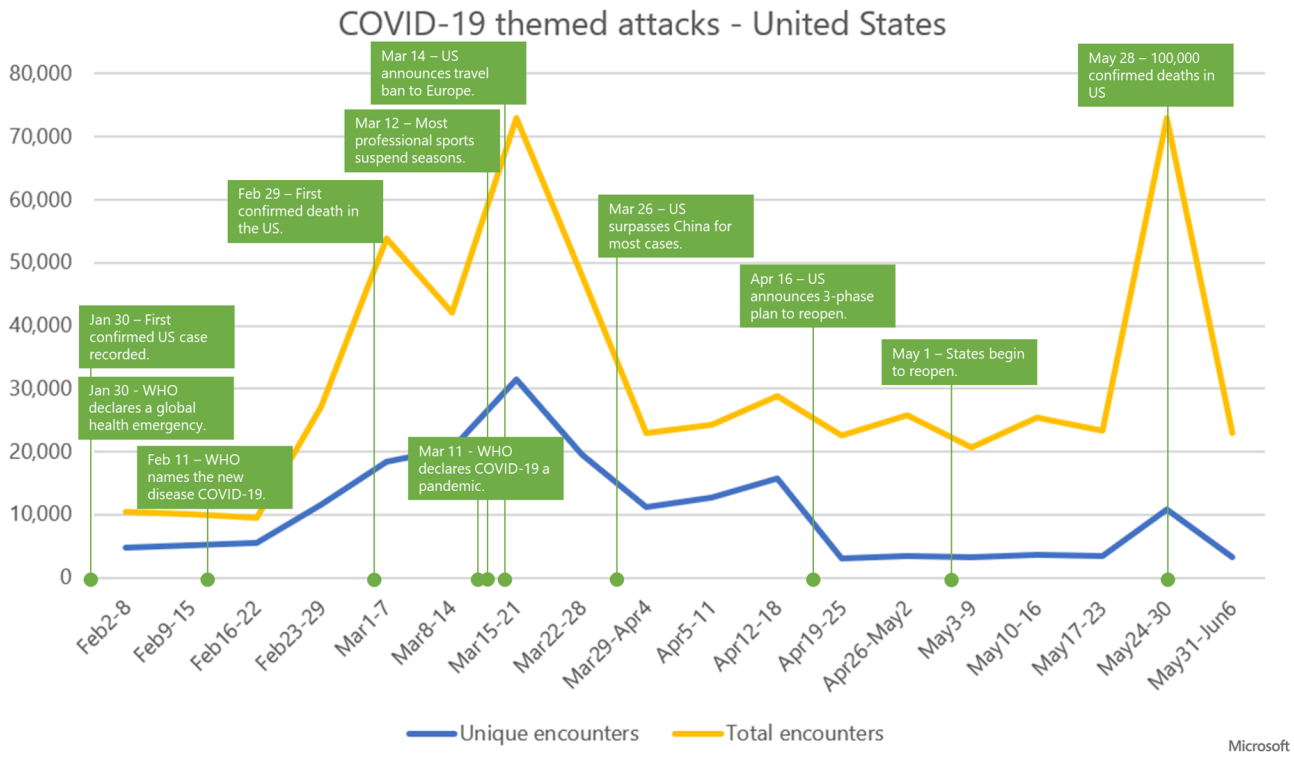


Figure 7. Trend of COVID-19 themed attacks in the United States showing unique encounters (distinct malware files) and total encounters (number of times the files are detected)

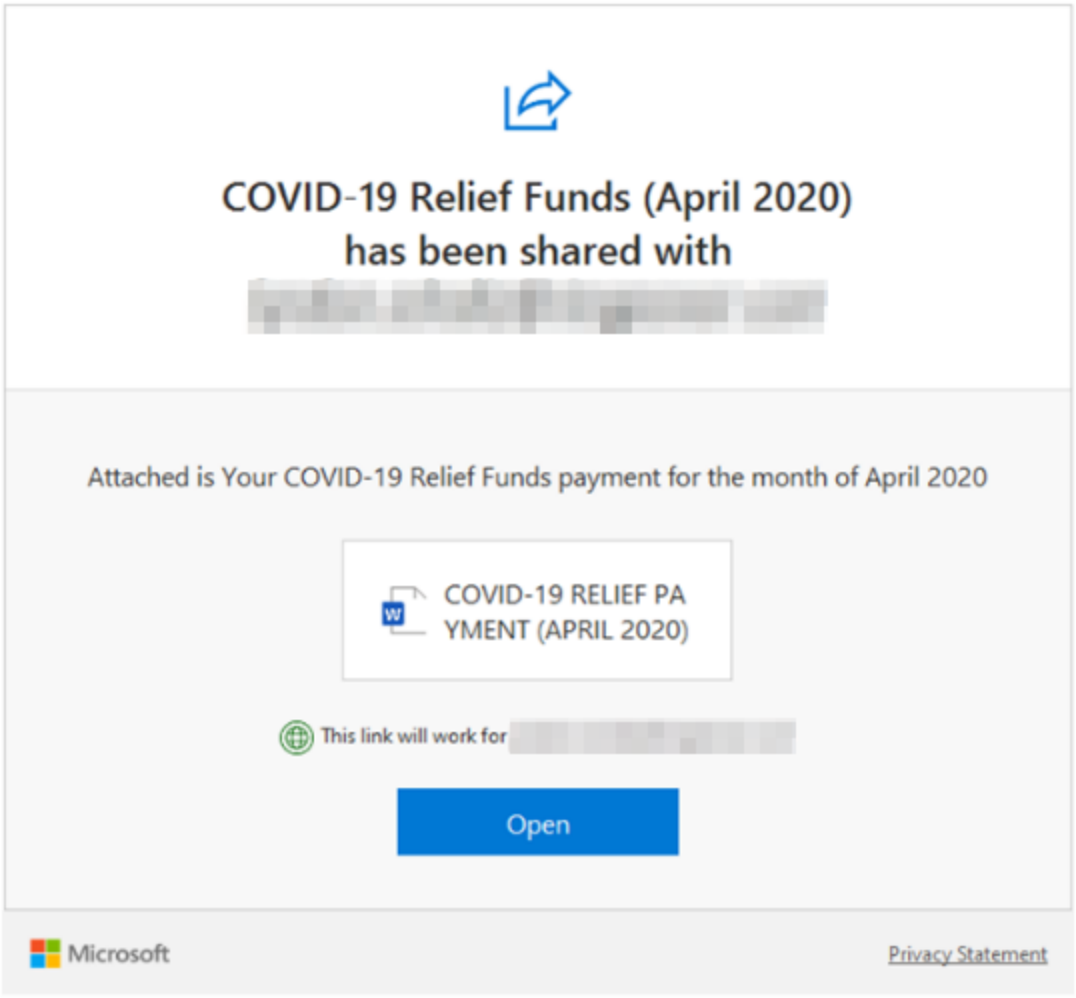


Figure 8. Sample COVID-19 themed lures in attacks seen in the US

Conclusions

The COVID-19 outbreak has truly been a global event. Cybercriminals have taken advantage of the crisis to lure new victims using existing malware threats. In examining the telemetry, these attacks appear to be highly correlated to local interest and news.

Overall, COVID-19 themed attacks are just a small percentage of the overall threats the Microsoft has observed over the last four months. There was a global spike of themed attacks cumulating in the first two weeks of March. Based on the overall trend of attacks it appears that the themed attacks were at the cost of other attacks in the threat environment.

These last four months have seen a lot of focus on the outbreak – both virus and cyber. The lessons we draw from Microsoft's observations are:

- Cybercriminals adapt their tactics to take advantage of local events that are more likely to lure victims to their schemes. Those lures change quickly and fluidly while the underlying malware threats remain.

- Defender investment is best placed in cross-domain signal analysis, update deployment, and user education. These COVID-19 themed attacks show us that the threats our users face are constant on a global scale. Investments that raise the cost of attack or lower the likelihood of success are the optimal path forward.
- Focus on behaviors of attackers will be more effective than just examining indicators of compromise, which tend to be more signals in time than durable.

To help organizations stay protected from the opportunistic, quickly evolving threats we saw during the outbreak, as well as the much larger total volume of threats, Microsoft Threat Protection (MTP) provides cross-domain visibility. It delivers coordinated defense by orchestrating protection, detection, and response across endpoints, identities, email, and apps.

Organizations should further improve security posture by educating end users about spotting phishing and social engineering attacks and practicing credential hygiene. Organizations can use Microsoft Secure Score to assesses and measure security posture and apply recommended improvement actions, guidance, and control. Using a centralized dashboard in Microsoft 365 security center, organizations can compare their security posture with benchmarks and establish key performance indicators (KPIs).

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft Threat Protection and Microsoft Defender ATP tech communities.

Read all Microsoft security intelligence blog posts.

Follow us on Twitter **@MsftSecIntel**.