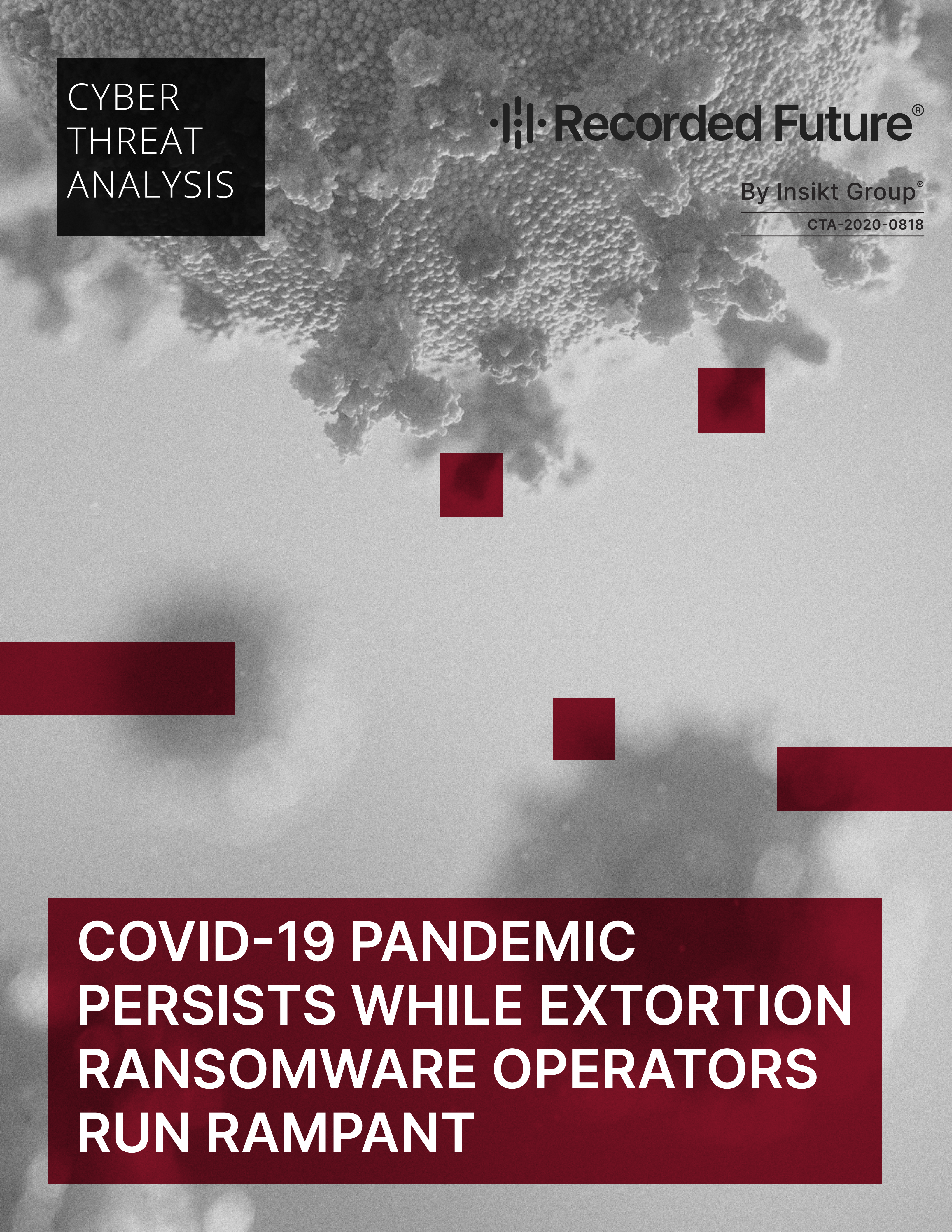


CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-0818

# COVID-19 PANDEMIC PERSISTS WHILE EXTORTION RANSOMWARE OPERATORS RUN RAMPANT

*This report is an extension of analysis Recorded Future released in Q1 and Q2, which outlined the trends in malware use, distribution, and development throughout the first half of 2020.*

*Insikt Group used the Recorded Future© Platform to look at mainstream news, security vendor reporting, malware and vulnerability technical reporting, security breach reporting, and dark web activity between January 1 and June 30, 2020, to examine major trends in malware. The trends outlined below illustrate the tactics, techniques, and procedures (TTPs) that had a major impact on technology.*

*This report will assist threat hunters and SOC teams in strengthening their security posture by prioritizing hunting techniques and detection methods based on this research and data.*

## Executive Summary

Two major trends in malware development and deployment dominated headlines throughout the first half of 2020: COVID-19 and extortion ransomware. 2020 has been a challenging year, and the cyber threat landscape was no exception.

As the world reacted to COVID-19, threat actors saw an opportunity to capitalize on the pandemic to propagate malware. Workers across the globe were forced to adapt to remote work, which created a major shift in the cyber threat landscape as threat actors saw the opportunity to target remote technologies. In addition, threat actors took advantage of fear and uncertainty worldwide to further exploit victims and spread malware through phishing lures and malicious maps and applications. Even government entities joined in to use and exploit mobile applications to monitor citizens during the COVID-19 pandemic. In the second half of the year, threat actors will likely again shift focus and develop phishing lures around the United States presidential election, and possibly a COVID-19 vaccine if one is discovered in the coming months.

At the start of 2020, Insikt Group tracked multiple ransomware operators as they adapted to ransomware mitigations and began using extortion tactics to increase the motivation for paying ransoms. This trend continued through Q1 and Q2 2020, with an evolution observed in Q2 as ransomware operators began to work together to form “cartels.”

Threat actors’ increased emphasis on extortionary tactics, usually by threatening to publish or leak stolen data if the ransom is not paid, means that simply backing up data to prevent data loss is no longer sufficient to mitigate these kinds of attacks. Organizations will need to be proactive in their approach to avoid falling victim to ransomware attacks involving extortion.

## COVID-19 Pandemic and Remote Work Security

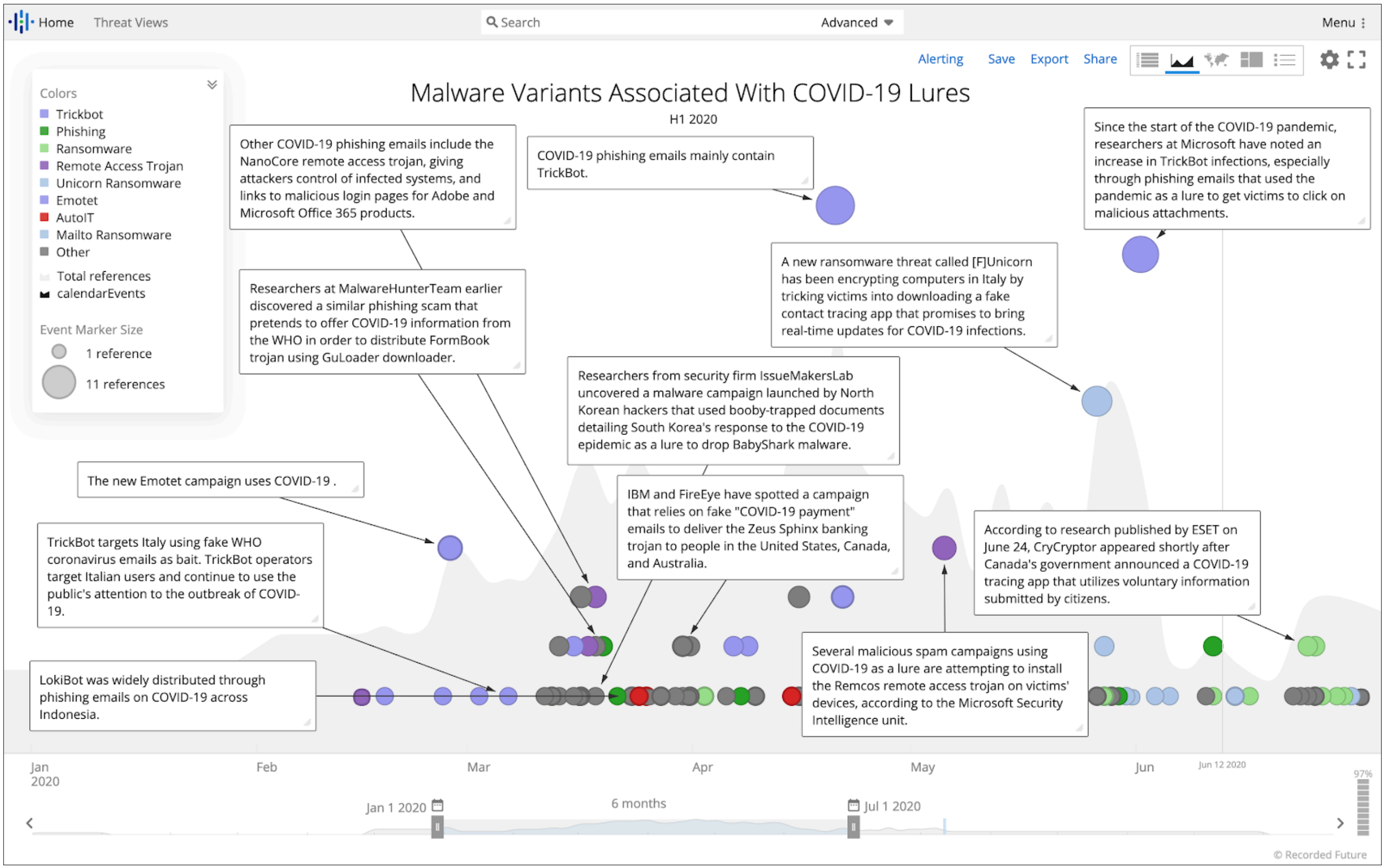
Recorded Future believes that the greatest risk to organizations in terms of remote work comes from threat actors targeting VPN and Remote Access Tools with weak or compromised credentials. Because remote working environments inherently grant users remote access to closed networks, threat actors pursue legitimate credentials rather than seeking to exploit services. Intrusion activity becomes more difficult to detect when legitimate credentials are used to gain access. While vulnerabilities to these technologies still present a threat to remote work, vulnerabilities in VPN and remote access tools themselves are not necessarily the greatest organizational risk.

For many organizations, the digital transformation they had planned to implement over the next several years has happened nearly overnight. As enterprise network baselines, operating schedules, and security operations are in flux, threat actors are seizing on this period of transition as an opportunity to target security gaps and unwitting victims.

Based on these new circumstances, Insikt Group recommends heightened vigilance and awareness of phishing campaigns that target commonly used remote working technologies. Even though a threat actor may not necessarily leverage malware or exploit a known or previously unknown vulnerability, phishing attempts can harvest credentials used to access otherwise secure networking products.

## COVID-19 Pandemic and Malware Propagation

Threat actors have propagated multiple forms of malware by employing references to the COVID-19 pandemic in various attack vectors, including COVID-19-themed lures in phishing emails, and malware embedded in COVID-19 maps and contact tracing applications, among other techniques, throughout the first half of 2020. They use various malware families, including AZORult, DanaBot Banking Trojan, Emotet, BabyShark, Zeus Sphinx, LokiBot, Nanocore, Trickbot, CovidLock, Mailto ransomware, NEMTY ransomware, and [F]Unicorn ransomware. Analysts observed increases in references to COVID-19 used alongside malware in March, April, and May as illustrated in the timeline below.



Malware Variants Associated With COVID-19 Lures

H1 2020

Other COVID-19 phishing emails include the NanoCore remote access trojan, giving attackers control of infected systems, and links to malicious login pages for Adobe and Microsoft Office 365 products.

COVID-19 phishing emails mainly contain TrickBot.

Since the start of the COVID-19 pandemic, researchers at Microsoft have noted an increase in TrickBot infections, especially through phishing emails that used the pandemic as a lure to get victims to click on malicious attachments.

A new ransomware threat called [F]Unicorn has been encrypting computers in Italy by tricking victims into downloading a fake contact tracing app that promises to bring real-time updates for COVID-19 infections.

Researchers at MalwareHunterTeam earlier discovered a similar phishing scam that pretends to offer COVID-19 information from the WHO in order to distribute FormBook trojan using GuLoader downloader.

Researchers from security firm IssueMakersLab uncovered a malware campaign launched by North Korean hackers that used booby-trapped documents detailing South Korea's response to the COVID-19 epidemic as a lure to drop BabyShark malware.

The new Emotet campaign uses COVID-19 .

IBM and FireEye have spotted a campaign that relies on fake "COVID-19 payment" emails to deliver the Zeus Sphinx banking trojan to people in the United States, Canada, and Australia.

TrickBot targets Italy using fake WHO coronavirus emails as bait. TrickBot operators target Italian users and continue to use the public's attention to the outbreak of COVID-19.

According to research published by ESET on June 24, CryCryptor appeared shortly after Canada's government announced a COVID-19 tracing app that utilizes voluntary information submitted by citizens.

LokiBot was widely distributed through phishing emails on COVID-19 across Indonesia.

Several malicious spam campaigns using COVID-19 as a lure are attempting to install the Remcos remote access trojan on victims' devices, according to the Microsoft Security Intelligence unit.

*Figure 1: Malware variants using COVID-19-themed lures throughout H1 2020. (Source: Recorded Future)*

As seen in Figure 1, COVID-19 was highly used as a lure throughout March to June 2020; however, between May and June 2020, Insikt Group observed a 60 percent decrease in references to COVID-19 alongside malware within our data set. This decrease coincided with a shift in media attention from the COVID-19 pandemic to the rise in Black Lives Matter (BLM) protests following the death of George Floyd while in police custody — Insikt Group observed threat actors shifting their lures from COVID-19 themes to BLM themes as seen in Figure 3 below. Notably, Trickbot operators are an example of threat actors who demonstrated their ability to adapt as world events and media attention shifted.

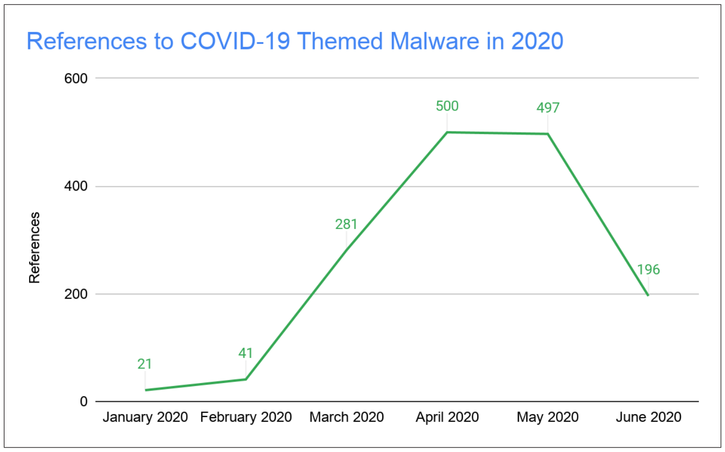


*Figure 2: References to COVID-19 related malware in the first half of 2020, according to Recorded Future data.*

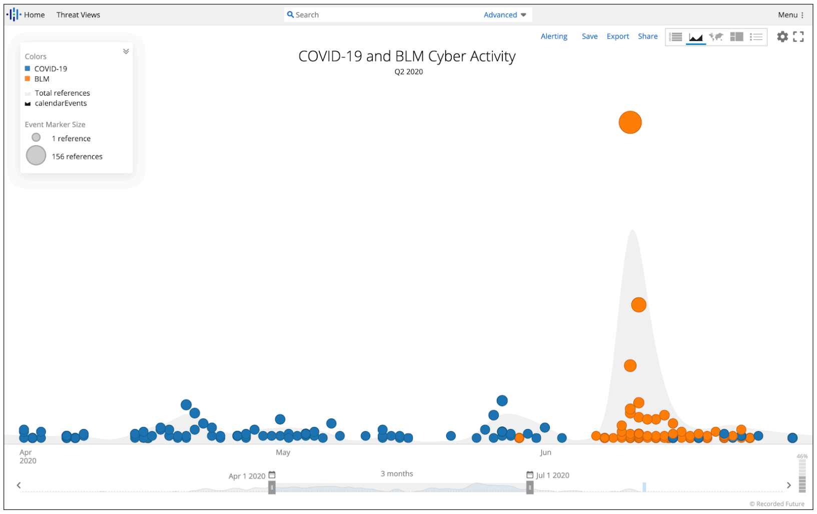


*Figure 3: COVID-19 cyber events and BLM cyber events in 2020. (Source: Recorded Future)*

Trickbot is an advanced banking trojan that attackers use to steal payment credentials from victims. On June 10, 2020, Swiss security firm Abuse[.]ch identified a Trickbot malware sample delivered via an email with the subject line "Subject: Speak out anon about Black Lives Matter." On June 26, 2020, @malware_traffic and @abuse_ch shared samples delivered from a malspam campaign via social media using the subject "Black Lives Matter" as a lure. The "e-vote" themed DOC files contain embedded macros that, when enabled, launch a document exploit that downloads files from malicious URLs.

Security teams should educate employees on new and emerging tactics used by threat actors, especially emails with themes related to worldwide events, as they could be the initial entry point of a major network compromise.

## COVID-19 Pandemic and Mobile Malware

In response to the first spike of coronavirus cases, governments released mobile applications containing information about health measures being taken and contact tracing functionality. Some of these applications were intentionally built with surveillance tools, such as the app Alipay Health Code in China, or were hastily built without proper security measures, such as the app Aarogya Setu in India. Regardless of intent, the outcome of these widely downloaded mobile applications has been that threat actors are able to more easily masquerade as state-sponsored applications and load malware onto unsuspecting users' devices.

As the novelty of COVID-19 recedes, there has been a notable decrease in coronavirus-related mobile malware lures. However, Recorded Future has observed continued and consistent use of mobile malware using spyware tactics such as geotracking and keylogging, as has been seen in use with malicious COVID-19-themed applications. Insikt Group assesses the trend of malware loaded into "legitimate" applications will increase in correlation with the constant growth of mobile device dependence.

### Extortion Ransomware Operators: Cybersecurity's Villains of 2020

Ransomware presented a major threat to organizations throughout the first half of 2020. Ransomware operators were able to add some major names to their list of victims, including IT services provider Cognizant, ATM provider Diebold Nixdorf, and aircraft maintenance company VT San Antonio Aerospace. Additionally, in May 2020, the FBI released a flash report containing indicators of compromise for ProLock, a new ransomware family first seen in March 2020. The flash report also warned that the ProLock decrypter does not function properly and may even corrupt files, a risk organizations should consider and assess when handling any ransomware. Threat actors will likely continue to consistently target large organizations, as their wide attack surface gives threat actors more chances to gain access and their abundance of resources makes them more likely to pay the ransom.

### Extortion Tactics Gaining Momentum in the Scene

Ransomware families with operators that employ extortion tactics dominated the ransomware threat landscape in the first half of 2020. In these attacks, in addition to encrypting files on the victim machine and demanding a ransom for decryption, threat actors also threaten to auction off (as Sodinokibi operators began doing in June 2020) or publish the stolen data on an extortion website if they do not receive payment. These attacks make mitigation more difficult for organizations, as maintaining data backups will prevent victims from losing ransomware-encrypted files, but will not keep threat actors from releasing those files.

The University of California, San Francisco (UCSF) confirmed in June 2020 that it paid a $1.14 million ransom to retrieve compromised data from the operators of Netwalker after a full day of negotiations over a live chat. While almost certainly intended by UCSF to be a private conversation, BBC News was able to follow the negotiations after receiving an anonymous tip. This serves as a reminder for organizations to be cautious in negotiating with any threat actor as their communications may not be secure. The Netwalker operators also recently released stolen data from Michigan State University and claimed to have stolen data from Columbia College of Chicago, which they are threatening to release if they do not receive payment.

The operators of Maze have joined forces with the operators of LockBit — a Ransomware-as-a-Service (RaaS) that has been operational since September 2019 — to form a "ransomware cartel" by sharing their extortion website, Maze News. A third group, RagnarLocker, later joined the cartel. Sharing an extortion website, as well as victims and other infrastructure, allows the operators of these ransomware families to focus on keeping their campaigns profitable rather than on managing infrastructure related to the extortion website. This collaborative model also makes attribution more difficult for investigators attempting to track ransomware operators and ransom payments.

When targeting large organizations, ransomware campaign operators are likely to continue using extortion websites to further incentivize victims to pay ransoms, as well as provide an additional income potential from stolen data sales if the ransom is not paid. Maze Cartel's success could encourage other reputable ransomware operators to join the cartel or create other extortion groups.

## Outlook

While stealing data, operating an extortion website, and possibly selling or auctioning off data requires significantly more time and effort from threat actors, Insikt Group believes that the demonstrated success of ransomware operators such as NetWalker and REvil/Sodinokibi will motivate other capable threat actors to adopt this method. Due to the additional overhead required to operate an extortion website, Insikt Group also believes that threat actors will be inclined to either join the Maze Cartel or establish another multi-group organization in order to share a common extortion website.

The incorporation of extortion websites into ransomware campaigns shifts the guidance for how organizations should protect their environments from ransomware towards the more preventative approach necessary for more data theft-oriented malware (such as trojans and stealers). While backing up data is sufficient to prevent data loss from traditional ransomware attacks, this will not protect stolen data from being published or sold. Organizations will need to be proactive in their approach, including keeping operating systems updated, educating employees (such as through interactive exercises in identifying phishing attempts), and implementing effective security software.

Recorded Future observed the continued exploitation of the COVID-19 pandemic by threat actors through the first half of 2020, and with a shifted focus as the nature of the pandemic changes around the world, including a rise in spyware and geolocation techniques used in mobile malware in particular. Though these tactics have been employed by governments for contact-tracing COVID-19, threat actors have implemented similar tactics into mobile malware, a trend that will likely transcend the pandemic.

Threat actors will always exploit news of, or response to, major global events and trends to target victims via remote technologies and social engineering. Insikt Group observed threat actors shifting their focus to take advantage of world events as they emerged, beginning with the COVID-19 pandemic in Q1 and shifting to other major events such as BLM protests as the year progressed. We predict that in Q3 and Q4 2020, threat actors will likely again shift focus to the United States presidential election, and possibly a vaccine if one is discovered in the coming months.