# THE CYBER PANDEMIC

**Etay Moor** *reports on the importance of defending against the advanced threat actors profiting from COVID-19*

**Troubled times have always created opportunities for threat actors, from common criminals to state-sponsored APT groups. With few events in living memory rivalling the upheaval of the COVID-19 pandemic, it is no surprise that cyber criminals have been out in force attempting to capitalise on the disruption.**

Our researchers have closely monitored shifting cyber criminal activity around the world during the pandemic and have collated some of the most prevalent tools, techniques and procedures (TTPs) being used to take advantage of the situation – as well best practice for minimising the risk while continuing to operate during the crisis.

As a rule, state-sponsored attackers tend to thrive during global crises, and COVID-19 has been no exception. Nation-state activity has taken a variety of forms with differing targets and motivations, with some specifically going after COVID-related targets, and others simply using the disruption as a convenient smokescreen for their usual activity.

Three major state-sponsored campaigns have particularly stood out during the pandemic so far:

## RUSSIA

In February, what is believed to be a Russian state-sponsored hacking group known as Hades was observed targeting Ukraine with a multi-faceted operation. This included both a campaign of disinformation as well as the spread of malware, with the apparent aim being to create panic and confusion around Coronavirus. The threat actors attacked the Center for Public Health of the Ministry of Health of Ukraine with malware-laden phishing emails as well as spreading fake news on social media, contributing to a series of riots and unrest that erupted shortly after.

More recently, in July the National Cyber Security Centre (NCSC) and international counterpart intelligence agencies reported with near certainty that Russian state-sponsored actors had targeted COVID-19 vaccine operations around the world. The group designated APT29, also widely known as Cozy Bear, is believed to have attacked drug companies and research groups in the UK, Canada and the US. Such attacks are unsurprising, as the country to develop the first successful vaccine will not only be able to better save the lives of its citizens, but will also stand to make enormous profits.

## NORTH KOREA

Later in February, government officials in South Korea were targeted with phishing emails again claiming to contain information about the country's response plan, but actually laden with the BabyShark malware. This has previously been used by a North Korean group labelled Kimsuky, which has previously launched multiple attacks on South Korean targets including governmental bodies and aerospace and defence companies.

## CHINA

The largest number of targeted spear phishing attacks we identified appeared to originate from China. Known APT groups such as Mustang Panda and Vicious Panda were found to target multiple individuals in countries including Vietnam and Mongolia. The phishing emails were again loaded with malicious files, this time in the form of .rar files that covertly installed backdoor trojans into the victim's machine.

Alongside elevated nation state level attackers, common cyber criminals have redoubled their efforts in recent months to exploit organisations struggling to cope with severely disrupted operations. Most have put a new COVID spin on old familiar techniques, while some more ruthless groups have specifically targeted organisations involved in fighting the pandemic.

Attackers have been quick to home in on the opportunities presented by the new regime of remote working. Many organisations were forced to quickly establish a fully remote workforce with very little time to prepare or test their operations. Tools such as VPNs can provide an easy route to access the network or hijacking a user's device, particularly when it comes to workers using their own personal machines to work from home.

In particular, threat actors have sought to exploit the use of online meeting platforms as a replacement for face-to-face meetings. Our Vulnerability Risk Analyser (VRA) found a sharp increase in cyber criminal discussions on vulnerabilities and exploits in the leading online chat and meeting platforms.

For example, before being resolved in an update, Zoom was vulnerable to unauthorised message processing. This would enable an attacker to spoof User Datagram Protocol (UDP) messages from a meeting attendee or Zoom server to invoke functionality in the target client. From here, the attacker can perform malicious actions including hijacking shared screens or spoofing messages from attendees.

**This year has seen a sharp increase in all forms of cyber threat**

Similarly, the Cisco Webex Meetings desktop app previously possessed a flaw that enabled an attacker to execute commands as a privileged user. This vulnerability required a locally based authenticated user, but a threat actor leveraging remote management tools would be able to gain access.

Phishing has long been one of the most popular cyber attack methods as it requires very little technical expertise and can largely be executed using legitimate software tools and contact lists easily acquired over the Dark Web.

Phishing is always centred on an element of deception, and criminals have frequently been found to weave key dates and events into their fraudulent narrative, from Christmas sales and Valentine's Day to the latest global news. Predictably, we detected a huge spike in phishing activity at the start of 2020, and especially after most countries entered national lockdowns in March.

We closely monitored the registration of new domains that included the words "Corona" and "COVID" and saw an exponential increase in just three months. In 2019 there were just 190 domains containing these key words, but this soon rose to over 1,400 in January and 5,000 in February. In March, numbers skyrocketed to over 38,000. While some of these domains were created for legitimate reasons, many we investigated were certainly used to host phishing attacks.

We also detected a huge spike in COVID-related phishing emails, and a large number continue to circulate. Criminals have incorporated the pandemic into their deceptive narratives in a variety of ways, but a popular theme is to pose as a known authority and offer advice. In one campaign we examined, attackers impersonated the US Department of Homeland Security (DHS) offering advice, with a link through to more information and testing for symptoms. The link redirected victims to a download address instead, infecting them with an information-stealing malware.

Some cyber criminal groups actually announced early into the pandemic that they would not be attacking medical or healthcare organisations during the crisis. The DoppelPaymer group even stated that if such an organisation was hit by mistake, they would provide it with a free decrypter code to undo the damage.

Unfortunately, the old adage that there is no honour among thieves holds true, and we have observed several major ransomware attacks targeting organisations involved in combating the pandemic.

One of the most prominent examples was the Maze ransomware group, previously known for targeting everything from small US-based law firms to the German Government. On 14 March, the group attacked London-based Hammersmith Medicines Research (HMR), a company that undertakes clinical

tests for drugs and vaccines. The company had previously worked on treatments for Alzheimer's and Ebola among others and had recently started work developing a COVID-19 vaccine. Luckily HMR was able to detect the ransomware outbreak in progress and was able to halt the infection and restore its systems in the same day. However, a week later Maze proceeded to leak over 2,300 medical records online.

In another early example, the Champaign Urbana Public Health District (CHUPD) in Illinois was attacked by the NetWalker ransomware group in early March. The attack commenced with a COVID-themed phishing email, including an attachment called "CORONAVIRUS_COVID-19.vbs" which included an embedded executable file for the NetWalker ransomware.

The NetWalker group has been prolific this year and has embraced the opportunity presented by COVID with gusto. Their MO has often centred around attacking educational institutions, and particularly those involved in virus research. Most recently they successfully struck the University of California San Francisco (UCSF) in June, which had been researching potential COVID-19 cures. The university eventually paid a colossal ransom of $1.4-million to restore operations and vital research data.

2020 has seen a sharp increase in all forms of cyber threat, from low-level opportunist criminals to state-sponsored APT groups. As the pandemic stretches on, all organisations involved in medical research related to COVID-19 are likely to remain in the cross hairs of both state-sponsored attackers working an espionage or geopolitical agenda, as well as the more callous organised cyber gangs. However, businesses in all sectors should be aware that they will be facing an elevated threat level for some time, particularly as they continue to utilise remote working practices.

The good news is that although the volume of attacks has increased and threat actors have adjusted their tactics to exploit the pandemic, most threats can be countered with the same core security strategies. Even APT groups still tend to commence their attacks using the same phishing techniques and the exploitation of software vulnerabilities.

Simple human error can swiftly open attack paths for threat actors, so organisations must be especially vigilant to try and compensate for a more isolated remote workforce. A drive towards employee education will help to keep the environment secure, particularly in regard to the proper and secure use of remote access tools and other software. Organisations should ensure that their remote workforce is only using authorised software that has been fully patched and updated, and ideally via a corporate machine rather than a personal one. Mandating strong passwords and the use of 2FA will also help to reduce the risk from phishing attacks targeting user credentials.

In addition to basic security hygiene, organisations should also ensure that they have access to intelligence on the latest threats. Organised groups such as Maze are quick to innovate and discover new software vulnerabilities and attack paths, so organisations must be ready to act quickly when intelligence on new exploits or active campaigns comes in.

Organisations should also be continuously assessing their risk profile as the situation develops, particularly whenever they adopt new software or working practices. Remote working and collaboration tools such as VPNs and virtual meeting rooms will continue to be high on the hit list, so a thorough risk assessment should be conducted before new tools are used. All existing assets should also be assessed for vulnerabilities as a matter of priority.

While we can continue to expect an increase in Corona-themed cyber attacks, getting the security basics right will continue to mitigate the threat of most strikes. Access to good threat intelligence will also be more valuable than ever in the coming months in order to keep track of fast-moving developments from threat actors. In particular, an organisation working in the medical field or with ties to governmental bodies will need to be armed with the latest intelligence to stand a chance against the APT groups and state-sponsored actors that may have them in their sights ●

**Etay Moor** is Chief Security Officer at IntSights. As CSO, Etay leads the security advisory practice where he works with CISOs and other senior cybersecurity executives to develop risk management-based cybersecurity programmes.

**Remote working tools such as VPNs and virtual meeting rooms will be high on the cyber criminal's hit list**