Orange
Cyberdefense

COVID-19:
A biological hazard goes digital
Examining the crisis within the crisis

Table of Contents

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Background:

A global crisis

As the COVID-19 coronavirus pandemic continues to spread worldwide, cyber-threat actors are trying to capitalize on the global health crisis by creating malware or launching attacks with a COVID-19 theme. However, this kind of exploitative behavior by the cybercrime ecosystem is only one part of a bigger cybersecurity picture. Orange Cyberdefense is releasing this paper in order to draw attention to a diverse set of facts that should be considered now.

As a global crisis, COVID-19 is having a significant impact on all aspects of personal and corporate life, including cybersecurity. In this mood of fear, uncertainty and doubt, there is an appropriately elevated level of threat awareness, but this can create an exaggerated level of anxiety. In this context, the following resource is our united effort as Orange Cyberdefense to share our knowledge, insights and experience regarding what we think about cybersecurity in the heat of this current COVID-19 crisis and in the post COVID-19 world that hopefully isn't too far away.

The analysis presented includes imputs from:

- Security Research Center (SRC)
- Computer Emergency Response Team (CERT)
- Malware Epidemiology Lab
- OSINT Unit
- CyberSOC
- Advisory & Architecture
- Global CISO Office
- Global CTO Office

Summary of findings

There are ten main themes we believe our customers should be considering:

1. **Malware and phishing** using COVID-19 as a pretext is likely to escalate. We have also seen sophisticated instances of watering hole attacks using COVID-19 maps to drop exploits and malware. This report describes several specific examples like this, and the trend is likely to persist and escalate in different forms.
2. There will be an uptick of **general misinformation campaigns** distorting COVID-19-related facts to further diverse political agendas. Fact checking is essential.
3. Positively, several **ransomware crews have committed to avoiding medical and research facilities** from their target lists. This is a welcomed reprieve but can't be relied upon to have any substantial impact. 'Traditional' threats like ransomware persist.
4. In the meantime, we have seen **targeted attacks against medical organizations** involved in researching, treating or otherwise responding to COVID-19, especially in the western world, apparently to undermine the response to the pandemic. We anticipate that this will continue as various state and hacktivist groups escalate their efforts.
5. The COVID-19 crisis is a global one. However, geopolitical tensions that predate the pandemic will likely be increased. We expect to see **new waves of state-sponsored cyber disruption** as the pandemic spreads, which may have an immediate effect on handling the pandemic.
6. As more people work from home using poorly designed and implemented remote access solutions, we anticipate that **attacks against remote access technologies**, VPN gateways and poorly secured home and shared Wi-Fi access points will increase and contribute to serious compromises occurring.
7. **The visibility of SIEM and security operations teams will become impaired** as endpoints connect via the VPN or directly to the Internet. The implication is that they are not subject to the same level of monitoring as when connected to the corporate LAN, thereby **reducing the overall level of security** a corporate can rely on. We also anticipate that CIRT and other Incident Response capabilities will be impeded, contributing to greater response delays and dwell times by attackers, or even a failure for attacks to be detected altogether.
8. During this time, more and more **computing activity will move to cloud**, forcing security programs to consider local and cloud infrastructures in their strategies.
9. **Most businesses are accelerating their move to online commerce**, if they have not done so already, especially in the retail sector. In the mad dash to go online, we expect there to be an accumulation of security debt as security is sacrificed in favor of speed-to-market.
10. As more and more people work from home, we anticipate that corporate and crucial shared Internet infrastructure will be put under enormous strain. **Performance will likely degrade**, and even fail in some instances. For most organizations, the IT function and business continuity plan has become significantly more strategic.

If you only have five minutes…

The COVID-19 pandemic has changed security threat models in five important ways:

Your employees are more vulnerable to social engineering and scams than normal.

You have less control and visibility over the IT systems you protect than you are used to.

Your users may be connecting from systems and environments that are fundamentally insecure or poorly configured.

You may have rushed to implement remote access systems without having the time to plan and execute as well as you would like.

You, your team and your providers may be operating with diminished capacity.

Recommendations summary:

We propose that you focus on the following responses, in order of importance:

- Establish emergency response procedures and systems.
- Establish a security support hotline and prepare to expand the team providing support.
- Review backup and Disaster Recovery (DR).
- Equip your users with the information they need to make good security decisions.
- Provide secure remote access.
- Establish visibility over remote endpoints.

Remaining rational during the crisis

Advice is cheap in time of crisis. But every business is different, and we won't pretend to know how individual businesses should respond to their particular security threat at this time. We would however offer the following high-level guidelines to businesses who are evaluating the security threat and considering their response to the threat at this time:

1. Understand that we are experiencing a state of heightened threat, but only slightly increased vulnerability. We cannot control the threat, but we can control the vulnerability, so let's focus on that.
2. Understand what has changed and what hasn't. Your business's threat model may be very different today than it was yesterday, but it may also not be. If it hasn't changed, then your strategy and operations don't have to either.
3. Form partnerships but avoid mobs. Your suppliers, service provider and even competitors are all in the same boat, never more so than now. They may not have all the answers either, but now is the time to reach out and find partners that have balanced and rational views and avoid communities that are promulgating hype and hysteria.
4. Maintain context. IT and the Internet have survived for twenty years despite our various security failures. There is no doubt that the situation today is worrying, and that the risk of a fundamental cybersecurity crisis in our lifetime is real and can't be ignored. However, right now, the crisis is medical and human. Don't let the hype about cybersecurity distract you from that.
5. Work smart, not hard. You will be able to achieve very little during this time of diminished capability, so spend time and energy on considering what your primary concerns are and focusing on those.

Part I:

Impact of the pandemic

Many fundamental security realities are not really changed by the pandemic. However, some critical challenges, particularly those concerning our own ability to monitor and respond to threats and vulnerabilities, have become considerably more difficult. On the other hand, we should note that the attacker is also human and that attacker behaviors may also shift due to the impact of the virus, perhaps even reducing the level of threat at this time.

How do we assess how our current level of threat is impacted by the COVID-19 pandemic?

In this section of the paper, we attempt to describe and summarize the impact that the COVID-19 pandemic is having on the cyber threat model.

Exacerbating factors

Like so many other things in this crisis, some of the elements facing IT security practitioners are, if not wholly 'unprecedented', certainly very much worse than we've ever seen before. Several attributes of the pandemic are aggravating the cybersecurity situation. We will discuss these in detail in the section below.

Increased vulnerability to coercion

The users we protect are more vulnerable to coercion at this time. For most workers, the daily routine has been abruptly interrupted, especially for those with school-age children or who provide care for older relatives.

Psychology suggests that at a time of crisis and exaggerated anxiety, people may reduce their vigilance and increase their appetite for other risk-taking behaviors. People should be acting more cautiously at this time, but the truth is they will probably do the opposite.

This riskier behavior, along with a generally heightened appetite for information and news updates, makes people more vulnerable to social engineering and scams of every kind.

People are furthermore generally psychologically predisposed to prioritize short-term acute risks over long-term vague risks, so they will be inclined to open a Word document promising a coronavirus vaccine even if they know it's possibly malicious.

But human psychology during a crisis could be bad for security in other ways also.

According to an article in Psychology Today[1], it is understood that people may in fact engage in more risky behavior, such as drinking and smoking to help them deal with their anxiety. The principle may apply equally to people opting to take risks with their cyber hygiene to help them cope with their anxiety about the pandemic.

Other elements are further elevating the risk level.

According to a report by Europol, factors that prompt changes in crime and terrorism include[2]:

- High demand for certain goods, protective gear and pharmaceutical products.
- Decreased mobility and flow of people across and into the EU.
- Citizens remain at home and are increasingly teleworking, relying on digital solutions.
- Limitations to public life will make some criminal activities less visible and displace them to home or online settings.
- Increased anxiety and fear that may create vulnerability to exploitation.
- Decreased supply of certain illicit goods in the EU.

Criminals are of course poised to take advantage of people's weaknesses at this time.

With millions of citizens across the globe in total or partial lockdown, there is a desperate desire worldwide for news and information on the pandemic and a generalised sense of fear and urgency. Attackers are presented with the perfect lure for all manner of attacks, including phishing, Business Email Compromise (BEC), watering holes and other scams. We should anticipate both an increase in the volume of social engineering attacks and our users' vulnerability to falling for such attacks.

Homeworking makes personal equipment vulnerable

In an attempt to slow the spread of the virus, many organizations who normally would not encourage their staff working from home have now been forced to hastily implement homeworking policies and remote access infrastructure.

This introduces several additional risks, including:

- An increased dependence on 'virtual' communications like email, social media, video conferencing, calls and texts, rendering users more vulnerable to social engineering attacks and less able to validate communications face-to-face.
- Boredom and social isolation leading to lowered vigilance and a heightened willingness to make riskier decisions.
- An increased dependency on home IT and personal devices with unknown configurations and risk profiles.
- An increased use of poorly patched and misconfigured home Wi-Fi routers, which are also increasingly being targeted by attackers.

We anticipate an escalation in attacks against VPN gateways and other remote access infrastructure as newly implemented solutions may not be as secure as they should be. Poorly secured home broadband routers and shared Wi-Fi access points could also lead to additional attacks and compromise. There is also the potential for insecure personal devices being used to remotely connect to the corporate network, which may indeed already be infected, potentially giving threat actors a foothold. This situation is exacerbated by a substantial decrease in the level of visibility SIEM and SOC operations have over user endpoints, and a still-prevalent generation of endpoint security solutions are that not yet adapted to counter contemporary threats.

Increased use of mobile and personal mobile devices

Mobile has been a challenging problem for the security industry for some time. Devices are difficult to manage via conventional security tools, don't lend themselves well to the deployment of agents, and are frequently not under the direct control of the enterprise. At the same time, direct (including exploits and malware) and indirect attacks (including malicious applications, phishing and smishing) have been increasing steadily and are a serious consideration for any security strategy. We should anticipate that remote workers will be making more use than ever of personal and corporate mobiles to access both personal and professional data and systems online.

We have addressed the risks of malware and malicious mobile applications elsewhere in this report , but patch management for mobile devices is also likely to become a problem during the crisis. As the 2018 data from our Security Research Center shows, it can take up to three months for just 40% of the Android installed base to adopt a new version of the operating system. Due to Apple's walled-garden approach, iOS devices fare much better. However between 5% and 20% of users across both platforms will never deploy important security patches.

As the crisis drives users to depend more than ever on corporate and personal mobile platforms to access data and services, the pre-existing challenges we faced with securing the mobile ecosystem are aggravated. Some threats, like phishing, are addressed by existing solutions. Others, however, like mobile malware, malicious applications and mobile operating system patching, continue to challenge us and are increasing as a result of the crisis.

Organizations have reduced capacity to perform security operations

The current security risk is further exacerbated by a reduction in capacity and operational agility within corporate blue teams:

- A reduced level of care and vigilance by corporate blue teams as they are personally distracted by the crisis, struggle to focus and indeed even fall ill.
- A reduced ability to patch and harden corporate computers that are not connecting to the company LAN.
- A reduced ability to deploy engineers onsite to conduct monitoring and patching of systems that are not remotely accessible.
- Rapidly deployed and poorly secured VPN and remote access solutions, which are also being specifically targeted by attackers.
- A substantial decrease in the level of visibility SIEM and SOC have over user endpoints, with users no longer connected to the corporate LAN. Even when using VPNs, common configurations (e.g. split tunneling) allow Internet access without the usual controls present when connecting from the office.
- A rapid adoption of cloud-based solutions will create even more blind-spots as users need to access the corporate network less and less. Attack detection in the cloud is a challenging endeavor, leaving blue teams with little choice but to focus on endpoint monitoring.
- A reduced ability to respond to suspected attacks and compromises, enforce endpoint isolation and perform forensics. This could lead to greater response delays and greater dwell times for attackers, or even a failure for attacks to be detected altogether.
- A reduced capacity to communicate and coordinate in the face of a cybersecurity crisis like Wannacry or notPetya.

Many IT teams have scrambled to cater for the sudden wholescale migration to a work-from-home paradigm and now need to continue operating through the crisis to ensure protection, detection and response for critical IT infrastructure, despite being themselves victims of the pandemic. We can anticipate some leeway from cybercrime ecosystems as they too are impacted by the crisis, but our observations to date suggest there won't be much. This leaves corporate IT significantly more vulnerable.

The supply chain is also at an increased level of risk

Supply chain threats have already been a growing factor in corporate risk models for several years. Indeed, for many businesses, there is a direct correlation between suppliers' level of security and their own, as recent incidents like the notPetya malware campaign have illustrated.

Earlier in 2020 the U.S. Department of Homeland Security reported, that biopharmaceutical companies were among ten industries strategically targeted by Chinese hackers to steal trade secrets, and that hackers were actively exploiting relationships between IT service providers and their pharmaceutical customers to affect successful compromises[3].

Supply chain compromise tactics have also been characteristic of APT41's most recent espionage campaigns. The Chinese group is believed to have access to production environments to inject malicious code into legitimate files, which are later distributed to victim organizations.

It's not only Chinese hackers that target the supply chain. The FBI also published a Private Industry Notification on March 30, warning of malware campaign named Kwampirs - loosely linked with Iranian state-backed hackers - that specifically targets the healthcare sector. Kwampirs is also believed to move laterally through the supply chain[4].

At this time of elevated risks, businesses must worry about the security of their suppliers and partners as much as their own. As in our response to the COVID-19 pandemic, we're directly dependent on one another to bring cybersecurity threats under control.

Reliance on insecure IoT and OT will increase

Significant concerns about the security and privacy of various IoT, OT and automation technologies (e.g. self-driving cars, and cleaning robots) have been expressed frequently elsewhere.

As human-to-human contact becomes less frequent and workers of all kinds are encouraged to stay away from public places, we anticipate that a reliance on robotics, automated vehicles and other IoT and OT technologies will develop faster than previously thought. This is not in itself a threat but exacerbates existing concerns about the security of such technologies.

Internet and cloud infrastructure are strained

This is an unprecedented time for the Internet, with our previous architectural paradigms being blown out of the water as businesses and their providers move en masse to accommodate their entire workforce connecting remotely overnight.

With the increase in people working from home, it is anticipated that there will also be a substantial strain put on crucial shared Internet infrastructure. This could result in critical infrastructure and services such as DNS, Microsoft Office 365, Zoom and WebEx, and other service providers, experiencing performance degradation or potential failure which could impact business continuity.

The IT supply chain is under strain

Everyone is affected by a crisis as insidious as the one we are facing today. This includes the hardware, software and service providers your business depends upon for its own IT operations, including its ability to respond to the cyber-threats exacerbated by the crisis.

As businesses across the globe in all sectors are impacted in diverse ways, their supply chains will also operate at reduced capacity. We can expect hardware and software supply, support, professional services, assurance, compliance, incident response, forensics and law enforcement all to be impacted negatively, thus further reducing a business' ability to deal with an escalated cyber-threat level.

Cyberconflicts are likely to escalate

COVID-19 is a crisis of unprecedented scale, and it's fair to say the entire world is at war. While such crises have the remarkable effect of drawing people together, such times can also sadly sharpen and escalate existing conflicts over resources and ideology.

We assess that the impact of the pandemic in the Middle East will serve to inflame anti-western sentiment[5]. Responses will likely include cyber warfare and could be targeting research- and medical facilities as well as government insitutions and important infrastructure.

Furthermore, various ongoing regional conflicts in the area may deteriorate even further, with the BBC reporting that COVID-19 may be a ticking time bomb for the region as a whole[6]. This might lead to further increasing hacktivism and other forms of cyber attacks.

Our OSINT Unit also offers the following insights specific to state-sponsored hacking:

Our threat intelligence considers APT41 one of the most active and dangerous hacker groups at this time (March 30, 2020). In the context of the COVID-19 outbreak, espionage activities will increase. We assess that patents and proprietary information used to manufacture vaccines and quick detection tests are at a high risk of being targeted.

Hacktivism

Another hypothesis revolves around ideologically motivated efforts to discredit the pharmaceutical sector, through "cyber-hacktivism". Anger generated by various conspiracy theories regarding the search for treatment for COVID-19 could lead hacktivists to launch denial of service attacks.

The pharmaceutical and healthcare industries are difficult sectors to protect. Several threats could pose risks, threatening data protection: high number of M&A activities, machine learning and artificial intelligence, numerous partner industries, but also threats from within the company (e.g. supply chain attacks).

In the case of successful cyber-attack , the consequences can be disastrous for the company. Data theft or espionage can lead to replication of clinical trials, considerable financial loss, litigation and even dangerous consequences for patient health: downtime, spillage of hazardous materials, production of ineffective or toxic drugs and more[7].

We anticipate that politically motivated attacks by state-supported actors against systems associated with COVID-19 response efforts will continue apace with various nation state attackers and hacktivists ramping up their efforts. Indeed, we believe that the impact of the pandemic in the Middle East could spark attacks to subvert COVID-19 response efforts, delaying the attempts to get the situation under control. State-sponsored hacker groups targeting the pharmaceutical industry are active and dangerous for the sector.

Constant factors

Many dreadful elements of today's crisis are completely beyond any prior experience for our generation. However, as much as criminals and other hackers are exploiting the strain that people and systems are under at this time, there is much about the current cybersecurity situation that is fundamentally not different from what we've faced in our previous reality. As this is the baseline assumption we should operate from, we will only highlight a small number of these previous realities here.

Social engineering has always exploited current events

As the COVID-19 pandemic spreads globally, so too have phishing and malware campaigns looking to play on people's fears and hunger information. These campaigns have been observed using legitimate online maps tracking the spread of the virus, fake mobile applications, and targeted email subjects and attachments as lures in phishing emails. The notion of using current events to capture victim attention or gain their interest and trust is as old as Internet security itself. So are the required responses.

Generalised anxiety over the pandemic, combined with people's increased need for information and vulnerability to coercion make the attacker's exploitation of the COVID-19 theme particularly insidious. However, these threats are not in themselves, fundamentally new and do not present us with any new challenges. Indeed, beyond reasoned messaging to our users to educate them appropriately, we would advise customers not to get caught up in daily hysteria on the subject and concentrate on strategically countering the human crisis we face.

Hackers gonna hack

An article on Bleeping Computer describes an escalation in Chinese APT41 activity, correlating with the outbreak of the coronavirus: "The Chinese state-sponsored group APT41 has been at the helm of a range of attacks that used recent exploits to target security flaws in Citrix, Cisco, and Zoho appliances and devices of entities from a multitude of industry sectors spanning the globe. It is not known if the campaign that started in January 2020 was designed to take advantage of companies having to focus on setting up everything needed by their remote workers while in COVID-19 lockdown or quarantine but, as FireEye researchers found, the attacks are definitely of a targeted nature."[8]

As the article suggests, there seems little doubt that threat actors of every kind will seek to leverage this crisis to their advantage.

We should note however that the "security flaws in Citrix, Cisco, and Zoho appliances and devices" predate the pandemic, are well understood and should have been remediated long before the pandemic broke out.

Even less obvious issues, like the risks posed by remote working via untrusted or poorly configured Wi-Fi access points, have been well understood by us and are discussed extensively in the industry. An article by journalist Geoff White describes a paper our Security Research Center delivered on the subject and illustrates this point: "The problem is, the Wi-Fi hotspot provider doesn't just temporarily receive your machine's Internet traffic – it can potentially manipulate it as well, and that can cause some serious security headaches."[9]

The security vulnerabilities, whether technical or procedural, though they may be targeted more aggressively now, are generally well known and understood by us and generally well within our abilities to remediate.

Humans have always been vulnerable

The social engineering lure presented by the COVID-19 crisis is only half of the problem. As we argued earlier, the other half of the problem is that humans are fundamentally predisposed to fall for these kinds of scams, even under the most 'normal' of circumstances.

As much as the current situation appears to favor the attacker, we should also note that the fundamental psychological biases that social engineering depends on are deeply baked into the human condition. This is perhaps bad news in that we've done poorly at addressing these vulnerabilities even under 'normal' circumstances. But it's also good news in that this isn't a new mountain to climb It's a mountain we're already halfway up.

Medical data has always been valuable to cyber-criminals

Targeted cyber-attacks against various industries have become increasingly common in recent years. The healthcare sector is no exception. In 2015, this reached its peak, especially affecting United States based healthcare companies, with more than 113.27 million records being exposed.

In a report released by Orange Cyberdefense in 2019, researchers concluded that "Health data is more attractive to an attacker because it brings more value due to its multitude of information, e.g. financial data, PII, medical history" and that "stolen health data is sold for a higher price per record on online markets in comparison to other stolen data such as financial data."[10]

A recent Reuters report also assessed that the financial value of health data can be as much as ten times that of a credit card number.[11]

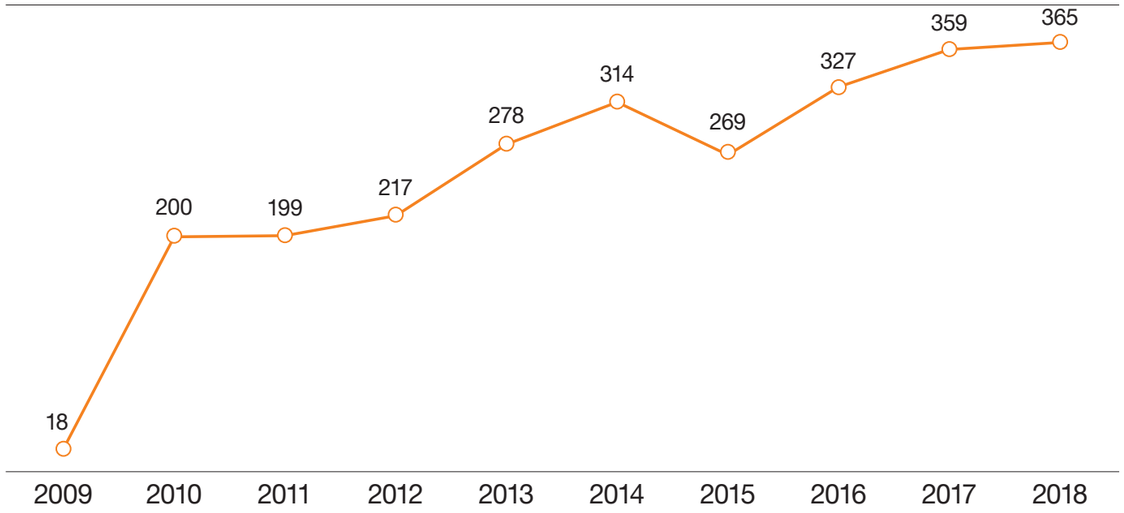
There are three reasons for the interest by hacker groups in the pharmaceutical industry: firstly, there is a profusion of intellectual property. Secondly, the sensitivity of patient data attracts potential hackers. Thirdly, the pharmaceutical sector is a controversial sector: it mixes public health issues and commercial logic.

Given the strong links between the commercial world and the scientific world, large laboratories are often accused of conflicts of interest. As a result, this sector has been targeted by whistle-blowers and cyber-hacktivists.

The threat model that healthcare services need to consider and address during the COVID-19 crisis is not actually new. Given the value of the data and systems that hospitals and similar organizations use, attacks and compromises against them were already commonplace.

Number of reported data breaches

Reported databreaches in the USA



Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Health services have a poor track record with security

In a 2019 paper published by Orange Cyberdefense we reported that "the number of health data exposed increased by 73.6% with a total of 3,452,442 healthcare records stolen".[12]

The healthcare sector, like any other sector, is undergoing massive digitalization to increase accessibility and increase information sharing for better patient care. The side effect of this is an increase in the attack surface. Security knowledge and awareness, as well as budget, are often in short supply.

Data is not the only concern either. Medical devices, such as heart rate monitors or insulin pumps, were designed to serve a medical purpose. Yet security is often not considered enough. The devices themselves might not have data storage capabilities, but they still provide an entry point to servers and other network devices that do store sensitive data and are often critical to the operation of a medical facility.

Ransomware attacks against healthcare providers have also been increasing over the past decade. Many healthcare providers migrated from paper-based processes to electronic medical record solutions without adequate cybersecurity controls, making them juicy targets for either intentional attacks or as collateral damage from drive-by ransomware campaigns. The most infamous example being the devastating incident with the NHS in the UK.[13]

While there is anecdotal evidence that activity by various actors, including state-sponsored groups, is accelerating currently, the reality is that healthcare-related industries have been highly targeted for a long time before this current crisis. Our 2019 study on the subject shows that medical records have a higher value than other PII on the black market, and of course medical services have been targeted due to the valuable intellectual property they hold, and because frankly they have proven to be a soft target for even the simplest attack vectors, like ransomware.

Mitigating factors

It's hard to see any silver lining in this cloud, but there are some elements of this crisis that may play to our favor and help to mitigate the cybersecurity risks we are likely to face.

Attackers are people too

While it is too early in the crisis to comment definitively on this, it would seem safe to assume that criminal hackers, scammers, hacktivists and state operators will all be impacted by this crisis, just like the rest of us.

> Offensive security operators, just like their defensive counterparts, are people with budgets and bosses. They fall ill like the rest of us, have families they care about and need to earn money to live. They need supplies, equipment and resources to operate. Some even have ethics and moral codes. Although we have seen early evidence of an escalation in both criminal and state-supported activity, it would be reasonable to expect that attacker capabilities will also be diminished at this time and may decrease even more as the full impact of the pandemic hits us and normal life is disrupted further.

The security community is rallying

"Hell hath no fury like the cybersecurity community during a pandemic."[14]

As is so often the case during real human crises, good people of the world are rallying together to offer their skills and resources. The same is true in cybersecurity, and several notable efforts to develop and apply community-driven initiatives are already emerging.

CV19 – "one newly formed group of information security professionals, including company CISOs, penetration testers, security researchers, and more, have vowed to do all they can to help provide cybersecurity support to healthcare services across the UK and Europe."[15]

According to the Forbes article above, the five working principles of this initiative are:

1. Be honest and supportive
2. Always act with integrity
3. Be kind and respectful to other volunteers
4. Be flexible and collaborative
5. Trust and use everyone's expertise

This kind of noble and altruistic thinking is exactly what the world needs right now, and may help us turn the tide on cybercrime.

BBC reporter Joe Tidy has created a web application, in conjunction with a number of corporate sponsors, to track corona-related phishing emails. The site can be found at https:// coronavirusphishing.com/.

The ThreatCoalition is another such global volunteer initiative focused on creating and sharing COVID-19 related threat intelligence.[16]

We were already working from home

A common 'joke' in the cybersecurity technical community is that blue teamers and red teamers alike were already socially isolated, living alone and never going out, even before self-isolation and lockdown became the new normal.

At Orange Cyberdefense, for example, we threw the switch on working from home and closed our offices worldwide almost overnight, with virtually no impact on operations.

> (Un)funny as it may be, there is some reassurance in the reality that most established IT security product, support and services businesses have well-established remote working structures and infrastructures. IT security support and service providers worldwide have thus far retained a high level of capability and can be expected to continue to adapt to new constraints, even as the crisis unfolds.

We know how to fix this

As should hopefully be clear if you've read this far in our report, there are no technical elements of the current coronavirus cyber-threat landscape that are fundamentally new.

> Even as conditions become more trying and appear to favor the attacker more than the defender, every single technical weakness we need to counter has been seen before, studied and addressed. We know how to solve these problems. The challenge remaining to us now is to think clearly, act strategically and work efficiently to address those problems that matter most using the few resources still available to us.

Part II:

Responding to the cyber side of the crisis

In light of the threats and concerns raised above, we offer the following guidance to businesses and professionals considering the cyber element of what might be the most serious threat to global well-being since the second world war.

Just like the virus itself, there is a real and frightening risk to cybersecurity. The consequences are not unavoidable, however, and the impact won't be irrecoverable. Consider your cyber response strategy in this light and keep your wits about you.

The world is currently overwhelmed with fear, uncertainty and doubt – emotions that the security industry has been sadly vulnerable to and shamefully guilty of exploiting.

Don't panic

The world is in panic right now over several real and imminent threats. Let's not make it worse by creating unnecessary panic over cyber-threats also. Our guidelines for remaining rational in the crisis are as follows:

1. Understand that we are experiencing a state of **heightened threat, but only slightly increased vulnerability.** We cannot control the threat, but we can control the vulnerability, so let's focus on that.
2. **Understand what has changed and what hasn't.** Your business's threat model may be very different today than it was yesterday, but it may also not be. If it hasn't changed, then your strategy and operations don't have to either.
3. Form partnerships but avoid mobs. **Your suppliers, service providers and even competitors are all in the same boat**, never more so than now. They may not have all the answers either, but now is the time to reach out and find partners that have balanced and rational views and avoid communities that are promulgating hype and hysteria.
4. **Maintain context.** IT and the Internet have survived for twenty years despite our various security failures. There is no doubt that the situation today is worrying, and that the risk of a fundamental cybersecurity crisis in our lifetime is real and can't be ignored. However, right now, the crisis is medical and human. Don't let the hype about cybersecurity distract you from that.
5. **Work smart, not hard.** You will be able to achieve very little during this time of diminished capability, so spend time and energy on considering what your primary concerns are and focusing on those.

Take the time to improve

This is not a black-and-white scenario. If there are elements of your infrastructure or processes that we're not ready when this crisis broke, there is time now to review and improve them. Home computing resources and remote access solutions can be improved incrementally. Just as with our response to the pandemic: every victory counts.

Hope for the best, plan for the worst

It is possible things could get worse. As soon as time allows, invest some effort in considering your corporate response in the event of a compromise or breach. Phishing, credential stuffing, compromise of remote access systems, DDoS, ransomware and other extortion attacks are of specific concern now. There are no single or simple formulae for response, but getting the people, systems and processes in place to respond quickly and safely to an incident is essential.

Talk sense to your people

As we discussed earlier in this paper, one area of exaggerated threat has to do with people's increased level of vulnerability to social engineering, and attackers' increased exploitation of the context to conduct social engineering attacks. Remind your employees and IT teams to remain vigilant, provide them accurate information and gentle guidance using examples.

However, to a team dealing with a global health crisis, the threat of not receiving essential communications may be bigger than the threat of receiving malicious communications. Consider this carefully when communicating with staff about emerging cyber-threats and their relative importance.

Check on your suppliers

For many businesses, there is a direct correlation between suppliers' level of security and their own, as recent incidents like the notPetya malware campaign have illustrated. At this time of elevated risk, businesses have to worry about the security of their suppliers and partners as much as their own. As in our response to the COVID-19 epidemic, we're directly dependent on one another to bring cybersecurity threats under control.

Security and risk teams should consider opening and maintaining channels of communication with suppliers, providers, consultants and partners who may have access to sensitive systems and data. Discuss their responses to the elevated threat levels at this time and ensure that that they remain appropriate and in line with your own.

Stay in touch with your partners

Service providers like Orange Cyberdefense are doing everything in their means to remain ready and available to support clients. As we've discussed already, IT service providers are generally well prepared to offer remote support and should by and large have resources available even as the crisis escalates. Not only is there a business driver for service providers to retain and make capability available, but many of them are also responding altruistically to this crisis, helping where they can, when they can.

There are also various government support initiatives (like the NCSC in the UK) and community initiatives (like CV-19, which we discussed before) that can offer guidance, advice and even direct support when required.[17]

Reach out, maintain communications and stay in touch. Our team and others have information, intelligence and other resources available that can greatly assist you if the worst should happen, or to reduce the likelihood that it does…

Prioritize

As we've argued previously, we want to focus our strained resources on elements of the threat that are of most concern to us right now. Determining what the 'important threats' are is, however, very difficult. Indeed, it's a challenge that we've spoken and written about extensively in the recent past. It's our assessment that the cyber-threat landscape (even without an exacerbating global crisis) is too complex and fluid to reduce to simple lists or cheat sheets. At the risk of falling into that trap, we suggest thinking about priorities during this crisis in terms of two realities – the things that have changed, and the things that haven't changed.

The things that have changed

As should be clear from reading this paper, we assess that only a small aspect of the cyber-threat landscape has substantially changed as a result of the pandemic. We believe these are:

1. Your people are more vulnerable to social engineering and scams than normal.
2. You have less control and visibility over the IT systems you protect than you're used to.
3. Your users may be connecting from systems and environments that are fundamentally insecure or possibly just poorly configured.
4. You have rushed to implement remote access systems without having the time to plan and execute as well as you'd like.
5. You, your team and your providers may be operating with diminished capacity.

The things that have not changed

As much as we are living through an unprecedented time in recent human history, there is really very little about the current threat landscape that is fundamentally new. As such, our priorities from a cyber point of view don't need to divert too much from what they were before the crisis:

1. Phishing, spear-phishing, Business Email Compromise (BEC) and other forms of social engineering attack are nothing new. Neither is the reality that our users are fundamentally predisposed to fall for these kinds of attacks. Our response to these attack vectors has not changed, despite the elevated threat level.
2. Attacks against cloud-based interfaces, remote access systems and VPN gateways have been escalating for some time now. Indeed, for this reason, a recent campaign by Chinese hacker group APT41 exploiting these techniques cannot definitively be linked to the crisis, despite the coincidental timing. The security weaknesses APT41 is exploiting, though perhaps more acute, are well understood and relatively simple to remediate.
3. Remote working and facilitating secure remote access for mobile workers is a very well understood problem and there are several technologies and approaches in our toolbox, suitable for almost any budget and level of technical sophistication.
4. The modern workforce has been mobile for two decades now, and vendors and IT teams can offer several methods for monitoring, maintaining and managing remote endpoints. Even more complex requirements, like remote isolation and triage, are easily met, even without a huge budget.

Our proposed list of priorities

Proceeding from the breakdown we've modelled above; we would propose the following general set of priorities that businesses should be considering in light of the current threat landscape.

If your own security priorities are not already clear to you, we propose that you focus on the following responses, in order of importance:

1. Establish emergency response procedures and systems.
2. Establish a security support hotline.
3. Review backup and Disaster Recovery (DR).
4. Equip your users with the information they need to make good decisions.
5. Provide secure remote access.
6. Establish visibility over remote endpoints.
7. Consider malicious mobile applications.
8. Consider patching and hardening of remote endpoints, including mobile.
9. Review your insurance.

Establish emergency response procedures and systems

Given everything that we've discussed, we need to assume that attacks will happen during this time and that successful compromises are more likely than usual. Under this assumption, planning and preparation are essential.

Take some time to facilitate a planning session with key IT and security role-players to consider your response capabilities in the event of a suspected compromise or breach. Areas to consider here include:

- How would you detect a breach? What indicators might be available to you beyond the conventional, e.g. reports from users or external service providers?
- Who needs to be informed and involved if there is a crisis?
- How might a response team communicate and collaborate, even under a worse-case scenario where trusted systems may be impacted?
- How would you communicate with other stakeholders like users, regulators, customers, board members and shareholders?
- Are you in a position to isolate an endpoint or server, whether remotely or onsite?
- Do you have access to a capable incident response team, whether in-house or via a partner?
- Do you have effective backup and Disaster Recovery plan in place? When last was it tested? Could it be tested now?
- Do you have a policy position on ransomware and extortion? If you believe you would pay a ransom, do you have the funds and systems available to do so? You should also consider your negotiating strategy and appoint a negotiating team ahead of time.
- Do you understand your regulatory requirements, for example with regards to the UK ICO, and are you prepared to follow them in the event of breach?

Establish a security support hotline

Your users are feeling highly anxious right now and cyber-threats are certainly adding to anxiety levels.

Providing users and even customers with a number or address they might use to speak to someone rationally about technical and cognitive attacks they may suspect, or about their own systems and behaviors, could be a powerful tool for reducing the level of anxiety and indeed improving your security posture. If you already have a support hotline, prepare for (at least initially) a rapid increase in the volume of calls, emails and other available methods of communication.

Review backup and DR

Two real threats even before the crisis, which have arguably escalated due to the pandemic, are ransomware and Denial of Service.

Take some time to review the state of your backups and the readiness of your data and Disaster Recovery processes.

In this process, you need to think about home workers and the data they may be working with locally. If you don't already have a suitable backup system for remote users, then readily available public cloud solutions like Google Drive, Dropbox and Microsoft OneDrive may present a viable alternative under the circumstances.

Equip your users with the information they need to make good decisions

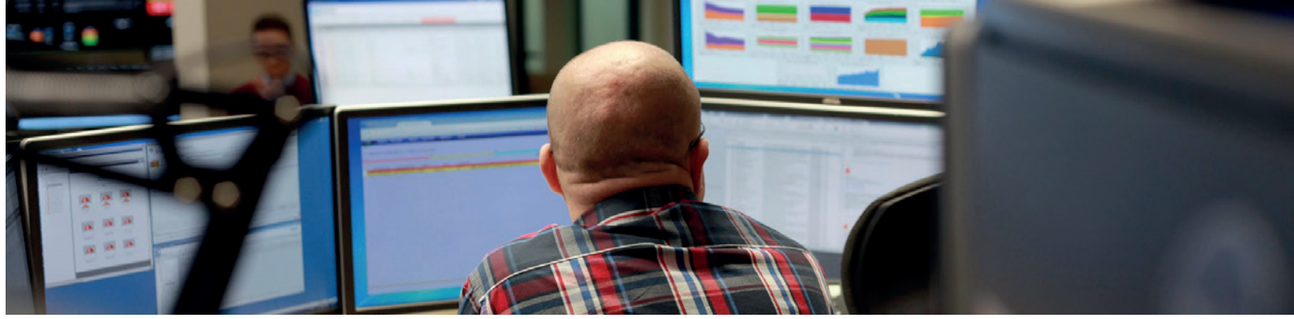
Users will more than ever form your first line of defense at this time. The better educated and equipped they are to recognize and counter cyber-threats, the better it will be for your overall security posture.

Our studies of the psychology of social engineering suggest that your goal should be to equip and educate users, rather than scare or punish them. Frequent examples of attacks and reminders of how to respond will be more useful than policies and testing at this time. Vigilance regarding malicious mobile applications and COVID-19 tracking sites should also be included here. Providing users with rich and ready locations for useful information and discussion on the developing crisis will also reduce their desire to look elsewhere.

Provide secure remote access

Secure and reliable remote access to the Internet and corporate systems appears to be the biggest challenge facing our customers right now. The best solution to this challenge will vary dramatically from customer to customer, but the following principles should serve to guide the design of any remote access architecture:

1. Clearly understand your threat model. We would assert at this time that the primary challenge is to provide appropriate authentication and access control to data and corporate systems. Encryption between the user endpoint and the Internet, via their mobile Internet or their own home Internet, is arguably less of a concern right now.
2. Make sure you secure DNS. Several contemporary attacks involve redirecting DNS requests in order to present phishing or watering hole sites or conduct Person in the Middle attacks. Pay careful attention to how you control the DNS servers that your workers use, whether by using VPN configurations or simply having them hardcode DNS resolvers on endpoints.



3. Implement multi-factor authentication. We would argue that, for most businesses, authentication is going to be a higher priority than confidentiality right now. Review all your remote access systems (including web interfaces, VPN and remote access gateways) and consider how strong authentication might be implemented. At this point, the form of the second factor is less important than having a second factor at all, so SMS and email-based systems are also an option. Given a choice, however, a full push-to-mobile solution – as is available from Okta, Duo, Google and Microsoft – is going to be the best option in terms of usability, security and perhaps even ease of deployment.
4. Clarify and communicate smart password policies. We emphasize again that currently, attacks against remote access technologies by using compromised password is one of the key threats. If you're not able to implement strong Multi-Factor Authentication (MFA), then consider what you can do to ensure users make strong password choices at this time. Specifically, users should be encouraged to:
   - Change their password (but not again until the crisis is over),
   - Chose a password that they have definitely not used elsewhere, and
   - Choose a passphrase that is long but easy to remember, rather than short and complex.
5. Manage your security devices. As discussed earlier, current campaigns like APT41 are actively targeting specific corporate systems like Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) servers, Zoho ManageEngine Desktop Central and Cisco RV320 and RV325 routers. Unpatched Pulse VPN servers are another popular target. These attacks are remarkable because they exploit known and patched vulnerabilities and even use free or commercial hacking tools. In other words – they are real, but they are not difficult to fix. Ensure that you know where all your Internet-facing remote access technologies are, and that each is appropriately patched and configured.

Establish visibility over remote endpoint

A shocking realization for many businesses at this time is how much their attack detection and security monitoring capabilities depend on the perimeter.

With users now working remotely on a large scale, enterprises without a robust endpoint detection and protection or response capabilities may find themselves flying blind through the eye of a crisis. Though endpoint visibility is not something that should be rushed into, businesses without any endpoint capabilities should be considering their options at this time.

The two obvious routes to take for most endpoint configurations are:

1. Microsoft Sysmon: Microsoft's own free System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network. Sysmon is relatively safe and easy to deploy, supports most contemporary Windows versions and there are numerous commercial and open source projects that offer configuration, management, collection and reporting support. See the MS-documentation for a starting point.[18]
2. Commercial EDPR: Several vendors offer reputable Endpoint Detection, Protection and Response products, including Crowdstrike, Cybereason, Cylance, Palo Alto TRAPS, SentinelOne and others. Many of these solutions are highly reliable, proven effective and easy to deploy and manage. Some also offer a variety of 'isolation' features that allow one to take an endpoint partially offline while incident triage and forensics can be performed.

Aside from these obvious solutions, other options exist to achieve the same ends. For example, VPN agents can be used to implement virtual network isolation, while open source products like Google's Remote Response (GRR) offer workable remote triage and forensics options.

Consider malicious mobile applications

As a paper published by the US National Institute of Standards and Technology, referenced below, points out: “Mobile devices are designed to make it easy to find, acquire, install, and use third-party applications from mobile device application stores. This poses obvious security risks, especially for mobile device platforms and application stores that do not place security restrictions or other limitations on third-party application publishing. Organizations should plan their mobile device security on the assumption that unknown third-party mobile device applications downloadable by users should not be trusted”.

As we previously mentioned, we’ve observed a five-fold increase in the number of malicious mobile applications detected between February and March this year. We can expect that this trend will continue as the crisis stretches out.

Options available to companies with regards to malicious applications include:

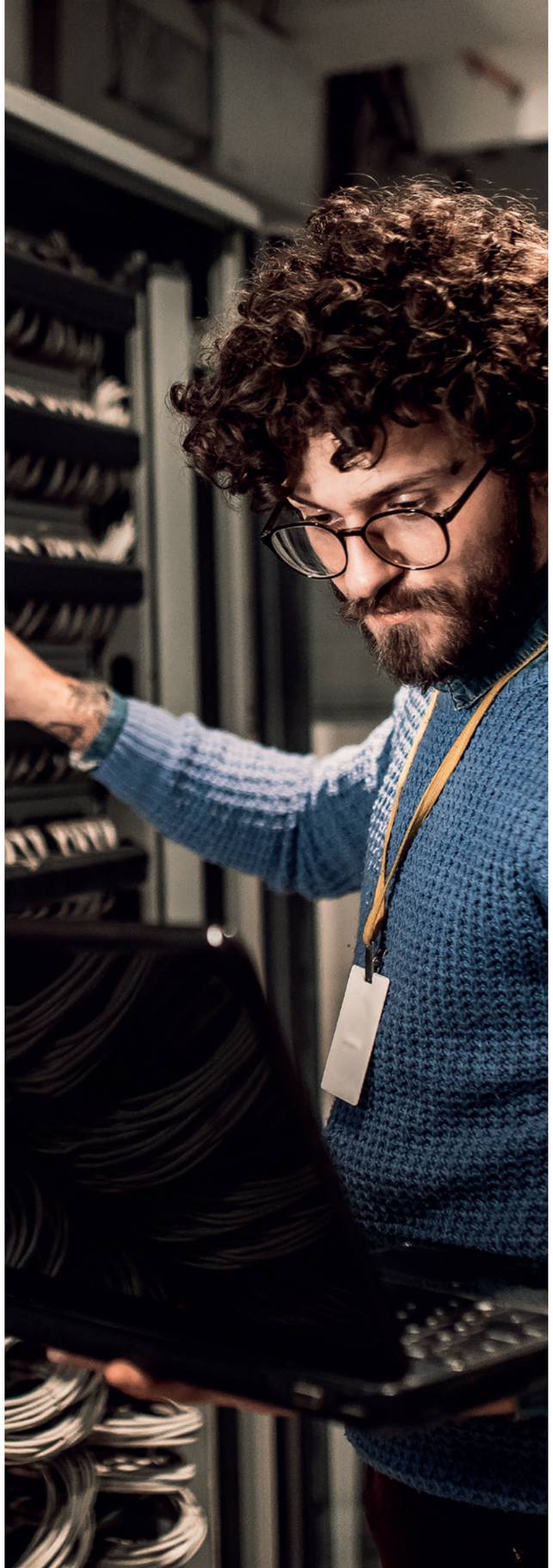
- Prohibiting all installation of third-party applications.
- Implementing whitelisting to allow installation of approved applications only.
- Verifying that applications only receive the necessary permissions on the mobile device.
- Implementing a secure sandbox/secure container that isolates the organization’s data and applications from all other data and applications on the mobile device.

For most businesses, the only practical technical solution is to provide their users with a mobile Anti-Virus solution or to provide company-issued mobile devices with Mobile Device Management (MDM) software installed.

“MDM is typically a deployment of a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure, for the purpose of simplifying and enhancing the IT management of end user devices”.[19]

For businesses without some form of MDM already in place, options to consider during the crisis including shipping users' dedicated mobile devices for use on work systems, offering users mobile anti-virus solutions to download onto their own mobiles, or simply educating users regarding the unique risks impacting mobile devices online.

The full NIST paper with associated guidance is available online.[20]



Consider patching and hardening of remote endpoints, including mobile

On March 25, we published a Security Advisory about two critical zero-day flaws in Windows systems. The vulnerabilities are present in all supported versions of Windows and could lead to remote code execution if successfully exploited. Microsoft warned that limited, targeted attacks had been detected in the wild.[21]

Prior to that, on March 11, we warned customers about a remote code execution vulnerability in the Microsoft Server Message Block 3.1.1 (SMBv3) protocol that would give an attacker the ability to execute code on the target SMB Server or SMB Client.[22]

These kind of vulnerabilities on Windows servers and desktops continue to appear and are actively being exploited. The same challenge exists for mobile devices, both personal and private. Although we don’t believe that they represent the most likely attack vector at this time, remote endpoints cannot be ignored and failure to address them will expose your business to unnecessary risk.

Once the other priorities we discussed in this section have been addressed, effort should be invested into considering how remote user endpoints might be patched at this time. One viable option (in lieu of a viable central patching solution) may be simply to advise users of essential patches via company communications and request them to apply the patch directly.

With lateral movement from compromised endpoints arguably less likely with remote workers, there is somewhat less pressure on us to patch everything. Specific patches that make user endpoints less exploitable are the primary concern right now, and every machine that’s patched reduces the attack surface and therefore the risk. This is far from a perfect response to the problem, but as suggested earlier: at this point every win counts.

Review your insurance

Cyber insurance is a complex topic in principle and the detail is almost certainly best left to experts. However, given that the cyber threat model has almost certainly changed at this time, we would recommend that businesses invest some effort in reviewing and reconsidering the appropriateness of their cyber insurance policies.

Cyber insurance should be considered the last line of defense in any security strategy, and certainly can’t be considered as a replacement for the other actions described in this paper. However, at this time, decent insurance may mean the difference between life and death for a business.

Though a domain best left to experts, our observations of the cyber insurance industry would have us encourage clients to consider two somewhat unusual factors:

1. Since current attacks and compromises are frequently perpetrated by so-called state sponsored attackers, reassure yourself that your policy doesn’t contain unreasonable ‘act of war’ clauses that would impact reimbursements if the actor was shown to be government affiliated.
2. Ransomware payments are a key element in modern cyber insurance policies. It’s important therefore to carefully review this part of the policy, both to ensure that you’re properly covered should you need to be, but also to ensure that your moral and ethical policy on paying ransomware is aligned with the insurer’s. You don’t want to be pressured by the insurer to pay a ransom as the cheapest way out of a compromise, when actually your business has a moral aversion to doing so.

A lesson to learn

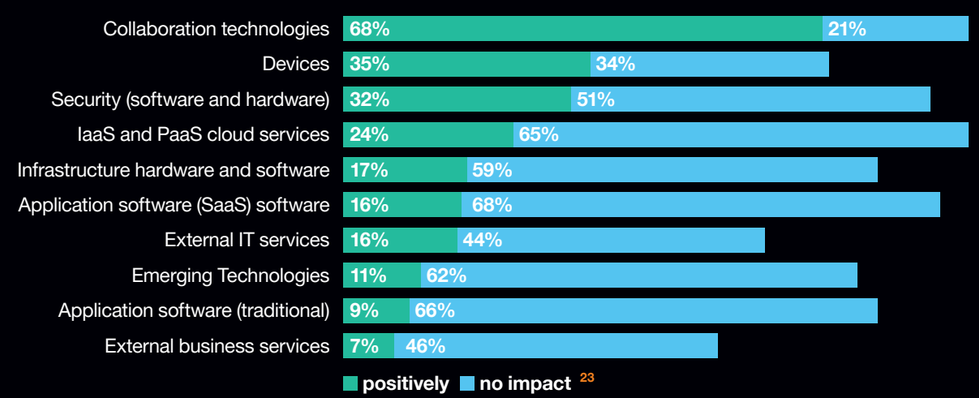
Finally, we believe the impact of this pandemic and our collective response hold valuable lessons for security practitioners; the virus demonstrates how closely-knit our societies and economies are, and how spectacularly a catastrophe in one area spills over to the other. In responding to the crisis, we are learning to appreciate the impact that our behavior has on the whole of society, and not just on us as individuals, families and businesses. This is an essential lesson for the security community too.

When we consider when, where and how much to invest in security, we must think beyond the single-dimensional risk we are addressing for our business and consider the impact of the secondary and tertiary effects on the broader economy when breaches and compromises happen. We need to recognize that what’s bad for society generally, is bad for us as businesses also.

What the future holds

These are the predictions regarding some of the ways in which demands for cybersecurity will change when the worst of the pandemic is behind us:

1. We expect pressure to revisit and improve or create BCP and DR plans conduct tests and incorporate "Contagious Illness Response" into corporate planning. We expect a surge in demand for consulting and support as a result of the interest in these types of policies and exercises.
2. We expect a realization that offices can be reduced in size and that hot desking is not as negative as once perceived.
3. We expect that demand will increase for "fuller" video conferencing and remote work capable applications, perhaps even a surge in VR-enabled applications.
4. We expect that demand for zero-trust and similar VPN-less technology will surge.
5. Conversely, we expect that demand for remote desktop (VDI) and Citrix front end services will also increase, or at least demand for a cloud-based web-browser remote desktop solution.
6. We expect an acceleration in demand for technologies protecting the new perimeter (zero-trust, data centric, IoT, etc.)
7. Online services (banking, payments, e-commerce, learning, entertainment) will continue to accelerate and therefore we expect an increase in the consumption and the development of application security technology platforms to secure online software. This includes:
   - Load balancing
   - DoS protection
   - Application security tools (SAST/DAST)
   - WAF
   - API Security
8. We expect innovation and the emergence of additional products and platforms addressing incident response and BCP such as simulators, ongoing BCP assessment and measurement.
9. We expect an increased perception of the risk from devices (laptops) not being connected to the mother network for longer periods of time (patching, AV, secure configuration etc.) and thus anticipate a demand for tools to quarantine devices out of compliance when returning to the network.
10. We expect an increased risk from staff having more relaxed access to the Internet e.g. O365 etc. that do not require access to the mother network, rendering features like URL filtering, firewalls and IDS/IPS abandoned for periods of time. New Next Generation Firewall features and architecture will be needed.
11. We expect moral, legal and law enforcement attitudes regarding hacking against healthcare facilities to harden considerably, perhaps even with charges as severe as manslaughter or culpable homicide being brought against hackers whose activities have disrupted medical services during this time. This could have far-reaching implications for the ability of law enforcement to counter cybercrime, even after the crisis is over.
12. IT and security budgets will certainly change off the back of this crisis. It's not clear yet whether that will be for 'better' or 'worse', but we do expect that there will be increased focus on and demand for clear and measurable ROI from spend on cybersecurity.



[23]

When it's all over

We live in the hope and believe that this terrible time will eventually be over, and that life will return to whatever form of 'normal' is left to us. For many, this will hopefully mean returning to a normal work life, back at the office.

We don't know how soon this might be, and we should expect the current reality to stretch for weeks or even months still. But eventually workers will return to their desks and it behooves us, before this happens, to give some thought to how to deal with that day from a security point of view.

We should expect to find at least some of the following, when workers return to the office:

1. There may be cobwebs on your systems. After weeks of stagnation and neglect, you should expect to find some elements of your system are rusty or in disrepair. In addition, cached data like endpoint logs, backups or backdated updates may be pushed all at once when users connect again, causing additional strain on your infrastructure. Consider staging the return to office work so that these kinks can be identified and ironed out without causing too much disruption.
2. A lot of data will be locally stored and not yet saved to safe enterprise repositories. Make it a priority to have secure and reliable locations ready for users to dump their data to reduce your reliance on endpoints as quickly as possible.
3. Unless you have been able to address some of the fundamental challenges of endpoint protection, detection and vulnerability management during this time, you should expect that some enterprise mobile endpoints will return to the office in a compromised state. This is not an entirely new problem, but it's a challenge we seldom face on such scale. There is no simple, single solution to dealing with this risk, but some thought should be given to how potentially compromised endpoints are dealt with as they return to the corporate network.
4. As previously suggested, a staged return program would allow IT and security operators to deal with the challenge in smaller chunks. Various endpoint security technologies (like Network Access Control – NAC) will allow endpoints to be isolated and checked for compliance before they are fully connected to the network. If it's feasible, the opportunity to re-provision endpoints from a safe and current build standard is worth considering.

One of the many ways that COVID-19 is unique is in its global effects. Typically, companies plan for localized or regional outages, not global ones affecting not just themselves and their employees, but also stretching back through their supply chains across the planet. Understanding that every company's response will also be unique, the following are a few highlights to consider.

Situational assessment

- Perform an assessment of the situation across the organization, determining which aspects of the business have been most affected. For example, have laptops been allowed to drift out of acceptable patch schedules? Has new equipment been procured to deal with the situation, without proper protection?
- Prioritize the business functions and move carefully to business as usual.
- Document as much as possible and ask other teams to do the same.
- Conduct a risk assessment.

Notification and communication

- Evaluate technology and security functions and apply return to BAU changes on affected systems.
- Identify any implicit or explicit changes that occurred in policy and determine whether to revert to the original or accept the changes., Evaluate your supply chain, including third parties, and notify them of any changes in security measure. As applicable notify government authorities.
- Work with the crisis management team, or if none exists, with your public relations, marketing, and legal departments to notify customers if there are security related changes (such as fraud and security notification procedures, bug bounty etc.).

Change control

- Initiate change control procedure for each of the affected systems (end-user, corporate systems, connectivity, telephony etc.).
- Conduct a lessons learnt session and update the BCP plan and scenarios accordingly.

Technical Security Measures

- End-user device security- review patching and secure configuration before connecting to the network (Quarantine zone, compromise assessments, and Host IPS deployment).
- Perform firewall rule review and access review to inspect changes and remove unnecessary rules/ access authorization.c. Physical security assessment to review physical access controls

Part III:

Analysis: what we have seen so far

In this section, we present a summary of activities and significant developments that our various intelligence teams have observed since the crisis started.

As of March 25, at least 20% of the global population was under coronavirus lockdown.[24] For businesses not already prepared for a large-scale remote work paradigm, this has meant a desperate rush to put the systems and processes in place required to accommodate a stark new reality.

As an established managed security services and support provider, we at Orange Cyberdefense have been able to observe this escalation in demand first-hand. Within our UK operations for example, the professional services team is accustomed to dealing with an average of one Pulse Secure VPN engagement per month. As of the March 23, 2020, they had responded to six.

The UK security operations center has seen a similar escalation in demand. In just the first three weeks of March we observed a 50% increase in service requests related to VPN products over February. There were similar increases between January and February.

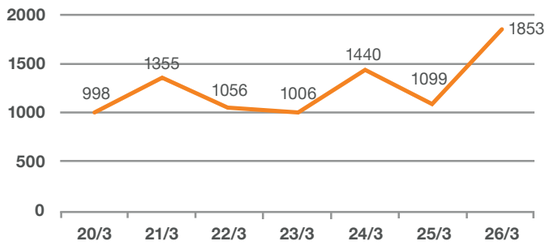
Anyone lucky enough today to still have a job, (that doesn't involve being onsite and exposed directly to the virus) will be able to attest to the dramatic change in reality for the global workforce. Home working is here for the world, and it may even stay forever.

The perfect lure

As the COVID-19 coronavirus pandemic spreads globally, so too have phishing and malware campaigns, looking to play on people's fears and need for further information.

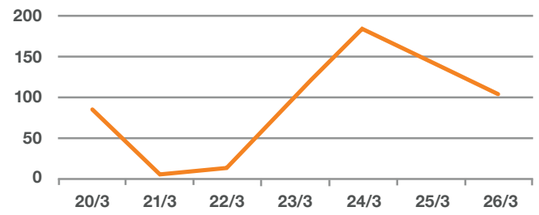
These campaigns have been detected using legitimate online maps tracking the spread of the virus to try and distribute information-stealing malware, as well as targeted email subjects and attachments as lures in phishing emails.

Registered domains linked to COVID-19



According to statistics published by our CERT team on 26 March, during the last week approximately 8900 new DNS domains related to the terms "corona-virus", "covid-19" and "ncov" were registered; more than double when compared to the previous week.

Number of potentially fraudulent emails transmitted by the CERT customers



On March 24 alone, our CERT team in France tracked 23 unique COVID-19-based phishing mails over a 24-hour period. Our CERT team also reported that during the same week, customers reported more than 600 potentially fraudulent emails, 10% of which has proven to be malicious.

The number of emails validated as malicious was 4 times higher than during the previous week.

Several examples illustrate this kind of 'pretexting' by RAT-COVID-19. We've seen some botnets and stealers such as Hancitor, NetWire, Formbook, Loda, JRat, Danabot and others exhibiting the same kind of behavior.

Coronavirus data map watering hole

The "Live coronavirus Data Map" from the John Hopkins Center for Systems Science and Engineering (CSSE) has been used as a lure to spread malware.[25]

The interactive dashboard is being used by malicious websites (and possibly spam emails) to spread password-stealing malware. According to Krebsonsecurity.com[26], a member of "several Russian language cybercrime forums began selling a digital coronavirus infection kit that uses the Hopkins interactive map as part of a Java-based malware deployment scheme. The kit costs $200 if the buyer already has a Java code signing certificate, and $700 if the buyer wishes to just use the seller's certificate."

Our Epidemiology Lab assesses that it was used to distribute a strain of Danabot malware. DanaBot is a modular banking trojan developed in Delphi and designed to steal banking credentials. However, it also compromises sensitive information by collecting form data, taking screenshots, logging keystrokes, harvest credentials from software (browsers/FTP/instant messengers/emails) and can run a local proxy, use the TOR network, provide remote control via RDP & VNC and more. A recent DanaBot variant detected by Check Point adds a ransomware module to its previous list of capabilities.[27]

Malware adapts

The cyber-crime ecosystem has always been remarkably agile and able to adapt to changes in the landscape. Hackers and scammers are acutely tuned to the dynamics of the pandemic and have moved rapidly to capitalize on it in various ways, some smart and some almost naively opportunistic. These responses range from smart but fake COVID-19 tracking applications and watering hole attacks, to the almost childish rebranding of existing products along COVID-19-related themes.

Malicious applications

According to our OSINT Unit, a division of Epidemiology Lab, information from approved external sources indicates that from early on in the crisis web links were sent to some Android phones promising applications to track coronavirus.[28] This was a lure. Once the application was downloaded, people suspected to be operating from Libya can watch through the smartphone camera, have access to text messages or listen through the microphone. The malware identified would be a customized version of SpyMax, a commercial spyware than can be acquired very easily online for free.

Bitdefender researchers have also recently analyzed telemetry regarding coronavirus-themed legitimate apps and malware and found huge spikes in application scans containing "covid" or "corona" in the package name or file path.[29]

On the March 26, our own CERT team reported that malware propagation campaigns were more and more numerous. Between February and March 2020, the total number of COVID-19-related malware campaigns increased by a factor of 5. As of the date of writing, our CERT team is tracking 39 malware families being distributed via COVID-19 related emails. These attempts are likely to persist and escalate the longer the pandemic goes on, reflecting threat actors' standard modus operandi to use global events to try and profit.

Home IT being attacked

As to be expected, hackers have started targeting home IT systems, and specifically vulnerable home routers. In an article from March 26 , ZDNet reported that "for almost a week, a group of hackers has been breaking into people's routers and changing DNS settings in order to point unsuspecting device users to coronavirus-related sites pushing malware".[30]

This kind of attack, which Orange Cyberdefense has reported on before, involves compromising a home router and then redirecting DNS requests from home users to malicious COVID-19-themed websites used for phishing or to download malicious applications.

According to Bitdefender, hackers are using brute-force attacks to guess the admin password of targeted routers.

"Once they guess a password and get in, hackers change the router's default DNS server settings, pointing the device to their own servers. This means that every DNS query made by users connected to a hijacked router goes through the hackers' DNS servers, giving the attackers full control over what sites a user accesses".[31]


NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Coronavirus: How hackers are preying on fears of Covid-19

By Joe Tidy
Cyber-security reporter

13 March 2020 | Share

Coronavirus pandemic

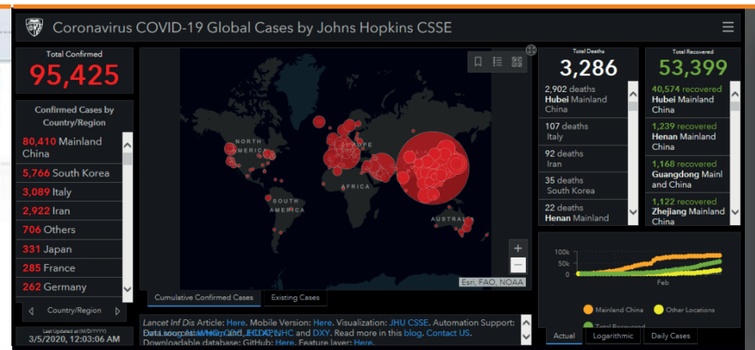

Subject: [W.H.O] COVID-19 VACCINE NOW AVAILABLE

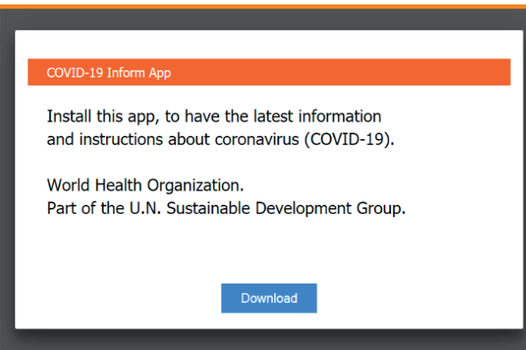
Message COVID-19 VACCINE.xlsx.iso

From: WORLD HEALTH ORGANIZATION (WHO) [mailto:healthcaresupport@who.int]
Sent: Thursday, March 26, 2020 3:05 PM
Subject: [W.H.O] COVID-19 VACCINE NOW AVAILABLE

World Health Organization

part(1):
AVALABLE COVID-19 VACCINE .doc 35 KB




COVID-19 Inform App

Install this app, to have the latest information and instructions about coronavirus (COVID-19).

World Health Organization.
Part of the U.N. Sustainable Development Group.

Download

Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

Cease fire?

On a positive note, several of the major ransomware distribution groups have announced that they either never target medical and research facilities or will now not target them while the pandemic is ongoing. Indeed, some are even offering decryption or data recovery at a discounted rate if such an organization is accidentally targeted.

The 'press release' above was issued by MAZE on March 18, 2020. The world then learned on March 24 that HMR Ltd - Hammersmith Medicines Research – had been compromised and breached by MAZE. Our cybercrime researchers have determined, however, that the HMR breach in fact dates back to the March 14, suggesting that MAZE has indeed kept its word thus far.

Indeed, on March 26 our CERT team reported that, contrary to what had been announced by several cybercriminal groups, some of them, such as the group behind the Ryuk ransomware, continue to target healthcare establishments. DDOS-type attacks against these establishments are increasing, as we saw on March 22 with the attack targeting the Assistance Publique-Hôpitaux de Paris (AP-HP).

Finally, we should note that the ransomware operator Doppelpaymer stated that, though they won't target hospitals in the context of the COVID-19 pandemic, they won't have mercy on pharmaceutical companies that are only interested in profit. Any ceasefire we may enjoy will certainly not be universal.

While ceasefire promises by major threat groups is a welcome reprieve, it can't be relied upon to have any substantial impact. 'Traditional' threats like ransomware persist.

Fake news!

In the public domain, we are observing a significant level of dis-information being propagated, about the origin of the virus, spread, fatality and possible cures. There are strong indications also at this time that state backed operators in China and the USA are running misinformation campaigns to shape the narrative around the virus and response efforts.

We have also observed a fair amount of mis/disinformation regarding technology offerings that have become prominent at the time of writing, specifically Zoom Videoconferencing and social networking application HouseParty– both of which received substantial criticism regarding security or privacy issues that appear either unsubstantiated or at least exaggerated.[32]

Crime capitalizing on the crisis

According to an article on Vice, "Hackers have taken over a wave of Twitter accounts to aggressively advertise a website that claims to be selling face masks and toilet paper during the coronavirus pandemic."[33] Numerous other similar cases are being observed in which criminals (cyber or otherwise) are exploiting concern about the crisis to run various scams and swindles.

Geopolitical escalation

COVID-19 is a crisis of unprecedented scale and it's fair to say the entire world is at war. While such crises have the remarkable effect of drawing people together, such times can also sadly sharpen and escalate existing conflicts over resources and ideology.

Since early in the crisis we have malicious attacks apparently targeting medical facilities. For example, Reuters reported on March 16 that "the U.S. Health and Human Services Department suffered a cyber-attack on its computer system, part of what people familiar with the incident called a campaign of disruption and disinformation that was aimed at undermining the response to the coronavirus pandemic and may have been the work of a foreign actor".[34]

Other attacks have seemingly attempted to target these kinds of facilities, especially in the western world, in order to try and disrupt or undermine COVID-19 research or treatment.

In another example, computer systems at the University Hospital Brno, in Czech Republic, were shut down on March 13 because of a cyber-attack . This hospital is the second largest one in the country and hosts one of the country's 18 laboratories used for testing the virus. According to Bleeping Computer, "systems serving laboratories like hematology, microbiology, biochemistry, tumor diagnostics, or radiology appear to be on a different network than the affected systems as they continue to work". The attack was nevertheless considered serious enough to switch off IT systems and shift acute patients to an alternative facility.

Healthcare in the firing line

The Orange Cyberdefense Malware Epidemiology Lab is scrutinizing attacks specifically targeting healthcare providers. The team cautions that in the short-term the disruption of business continuity can lead to health risks for patients. [35]

Pharmaceutical companies are a prime target for hackers, whether for intellectual property or sensitive data. Several pharmaceutical companies have been affected by cyber-attacks over the last few years. Some are collateral victims; others are infected for spying or ransoming purposes. Regardless of the motive and method, the consequences can be disastrous.

Among the hacker groups targeting the pharmaceutical industry, state-backed actors seem very active and dangerous. Several appear to have links with to governments and APT 41 – an alleged Chinese State backed operator - seems particularly dangerous at this time .

Recent hacker interest in the biopharmaceutical industry, is also worth noting. It is reported that biopharmaceutical companies are among the favorite targets of hacker groups, state-sponsored and otherwise, from which to steal trade secrets.

Iran appears to be targeting the healthcare sector also. On 30 March the US Federal Bureau of Investigation (FBI) published a Private Industry Notification warning of a malware campaign named Kwampirs, loosely linked with Iranian state-backed hackers, that specifically targets the healthcare sector and has the ability to move laterally through the supply chain. According to the report "The Kwampirs RAT is a modular RAT worm that gains system access to victim machines and networks, with the primary purpose of gaining broad, yet targeted, access to victim companies to enable follow-on computer network exploitation (CNE) activities.

Through victimology and forensic analysis, the FBI found heavily targeted industries include healthcare, software supply chain, energy, and engineering across the United States, Europe, Asia, and the Middle East".[36]

Dr David Day Retweeted

Rory Cellan-Jones @ruskin147

How secure is Zoom? Well if you happen to guess the meeting number you'd be able to join them. Mind you I am not sure you'd be enthralled by my meetings

Dr David Day @drdavidjday · Mar 26

As promised this morning. #Zoom is vulnerable by default. We couldn't show how we compromised it, only that it can be hacked, and the hack can be prevented. Credit to Neil Richardson, Luke and Thomas w. #remoteworking #workfro...lnkd.in/eKqXkWE lnkd.in/eKWZkvV

NSC @WHNSC

Text message rumors of a national #quarantine are FAKE. There is no national lockdown. @CDCgov has and will continue to post the latest guidance on #COVID19. #coronavirus

5:48 AM · Mar 16, 2020 · TheWhiteHouse

17.9K Retweets **33.9K** Likes

Joe Hancock @joehancock

We've also seen a rise in fake vaccine scams, counterfeit mask sales and general misinformation. We've a long way to go, and with more remote work we expect further Covid-19 related issues. 4/4.

26/03/2020, 10:48

TLP: WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

30 March 2020

PIN Number 20200330-001

Please contact the FBI with any questions related to this Private Industry Notification via your local Cyber Squad or FBI CyWatch.

www.fbi.gov/contact-us/field | E-Mail: cywatch@fbi.gov | Phone: 1-855-292-3937

Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector

The FBI example above also illustrates the risk presented by supply chain compromises, which we will address elsewhere in this paper.

The Internet under strain

As retailers and service providers rush to move their products and services online, some are encountering unprecedented levels of traffic and demand. Just like 'Zooming', 'Virtual Queues' has become a part of our vernacular almost overnight.

Although we haven't observed many instances of large-scale failure, we consider it prudent to anticipate that demand for online trading and other services will continue through the crisis and beyond.[37]

Concerns about video conferencing

We've observed concern being raised regarding the privacy policies and practices of video conferencing platforms like Zoom, which appears to be emerging as the clear industry leader through the coronavirus crisis.

Some of these concerns are valid. Specifically, an attack called 'Zoombombing', in which trolls permutate through possible Zoom IDs until they find one that's active and join the call uninvited, is a cause for concern.[38]

This wouldn't be the first-time significant security issues have been reported for Zoom (or indeed any other video or web conferencing software).

The digital right advocacy foundation –Electronic Freedom Foundation (EFF) –summarizes its thinking on its homepage.[39]

Zoom, for its part, of course "takes its users' privacy extremely seriously" and has indeed responded to a motherboard report by changing some of the application's behaviors.[40]

As is to be expected the massive new interest in Zoom is also being observed and exploited by attackers capitalizing on the rush of inexperienced new users to the platform. On 31 March, for example, our Epidemiology Lab reported on hackers using malicious Zoom software installers to spread Neshta malware and potentially unwanted applications (PUA) such as InstallCore, a software installer that is classified as riskware.

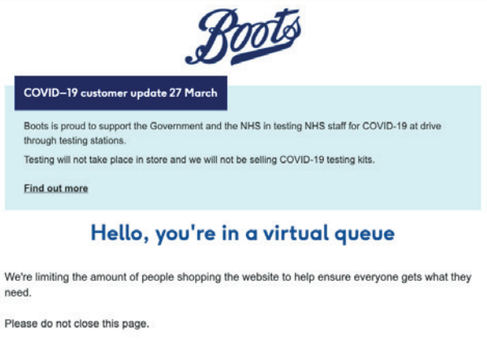
The team also noted 197 new Zoom-related DNS domains in an advisory on that day, though these are not necessarily all malicious.

Orange Cyberdefense

Epidemiology Lab

Cyber-threats affiliated with COVID-19/ coronavirus (OSINT source)

This graphic summarizes the current observations of our Malware Epidemiology teams of the cyber-threats affiliated with COVID-19 and the coronavirus that have links with COVID-19 cyber-threats.



Contributors & Sources

Contributors

We recognize and appreciate the valuable contributions of the following experts from across the Orange Cyberdefense group, whose collective insights have made this report possible:

Marc Germain-Laurent Blanchard	Orange Cyberdefense OSINT Unit (France)
Alina Ribeiro	Manager CERT Cybercrime Unit (France)
Laurent Celerier	Executive VP Technology & Marketing (France-Global)
Diana Selck-Paulsson	Threat Research Analyst (Sweden)
Samsher Sagoo	Director of Professional Services and PMO (UK)
Mark Smith	Pre-Sales Manager (UK)
Richard Jones	Global CISO (Sweden)
Nadav Shatz	Director of Advisory and Architecture (UK)
Mark Sprules	CISO (UK)
Feras Batainah	Senior Advisory Services Consultant (UK)
Wicus Ross	Group Security Research Center (South Africa)
Carl Morris	Group Security Research Center (UK)
Charl van der Walt	Head of Security Research (South Africa-Global)
Etienne Greeff	Global CTO (UK-Global)
Chris Miles	SVP Global Portfolio Management (UK-Global)
Tatiana Chamis-Brown	VP Global Marketing (UK)
Franz Haertl	Head of Global Content Marketing (GER)
Lisanne Meerkerk	Head of Global Marketing Campaigns (NL)
Madina Maglione	Head of Global Field Marketing (UK)

Sources

[1] https://www.psychologytoday.com/za/blog/anxiety-files/200806/knowing-what-you-should-really-worry-about

[2] https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic

[3] https://www.securingindustry.com/pharmaceuticals/charles-river-is-latest-pharma-co-to-face-cyber-attack/s40/a9763/#.XlefbKhKhhE

[4] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf

[5] https://www.washingtonpost.com/world/middle_east/as-coronavirus-cases-explode-in-iran-us-sanctions-hinder-its-access-to-drugs-and-medical-equipment/2020/03/28/0656a196-6aba-11ea-b199-3a9799c54512_story.html

[6] https://www.bbc.co.uk/news/world-middle-east-52103958

[7] https://cyberdefense.orange.com/en/2020/03/20/the-threat-of-cyberattacks-on-healthcare-establishments-during-the-covid-19-pandemic/

[8] https://www.bleepingcomputer.com/news/security/chinese-hackers-use-cisco-citrix-zoho-exploits-in-targeted-attacks/

[9] https://geoffwhite.tech/2019/11/08/more-trouble-with-free-wifi/

[10] https://orangecyberdefense.com/uk/white-papers/databreaches-in-healthcare-the-attractiveness-of-leaked-healthcare-data-for-cybercriminals/

[11] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-creditcard-idUSKCN0HJ21I20140924

[12] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[13] https://www.bbc.co.uk/news/health-39899646

[14] https://www.verdict.co.uk/ coronavirus-hackers-wrath/

[15] https://www.forbes.com/sites/daveywinder/2020/03/23/meet-the-volunteer-covid-19-cyber-fighters-helping-healthcare-fight-the-hackers/

[16] https://www.cyberthreatcoalition.org/

[17] https://www.ncsc.gov.uk/

[18] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[19] https://en.wikipedia.org/wiki/Mobile_device_management

[20] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[21] https://threat-advisories.secdata.com/threats/viewSignal/SIG-4618

[22] https://threat-advisories.secdata.com/threats/viewSignal/SIG-4467

[23] Source: IDC European Survey - Impact of COVID-19 on European ICT Market and Ecosystem, March 2020

[24] https://www.businessinsider.co.za/countries-on-lockdown- coronavirus-italy-2020-3

[25] Security Affairs, https://securityaffairs.co/wordpress/99446/cyber-crime/coronavirus-map-delivers-malware.html

[26] https://krebsonsecurity.com/2020/03/live- coronavirus-map-used-to-spread-malware/

[27] https://www.bleepingcomputer.com/news/security/danabot-banking-trojan-upgraded-with-non-ransomware-module/

[28] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#396f2a8c75fd

[29] https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/

[30] https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/

[31] https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/

[32] https://www.grahamcluley.com/houseparty-hack-claims-reward/

[33] https://www.vice.com/en_us/article/y3m4b7/hackers-twitter-accounts-advertising-face-masks-coronavirus

[34] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[35] https://cyberdefense.orange.com/en/2020/03/20/the-threat-of-cyberattacks-on-healthcare-establishments-during-the-covid-19-pandemic/

[36] https://www.documentcloud.org/documents/6821580-Kwampirs-PIN-20200330-001.html

[37] https://www.thesun.co.uk/money/11276203/boots-shoppers-queue-hour-website/

[38] https://www.theguardian.com/technology/2020/mar/27/trolls-zoom-privacy-settings-covid-19-lockdown

[39] https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis

[40] https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook

Additional sources (twitter quotes and screenshots):

https://twitter.com/TProphet/status/1245170055043825669?s=20

https://twitter.com/WHNSC/status/1239398218292748292?s=20

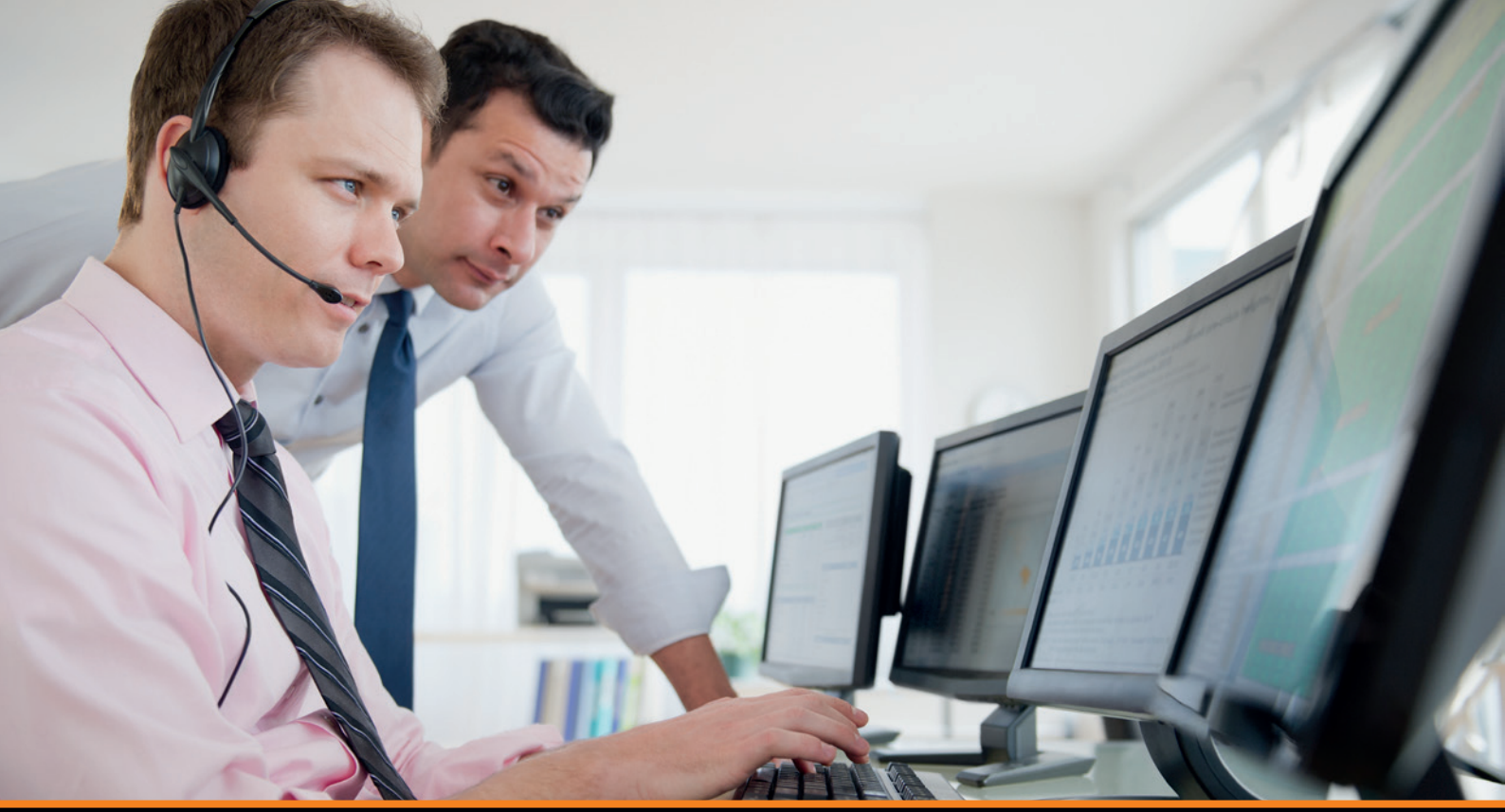
https://www.grahamcluley.com/houseparty-hack-claims-reward/ (House Party)

https://twitter.com/joehancock/status/1243097550841757696

https://twitter.com/drdavidjday/status/1243132223840227328?s=20

https://twitter.com/ruskin147/status/1243265319176732672?s=20

https://twitter.com/drdavidjday/status/1243814550530596865?s=20



Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

Contact us on orangecyberdefense.com