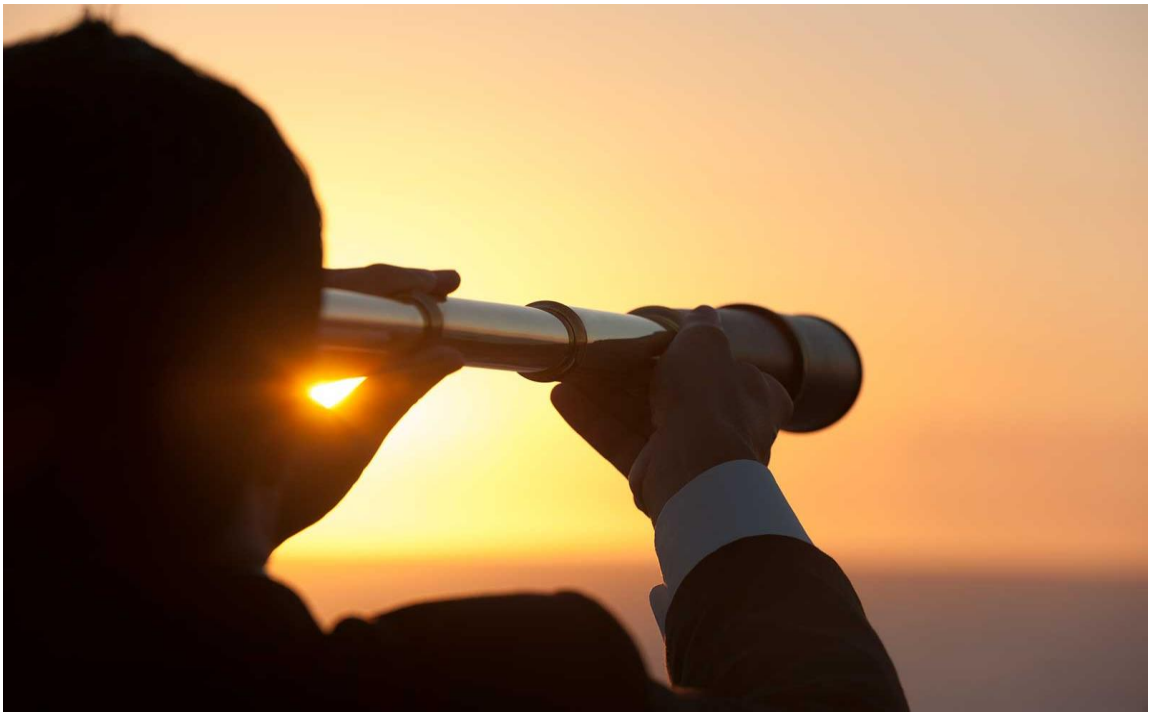
Crowe

Threat Intelligence

05 August 2020

Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.



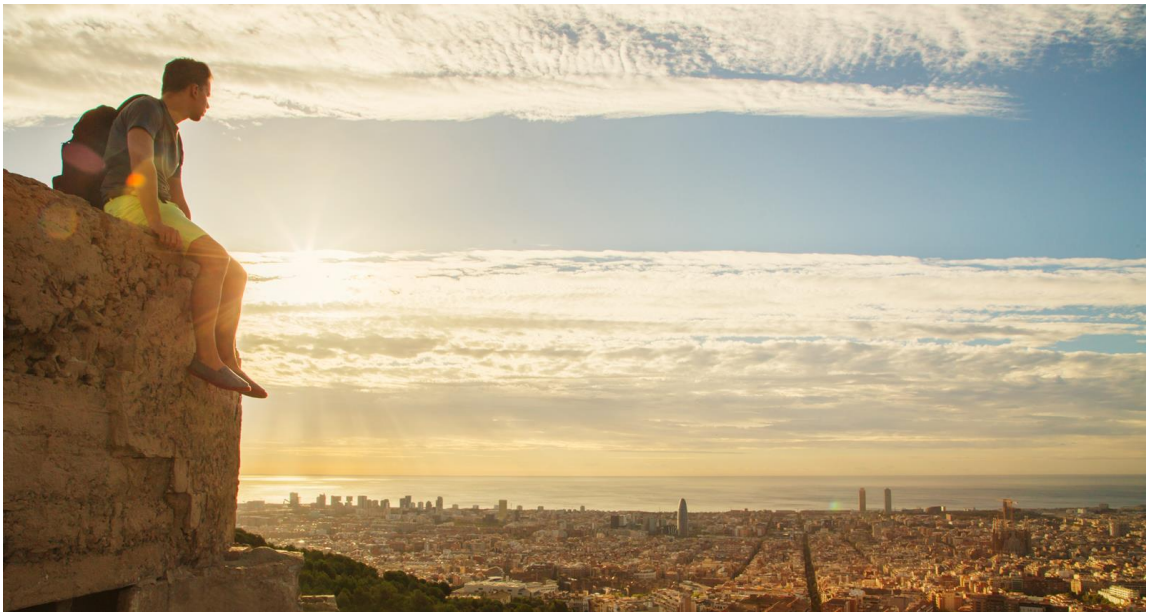
Introduction

This threat intelligence report covers the period 30 July to 06 August 2020 and is based on information obtained from both open and confidential sources. It is designed for UK-centric organisations but includes information regarding matters outside the UK where these may have an impact on activity within the UK. Crowe is able to provide country- or sector-specific threat intelligence reports where required.

The impact of the pandemic has seen many companies go out of business during the last few weeks, with many more anticipated to meet the same fate, leading to opportunities for fraudsters to take advantage of premises and government support schemes. As customer-facing companies start recording contact details in compliance with Track and Trace requirements, opportunities for this data to be exploited are appearing.

Western-China relations still appear to be in a downwards trend, continuing to pose risks and challenges in doing business with entities within that state; companies likely to be affected should scenario plan for interruptions to their supply chain or payments.

As can be expected there is still plenty of activity on the cyber front, with the worrying warning from researchers on how the Internet of Things can be manipulated to affect financial markets. The advice from the National Cyber Security Centre on securing cyber insurance is therefore timely. The cautionary tale in 'Business threats' should be a lesson to us all!



Physical & business threats

- A court in the city of Strasbourg rejected a bid by Chinese conglomerate Jingye Group to acquire the Hayange factory in northern France that belonged to British Steel. The UK-based steelmaker avoided bankruptcy after being bought by Jingye last year. Hayange was not part of the transaction. The court decision awarded UK-based industrial firm Liberty House permission to acquire the site, deemed as strategically important by the French government. France's finance ministry is expected to approve the deal. The current context makes the decision particularly notable. As Europe seeks to recover from the COVID-19 pandemic, governments have sought to protect national assets from takeovers by non-EU entities. This trend of targeted protectionism will likely continue to accelerate across the EU. The case of Hayage makes this clear. Under current circumstances, there is little political appetite to approve acquisitions that could leave non-EU companies in control of assets of national importance. Heightened scrutiny on foreign investments will complicate plans for companies seeking to attract capital investment from non-EU investors.
- The London-based European Bank for Reconstruction and Development (EBRD) reported on 29 July that several of its Twitter accounts were hacked. Companies frequently using social media for communications campaigns should anticipate the potential impact a hack may have on operations. Precautionary actions should be taken, including regularly changing passwords and instructing relevant staff to exercise heightened caution, to mitigate the elevated cybersecurity threat.
- On 30 July the EU imposed sanctions on several individuals and organisations believed to have been involved in a series of major cyberattacks. The measures include asset freezes and travel bans on members of Russian military intelligence, two Chinese firms, including Haitai Technology Development, and Chosun Expo, a North Korean export firm.
- The Financial Times reported on 28 July that Anglo-Australian mining group Rio Tinto was in discussion with the Serious Fraud Office (SFO) to obtain a deferred prosecution agreement over suspected bribery committed when securing a major iron ore contract in Guinea. Neither Rio Tinto nor the SFO have confirmed the negotiations but this re-enforces the need for clients to ensure that their anti-bribery measures are robust and will stand up to scrutiny.
- Iraq's crude oil exports have increased in July, in breach of an OPEC agreement, in an effort to stabilise its economy. This is likely to escalate tensions with other OPEC members, particularly Russia, with the probability of global oil price volatility in 2021.

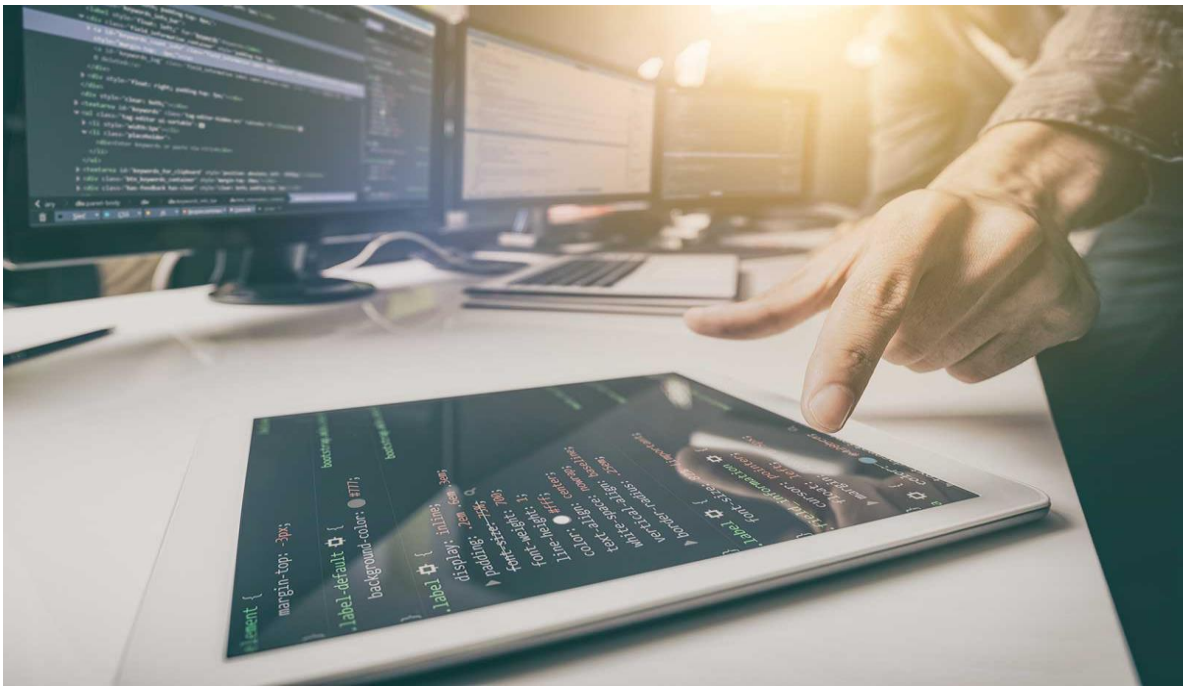
- Rural crime rose in every region and nation in the UK as criminal gangs targeted expensive tractors, quad bikes and large numbers of livestock, according to a report published this week by insurer NFU Mutual. Theft of high-value GPS equipment is on thieves' shopping list to satisfy a growing overseas demand.
- An INTERPOL assessment of the impact of Covid-19 on cybercrime has shown a significant recent target shift from individuals and small businesses to major corporations, governments and critical infrastructure.
- The number of struggling London businesses has risen by 4% since quarter one of 2020 with135,760 of the capital's companies now in significant financial distress The total number of struggling businesses in the UK exceeds 527,000, a rise of 3%, with, as might be expected, the hospitality sector suffering the most.
- The forecasted hot weather for the south of the UK for the coming weekend is likely to see a number of dispersal orders being issued in some major cities, with expected large gatherings of people at numerous licensed premises.
- Russia's economic development minister, Maxim Reshetnikov, has warned that EU plans to introduce a carbon border adjustment mechanism (referred to as a carbon border tax) by 2023 will violate World Trade Organisation (WTO) rules. The carbon border tool, which is still being developed, would see additional levies being applied on imported goods manufactured unsustainably. The tax will reflect the amount of carbon emissions generated during the production of imported goods. This is aimed at encouraging non-EU exporters to prioritise environmental protection as well as bolster post-COVID production within the EU. UK exporters to Europe should include the introduction of this tool into their market plans.
- U.S. Defence Secretary Mark Esper has expressed concerns about Beijing's "destabilizing" activity near Taiwan and the South China Sea in a call with Chinese Defence Minister Wei Fenghe, the Pentagon said on Thursday. This is the first time the two are believed to have spoken since March and indicates increasing concern in Washington. The call came as U.S.-China relations have rapidly deteriorated this year over a range of issues, including Beijing's handling of the coronavirus, telecommunications equipment maker Huawei, China's territorial claims in the South China Sea and its clamp-down on Hong Kong. Clients with business interests in China or with Chinese suppliers should continue to monitor the situation and have contingency plans in place if matters deteriorate.
- Finally, a cautionary tale for clients who record Zoom meetings: You may have read that the person responsible for the recent Twitter hack was a 17-year old from the UK who lives in the US. His court hearing this week was conducted by Zoom video link due to the pandemic. It was interrupted numerous times by outsiders because the judge didn't know how to enable settings to prevent that; the final interruption was by someone streaming pornography. Many reporters were recording the proceedings – if that had been child pornography then they would all immediately have been in possession of indecent images of a child and at risk of 5 years in prison. Make sure that you know how to secure the systems that you're using!

Financial crime

- Reports of furlough fraud to HMRC have increased by 53% compared to June. On 22nd July 2020HMRC were given new powers to investigate furlough claims, with both civil and criminal tools being made available. Employers should undertake audits of their use of the Coronavirus Job Retention Scheme to ensure compliance and to notify HMRC of any abuses of the scheme.
- Similarly, the 'Eat out to Help out' scheme, where the government will meet half the cost of a meal up to a value of £10, is open to abuse with alcohol being recorded as food or 'ghost' customers being served with non-existent food. Again, clients should ensure that the use of the scheme is being properly audited with transgressions by staff being quickly addressed.
- On Wednesday Europol warned of increasing focus of organized crime groups in sports corruption. Criminals involved in the sector have quickly adapted to the Coronavirus crisis to exploit new opportunities despite the virus' disruptive impact. "Criminal business continued and it is anticipated that the long-term impact of the COVID-19 pandemic may be particularly significant in the area of organized crime, including money laundering and corruption," Europol said. With only a limited number of competitions offered on betting markets because of the pandemic, criminals turned their focus to lower-tier games, youth games and friendly matches. Companies that sponsor teams operating in the lower tiers should ensure that sufficient action is being taken by the team, to prevent and deter such activity.
- The former owner of PrivatBank, a Ukranian-based financial institution, has been accused of laundering billions of pounds through a complex array of companies based in the US and western Europe. The companies were involved in steel plants, technology manufacturing, office buildings and other real estate. Ihor Kolominsky has ties to the prime minister of Ukraine and played a role in the events that led to the impeachment of President Trump last year. This illustrates the need for through due diligence to identify the final beneficial owner of any company that clients are contemplating doing business with.

Financial crime: continued

- The sanction by the US Treasury of Adnan al-Rawi for financing ISIS has demonstrated the lax regulatory environment operating in Turkey, as far as financial crime is concerned. Turkey has been the only NATO state to be targeted by US sanctions for breaches of anti-Terrorist Funding financial controls and clients should exercise additional caution when dealing with entities based in Turkey or where funds have passed through that jurisdiction.
- Researchers have discovered another coronavirus-related lure being used in a phishing campaign promising the recipient a government-funded tax cut. The email claims to come from the UK 'Government Digital Service Team', and offers a tax rebate of £385.50. This rebate will supposedly be transferred directly to the recipient's credit or debit card. The scam is designed to steal recipients' personal and financial information.
- With the increase of businesses becoming insolvent and premises becoming empty, the City of London Police has warned that fraudsters will be targeting these to use as fronts for new fraudulent enterprises or as 'drop-points' for goods ordered using stolen payment cards.
- Opportunities for fraudsters have arisen as part of the 'Track and Trace' system, where businesses are collecting customer contact details. Clients should ensure that processes are in place to ensure that these details remain secure.
- The National Cyber Security Centre has published advice on cyber insurance and urges businesses to consider seven key questions when considering cover.
- This week hundreds of UK consumers have been targeted with a text message scam offering a free TV license for over 75s. The was identified by Parliament Street Researchers who describe it as, "fraud designed to steal the personal financial data of victims". Victims are asked to enter various pieces of personal information including name, date of birth, home address and banking details, which are then stolen



Cyber threats

- The US government anticipates foreign interference in the 2020 election and has offered a $10million reward for information leading to cybercriminals aiming to influence the outcome. The U.S. Department of State's Rewards for Justice (RFJ) program, overseen by the Diplomatic Security Service, will pay for information that can identify or locate someone working with or for a foreign government "for the purpose of interfering with U.S. elections through certain illegal cyber activities," according to a release posted on the department's website.

- Researchers are warning that a new class of botnets could be marshalled and used to manipulate energy markets via armies of power-hungry connected devices such as air conditioners, heaters, dryers and digital thermostats. A coordinated attack could cause an energy stock index to predictably go up or down – creating an opportunity for a rogue operator to cash in. Researchers with the Georgia Institute of Technology laid out the scenario warning that high-wattage 'Internet of Things' devices are vulnerable to takeover by threat actors who can hijack them in the same way that millions of CCTV cameras, DVRs and home routers are recruited into botnet armies to conduct distributed denial-of-service attacks and mine cryptocurrency.

- A new vulnerability, dubbed BootHole, has recently been discovered in the GRUB2 bootloader. It impacts most Linux systems worldwide. Successful exploitation can lead to arbitrary code execution during the boot process, even when Secure Boot is enabled. This issue impacts every system using Secure Boot because almost all signed versions of GRUB2 are vulnerable. This means that most laptops, desktops, servers, and workstations are affected, alongside network appliances and other special-purpose equipment used in industrial, healthcare, financial and other industries.

- The US Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) released a joint security alert about the QSnatch malware, which has been infecting network-attached storage (NAS) devices from Taiwanese device maker QNAP. QSnatch attacks have intensified over the last year: the number of reported infections grew from 7,000 devices in October 2019 to more than 62,000 in June 2020. CISA and NCSC are urging companies to patch QNAP NAS devices to the most recent update available.

Cyber threats: continued

- Attacks continue from the Emotet botnet, one of the most potent threats of 2020. Early in the week, a wave of spam emails targeted English-, Italian-, and Polish-speaking users. In Italy, the domain belonging to the Ministry of Cultural Heritage was compromised and leveraged to distribute Emotet for over four days. Japanese and South Korean users were targeted with English language lures towards the middle of the week. The botnet's TTPs were identified as having changed once again. Cofense Labs identified spam emails containing Emotet using not only stolen email bodies but also stolen attachments, making them more authentic and convincing.
- As a result of misconfigurations in their infrastructure, source code from the repositories of more than 50 companies across various sectors has been made publicly available. These include companies operating in the fields of technology, finance, retail, food, e-commerce, and manufacturing, with some large businesses such as Microsoft, Adobe, Lenovo, AMD, Qualcomm, Motorola, GE Appliances, Nintendo and Disney being involved. The repositories were collected from various sources, and some contain confidential or proprietary information. While these exposures appear severe at first, the researcher actively complies with takedown requests and has already removed the repositories for Lenovo, Daimler AG, and Mercedes-Benz..
- A misconfigured cloud server at global cosmetics brand Avon has exposed 19 million records, including personal information and technical logs. The Elasticsearch database was found on an Azure server with no password protection or encryption – meaning it could be found by anyone in possession of the server's IP address. The database was exposed for nine days before being discovered on 12 June. It contains personally identifiable information about customers and, it is believed, also employees.
- Researchers have reported four distinct malware families being used by North Korean APT Lazarus to target Apple's macOS platform. These included previously observed malware such as the DaclsRAT which is believed to be a part of the recently disclosed MATA framework, also used by Lazarus. Sentinel One claims that all of these samples have appeared in the last eight to ten weeks, which shows that Lazarus is still highly active.
- In more Lazarus-related news, the group was observed targeting the US aerospace and defence sector in a campaign dubbed Operation North Star. These attacks used common spear-phishing emails posing as a potential job opportunity. McAfee was not able to retrieve a copy of the emails, so the companies that were targeted in these attacks are unknown. These lures were used to install malware through malicious DLLs onto a target's device, with the attacks specifically focused on cyber-espionage and intelligence-gathering efforts. This campaign bears a striking resemblance to Operation Interception, also conducted by Lazarus, which targeted European and Middle Eastern aerospace and military companies. Both campaigns use similar bogus job offer lures.
- A new Android SMS worm is circulating disguised as TikTok Pro. Once a user installs the app, it sends an SMS to all the contacts on the device with a link to the malicious app.
- Multiple 0day vulnerabilities for Tor have been disclosed by well-known computer forensics researcher, Dr Neal Krawetz. Dr Krawetz claims he first discovered some of these bugs as far back as 2012 and that, despite having reported them to the Tor Project, they all remain unpatched. These vulnerabilities potentially enable the tracking and detection of any connection to Tor nodes. The Tor Project has not yet commented on the disclosure of these vulnerabilities.

- Security researchers have discovered a way to use the Microsoft Teams Updater to download malware, bypassing a patch released earlier this year and flying under security teams' radar. This method would let an attacker use Microsoft Teams Update[.]exe as a living-off-the-land binary (LOLbin). Living off the land is an especially dangerous technique as it uses known, common tools to download and execute malware from a location of the attackers' choosing.
- This week saw the British Dental Association becoming the victim of a cyber attack, resulting in its website being taken offline. It is not known what other systems have been affected or weather data has been deleted or stolen.
- Misconfigured storage services in 93% of cloud deployments have contributed to more than 200 breaches over the past two years, exposing more than 30 billion records, according to a report from cloud-security firm Accurics, which predicted that cloud breaches are likely to increase in both velocity and scale. The researchers found that 91 percent of the cloud deployments analysed had at least one major exposure that left a security group wide open, while in 50% unprotected credentials were stored in container configuration files, significant because 84 percent of organizations use containers.
- Analysis of the WastedLocker attack on Garmin has revealed the sophisticated nature of the malware. Researchers from Sophos have identified that it interacts with Windows API functions from within the memory itself, where it's harder to be detected by security tools based on behavioural analysis. WastedLocker uses a trick to make it harder for behaviour based anti-ransomware solutions to keep track of what is going on, by using memory-mapped I/O to encrypt a file. This technique allows the ransomware to transparently encrypt cached documents in memory, without causing additional disk I/O, which can shield it from behaviour-monitoring software.

Technical matters

- Unit 42 has issued a security advisory concerning a recently disclosed vulnerability in Kubernetes. Successful exploitation can lead to unauthenticated attackers gaining complete control over the cluster.
- Tencent has issued a security advisory over an important update for the Elastic Stack. Successful exploitation of unpatched systems can lead to stored XSS, information disclosure, and denial of service via CPU exhaustion.
- A critical vulnerability has been discovered in the wpDiscuz WordPress plugin installed on over 80,000 WordPress sites. This flaw can allow an attacker to remotely execute code after uploading arbitrary files to servers hosting vulnerable sites.
- Cisco has released security updates to patch three critical vulnerabilities affecting Cisco Data Center Network Manager (DCNM) and multiple Cisco SD-WAN software Updates were also released for eight high and medium severity flaws.
- Multiple vulnerabilities have been disclosed in Mitsubishi, Philips, and Inductive Automation ICS products, warns US CISA. Successful exploitation can lead to denial of service, arbitrary code execution, unauthorised access, information disclosure, and provide misleading information.

Start the conversation

Jim Gee
Partner and Head of Forensic Services
+44 (0)20 7842 7239
jim.gee@crowe.co.uk

About us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

www.crowe.co.uk

@CroweUK