Section 1: **Executive Summary**

Key Judgements

To date, no observable destructive cyber incidents have been achieved by terrorist groups and monitored chatter does not indicate the behaviour of an organisation marshalling their resources around cyber physical destruction. The past six months have seen the field complicated and crowded by new actors and ambitions, however. Terrorist groups have adopted simplistic nation state techniques in plotting cyber attacks and gaining access to systems but have been thus far unsuccessful in carrying out attacks which aspire to be anything more disruptive. The intensified geopolitical situation in the Middle East, however, hints that a future collaboration between terrorist groups and nation states may suddenly accelerate cyber capabilities for an initially limited number of cells. Continued monitoring of this situation is a requirement.

Additional Key Judgements will be derived from information throughout the report and impart a high-level summary of the main conclusions of each section. These judgements should be viewed as a conclusion, estimate or trend to the analysis rather than a pure data source. Key Judgements will be presented in bullet form.

Analysis & Substantiation

Terrorist Related Cyber Incidents and Terrorist Chatter

Proscribed terrorist groups and organisations continue not to significantly increase their capabilities in the cyber field, although a small number of more ambitious cyber incidents have occurred. These incidents demonstrate terrorist entities copying or adopting nation state methodologies rather than establishing novel or creative schemes of attack. In each of the cases described, a high degree of success was not achieved, demonstrating that, for the time being, reaching success in the cyber realm still exceeds terrorist groups' grasp. Overall, however, events in the past six months show an understanding of what can be achieved using cyber means, if not a meaningful development of the engineering and programming skills needed or how plots can be carried out once access is secure.

There persists some potential for a convergence of interests between terrorist, non-state, and state groups, particularly in the Middle East. Such a series of events would like lead to a distribution of intelligence and tools between groups which would accelerate related terrorist groups up the cyber 'value chain'.

For the most part, terrorists continue to focus on real-world attacks and damage and does not advocate for the development of cyber capabilities. Chatter in this regard is becoming limited due to crackdowns on apps and websites. Indeed, the online activity so far associated with known terrorist threat actors – use of social media, website defacement, release of propaganda materials – is in decline.

Non-terrorist Activity Relating to Disruptive or Destructive Events

The major developments in nation state activity and abilities continue to be informed by the major cyber events of 2017 – the use of the EternalBlue exploit and discovery of the TRITON malware at Petro Rabigh. This two-year reporting lag in the changing landscape demonstrates how deep the roots of successful attacks may reach and the speed at which anything can be said for certain in sophisticated cyber attacks. Indeed, complicated political and somewhat irresponsible reporting has complicated the view of what cyber attacks have occurred and who is irresponsible – this issue is likely to exacerbate as incidents continue. The likely strategic decision by some nation state cyber groups to adopt the toolsets used by cyber criminals further complicates questions of attribution and forensic timelines, contributing greater risk to any unsecured declarations by media or government.

Although EternalBlue and the related exploits published by ShadowBreakers in 2016 have been patched by Microsoft, nation states have been observed historically using latent vulnerabilities to access industrial control

systems. The use of this exploit by nation states contributes to the understanding of how much foreign presence may exist in ICS globally.

Overall, the past six months has seen nation states dedicate themselves substantially to explicit cyber strategies, not limited to espionage, surveillance, and pre-emptive attack. This was most notably seen in the restructuring the US cyber strategy to 'Defend Forward', striking against adversarial states and teams before more destructive actions can be taken.

Miscellaneous – Cyber crime, penetration testing and vulnerabilities

Cyber crime continues to take the major part of publicity for major events and step changes. The trend in holding whole companies and cities to ransom with tenacious strains of ransomware has driven significant losses, if not actual gains. Among these incidents is shutting down of the city of Baltimore by an unknown exploit, resulting in $18 million in damages, and the LockerGoga infection of Norsk Hydro, which slowed production at the company's aluminium plants for weeks for a loss of more than $46 million.

Cryptojacking has emerged as a damaging competitor to ransomware, allowing actors to 'poison' networks and siphon off processing power and energy for mining cryptocurrencies, slowing systems and machinery for weeks before detection. Incidents of cryptojacking in the past six months have badly affected industrial facilities production rates, raising large funds for those responsible for the infection. In a notable incident, the commodification of cyber access demonstrated vulnerability in China's rail network, presenting a real risk to civilians.

Additionally, the release of patches for two more zero-days found in Microsoft Windows systems raises concerns about future attacks. Given the delay on discovery of attacks demonstrated by reporting in nation state cyber activity, and the lapse in patching for many computers and industrial systems, these vulnerabilities may provide a foothold for future, highly disruptive and costly cyber attacks.

Section 2: **Methodology**

Collection

Data collection is based on open source, publicly available information, including: media sources, cyber security and threat intelligence companies, government and intergovernmental agencies, social media, subject matter experts, academics and threat actor behaviour, e.g. statements and postings, defacements, propaganda, dissemination of tactics, techniques and procedures (TTPs) and attacks.

Under CCRS and Pool Re definitions, a cyber incident constitutes a threat when it is *an act of politically-motivated violence involving physical damage or personal injury caused by a remote digital interference with technology systems.*

There have been few demonstrated or confirmed examples of physically destructive cyber attacks and no known incidents carried out by proscribed terrorist organisations. Therefore, incidents must meet one of three criteria in order to warrant inclusion in the cyber threat assessment:

A) Incidents must have enabled or have resulted in cyber physical damage, disruption or have nearly done so (i.e.: near miss);

B) Incidents must demonstrate capability of possibly enabling or causing the above (A) in the future;

C) Incidents must indicate or strongly suggest increasing capability for both cyber and physical incidents, e.g. propaganda dissemination, material support, social media communications and direction, defacements, the acquiring of toolsets and marked improvement in education, skillset and TTPs.

*Further information on collection and processing can be found in the CCRS & Pool Re Database Codebook.

Thematic Sections

Thematic sections will be grouped according to Pool Re Threat Actor Classifications. Sub-grouping within the Thematic Sections will be driven by Pool Re Intelligence Requirements. As such, Thematic sections will be non-linear.

Thematic Sections will contain:

- Key Statement
- The Tipping Point
- Key Judgements
- Analysis & Substantiation
    - Threat Actor + Classification
    - Incident + Intent + Capability

Section 3: **Terrorist Related Cyber Incidents**

Key Statement

There are minimal indicators suggesting that online extremists are attempting to increase capabilities and move up the cyber 'value chain' by mimicking nation state vulnerabilities, exploits and TTPs. There are indications that online defacements, the spreading of propaganda, and other disruptive behaviour are all on a downward trend. The most high-profile instances have failed in their objectives.

The Tipping Point

Further refinement of nation state tradecraft can lead to more sophisticated attacks. If combined with exploits like EternalBlue then the impacts of attacks could be wide-ranging. Increased convergence with nation state interests, especially geopolitically, can increase the potency and scale of cyber attacks, for example: a convergence between Iran, Hezbollah and Hamas.

Key Judgements

- Online extremists are slowly building the capabilities to perpetrate sophisticated attacks. Most activity involves taking incremental steps up the cyber 'value chain.' For example:
    - Adopting nation state TTPs such as exploiting vulnerabilities in DNS and vulnerability scanning for dual attacks (Ransomware + Defacements) as seen in #OpJerusalem. Using public sources to host infrastructure to ensure the longevity of operations and obfuscate attribution, as seen in recent Gaza Cybergang campaigns.
    - Engaging in espionage, which would indicate prioritising long-term strategic goals over cheap headlines such as defacements, as seen in recent Gaza Cybergang campaigns.
- Online extremists are having difficulty achieving success outside of their traditional areas of expertise – defacements and other unsophisticated attacks. For example, a recent Hamas attack which attempted to hack into a Eurovision web broadcast and disseminate a propaganda video lasted only minutes.
- The recent hijacking of dormant Twitter accounts by Islamic State affiliates is relatively unsophisticated and the methodology is widely known. Hacking Twitter accounts to spread propaganda actually suggests disfunction in IS cyber ranks, as the need to hijack Twitter accounts indicates they have lost the capability of generating their own Twitter accounts and maintaining them long-term.

Analysis

Cyber 'Value Chain'

Threat Actor: (2) Self-affiliated terrorist: actors operating independently of proscribed terrorist groups but claiming to act on their behalf

Intelligence Requirements: (4) Indications of terrorist groups moving up the cyber 'value chain', even if it does not involve destructive attack (e.g. going from mere web site defacement to starting to use ransomware);

On 4 March, Bleeping Computer reported that participants of #OpJerusalem engaged in a defacement campaign that attempted to distribute JCry ransomware. When the ransomware detected Windows systems, it distributed a fraudulent Adobe update designed to distribute the ransomware. If the systems detected were not Windows, a defacement occurred. Due to errors in the code, the ransomware campaign failed and the attack instead reverted to default distributions of defacements.

Several aspects of the attack can be nominally linked to other threat actor TTPs. For instance, Bleeping Computer notes that 'the attackers modified the DNS record for a popular web accessibility plugin.' Exploiting vulnerabilities within Domain Name System (DNS) is becoming increasingly popular. In the Middle East, Iran has been known to be particularly proficient in launching DNS attacks. The Centre most recently reported on one such Iranian campaign, DNSpionage, in RFI: Threat Assessment Hamas. Interestingly, DNSpionage was recently part of a Telegram leak in which several Iranian exploits, vulnerabilities, toolkits and TTPs were disclosed. The veracity of this leak is still being debated. Known as MuddyWater, the leakers are thought to be hacktivists aligned with Iran's Green Movement. On 17 April a report by Cisco Talos Intelligence divulged that they have observed another Iranian DNS campaign, dubbed Sea Turtle. Cisco Talos Intelligence believes that Sea Turtle and DNSpionage contain similarities and overlap but are operationally distinct.

The potential for a convergence of extremist and state interests in cyber appears to be the strongest in the Middle East. The Centre's RFIs on Hezbollah and Hamas have gone into detail as to how extremist and state cyber operations, infrastructure, and interests align. On 7 April, one month prior to the JCry attack, Western activists doxed Israeli Internet infrastructure and government employee details on a popular paste site during #OpIsrael. Three weeks prior to #OpIsrael, Israeli news sources indicated that Benny Gantz, a candidate for Prime Minister and former IDF chief of staff, had been the victim of a mobile malware attack attributed to Iran.

Threat Actor: (2) Self-affiliated terrorist: actors operating independently of proscribed terrorist groups but claiming to act on their behalf

Intelligence Requirements: (4) Indications of terrorist groups moving up the cyber 'value chain', even if it does not involve destructive attack (e.g. going from mere web site defacement to starting to use ransomware);

On 10 April, Kaspersky reported on several Gaza Cybergang operations termed 'SneakyPastes'. Kaspersky assesses that the campaigns were designed to install remote access trojans (RATs) on targeted systems, likely for purposes of espionage. The campaigns widely targeted systems in the Middle East, most prominently in the Palestinian Territories, Jordan, Israel and Lebanon.

Kaspersky analysis indicates that SneakyPastes initially used phishing emails to gain access to systems. These emails contained malicious links that hosted the first stages of the malware. Kaspersky assesses that several public sites, such as pastebin.com, were used to host the phishing emails and malware and acted as command and control infrastructure throughout the operations. Interestingly, one of the sites that Kaspersky identifies is dev-point[.]com, an Arabic language cyber forum in which the Centre reported chatter regarding EternalBlue in Threat Assessment Q3-Q4 2017. The targeting of this incident remains consistent with previous espionage campaigns in the region, most recently in RFI: Hamas and Hezbollah Threat Assessments.

General Use

Threat Actor: (1) Proscribed terrorist organisation: actors affiliated with a political organisation proscribed as a terrorist group by one or more NATO or EU states

Intelligence Requirements: (3) Information on terrorist use of cyber in general (e.g. is there an increase in web site defacements, or a reduction);

On 15 May, *Times of Israel* reported that a Pro-Palestinian group hacked the Israeli web broadcast of the Eurovision song contest. The hackers replaced the broadcast with a two-minute propaganda video in which they stated, 'Israel is not safe.' The hack lasted only minutes before being thwarted. The *Jerusalem Post* claims that Hamas was responsible for the attack. Ten days earlier, on 5 May, the Israeli Defence Forces tweeted that they had targeted Hamas cyber HQ in the Gaza Strip with a missile strike in real-time. It is unclear what affect the strike has had on Hamas cyber operations. The Eurovision hack lasting only minutes could mean that Hamas cyber capabilities were significantly degraded. On the other hand, the hack occurring at all could indicate that the strike had only had a limited effect on resources.

Threat Actor: (2) Self-affiliated terrorist: actors operating independently of proscribed terrorist groups but claiming to act on their behalf

Intelligence Requirements: (3) Information on terrorist use of cyber in general (e.g. is there an increase in web site defacements, or a reduction);

On 2 January, Engadget and TechCrunch reported that Islamic State supporters were hijacking dormant Twitter accounts in order to spread propaganda and increase recruitment. The tactic exploits flaws in Twitter's old account generation in which email confirmations were not requires to register. For years, several methods for hijacking Twitter accounts have been disseminated on Google. Currently a Google search of 'how to hack old Twitter account' returns 136,000,000 results. IS supporters were able to guess basic credentials based on Twitter handles and take over the accounts through the reuse of dormant email handles.

IS willingness to observe and adopt common cyber practices disseminated on the Internet makes extremist cyber operations resilient. The hijacking of dormant accounts that have already been verified by social media represents a way in which IS can maintain their presence on social media and circumvent social media rules and government legislation.

Section 4: **Terrorist Chatter Relating to the Internet**

Key Statement

Online extremist chatter is still preoccupied with terrorism in the physical world and dedicates limited space to discussion of cyber.

The Tipping Point

Increased dedicated advocacy for cyber. Increased dissemination of hard cyber skills. The spread of sophisticated tools, exploits, and vulnerabilities.

Key Judgements

- Propaganda dissemination has dropped significantly, especially on the most visible parts of the Internet.
- The use of Telegram to distribute propaganda is operationally secure but not far-reaching, the exact opposite of the purpose of propaganda.
    - Experimenting with alternative and lesser-known social media platforms such as Mastodon would likely only exacerbate online extremists reachability problems.

- Periodicals advocate for general cyber skills in a limited fashion, often dedicating only minimal space for cyber talk.
    - A recent issue of Youth of the Caliphate mentions sources for zero-day exploits.

Analysis

Threat Actor: (2) Self-affiliated terrorist: actors operating independently of proscribed terrorist groups but claiming to act on their behalf

Intelligence Requirements: (5) Evidence of terrorists, and in particular leadership figures, advocating or endorsing the use of cyber (or the reverse);

On 13 May, IFI monitoring reported on the eighth issue of Youth of the Caliphate, an Islamic State affiliate periodical. The periodical was originally distributed on Telegram by YOTCBOT3. A limited section of the issue is dedicated to English, although those sections do not cover cyber. However, pg.17 introduces several passages dedicated to cyber in Arabic. Both Telegram and Twitter logos are pictured, along with generic symbols for malware, email, virus and surveillance. Two additional Telegram contacts, @Bankalansar and @Numbersbank, are given. English words that appear include Hacking Team, Celebrite, Zerodium and Zero Day. These keywords strongly suggest desire to learn or acquire exploits and vulnerabilities.

Due to English legislation and IS movement to Telegram, the collection of primary sources, especially in English, has become increasingly difficult. Extremists are still disseminating the ideals of the Islamic State and online actors continue to aid in this process. For instance, on 12 March, Kim Ahn Vo was charged by US authorities with conspiring with other actors to pledge allegiance, recruit and spread propaganda on behalf of Islamic State cyber operations. Sources indicate that online extremists are experimenting with alternative social media accounts, such as Mastodon, an open-source social media platform.

Section 5: **Non-terrorist Activity Relating to Destructive or Disruptive Attacks**

Key Statement

Threat Actor: (7) State actor: agents of a nation state

There are indications that nation state cyber activity, especially that focused on disruptive or destructive intent, has increased. Threat actors have been observed deploying scalable exploits, such as EternalBlue. Threat actors have also increased their targeting of ICS/OT networks, especially against CNI.

The Tipping Point

Sustained and increased targeting of ICS/OT networks increases the chances of an accidental loss of control or miscalculation of adversary intentions, which may lead to a series of escalating cyber attacks if defenders strike back.

Key Judgements

- Nation states continue to support the development, acquisition, and deployment of scalable tools and exploits, especially for espionage. For example, both Chinese and Russian threat actors have been observed deploying versions of EternalBlue, the exploit used in both WannaCry and NotPetya in 2017.
    - The Chinese deployment of EternalBlue is thought to predate the ShadowBrokers leak of EternalBlue by one year. Chinese versions of EternalBlue also can exploit newer systems, widening the scale of potential attacks.
    - Russian use of EternalBlue overlaps with other threat actor use in the Middle East, like the previously reported Iranian Leafminer campaign.

  - Russia's deployment of EternalBlue on hijacked Iranian infrastructure helps support the Centre's assumptions about misattributed infrastructure from RFI: Threat Assessment Hezbollah.
  - Using hijacked infrastructure also raises interesting questions about Russia's deployment of EternalBlue and obfuscation: was the goal to deploy EternalBlue for a genuine espionage campaign or was EternalBlue used because other threat actors on the same infrastructure were using the same exploit? The use of the particular exploit may be intended to further complicate the attribution process.
  - There is debate over the effectiveness and reasoning behind nation state and cyber criminal use of EternalBlue. For example, journalists such as Nicole Perlroth, academics such as Thomas Rid, ex-agency employees such as Robert M. Lee and Jake Williams, and industry, are increasingly at odds over the scale and scope of the use of EternalBlue and the National Security Agency's culpability in its use by malicious groups. The continued reporting of EternalBlue's effectiveness undermines US intelligence agency operations, trustworthiness and political support. In effect, reporting on the use of EternalBlue has becoming an exercise in Russian active measures.
  - Threat intelligence companies like We Live Security's reporting metrics on the use of EternalBlue are poorly explained and often misinterpreted by journalists.
- Nation states have begun to articulate offensive cyber security postures through doctrine, strategy, leaks and demonstrations of capabilities. Examples of offensive security postures are numerous:
  - The best example is the US Department of Defense Cyber Strategy's line of effort 'Defend Forward,' as seen in reports of US offensive cyber operations against Russian electricity grids and the alleged US deployment of wipers against Iranian military infrastructure. Both stories were confirmed by leaks and are in keeping with Defend Forward strategy.
  - Offensive cyber security postures have led to an increase in the targeting of ICS/OT networks for likely future disruptive or destructive attacks. For example:
    - Both FireEye and Dragos note that the threat actor behind TRITON has been observed targeting an increasing number of ICS/OT facilities related to CNI. Neither FireEye nor Dragos believe that this targeting is consistent with espionage.
- Both Chinese and Russian threat actors are using the same off-the-shelf toolsets and exploits as cyber criminals, such as Mimikatz, RDP, PsExec and supply chain attacks. This overlap in tool usage complicates public analysis of cyber incidents and distorts previous assumptions about threat actor intentions, creating doubt about the motivation behind cyber incidents and who is responsible.
- Nation states have begun to use cyber attacks that cause real world destructive effects, even if those effects are not triggered digitally. For example:
  - Israel supposedly bombed and reported on the HQ of Hamas cyber operations in real time.
  - Russia has continuously used electronic warfare such as GPS spoofing to redirect air and sea traffic, which could easily lead to loss of life.

Analysis

Nation states and their proxies continue to develop and deploy disruptive and destructive cyber capabilities. In the first two quarters of 2019 nation states have been observed increasing their cyber espionage operations through use of tools such as EternalBlue and DoublePulsar; sustained attempts to establish footholds in critical national infrastructure (CNI) for future offensive operations; the use of electronic warfare such as GPS spoofing and; the kinetic targeting of malicious cyber operatives in real time.

EternalBlue

Threat Actor: (7) State actor: agents of a nation state. (6) State Proxy: non-governmental actors operating in support of a nation state's policy objectives

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 7 May, Symantec reported that a Chinese advanced persistent threat (APT) had utilised NSA/TAO exploits and tools one year before the ShadowBrokers leak. The group, known as Buckeye/APT3, allegedly used DoublePulsar, EternalRomance and EternalSynergy, presumably for cyber espionage. Symantec claims that the APT created 'a custom exploit tool (Trojan.Bemstour) to initially install DoublePulsar (Backdoor.DoublePulsar)' that takes advantage of two Windows zero-days, CVE-2017-0143 which was patched in March 2017 and CVE-2019-0703 which was patched in 2019. Symantec considers both vulnerabilities Trojans that have been used by a variety a Chinese APT campaigns. Both zero-days are designed to 'exploit [SMB] vulnerabilities via port 445,' which is consistent in other attacks using NSA/TAO exploits and tools, such as WannaCry and NotPetya. Symantec assesses that the exploits and tools were likely acquired through reverse engineering 'from artifacts captured in network traffic,' cyber espionage or a possible leak, due to differences between the Chinese and ShadowBrokers versions. A significant difference is that the Chinese version has the ability to target newer systems such as Windows 8.1 and Windows Server 2012 R2, which in theory should allow for a wider scale of targeting (more systems available to compromise). Symantec further substantiates their assessment by noting that the Chinese version lacked the use of the FuzzBunch framework, which is commonly used to manage NSA/TAO tools. Symantec believes that FuzzBunch's absence means that the APT was unable to gain full access to NSA/TAO tools. The New York Times links Buckeye/APT3 to three individuals of Chinese origin indicted by the United States in September 2017. The individuals worked for Boyusec, a Chinese cyber security firm. Recorded Future has alleged that Boyusec is a contractor for the Chinese Ministry of State Security (MSS) and is partners with Huawei and other Chinese technology firms.

Threat Actor: (7) State actor: agents of a nation state. (6) State Proxy: non-governmental actors operating in support of a nation state's policy objectives

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 20 June, Symantec reported a new espionage campaign that they attribute to the Russian APT Waterbug/Turla. While the attacks do not demonstrate direct destructive or disruptive intent in this case, certain technical aspects of the campaigns are relevant to previous and future assessments. Symantec notes that the campaign had three distinct phases, some of which utilised what Symantec terms a custom tool combining features of EternalBlue, EternalRomance, DoublePulsar and SMBTouch, all leaked NSA/TAO tools. Symantec also notes that the campaigns used PsExec for lateral movement and a heavily modified version of Mimikatz for credential harvesting. Symantec believes that in at least one phase the campaign hijacked Iranian OilRig/APT34/Crambus command and control infrastructure with Mimikatz in order to spread their malware. The hijacking of other APT infrastructure confirms assumptions made in RFI: Threat Assessment Hezbollah, in which Lebanese and Russian infrastructure overlapped over multiple years, campaigns and threat actors (Dark Caracal, Let's Get Fancy, Strontium). In addition, previous reporting on the Iranian Leafminer campaign saw the use of EternalBlue, FuzzBunch and Mimikatz. Although the campaigns are not connected, there seems to be at least nominal overlap of activities between 2017-2018. The Waterbug campaign also contains technical indicators related to CVE-2019-0604 Microsoft SharePoint Remote Code Execution Vulnerability, a vulnerability disclosed in February 2019. Likewise, some technical indicators (namely, the targeting of infrastructure) overlap with previous Turla Campaigns.

Sources such as ESET's We Live Security have alleged that attacks using EternalBlue have reached 'historical peaks.' ESET uses its own telemetry, Shodan scans and client reporting to support their assessment. Reporters such as the New York Times' Nicole Perlroth have cited the We Live Security blog as strong evidence for the increasing use of EternalBlue, especially in ransomware attacks against communities. We Live Security's assessment admits that internal security team use of EternalBlue in penetration testing could account for a large amount of their detections. On the other hand, We Live Security fails to acknowledge the difference between APT packaging of EternalBlue with other cyber espionage exploits vs. actual use, nor the often limited scale of espionage operations. We Live Security also does not make clear if they are

detecting true EternalBlue use or attempted breaches through port 445 and SMB, which could lead to false positives from other similar exploits. Likewise, the Shodan scans are unclear as they do not distinguish between personal or business systems. If several thousand systems detected are for personal use, EternalBlue is not as scalable. We Live Security detects 22,173 systems vulnerable to EternalBlue in the UK, less than half of the systems Maersk had to rebuild after NotPetya.

TRITON/TRISIS/XENOTIME

Threat Actor: (7) State actor: agents of a nation state. (6) State Proxy: non-governmental actors operating in support of a nation state's policy objectives

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 7 March Blake Sobczak of E&E News named Petro Rabigh, a Saudi-based chemical and refining facility, as the victim of the 2017 TRITON attack. Sobczak reported that Petro Rabigh first called Schneider Electric to respond to a 'malfunctioning Triconex unit' in June 2017. On 4 August, outside incident responders were called to the facility to investigate 'unusual communications' between information and operational technology within the facility. Normally air-gapped, the incident responders found malicious files (TRITON), that threat actors managed to deliver to OT after 'pivot[ing]' from information technology networks to operational technology due to a 'poorly configured firewall.' Sobczak claims that 'at least six Triconex controllers were compromised by the malware.' Researchers have stated that Petro Rabigh's information and operational technology networks 'were riddled with other [unspecified] malware.' Sobczak's reporting also aligns with FireEye's original assessment of threat actor intent of gaining a foothold, maintaining persistence and attacking sometime in the future when strategically required, inferring that the triggering of the safety systems was likely an accident. Researchers ruled out an insider threat after the discovery of the TRITON files and analysis of network activity. The threat actors used a number of evasive tactics to obfuscate their activities once discovered, including the deletion of files, the changing of passwords and phone numbers and implementation of two-factor authentication to slow down response times. They also rerouted phone traffic to threat actor controlled infrastructure, allowing them to further harvest credentials. The APT's obfuscating behaviour is consistent with information given to the Centre from sources (incident responders) with first-hand knowledge of TRITON's reaction to being discovered.

On 10 April, FireEye disclosed that they had observed the TRITON framework deployed in at least one other facility. The disclosure focuses on technical details and threat actor intent. FireEye believes that the TRITON threat actor's long-term goals are to gain access to IT networks and then pivot to operational technology (OT) in order to maintain a persistent presence in target facility networks. Long-term persistence infers likely intent for disruptive or destructive attacks, as FireEye has not observed common espionage activity like data exfiltration, keylogging or screenshot grabbing. Interestingly, the TRITON threat actor uses a number of customised open source tools such as the credential harvester Mimikatz. The TRITON threat actor also heavily relies upon remote desktop protocol (RDP) and PsExec for lateral movement, which the Centre has reported as being increasingly used for lateral movement by cyber criminals, especially in the case of ransomware, such as RobbinHood and Ryuk. The FireEye blog was poorly written and FireEye conflated their 14 December 2017 incident with their 10 April 2019 incident. Evidence of the confusion can be found in this Vice article, which later had to retract parts of their analysis. A later tweet by FireEye's Steve Miller confirmed that FireEye did not observe TRITON malware deployed in the second incident, rather they observed similar TTPs.

On 14 June, Dragos reported that they have observed increased activity from the TRITON threat actor, which they term XENOTIME. Dragos characterises increased activity as 'significant external scanning, network enumeration, open source research…[and] attempts at external access.' Dragos does not believe that XENOTIME has breached operational technology or has deployed TRITON malware at the time of reporting.

Dragos has observed XENOTIME expanding their scope, specifically highlighting repeated targeting of North American, European and Asia-Pacific electric utilities, in addition to XENOTIME's original specialisation in the oil and gas sector. Dragos also notes that multiple ICS vendors have been subject to XENOTIME intrusions, which Dragos believes could lead to future supply chain attacks, such as the M.E.Doc supply chain attack witnessed in NotPetya. Dragos believes that XENOTIME is seeking to attain the prerequisites for future ICS/OT intrusions, which in turn can lead to disruptive or destructive incidents. Dragos stresses that XENOTIME's targeting is now threatening all ICS/OT environments, rather than a specifically targeted industry like oil and gas.

Offensive Cyber Operations

Threat Actor: (7) State actor: agents of a nation state.

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 15 June, David E. Sanger and Nicole Perlroth of the *New York Times* reported that the United States has increased offensive computer network attacks (CNA) against Russian interests, including Russian electricity grids. Sanger and Perlroth claim that the US has aggressively placed 'implants – software code that can be used for…attack – inside the Russian grid.' Quotes from several US officials suggest that the CNA operation has a variety of motivations, from signalling US intent and capabilities to Russian policymakers, to gaining footholds in Russian networks to maintain a 'persistent presence,' presumably in order to respond in kind to any future attacks from Russia. Sanger and Perlroth believe that the operations were carried out following the release a recent military authorisation bill. However, the language within the military authorisation bill itself is in close keeping with the high-level language of Defend Forward, an offensive cyber posture which appeared in the US Department of Defence's 2018 Cyber Strategy. The strategy defines Defend Forward as a plan 'to disrupt, or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.' Defend Forward was first reported by the Centre as a possible point in escalation of nation state cyber operations that could potentially turn destructive in Q3-Q4 2018.

The accuracy of the *New York Times* cyber reporting has been questioned in the past, most recently during the Baltimore ransomware incident and the Department of Defense has claimed that the story is inaccurate. Thomas Rid has critiqued the story, claiming that it erodes deterrence by disclosing capabilities and undermines the complexity and resiliency of the Russian electricity grid. Several Russian sources have commented that intrusions in their electricity grid are 'hypothetically possible' or that any attacks from the US could potentially escalate into cyber war.

If the *New York Times* story is accurate, then the US would likely have similar capabilities to BlackEnergy and Crashoverride, the two APTs thought to have disrupted Ukrainian electricity utilities in 2015 and 16, to disrupt Russian energy grids. The Centre has reported on BlackEnergy and Crashoverride in multiple assessments.

Threat Actor: (7) State actor: agents of a nation state.

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 22 June, Yahoo News reported that the United States responded with retaliatory cyber operations against Iran for their recent targeting of tankers in the Strait of Hormuz and the downing of a US drone. The *Washington Post* later confirmed that the US CNA operations targeted Islamic Revolutionary Guard Corps (IRGC) rocket and missile command and control infrastructure, likely resulting in a temporary loss of capabilities. The Washington Post article purports that the US CNA operation likely used the same capabilities by which the US attacked Russia's Internet Research Agency (IRA) in retaliation for election meddling, which

were first reported on 27 February. ZDNet explains that the US attacks are designed to degrade IRA IT networks and infrastructure by infecting RAID controllers and using a wiper to destroy hard drives. ZDNet believes at least two of the four hard drives connected to the RAID controller were wiped. ZDNet claims that their analysis was confirmed by Russia's Federal News Agency.

The Washington Post notes that wiper attacks are a common attack amongst Iranian APTs, most notably used in the 2012 Saudi Aramco wiper attack. The Centre recently reported the re-emergence of the Shamoon wiper in Q3-Q4 2018, in which 300-400 servers were wiped at the oil and gas facility. Symantec believes that the Shamoon wiper has nominal ties to Elfin/APT33, an Iranian APT. Symantec reported an uptick of Elfin activity in 2019. The US Department of Homeland Security (DHS) recently stated that they have observed increased 'malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies.' The DHS specifically warned about Iran's proclivity for destructive wipers.

Threat Actor: (7) State actor: agents of a nation state.

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 26 June, Haaretz reported that aircraft around Tel Aviv's Ben Gurion Airport experienced disruption to their GPS signals, leading to irrational flight paths, rerouting, and navigation by instrumentation. On 27 June, the *Times of Israel* reported that the disruption was likely caused by Russian electronic warfare, possibly as a result of ongoing Russian operations in Syria. The *Times of Israel* characterised the incident as a GPS spoofing attack, which Russian officials swiftly denied. GPS spoofing and other forms of electronic warfare have become a well-known component of Russian activity, as detailed in a recent C4ADS white paper. The C4ADS white paper asserts that Russian GPS spoofing and other forms of electronic warfare are used to protect VIPS, to defend strategic facilities, and to project military power abroad. The Centre has reported on multiple suspected Russian GPS spoofing campaigns, most recently in Q3-Q4 2018, when Russia was accused of disrupting Finnish and Norwegian GPS signals during NATO's Trident Juncture exercises in October 2018. GPS spoofing raises the dangers of cyber escalation, as deliberately obfuscating an aircraft's true location can lead to accidents that pose a mortal risk. Although the ability to cause disturbances at the scope and scale of the Russian incidents is almost certainly restricted to nation states, GPS spoofing is an extremely attractive attack vector that extremists wish to utilise or emulate. A recent deadly helicopter crash in New York City, in which the pilot became disoriented and lost before crashing into an office building, demonstrates how loss of navigation control can turn fatal.

Threat Actor: (7) State actor: agents of a nation state.

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 5 May, the Israeli Defense Forces (IDF) admitted to bombing a building thought to contain Hamas cyber operatives and infrastructure. Termed HamasCyberHQ.exe, the IDF claims to have been responding to a Hamas cyber attack in real time. Tensions between Israel and Hamas have been building through the spring of 2019, and on 4 May Hamas fired at least 250 rockets into Israel. By 5 May, the estimate had been raised to 600 rockets. The IDF has not disclosed the type of cyber attack Hamas was attempting to undertake and the operational impact on Hamas cyber operations remains unknown. Researchers have questioned whether the attack was truly in response to a real time threat or if a pre-cleared target was the motivation behind the strike. Targeted killing has been instrumental in the war on terror and the Israeli strike against cyber operatives would not be the first strike against cyber operatives. In the fight against the Islamic State, Junaid Hussain, a British born IS cyber operative was killed by a drone strike in 2015. Hussain had been described as a high

value target, although it remains unclear if he was the subject of a targeted killing or if his death was unintended.

See annex for additional APT activity: Elfin (Shamoon leak), OilRig/MuddyWater (Iranian toolset leak), & Stealth Mango (Pakistani mobile malware campaign)

Section 6: **Miscellaneous – Cybercrime, Pen Tests & Research**

Key Statement

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

There are no indications that cyber criminal activity has significantly advanced or increased in the first half of 2019. No systemic events have taken place. Ransomware targeting critical national infrastructure (CNI) and local communities remains the most disruptive cyber criminal activity.

The Tipping Point

An uptick in wares for sale which claim to adopt nation state exploits and tools capable of triggering systemic events and driving cascading loss, such as EternalBlue. Extensive collateral damage and loss of control of the campaign by cyber criminals would likely follow. There are no indications that cyber criminals have adopted those capabilities. Cyber criminals have only sporadically marketed these capabilities since WannaCry and NotPetya. A similar significant event is yet to occur.

Key Judgements

- Ransomware targeting industry, local communities (towns, cities, counties, states) and CNI continues to be the most disruptive cyber criminal activity.
    - LockerGoga has proven to be a particularly potent ransomware strain, disrupting at least four industrial companies.
        - The most prominent LockerGoga attack was against Norsk Hydro, a Norwegian based aluminium producer.
        - Researchers claim LockerGoga has been used in dozens of other cases.
    - Cyber criminal use of ransomware to extort local communities appears to be increasing. Collection indicates that communities in the United States remain the most targeted.
        - One county in Georgia elected to pay a $400,000 ransom.
        - Two cities in Florida paid a combined total of $1 million in ransom.
        - One county in California refused to pay a $1.2m ransom and spent over $1.4m in rebuilding costs after being targeted by Ryuk.
        - Baltimore experienced a ransomware incident that the *New York Times* attributed to an EternalBlue exploit. The incident remains hotly debated in the media, academia and industry communities. It is the Centre's assessment that the Baltimore ransomware incident was not EternalBlue (low confidence).[1]
- Other cyber criminal activity other, such as cryptojacking, has begun to target and disrupt companies with industrial processes.
    - One manufacturer in Japan was targeted in an attempted cryptojacking attack in which two of their industrial facilities experienced a drop of 60% in production.

[1] Special write up in annex under Baltimore Ransomware

  - Cryptojacking is a greater threat to ICS networks than ransomware. Cyber criminals can maintain persistence within company networks and drain resources for extended periods of time before being discovered. Lack of detection creates ample opportunities for reconnaissance and the scanning/mapping of ICS networks.
  - Cryptojacking can also be used as a prerequisite to establish the infrastructure for future destructive attacks in ICS networks.
  - Intense cryptojacking can cause ICS/OT networks to experience a denial of service (DoS) attack.
  - Nation states could also use cryptojacking to create doubt with regard attribution, as described in Section 5's key judgements.
- Commodification of disruptive malware and capabilities by cyber criminals can allow inexperienced threat actors perpetrate attacks.
  - Ransomware-as-a-service continues to be marketed on forums and social media.
  - One ransomware, Yatron, claimed to have self-propagating capabilities based on EternalBlue. Initial analysis claims that Yatron is not functional.
    - Previous Centre assessments have indicated ransomware sellers claiming to have products featuring EternalBlue and other ShadowBrokers exploits. There are no indications that ransomware campaigns linked to cyber criminal units have utilised EternalBlue thus far.
  - Cyber criminals continue to sell access to CNI networks, such as to a Chinese railroad company. Last year's assessment noted cyber criminals selling access to airport networks, among others.
  - Several threat intelligence companies have noted that the Mirai botnet, one of the world's most capable botnets for perpetrating DDoS attacks, is increasingly targeting embedded IoT devices for its botnet. This would significantly add to the power of a DDoS attack from Mirai.
  - An unspecified Western US electricity utility experienced disruption due to a denial-of-service attack.
    - An increase in the power of Mirai or other DDoS malwares could prove to be highly disruptive, including to CNI, in the future. It is thought that the 2016 Fidelix attack was collateral damage of a mis-targeted DDoS attack.
    - Several incidents throughout this assessment note an increase in malware targeting CNI, such as FireEye, Dragos, E&E News, NERC and the NYT.

Analysis

Cyber Criminals remain a persistent threat to global business and local governance. In the first half of 2019, Cyber Criminals' use of denial-of-service (DoS) attacks, data exfiltration and ransomware against Critical National Infrastructure (CNI), industry and local governments continues to remain a disruptive endeavour, driving significant losses.

CNI Threats

Threat Actor: (9) Not applicable: attribution not applicable to event

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

The most impactful disruptive cyber incident in the first half of 2019 was reported on 30 April by Blake Sobczak of E&E News. Sobczak discovered that an unspecified Western US energy grid suffered a 'cyber event' on 5 March that led to disruption in California, Utah and Wyoming. Sobczak confirmed his findings through a US Department of Energy (DOE) Electric Emergency and Disturbance Report. On Twitter, Sobczak went on to describe the incident as 'disrupting power flows or grid communications' and 'unprecedented.' On 2 May, Sobczak reported that a DOE official had confirmed his findings, commenting that the interruption was

due to a DoS attack, although the official also noted that 'the event did not impact generation.' Sobczak also confirmed through the DOE official that the DoS attack was deployed to an unpatched system, taking advantage of a known vulnerability. Sobczak was unable to confirm the identity of the victim nor garner any other statements from officials. It is unclear if the incident was a DoS, DDoS, or telephony-denial-of-service (TDoS) attack.

Limited details of the incident have been released and, at time of reporting, E&E News remains the only outlet to cover the incident in depth with Sobczak the only main contributor on Twitter. Attribution remains elusive, but analytic inference can lead to a number of plausible actors ranging from state or state-backed actors, cyber criminals, hacktivists or security researchers. The 2015 BlackEnergy and the 2016 Crashoverride attacks against Ukrainian electricity utilities had the capabilities to launch DoS attacks. In 2017, Flashpoint reported that affiliates of the Islamic State were experimenting with DDoS-for-hire services and developing their own DDoS capability, dubbed the 'Caliphate Cannon.' The effort failed.

The North American Electric Reliability Corporation recently released their annual report on reliability of the North American electricity grid. The report states that in 2018 'no cyber or physical security incidents leading to unauthorized control actions or loss of load occurred.' However, the report stresses that cyber threats are increasing, confirming many of the assumptions in this and previous Centre assessments. Several NERC assessments align with the Centre's viewpoints, such as the disruptiveness of ransomware, the threat of supply chain attacks, an increase in customised malware targeting ICS and the use of common tools to move laterally throughout ICS/OT networks. NERC believes that under the right circumstances cryptojacking can cause a denial of service (DoS) attack. NERC places special emphasis on cryptojacking, stating: 'ransomware is quick and easy to detect due to its disruptive nature...Comparatively, cryptojacking incidents typically seek to avoid detection by using only a small portion of the victim's computer processing power to mine currency. While most cryptojacking infections will not make the target system unusable, infected hosts are still negatively impacted. Prolonged operations of cryptominers can burn out components, requiring more frequent replacement, and some cryptojacking malware ignores stealth—by design or poor coding—and uses all available processing power, effectively causing a denial-of-service condition on the system.'

Threat Actor: (9) Not applicable: attribution not applicable to event

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 29 April, Citrix, a company that offers networking, virtualisation and software products globally to industry and governments disclosed that they were the target of a data exfiltration campaign on 6 March. Citrix believes that the threat actor maintained access to Citrix's internal network from 13 October 2018 to 8 March 2019. Citrix disclosed that the threat actor exfiltrated personally identifiable information of present and past employees and their dependents. Earlier, on 4 April, Citrix stated that the threat actors used password spraying to gain initial entry into Citrix networks.

The nature of Citrix's business and the use of its products in the defence industry, CNI and government position Citrix as a valuable target. For instance, a threat actor could penetrate Citrix to conduct supply chain attacks to gain footholds in strategic industries. Supply chain attacks have become increasingly common. In March, Symantec reported that ASUS users were distributed malicious updates containing backdoors, likely for espionage. Malicious updates are the same infection vector used during NotPetya.

Ransomware

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

On 19 March, LockerGoga targeted Norsk Hydro, a Norwegian aluminium and renewable energy company and severely impacted the firm's global operations. Press releases from Norsk Hydro indicate that LockerGoga had lain undetected for an undefined period of time in the company's network and only began encrypting on 19 March, followed by weeks of containment and remediation by Norsk Hydro. Containment measures included disconnecting all PCs and other infrastructure, reviewing and restoring PCs, and rebuilding encrypted PCs from backups.

Keven Beaumont extensively covered Norsk Hydro's initial incident response, which included full public disclosure and reverting to manual operations. Beaumont noted that the same certificate used in the Altran incident was used to conduct the Norsk Hydro incident until it was revoked by its issuer. Beaumont also noted that as in the Altran attack the malware did not utilise C2 infrastructure and lacked the ability to self-propagate.

E24 reported that the National Crime Investigation Service (Kripos) and the National Security Authority (NSM) of Norway had begun investigating the incident and collaborated with the French ANSSI, which responded themselves to the Altran incident weeks earlier. During the incident response, Norsk Hydro experienced a power outage interrupting production at Hydro Karmoy, one of their primary aluminium production facilities. It is unclear if the power outage was a direct result from the LockerGoga incident, though Norsk Hydro includes the power outage in a publicly released timeline of the LockerGoga incident. By 12 April, Norsk Hydro reported a return to 85-90% of production capacity. By 30 April, The Local reported that the LockerGoga incident is estimated to cost Norsk Hydro between $46-52m.

It is important to note that LockerGoga likely affected IT systems and was not specifically designed to manipulate operational technology (OT) or industrial control systems (ICS). Researchers such as Joe Slowik have acknowledged the possibility of an APT using LockerGoga as a wiper to obfuscate an espionage operation, though these comments are unsubstantiated and may have been said in jest.

For more information on LockerGoga see annex: Norsk Hydro (LockerGoga writeup, Altran, Hexion and Momentive)

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area; (8) Increase in commodification, or availability as a service, of attack tools.

On 6 April, Japanese eyeglass manufacturer Hoya disclosed that they had suffered a cyber attack. Kyodo News reported that on 1 March a cyber criminal used credential harvesting with the goal of installing cryptojacking malware to mine cryptocurrency. The credential harvesting overloaded Hoya servers which in turn alerted Hoya to an intrusion, preventing the cyber criminal's ability to install their cryptojacking malware. Two plants in Thailand experienced a slowdown in production of 60% and offices in Tokyo struggled to complete administrative duties.

Symantec notes that cryptojacking significantly decreased in 2018 due to a drop in the value of cryptocurrency. In certain instances cryptojacking can cause a denial of service attack, as described above.

For ransomware against Local communities & industry see Annex: Baltimore & Container World.

Commodification

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

Intelligence Requirement: (8) Increase in commodification, or availability as a service, of attack tools.

Ransomware also continues to be commodified through as-a-service providers. In March, researchers noted a Ransomware-as-a-Service (RaaS) named Jokeroo for sale on underground forums and Twitter. Prices ranged from $90-600. Similarly, researchers discovered a RaaS termed Yatron advertised on Twitter for $100. Yaltron supposedly utilises EternalBlue and DoublePulsar. However, researchers believe that there are flaws in this code and that Yaltron has not been purchased as of reporting.

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

Intelligence Requirement: (8) Increase in commodification, or availability as a service, of attack tools.

On 4 March HackRead reported that the threat intelligence firm Sixgill had discovered a cyber criminal 'selling access to the admin panel of a Chinese rail control system.' HackRead derived their information from a Sixgill PDF. The PDF claims that the seller was marketing access on a Russian and English-speaking Dark Web forum, and that the seller provided proof of Administration access to 'system configuration, information management and personal management, which would allow further access to the module, navigation, and employee management systems, as well as codes for the locomotive segment,' Sixgill asserts that some of the information could result in a loss of life if exploited.

Penetration testers have shown that it is common for critical physical safety and SCADA components, such as brakes, to be insecurely connected to train WiFi networks, and that trains can be made to derail if these connections are exploited. Obtaining administration rights to these systems would give threat actors access to the entire train network and negate the need to be physically present in order to hack specific train WiFi networks.

Limited details and news coverage on this story are available. The original Sixgill PDF no longer appears on the group's website. A link provided by HackRead to the Sixgill blog detailing the research also lacks a Sixgill primary source. However, Sixgill's News and TV Interviews section does link to the HackRead article and a CSO article reporting on the Sixgill research. The latest issue of the online al-Qaeda periodical *Inspire*, published in August of 2017, advocated committing train derailment operations in the West. Details on construction of homemade derailment devices, operational security and preparation and perpetration of the attack were disseminated. There are no known instances of extremists successfully derailing a train. On 27 March, an Iraqi national accused of supporting Islamic State, was arrested in Vienna for attempting to derail two trains in Germany. His attempts were decidedly less sophisticated than what *Inspire* advocated: in one instance, hanging a steel wire across tracks. The second instance involved placing cement blocks on tracks.

Threat Actor: (5) Criminal: actors operating in pursuit of financial gain

Intelligence Requirement: (8) Increase in commodification, or availability as a service, of attack tools.

In March, Unit42 of Palo Alto Networks released research on a new version of the Mirai botnet. Unite42 first observed the new version of Mirai in January 2019 and believes that Mirai now has the capability of targeting embedded IoT devices ranging from routers, network devices, cameras, presentation systems and T.V.s. Unit42 assesses that the targeting of IoT devices can ultimately increase Mirai's attack surface and add bandwidth (power) to future attacks. Trend Micro and Kaspersky released similar research, confirming Unit42's conclusions.

Vulnerabilities

Threat Actor: (9) Not applicable: attribution not applicable to event

Intelligence Requirement: (2) Other instances of cyber being used for destructive or disruptive effect, regardless of actor, to help get a sense of trends in this area;

CVE-2019-0604 Microsoft SharePoint Remote Code Execution Vulnerability

On 12/02/2019 Microsoft disclosed CVE-2019-0604. According to Microsoft:

'A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account.'

The vulnerability has importance for Pool Re due to its ability to enable lateral movement. The NCSC claims that they have monitored several successful attacks against UK organisations using the vulnerability. The details of these purported attacks are lacking but initial reporting indicates organisations in Saudi Arabia and Canada have been targeted.

Technical indicators disclosed by Symantec in their 20 June Waterbug report indicate that Russian APTs have been exploiting the vulnerability. Waterbug, as detailed above, is a Russian APT that hijacked Iranian infrastructure to spread malware with EternalBlue, especially throughout the Middle East. Waterbug's noted targeting in the Middle East lends credence to the Twitter report documenting a likely victim in Saudi Arabia.

CVE-2019-0708 Microsoft Remote Desktop Services Remote Code Execution Vulnerability

On 14 May Microsoft disclosed a vulnerability, CVE-2019-0708. According to Microsoft;

'A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.'

The vulnerability has been nicknamed BlueKeep. BlueKeep threatens RDP at the pre-authentication stage, requires no user interaction and is believed to be wormable like WannaCry. Microsoft believes that exploits likely exist and referenced Robert Graham's blog , in which he found over 1 million machines exposed on Shodan. The NSA believes the vulnerability to be a priority threat and believes that malicious actors, especially cyber criminals deploying ransomware, are likely to exploit the vulnerability. Several ransomware strains reported on in this assessment utilise RDP, such as Ryuk and RobbinHood. Following a DHS CISA Alert, sources believe that the DHS has developed a working exploit that incorporates BlueKeep.