Overview of State-Sponsored Threat Activity Pertinent to OT Asset Owners

Critical Infrastructure (CI) | Fusion (FS)

August 17, 2021 05:58:12 PM, 21-00018084, Version: 1.4

Executive Summary

- Given the high-volume of state-sponsored threat activity pursuing a variety of objectives, it can be difficult to accurately distinguish and prioritize threats to operational technology (OT). We observe four broad types of cyber threat activity pertinent to OT asset owners: ambiguous threat activity, computer network attacks, OT-targeted espionage, and cyber physical attacks.
- While most state-sponsored threat activity against IT assets corresponds to cyber espionage, certain ambiguous, high-risk activity could indicate a willingness to conduct destructive attacks or pre-positioning for future OT activity. We are aware of a large amount of ambiguous threat activity and a moderate number of publicly documented state-sponsored computer network attacks.
- OT assets can be sabotaged via integrity-attacks and availability-attacks or targeted in confidentiality-attacks focused on OT assets or data. We are aware of a minor number of OT-targeted espionage operations and four publicly documented state-sponsored cyber physical attacks.
- State-sponsored threat actors will likely continue targeting the corporate infrastructure of OT-reliant organizations at a high frequency, which will provide many opportunities to pivot to OT assets if desired. While the risk of reprisal will likely limit cyber physical attacks to select targets, these attacks remain a high-risk to OT environments due to the potential for catastrophic impacts and physical harm.

Threat Detail

Given the high-volume of state-sponsored threat activity pursuing a variety of objectives, it can be difficult to accurately distinguish and prioritize threats to operational technology (OT). State-sponsored threat actors motivated to target cyber physical systems can reach their objectives in different ways. They can direct activity against IT assets to attempt to facilitate lateral movement to OT systems or attack IT assets and demonstrate a willingness for disruption. They can target OT assets to generate physical impacts or conduct espionage to gather intelligence for future attacks. Mandiant Threat Intelligence considers a variety of factors to help enumerate and prioritize threats to OT, such as sector targeting, aggression, capability, and actor motivation. We observe four types of non-mutually exclusive state-sponsored threat activity pertinent to OT asset owners, loosely ordered by ascending risk to OT:

- *Ambiguous Threat Activity*: Cyber activity with unclear objectives that poses a threat to OT-reliant organizations. This includes operations that overwhelmingly target public utilities or OT vendors and operations that pose a threat to such industries by leveraging aggressive initial access or lateral movement techniques (e.g., supply-chain attacks, worm-like malware, etc.). The ambiguity of intent leaves open the possibility that the activity will evolve into the higher-risk types listed as follows.
- *Computer Network Attacks*: Cyber attacks designed to disrupt data processes and workflows
- *OT-Targeted Espionage*: Cyber espionage in which the target is either OT or OT-related information
- *Cyber Physical Attacks*: Cyber attacks designed to sabotage physical processes

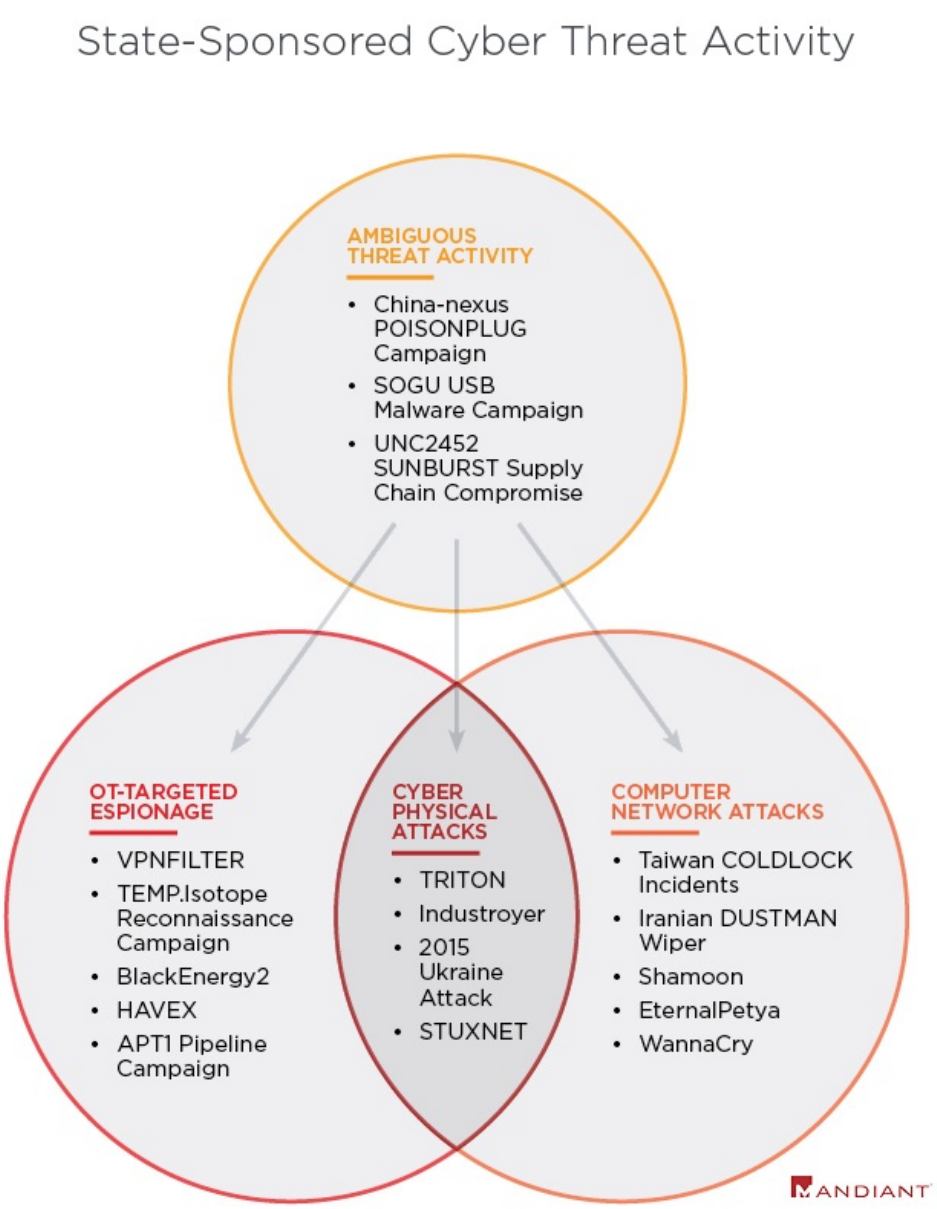

Figure 1: Types and examples of state-sponsored cyber threat activity pertinent to OT asset owners

Types of Threat Activity

Ambiguous Threat Activity

Cyber espionage is problematic for OT asset owners because it provides the threat actor with the same initial access to an organization they would need in other higher-risk operations, such as the early stages of a cyber physical attack. While the intent of cyber espionage can be difficult to discern, certain ambiguous, high-risk activity is more relevant to OT assets owners. Cyber activity overwhelmingly focused on public utilities and OT vendors could be an interpreted as reconnaissance for future attacks. Operations that leverage aggressive lateral movement techniques, such as self-propagating malware and supply-chain attacks, could facilitate initial access to a large number of OT-reliant companies in various industries beyond the intended target. We are aware of a large amount of ambiguous threat activity, so we highlight only a select number of recent incidents. More examples are detailed in the Appendix.

- In May 2021, we reported on Chinese espionage operators deploying POISONPLUG against India in long-running campaigns targeting critical infrastructure. Technical indicators released in public reporting linked to the "Red Echo" operation overlap with previously identified Chinese espionage activity including APT41, APT5, and multiple uncategorized clusters of activity. While open sources have implied a link between these operations and a power outage in mid-October 2020 and the possibility that the incident was the result of a purposeful attack, we have not seen any indications of follow-on activity affecting OT (21-00007495).
- In February 2021, we identified a SOGU variant deployed to Vietnamese entities in the financial, utilities, energy, and aviation services industries. The variant is capable of spreading via USB devices, which poses a heightened threat to air-gapped systems and networks associated with cyber physical systems. We identified potential links with China-nexus threat actor TEMP.Hex (21-00004534, 20-00010857).
- In December 2020, we uncovered a global intrusion campaign by UNC2452, which consisted of a supply chain attack trojanizing SolarWinds Orion business software updates to distribute SUNBURST malware. The North American Electric Reliability Corporation (NERC) later revealed that 25 percent of approximately 1,500 electric utilities sharing data with the North American power grid installed SUNBURST. In some of those cases, the SolarWinds Orion product was supporting OT. Mandiant assesses that UNC2452 activity aligns with nation-state priorities and that the group's targeting patterns are consistent with Russian strategic interests (20-00026220, 21-00008599).

- In October 2019, the Nuclear Power Corporation of India (NPCI) issued a statement confirming that a malware infection reached Kudankulam Nuclear Power Plant's (KKNPP) corporate network. We identified related malware samples, which suggest that a suspected North Korean threat actor had been active in the environment since as early as March 2019 (19-00018852).
- In October 2019, we observed password spraying activity against cloud-hosted infrastructure similar to public reporting of APT33 activity by Microsoft and TrendMicro. The activity targeted numerous verticals; however, public reporting suggests APT33's strongest interest was in OT vendors and service providers (19-00020649).

Computer Network Attacks

Computer network attacks (CNAs) are typically accomplished via availability-attacks, such as deploying wiper malware and performing denial-of-service (DoS) attacks. CNAs indicate that the threat actor and state sponsor are willing to conduct disruptive cyber operations, which may manifest as OT attacks in the future. These attacks are also relevant to OT asset owners because the attacks may impact OT-related assets on corporate networks and because the attack could propagate directly to OT assets. We are aware of a moderate number of state-sponsored CNAs, more of which are detailed in the Appendix.

- In May 2020, two Taiwan-based companies in the oil and gas sector were impacted by incidents that involved the distribution of COLDLOCK ransomware. DUSTCOVER, a dropper tied to China-nexus APT41, was likely leveraged to deploy COLDLOCK. Authorities in Taiwan issued a statement suggesting China-nexus threat actors were responsible; however, we have not attributed the incident to a specific threat actor (20-00008620, 21-00016858).
- In December 2019, DUSTMAN wiper malware was deployed against entities in Saudi Arabia and Bahrain. We believe DUSTMAN is Iranian in origin based on similarities to other suspected Iranian wipers, such as ZEROCLEAR (20-00001090).
- In December 2018, threat actors leveraged a variant of Shamoon malware against oil, gas, and mining organizations who had operations based out of Saudi Arabia and the United Arab Emirates (UAE). We identified tentative links between Shamoon infections and Iran-nexus APT33 (16-00019328, 18-00021070, 18-00021316, 18-00021437).
- In June 2017, Sandworm Team targeted Ukrainian financial entities with EternalPetya ransomware. Though initially designed to target a single industry, the ransomware quickly spread, causing global disruption and, according to some estimates, $10 billion USD in damage. Our examination of EternalPetya ransomware indicates the malware was configured in a way that does not make decryption possible, suggesting the campaign was designed purely as an attack (17-00006894, 17-00006864, 17-00006904).
- In May 2017, the highly prolific WannaCry ransomware campaign, later attributed to North Korean actors, infected more than 230,000 computer systems in 150 countries. Given various flaws in the malware, the threat actors could be of limited sophistication and possibly did not anticipate the malware would spread as widely as it did. Alternatively, the malware could have been inadvertently distributed prior to completion (17-00005158, 17-00004894, 17-00005349, 18-00016353).

OT-Targeted Espionage

OT-targeted espionage is a confidentiality-attack in which a threat actor makes an unambiguous attempt to compromise OT assets or obtain OT network and system information, engineering and design information, or OT user credentials. OT-targeted espionage serves multiple purposes, including economic espionage, OT network reconnaissance, and contingency war planning. We are aware of a minor number of OT-targeted espionage operations, however, ambiguous threat activity where we cannot directly attribute a motivation may also target this type of information. More examples are detailed in the Appendix.

- In July 2021, media reported on a set of documents ostensibly internal to the Iran's Islamic Revolutionary Guard Corps (IRGC) that discuss the possible physical impacts of cyber operations targeting OT, the feasibility of conducting such attacks, and internet-accessible devices that could be potential targets. While we have no evidence to confirm the authenticity of these documents, their contents are consistent with our observations of Iranian cyber operations planning and IRGC mandates (21-00016966, 21-00016766).
- In June 2019, media reported that U.S. Cyber Command (CYBERCOM) had increased covert efforts to establish a persistent presence inside Russia's electric power systems and other sensitive targets. The deployment of code in Russia's grid was allegedly carried out using authorities granted by Congress and the White House in the prior year (19-00010254).
- In June 2018, researchers published information on VPNFILTER actors deploying an OT-tailored packet sniffing module focused on Modbus traffic. The observed samples of the packet sniffer appear reconnaissance-focused and not tooled for sabotage capabilities. Based on technical and targeting information, we assess with moderate confidence that the activity is consistent with Russian cyber espionage activity (18-00008818, 18-00009458).
- In October 2017, US-CERT published Alert TA17-293A describing reconnaissance activities targeting energy and other critical infrastructure sectors, which we have largely attributed to Russia-nexus threat actor TEMP.Isotope. TEMP.Isotope reportedly accessed OT engineering diagrams and documentation from victim corporate networks and public-facing websites (17-00012280).
- From 2011 to at least October 2014, Sandworm Team leveraged BlackEnergy2 malware to target internet-connected human-machine interfaces (HMIs) by exploiting software vulnerabilities (Intel-1289248, Intel-1273358).
- In July 2014, Russia-nexus Koala Team deployed HAVEX, aka PEACEPIPE or FERTGER, through a strategic web compromise focused on energy-related websites and trojanized OT utilities. HAVEX actively scans OPC servers, a client/server technology widely used in OT applications (Intel-1153508, 14-00000172).
- From December 2011 to 2013, China-nexus APT1 targeted the OT networks of a U.S. oil and natural gas pipeline. According to an alert by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), 23 U.S. natural gas

pipeline operators were targeted in a spear-phishing campaign, and at least 13 were successfully compromised. Several OT networks were successfully accessed in these compromises, although there were reportedly no attempts to modify operations (Intel-578154, 21-00016485).

Cyber Physical Attacks

Cyber physical attacks are accomplished via integrity-attacks, such as manipulating the expected behavior or parameters of a control system or via availability-attacks, such as wiping or encrypting data on key OT assets. While these attacks are rare, they represent a high risk to OT environments due to the potential for catastrophic impacts and physical harm. We are aware of four publicly documented state-sponsored cyber physical attacks.

- In November 2017, the Russia-nexus threat actor TEMP.Veles deployed TRITON malware against a critical infrastructure organization in an attempt to compromise the organization's safety instrumented system (SIS). We assess with moderate confidence that the threat actors' primary objective was to use TRITON to inflict physical damage. We assess with moderate confidence that the threat actor inadvertently caused the targeted SIS controller to fail, preventing the operation from causing physical damage to the system (17-00014211, 18-00006335, 18-00000697, 18-00000638, 18-00001610, 18-00003202, 18-00016550, 18-00020888).
- In December 2016, the Russia-nexus threat actor Sandworm Team leveraged Industroyer malware against the OT systems of a Ukrainian transmission substation, subsequently taking offline one-fifth of Kiev's power for 75 minutes. We assess that this is the first publicly known instance of a power outage directly caused by malware as Ukraine's 2015 power outage leveraged an attack that required manual interaction (16-00021034, 17-00000447, 17-00006337).
- In December 2015, Sandworm Team manually manipulated HMIs and deployed KillDisk malware in an operation against Ukrainian energy entities. The attack caused damage to OT equipment, disrupting the electric flow and resulting in a power outage affecting at least 80,000 customers (15-00013102, 15-00014822, 16-00001496, 16-00001698, 16-00000208).
- In 2009, a suspected U.S. and Israeli operation leveraged STUXNET malware at an Iranian nuclear facility. The incident sabotaged programmable logic controllers (PLCs) used to control centrifuges, causing the equipment to malfunction (17-00002192, 18-00020235).

Outlook and Implications

During the past several years, state-sponsored threat actors have conducted a variety of cyber activity relevant for OT asset owners. These actors will likely continue targeting corporate infrastructure of OT-reliant organizations at a high frequency, which will provide many opportunities to pivot to OT assets if desired. Cyber operations targeting OT can be an effective method of harming an adversary's infrastructure; however, the risk of reprisal is likely to limit cyber physical attacks to select targets. We believe state-sponsored threat actors conduct these types of activities due to geopolitical tensions, state conflicts, and a lack of clear norms and deterrents. The convergence of IT and OT and expansion to cloud technology indicates that self-propagating malware and supply-chain attacks will increasingly impact OT. Hostile actions in various geopolitical hotspots may drive future growth in threat activity.

Appendix: Selected State-Sponsored Threat Activity Pertinent to OT Asset Owners

Date	Activity Overview	Activity Type	Associated Actor	State Attribution
July 2021	Media reported on a set of documents ostensibly internal to the IRGC that discuss the possible physical impacts of cyber operations targeting OT, the feasibility of conducting such attacks, and internet-accessible devices that could be potential targets (21-00016966, 21-00016766).	OT-Targeted Espionage	N/A	Iran (Possible)
June 2021	We discovered a suspected Chinese operation targeting a Taiwanese information services corporation involved with the internet of things (IoT) (21-00012355).	Ambiguous Threat Activity	N/A	China
June 2021	Media reported on a suspected Pakistan-linked threat actor targeting energy organizations in the South and Central Asia regions using the "ReverseRAT" .NET backdoor to steal sensitive data. Reports indicate that the targets included power transmission and power generation organizations (21-00014450, 21-00008616).	Ambiguous Threat Activity	N/A	Pakistan (Possible)
	We reported on Chinese			

May 2021	espionage operators deploying POISONPLUG against India in long-running campaigns targeting critical infrastructure. Technical indicators released in public reporting linked to the "Red Echo" operation overlap with previously identified Chinese espionage activity including APT41, APT5, and multiple uncategorized clusters of activity (21-00007495).	Ambiguous Threat Activity	APT41, APT5	China
May 2021	South Korea's Korea Atomic Energy Research Institute (KAERI) revealed that a North Korean Government-linked threat group exploited a vulnerability affecting an unnamed VPN provider to breach its internal network. The targeting and infrastructure reported as being associated with this incident align with activity we track as UNC2410 (21-00014450, 21-00011303).	Ambiguous Threat Activity	UNC2410	North Korea
May 2021	We identified a global spear-phishing campaign tracked as UNC2743 that targeted government, defense, international development, energy, and telecommunications organizations in the U.S., Europe, and South Asia. The broad-based attack is reminiscent of more aggressive activity observed during China's nascent years conducting cyber espionage campaigns (21-00009345).	Ambiguous Threat Activity	UNC2743	China
April 2021	A user we suspect is a victim of UNC2448 operations uploaded a LOCKBIT ransomware sample to a public malware repository five days before submitting FRP configuration files containing references to UNC2448 infrastructure (21-00011144).	Computer Network Attack (Possible)	UNC2448	Iran
March 2021	We discovered that suspected Russia-nexus activity targeted the Kazakhstan energy sector using memo lures and KEYSHOW malware (21-00005375).	Ambiguous Threat Activity	N/A	Russia
March 2021	Public sources reported that an Israeli car insurance company had been breached and that the BlackShadow persona, which is possibly connected to UNC2428, was leaking allegedly stolen documents. The actors claimed to have "destroyed" the company's servers and demanded 10 BTC in ransom (21-00010874).	Computer Network Attack (Possible)	UNC2428	Iran
February 2021	We identified a SOGU variant deployed to Vietnamese entities in the financial, utilities, energy, and aviation services industries. The variant is capable of spreading via USB devices, which poses a heightened threat to air-gapped systems and networks associated with cyber physical systems (21-00004534, 20-00010857).	Ambiguous Threat Activity	TEMP.Hex (Possible)	China
	We uncovered a global intrusion campaign, which consisted of a supply chain attack trojanizing			

December 2020	SolarWinds Orion business software updates to distribute SUNBURST malware. NERC later revealed that 25 percent of approximately 1,500 electric utilities sharing data with the North American power grid say they installed SUNBURST. In some of those cases, the SolarWinds Orion product was supporting OT (20-00026220, 21-00008599).	Ambiguous Threat Activity	UNC2452	Russia (Possible)
November 2020	SALTYBOAR, a custom backdoor leveraged by UNC2428, was reportedly discovered on the network of an Israeli insurance company. The persona BlackShadow claimed to have encrypted files and damaged data centers and began publishing Shirbit data on social media. During this time, an Israeli user submitted a screenshot of indicators of compromise (IOCs), which suggested a wiper tool may have been deployed (21-00010874).	Computer Network Attack (Possible)	UNC2428	Iran
May 2020	Two Taiwan-based companies in the oil and gas sector were impacted by incidents that involved the distribution of COLDLOCK ransomware. DUSTCOVER, a dropper tied to China-nexus APT41, was likely leveraged to deploy COLDLOCK. Authorities in Taiwan issued a statement suggesting China-nexus threat actors were responsible (20-00008620, 21-00016858).	Computer Network Attack	N/A	China (Possible)
May 2020	Media reports indicated that Israel launched a cyber attack on computer systems at a maritime trade hub in Iran in response to accusations of Iran's involvement in targeting Israel's water infrastructure (20-00008653).	Computer Network Attack (Possible)	N/A	Israel (Possible)
April 2020	A threat actor accessed and modified the control logic on multiple internet-accessible PLCs at several Israeli water sector facilities. Media reports suggested Iran was behind the incident, and Israel reportedly responded by conducting a disruptive cyber operation against an Iranian port facility (20-00008202).	Cyber Physical Attack	N/A	Iran (Possible)
April 2020	Media reported on a threat actor deploying DIRTPYLE in a campaign reportedly targeting OT related to wind turbines in Azerbaijan. It appears to be a follow-up of an initial campaign that Mandiant uncovered in late March 2020, which involved a cloned Azerbaijan government webmail portal for harvesting user credentials and a malicious file containing a DIRTPYLE payload capable of exfiltrating files and screenshots (20-00005288, 20-00004096).	OT-Targeted Espionage (Possible)	N/A	N/A
	DUSTMAN wiper malware was deployed against entities in Saudi Arabia and Bahrain. We believe	Computer		

December 2019	DUSTMAN is Iranian in origin based on similarities to other suspected Iranian wipers (20-00001090).	Network Attack	N/A	Iran
October 2019	The NPCI issued a statement confirming that a malware infection reached the KKNPP corporate network. We identified related malware samples, which suggest a North Korean threat actor had been active in the environment since as early as March 2019 (19-00018852).	Ambiguous Threat Activity	N/A	North Korea
October 2019	We observed password spraying activity against cloud-hosted infrastructure similar to public reporting of APT33 activity by Microsoft and TrendMicro. The activity targeted numerous verticals; however, public reporting suggests APT33's strongest interest was in OT vendors and service providers (19-00020649).	Ambiguous Threat Activity	APT33	Iran
June 2019	U.S. CYBERCOM reportedly launched a series of cyber attacks against Iran, targeting systems belonging to IRGC and successfully disabling Iranian computer systems that control rocket and missile launchers (19-00010387).	Computer Network Attack (Possible)	N/A	U.S.
June 2019	Media reported that U.S. CYBERCOM had increased covert efforts to establish a "persistent presence" inside Russia's electric power systems and other sensitive targets. The deployment of code in Russia's grid was allegedly carried out using authorities granted by Congress and the White House in the prior year (19-00010254).	OT-Targeted Espionage (Possible)	N/A	U.S.
December 2018	Threat actors leveraged a variant of Shamoon malware against oil, gas, and mining organizations who had operations based out of Saudi Arabia and the UAE. We identified tentative links between Shamoon infections and APT33 (16-00019328, 18-00021070, 18-00021316, 18-00021437).	Computer Network Attack	APT33 (Possible)	Iran
June 2018	TEMP.Tick leveraged two energy-themed lure messages against South Korean public and private entities with a vested interest in the energy sector. We believe TEMP.Tick is primarily an espionage focused group (18-00013547).	Ambiguous Threat Activity	TEMP.Tick	China
May 2018	Open-source reporting indicates that APT38 targeted financial institutions in Latin America with disruptive malware. Some of the publicly reported attempted heists attributable to APT38 in 2018 include Bancomext in January and Banco de Chile in May (18-00016353, 19-00001539).	Computer Network Attack	APT38	North Korea
	Researchers observed VPNFILTER actors deploying an additional stage 3 OT-tailored packet			

May 2018	sniffing module. We believe that VPNFILTER is consistent with Russian-sponsored cyber espionage activity on technical and targeting levels (18-00009458, 18-00008818).	OT-Targeted Espionage	N/A	Russia
April 2018	An advisory published by the UK National Cyber Security Centre (NCSC) details Temp.Isotope activity targeting critical infrastructure in the UK. The report includes limited information on OT but details the threat actors' activities against IT (17-00012280).	Ambiguous Threat Activity	TEMP.Isotope	Russia
February 2018	We assess with high confidence that Sandworm Team was behind a destructive campaign leveraging SOURGRAPES wiper malware to disrupt the 2018 Winter Olympics in PyeongChang, South Korea (18-00002527, 18-00008982).	Computer Network Attack	Sandworm Team	Russia
November 2017	Threat actors deployed TRITON malware against a critical infrastructure organization to interact with safety instrumented systems. We believe the threat actor inadvertently halted their operations during the malware's deployment, preventing the operation from causing physical damage to the system. We assess with high confidence that this activity is linked to Russia (17-00014211, 18-00006335, 18-00000697, 18-00000638, 18-00001610, 18-00003202, 18-00016550, 18-00020888).	Cyber Physical Attack	TEMP.Veles	Russia
November 2017	We observed an incident at a critical infrastructure organization where Iran-nexus APT34 compromised workstations and servers in IT networks and planted backdoors to servers located in an OT demilitarized zone (DMZ). While the actor did not appear to exfiltrate any critical process data or documentation, the compromise indicates an intention to persist in the environment for future activities (19-00018094).	OT-Targeted Espionage	APT34	Iran
November 2017	Suspected APT38 activity leveraged BOOTWRECK wiper malware against Latin American financial institutions to conduct fraudulent SWIFT transfers (18-00001656, 18-00001941).	Computer Network Attack	APT38	North Korea
September 2017	Spear-phishing emails with malicious attachments were sent to multiple U.S. utilities from an actor-controlled account. The attached document leveraged a MONKEYCHERRY macro to deliver previously unseen malware. The malware shares characteristics with previously examined TEMP.Hermit malware and communicates over compromised infrastructure (17-00010597).	Ambiguous Threat Activity	TEMP.Hermit	North Korea
	Ukrainian media reports indicate a ransomware campaign targeted transportation entities in Kiev and			

October 2017	Odessa. We assess that threat actors leveraged BADRABBIT malware in the campaign and that the incident is consistent with previous Sandworm Team activity (17-00011900).	Computer Network Attack	Sandworm Team	Russia
October 2017	US-CERT published Alert TA17-293A describing reconnaissance activities targeting energy and other critical infrastructure sectors, which we have largely attributed to TEMP.Isotope. TEMP.Isotope reportedly accessed OT engineering diagrams and documentation from victim corporate networks and public-facing websites (17-00012280).	OT-Targeted Espionage	TEMP.Isotope	Russia
October 2017	APT38 targeted Taiwan's Far Eastern International Bank (FEIB). Foreign-language sources reported that the operation deployed HERMES ransomware, which is not configured to collect a ransom, on the bank's systems. We assess that this was a technique to distract investigators while the group performed other malicious activity, such as fund transfers and destroying evidence of threat activity (17-00011678, 18-00013136, 18-00016353).	Computer Network Attack	APT38	North Korea
June 2017	Sandworm Team initially leveraged EternalPetya ransomware against the Ukrainian financial sector prior to the nation's Constitution Day. The malware's self-propagating capabilities led it to rapidly spread, causing disruption on a global scale (17-00006894, 17-00006864, 17-00006904).	Computer Network Attack	Sandworm Team	Russia
May 2017	The highly prolific WannaCry ransomware campaign, later attributed to North Korean actors, infected more than 230,000 computer systems in 150 countries. Given various flaws in the malware, the threat actors could be of limited sophistication and possibly did not anticipate the malware would spread as widely as it did. Alternatively, the malware could have been inadvertently distributed prior to completion (17-00005158, 17-00004894, 17-00005349, 18-00016353).	Computer Network Attack	N/A	North Korea
May 2017	German press reports revealed Russian-nexus intrusions into the networks of at least two German energy providers, including an energy company-owned internet service provider (ISP). The intrusions did not appear to progress beyond the reconnaissance stage, and, based on available intelligence, we have moderate confidence that this intrusion mirrors tactics, techniques, and procedures (TTPs) employed by TEMP.Isotope (17-00012280).	Ambiguous Threat Activity	TEMP.Isotope	Russia
	APT37 deployed the destructive			

April 2017	RUHAPPY wiper onto South Korean government and military systems. Although this wiper was found on targeted systems along with DOGCALL, there was no evidence that the group used RUHAPPY's primary utility to render victim systems inoperable (17-00004886, 18-00002542, 18-00002820).	Computer Network Attack (Possible)	APT37	North Korea
February 2017	We observed APT10 conduct a sustained espionage campaign against major corporations in the Nordic region. The threat actor employed SOGU malware over identified communications infrastructure. The activity was part of a global campaign aimed at the energy, industrial, extractive, and technological sectors (17-00001858).	Ambiguous Threat Activity	APT10	China
January 2017	Threat actors leveraged a variant of Shamoon wiper malware against Saudi Arabian energy, government, transportation, industrial, and financial sector entities in January 2017. The widespread nature of this wave of Shamoon attacks within Saudi Arabia weakens assertions that attackers specifically intended to shut down specific OT operations (16-00018688, 16-00019328, 17-00000745, 17-00000883, 17-00002343).	Computer Network Attack	N/A	Iran
December 2016	Sandworm Team leveraged Industroyer malware against OT systems of a Ukrainian transmission substation, which removed one-fifth of Kiev's power for 75 minutes. We assess that this is the first publicly known instance of a power outage directly caused by malware as Ukraine's 2015 power outage leveraged an attack that required manual interaction (16-00021034, 17-00000447, 17-00006337).	Cyber Physical Attack	Sandworm Team	Russia
December 2016	Sandworm Team leveraged a variant of KillDisk wiper malware called WHITEROSE against Ukrainian financial entities. Foreign-language media reports indicate the campaign affected Ukraine's Treasury, its Pension Fund, and the Ministry of Finance. These reports also suggest threat actors deleted critical data from government financial organizations, disrupting public-facing services (16-00020050).	Computer Network Attack	Sandworm Team	Russia
August 2016	The U.S. Department of Justice (DOJ) indicted seven individuals affiliated with the Main Intelligence Directorate of the General Staff of the Russian Armed Forces (GRU) deemed responsible for carrying out a variety of cyber espionage and influence operations, including targeting the Westinghouse Electric Corporation (WEC), an American nuclear power	Ambiguous Threat Activity	APT28	Russia

	company. GRU Unit 26165 in the indictment corresponds to reporting on APT28 (18-00017368).			
December 2015	Sandworm Team leveraged KillDisk malware in an interactive compromise against Ukrainian energy entities in December 2015. The attack caused damage to OT equipment, disrupting the electric flow and resulting in a power outage affecting at least 80,000 customers (15-00013102, 15-00014822, 16-00001496, 16-00001698, 16-00000208).	Cyber Physical Attack	Sandworm Team	Russia
April 2015	In an attack generally attributed to Russia (running as a false-front Islamic hacktivist group), attackers incapacitated television transmission equipment of France-based Global Media company TV5Monde (15-00002828, 16-00012858).	Computer Network Attack	APT28	Russia
March 2015	We discovered that APT12 had compromised a computer at a prominent Asian manufacturer of power and other OT systems. We believe the victim host was associated with OT operations given its hostname and the presence of a user account on the host that is likely associated with Open Platform Communications (OPC) (16-00006296).	OT-Targeted Espionage	APT12	China
December 2014	Actors with a North Korea nexus leveraged WHOAMI wiper against a South Korean nuclear facility in December 2014. The intrusion did not impact facility operations (15-00001060, 17-00002192).	Computer Network Attack	N/A	North Korea
October 2014	ICS-CERT published details of a Sandworm Team campaign leveraging BlackEnergy2 malware to target internet-connected HMIs by exploiting vulnerabilities in the software (Intel-1289248, Intel-1273358).	OT-Targeted Espionage	Sandworm Team	Russia
November 2014	A group calling itself the Guardians of Peace compromised an entertainment company using DESTOVER wiper malware. The group wiped data from 3,262 of 6,797 personal computers, erased 4,099 hard drives, and erased data from 837 of the company's 1,555 servers. A public FBI statement indicates actors with a North Korea nexus are linked to the incident (Intel-1300397, Intel-1314858, Intel-1311691, 17-00002192, 17-00003421).	Computer Network Attack	N/A	North Korea
July 2014	Threat actors we track as Koala Team deployed HAVEX, aka PEACEPIPE or FERTGER, through a strategic web compromise focused on energy-related websites and trojanized OT utilities (Intel-1153508, 14-00000172). HAVEX actively scans OPC servers, a client/server technology widely used in industrial control systems (ICS).	OT-Targeted Espionage	Koala Team	Russia
	Media reports indicate the Iranian			

February 2014	Government sponsored a destructive compromise leveraging wiper malware against a U.S. casino company.	Computer Network Attack	N/A	Iran
June 2013	South Korean government and commercial targets were hit with wiper malware, Castov. This data destruction was part of a broader wave of North Korean threat activity that also included distributed denial-of-service (DDoS) attacks, website defacements, and data breaches (Intel-874824, 13-26579, 17-00002192).	Computer Network Attack	N/A	North Korea
March 2013	Threat actors with ties to North Korea successfully targeted South Korean media and financial entities. Operators leveraged the DarkSeoul (aka Jokra) wiper to delete critical system files and damage up to 30,000 systems. The timing of the campaign coincided with heightened political tensions between both countries due to disagreements regarding North Korea's nuclear programs and missile development (Intel-780278, 13-24908, Intel-791408, Intel-1130370, 16-00006676).	Computer Network Attack	N/A	North Korea
October 2012	We responded to an intrusion at an energy company where we identified both APT1 and APT24 (16-00007016). The threat actors appeared to seek information pertaining to the company's processes and technologies. Both actors compromised one of the company's OT applications; however, we cannot confirm whether the threat actors intentionally targeted the system because of its OT applications.	OT-Targeted Espionage	APT1, APT24	China
September 2012	Telvent, an industrial automation software provider, interrupted its operations in the U.S., Canada, and Spain after discovering evidence of a network intrusion. Officials from Schneider Electric, Telvent's parent company, stated that the threat actors responsible for the breach stole information pertaining to customer projects involving the use of Telvent's OASyS SCADA product for remote system monitoring and control (16-00007016).	OT-Targeted Espionage	APT1	China
August 2012	A previously unknown group, the Cutting Sword of Justice, claimed responsibility for a campaign targeting Saudi Arabian Oil entities with Disttrack (aka Shamoon) wiper malware. Given the sophistication of the incident, we do not believe a hacktivist group was responsible for the incident (Intel-628750, 12-21704, 16-00006862, 16-00019328).	Computer Network Attack	N/A	Iran
	We reported that the OT security firm Digital Bond was sent a spear-phishing email from an actor claiming to be Dale Peterson, the founder and CEO of			

June 2012	Digital Bond. Digital Bond is a well-known OT security company that had made recent headlines for its vulnerability disclosure efforts, namely the PLC-hacking "Project Basecamp" (Intel-590310).	OT-Targeted Espionage	APT1	China
May 2012	The U.S. Government reported that a China-nexus cyber espionage campaign targeted the OT networks of a U.S. oil and natural gas pipeline. 23 U.S. natural gas pipeline operators were reportedly targeted in a spear-phishing campaign, and at least 13 were successfully compromised. Several OT networks were successfully accessed in these compromises, although there were reportedly no attempts to modify operations (Intel-578154, 21-00016485).	OT-Targeted Espionage	APT1	China
July 2011	We reported that APT1 targeted and successfully exploited the networks of a company involved in rare earth metal extraction and manufacturing. There were strong indications that the victimized firm's OT was compromised, including system commands using the strings "OPERATO," "Plantadmin," and "HMI" (Intel-436536).	OT-Targeted Espionage	APT1	China
March 2011	In an attack generally attributed to North Korea, the Koredos malware facilitated DDoS attacks against many of the same websites as the previous Dozer malware. The malware also had destructive capability, which it reportedly used against nearly 200 infected computers (Intel-370167, 13-26579).	Computer Network Attack	N/A	North Korea
July 2009	In an attack generally attributed to North Korea, the Dozer malware infected computers and conducted DDoS attacks primarily against South Korean government websites. Malware could then corrupt the hard drives of infected machines (13-26579).	Computer Network Attack	N/A	North Korea
July 2009	A compromise leveraged STUXNET malware at an Iranian nuclear facility in 2009. The incident disrupted the PLCs controlling centrifuges, causing the equipment to fail. The compromise is generally attributed to the U.S., and there is also public speculation regarding Israeli involvement in the incident (17-00002192, 18-00020235).	Cyber Physical Attack	N/A	U.S., Israel

Table 1: Selected state-sponsored threat activity

Please rate this product by taking a short four question survey

Threat Intelligence Tags

Actors

- APT12
  Aliases

    - APT 12
    - APT-12
    - APT12
- APT37
  Aliases
    - APT 37
    - APT-37
    - APT37
- APT38
  Aliases
    - APT 38
    - APT-38
    - APT38
- APT28
  Aliases
    - APT 28
    - APT-28
    - APT28
- APT33
  Aliases
    - APT 33
    - APT-33
    - APT33
- Koala Team
  Aliases
    - Koala Team
- TEMP.Tick
  Aliases
    - TEMP.Tick
- TEMP.Hex
  Aliases
    - TEMP.Hex
- APT24
  Aliases
    - APT 24
    - APT-24
    - APT24
- APT5
  Aliases
    - APT 5
    - APT-5
    - APT5
- UNC2743
  Aliases
    - UNC 2743
    - UNC-2743
    - UNC2743
- Sandworm Team
  Aliases
    - Sandworm Team
- UNC2452
  Aliases
    - UNC 2452
    - UNC-2452
    - UNC2452
- APT41
  Aliases
    - APT 41
    - APT-41
    - APT41
- TEMP.Hermit
  Aliases
    - TEMP.Hermit
- APT10
  Aliases
    - APT 10
    - APT-10
    - APT10
- APT1
  Aliases
    - APT 1

    - APT-1
    - APT1
- TEMP.Isotope
  Aliases
    - TEMP.Isotope
- APT34
  Aliases
    - APT 34
    - APT-34
    - APT34
- UNC2448
  Aliases
    - UNC 2448
    - UNC-2448
    - UNC2448
- UNC2428
  Aliases
    - UNC 2428
    - UNC-2428
    - UNC2428

Affected Industries

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Construction & Engineering
- Energy & Utilities
- Legal & Professional Services
- Oil & Gas
- Pharmaceuticals
- Transportation

Affected Systems

- Users/Application and Software
- Control Systems and Applications
- Industrial Network Protocols

Intended Effects

- Military Advantage
- Political Advantage
- Disruption
- Degradation
- Destruction
- Interference with ICS

Motivations

- Military/Security/Diplomatic

Malware Families

- BADRABBIT
  Aliases
    - BADRABBIT
- SOGU
  Aliases
    - SOGU
- TRITON
  Aliases
    - TRITON
- SHAMOON
  Aliases
    - SHAMOON
- RUHAPPY
  Aliases
    - RUHAPPY
- INDUSTROYER
  Aliases
    - INDUSTROYER
- COLDLOCK

Aliases
    - COLDLOCK
- SALTYBOAR
Aliases
    - SALTYBOAR
- HERMES
Aliases
    - HERMES
- ZEROCLEAR
Aliases
    - ZEROCLEAR
- VPNFILTER
Aliases
    - VPNFILTER
- KILLDISK
Aliases
    - KILLDISK
- PEACEPIPE
Aliases
    - PEACEPIPE
- MONKEYCHERRY
Aliases
    - MONKEYCHERRY
- POISONPLUG
Aliases
    - POISONPLUG
- DUSTCOVER
Aliases
    - DUSTCOVER
- SOURGRAPES
Aliases
    - SOURGRAPES
- BOOTWRECK
Aliases
    - BOOTWRECK
- WANNACRY
Aliases
    - WANNACRY
- BLACKENERGY
Aliases
    - BLACKENERGY
- LOCKBIT
Aliases
    - LOCKBIT
- WHITEROSE
Aliases
    - WHITEROSE
- DIRTPYLE
Aliases
    - DIRTPYLE
- WHOAMI
Aliases
    - WHOAMI
- DUSTMAN
Aliases
    - DUSTMAN
- DOGCALL
Aliases
    - DOGCALL
- SUNBURST
Aliases
    - SUNBURST

Source Geographies

- China
- Iran
- North Korea
- Pakistan
- Russia
- United States of America

Tactics, Techniques And Procedures (TTPs)

- Network Reconnaissance
- Malware Propagation and Deployment
- Hardware/Supply Chain Compromise
- Ransomware

Target Geographies

- Global

Targeted Information

- Intellectual Property
- Credentials
- IT Information