An Analysis of Malware Threats Facing the IoT:
A taxonomy of IoT malware

Mr Ross Heenan
Cybersecurity and Computing
Abertay University
Dundee, United Kingdom
email: r.heenan@abertay.ac.uk

Prof Ian Ferguson
Cybersecurity and Computing
Abertay University
Dundee, United Kingdom
email: i.ferguson@abertay.ac.uk

Dr Laith Al-Jobouri
Games technology and maths
Abertay University
Dundee, United Kingdom
email: l.al-jobouri@abertay.ac.uk

Abstract – **From its origins in "Weiser's vision" in the 90's there has been widespread adoption of Internet of Things (IoT) technologies across consumer, commercial, industrial, logistics, utilities, and healthcare environments. This has brought with it an expansion and rise in vulnerabilities and malware threats due to an increase in potential vectors of attacks and the general discovery, privacy and security issues facing IoT solutions. Many IoT systems across these sectors contain a mixture of Information Technology (IT) and Operational Technology (OT) network segments and many existing legacy networks of systems have incorporated or adopted IoT components or services into their networks. These are generally built with compatibility and operability in mind with security usually less considered or as an afterthought. A large variety of IoT malware exists including botnet and Denial of Service (DoS) variants, brickers, cryptominers, ransomware, stalkerware and Industrial Controller Systems (ICS) malware variants and there can also be significant threat leveraged from IoT malware to certain critical systems or services being controlled or monitored. Threats can also be leveraged from a compromised IoT system and used for deployment of threats including DoS reflection or amplification attacks. The research presented here provides a review and threat analysis of the varieties of IoT malware that currently exist with a case analysis and comparison of two high profile ICS capable targeting malware known as BlackEnergy and Industroyer. These variants were responsible for the attack and compromise of energy utilities providers networks in Ukraine between 2014 and 2022 and show examples of malware threats using different routines to gain compromise of critical ICS systems.**

Keywords – IoT Malware; IoT Threat analysis; IoT security; BlackEnergy; Industroyer

I. INTRODUCTION

Malware has remained a persistently increasing threat to computer systems and networks from the first computer worms and viruses in the 1980's, to the evolution of variants utilising more advanced techniques including fileless deployment, process ghosting or hollowing or targeted Common Vulnerability Exposure (CVE) use in more recent years. The past four decades have seen the birth of the internet, the .com boom of the 90's, the emergence of Cloud computing and Blockchain technologies, revisiting Artificial Intelligence (AI) technologies and the introduction of IoT. This has brought an evolution in types of threat and seen the emergence of targeted types of malware including ransomware, stalkerware, brickers, cryptominers and ICS malware among others. IoT has seen rapid growth in recent years with mass adoption of IoT solutions into many aspects of life including automotive, consumer, commercial, industrial and healthcare solutions with estimates of over 14 billion devices to be in use by 2023 [2]. A significant fraction of these are estimated being deployed as consumer products, utilities management and monitoring solutions and also automotive, asset and logistics tracking and management and monitoring solutions. Cisco also estimates a future global market value of around $14 trillion [3]. Thus, there is a clear requirement for priority of provision in appropriate protection for these assets.

There are many challenges in developing and maintaining an effective security posture for IoT systems or networks including lack of capability or availability of computational resource, ensuring compatibility for cross platform systems and technologies or other constraints concerning case specific operational or environmental requirements. The adoption of numerous communications technologies and protocols, such as purpose built lightweight protocols like Low Power Wide-Area (LPWA) or Long Range Wide-Area (LoWRAN) and also the wider use of communication protocols in general including Cellular communications like 3, 4 and 5th Generation (5G), Narrow-band IoT (NB-IoT), Extended Coverage GSM (EC-GSM), Satellite, Long-Range (Lora), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Multicast DNS (mDNS), Bluetooth, ZigBee and various others means there is a wider footprint to consider in terms of consideration of threat and provision of secure systems and network communications.

Since the emergence of IoT technologies there have been significant and growing numbers of vulnerabilities and cases of exploitation being identified or reported concerning IoT systems or solutions [4]. The common types of threat being initially targeted and leveraged in these cases include ransomware, Distributed DoS (DDoS), brickers, botnets and also cross-platform malware or threats, many of these were able to be leveraged due to lack of awareness in implementing appropriate security mechanisms and often products of insecure development practice in the products themselves [4]. Insecure development practices include the use of insecure, predictable or hardcoded default settings or credentials and the use of insecure technologies or ecosystem interfaces, such as Application Programming Interface (API's).

Whether an IoT system is targeted in a consumer, commercial, industrial, healthcare or other type of setting there can be a variety of severity of threat facing it ranging to severe and even life-threatening from potential compromise. There has been widespread incorporation of IoT solutions in sensitive or critical settings across industry sectors including utilities, industrial and healthcare. In these settings, one vulnerable IoT endpoint could allow for propagation of threat which dependent on the system concerned could manifest into a significant increase in damage or disruption. There have

already been severe examples of the exploitation of critical IoT systems through the use of malware. One of the first recognised examples of this would be the Stuxnet incident in 2010 where malware was used to compromise critical ICS systems in an Iranian Nuclear facility [64] in Natanz, with many researchers and officials suggesting the incident being attributed to a collaborative operation between United States and Israeli forces.

A more recent example of the use of malware in compromising IoT systems is the Mirai botnet malware which was reported in one instance to have compromised around 300,000 devices to leverage a botnet to deploy various DDoS flooding attacks that were reported to reach volumes of over 1 Terabits per second (Tbps) [19]. Other examples include the Bricker malware variants Brickerbot and Silex that corrupt or overwrite areas of compromised devices to leverage DDoS or Permanent DoS (PDoS) or ICS capable targeting malwares including the Lemonduck, Industroyer or BlackEnergy variants. These will be discussed further in the following sections of the paper.

Due to the varied nature of the IoT landscape and also the widespread use of certain types of devices or technologies, another factor of compounded threat is the increasing emergence of CVE threats against widely used software, hardware or communication technologies like Wireless, 4G, 5G or Bluetooth. A good example of this is the recently discovered vulnerability in the Thales m2m module (CVE-2020-15858) [5], which is widely used in Wireless IoT technologies. Vulnerable widely used software has also been shown to be an example of this in the various OpenSSH vulnerabilities [6] that allow compromise of endpoints for use in generation and forwarding of malicious traffic or the recent Key Reinstallation Attack (KRACK) vulnerability [7] that allows reinstallation of cryptographic keys to hijack wireless connections. There have also been vulnerability disclosures in Bluetooth technologies, such as the Bluetooth Impersonation Attacks (BIAS) [8] or Key Negotiation of Bluetooth (KNOB) [9] CVE disclosures and also vulnerabilities in cellular technologies including potential interception and eavesdropping through exploitation of the Recovering encrypted Voice over LTE (ReVOLTE) vulnerability [10] or other methods.

Another significant issue is the emergent threat to IoT systems of cross platform malware, these variants have the ability to compromise different architectures and types of systems. Combination of such variants with bricker or ransomware payloads could represent a notably increased threat to an IoT system. Malware targeted at IoT presents a heightened threat towards potential intrusion through a single vulnerable endpoint's presence, a wider variety of potential CVE threats and a likely increased number of devices to target. This all provides a much larger threat surface that malware authors are capable of utilising in targeting and development of a malicious threat payload in order to translate to as substantial compromise as possible which can often amount to the compromise of millions of IoT devices. There has already been a collection of malware threats discovered successfully leveraging exploitation of IoT systems, such as bricker variants including, Brickerbot [11] and Silex [12], botnet malware including Mirai [13] or Hajime [14] and also ICS or Supervisory Controller and Data Acquisition (SCADA) threat capable malware including the LemonDuck [15], Industroyer [16] and BlackEnergy [17] variants.

Malware threats are capable of deployment against a target using a wide range of exploitation methods with popular techniques including the use of Remote Code Execution (RCE), process injection techniques or fileless compromise methods, or the use of social engineering, phishing campaigns or Hypertext Markup Language (HTML) smuggling to leverage deployment of malicious payloads [20].

It is also important to note that some variants will use what is known as a zero day, this is an exploitation method that has not been previously observed or recorded.

There are various methods that can be used for the analysis of malware, these are categorised into static, dynamic and hybrid techniques. Static analysis of a malware source is where a malware payload is analysed using passive techniques like hashing and file header, strings, dependencies and source analysis. Dynamic analysis of a malware source will utilise behavioural analysis techniques to monitor system and network activity during the malwares execution. There are also hybrid analysis methods that utilise other advanced techniques like disassembly where the source code can be reverse engineered and memory analysis or debugging which will allow live interaction with a running program or in this case malware. These methods allow extraction of evidential artefacts, such as hashes of unique signatures of files and Indicators of compromise (IOC's) which are unique system or network evidential artefacts that show evidence of compromise. These can be used to create what is known as Yara detection rules which can be used by Intrusion Detection Systems (IDS) and Anti-virus software as detection rules for classification. Using dynamic methods like memory or behavioural analysis and reverse engineering the tactics, techniques and procedures (TTP's) used by a malware threat can also be distinguished which again can be used for response, classification and detection.

IoT malware has the advantage of being able to target a larger threat surface in exploitation of IoT systems, this is due to the larger numbers of limited capability devices which constitute a typical IoT architecture and also a wider variety of hardware, software or networking technologies being present to target in comparison to a traditional computer network.

This can result in a higher potential in commonality of presence of vulnerable software, hardware or network technology components due to the increased amounts of devices or components in some IoT systems. This can create the potential for the threat to be exponentially increased particularly the more evolved that IoT malware variants become. The FLocker [42] Android ransomware, Trickbot [43] botnet malware and the LemonDuck [15] [44] cryptomining malware are recent examples of these types of evolving malware with modular or advanced capabilities.

There have been sustained discoveries of vulnerabilities across consumer, commercial, industrial, healthcare and other IoT products in recent years with various high-profile vendor products being concerned including Amazon [26], Apple [27], Fitbit [28], Google [29] [30] and Ring [30]. There have also been vulnerabilities discovered in various automotive manufacturers products, such as BMW [32], Chrysler [33], Ford [34], Honda [35], Jeep [33] and Tesla [36] vehicles that allowed intrusion through keyless hacks or replay attacks, compromise of the vehicles Electronic Control Unit (ECU), hijacking control of the vehicles lights, wipers, locks,

dashboard readings and even the vehicle's steering, gearing, and braking controls.

The evolution of the IoT has seen with it the emergence of a variety of malware threats including botnets, cryptominers, brickers, and ransomwares with recent case examples including the well-known and now evolved Mirai botnet malware [21], the Darlloz and Muldrop cryptominer malwares [22], the Brickerbot [23] and Silex [22] bricker malware variants and also recent ransomware compromises against high profile consumer targets including the WastedLocker Ransomware [24] used in the attack against Garmin in 2020 [25].

Many initial examples of compromises were often products of insecure development or deployment, however there is also an increasing use of CVE's [62], zero-day threats or more advanced threat vectors being utilised for example cross-platform malware or complex malware with modular or advanced capabilities [15] [45] [46] [47].

An additional concerning threat to the IoT is the emergence of collections of vulnerabilities identified in widely used Transmission Control Protocol/Internet Protocol (TCP/IP) stack libraries by IoT devices. These include the Ripple20 [37], NAME:WREK [38], NUCLEUS13 [39], ANMESIA33 [40], and URGENT/11 [41] disclosures. These collections of threats contain differing amounts of vulnerabilities in a number of vendors products including HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxte and many others across medical, transport, industrial, commercial, utilities, and consumer IoT products. These concern CVE's in protocol or TCP stack vulnerabilities that allow leveraging of DoS, corruption of memory and code execution capabilities against a target and are estimated to amount to billions of devices being at risk.

The collection of previously discussed issues presents an expanded threat surface facing these environments which can imply an increased severity or wider propagation of threat to a target network through the presence of a single vulnerable endpoint making malware a more pervasive threat to IoT systems or networks in comparison to traditional computer networks.

This paper aims to present a review of the variance of the malware threats facing the IoT and provide understanding of the evolvement of the threat landscape and the range and severity of potential compromise possible.

This will be achieved by providing a taxonomy of the range of existing IoT malware threats in a review of emergent trends and research with analysis of example variants and a case study of analysis of two recent significant malware threats to industrial IoT in the BlackEnergy and Industroyer malware variants. This research aims to provide the reader with an awareness of the malware threat landscape facing the IoT and an awareness of the capabilities that these variants of malware can possess. It also aims to improve levels of confidence in capability of analysis and ability of identification of countermeasures or advisory measures if performing analysis of similar types of threats.

The remainder of this paper will be structured as follows, the following section will look at an examination of related academic literature. Subsequent sections will include a case study analysis section looking at the analysis of two IoT malware variants. This will be followed by a discussion section providing summative and critical discussion of the research explored and the findings after which a short conclusion section is provided.

II. LITERATURE REVIEW

The following section will review related research in the fields of IoT malware and attacks against IoT solutions as well as recent proposed approaches or solutions for detection and analysis of IoT malware.

A particular issue with malware threats and analysis is attribution. Research by Jinchin Choi et al [60] looks at the area of IoT malware with a concentration on vulnerable endpoints and dropzones used in the deployment of malware threats to IoT endpoints. The study uses 2.423 IoT malware samples from 4 families of malware including Gafgyt, Tsunami and LightAidra [61]. By reverse engineering the samples using the Radare2 open-source framework and other tools including Censys, Shodan and UltraTools the extraction of strings provided identification of dropzones and target IP addresses. These were used to identify patterns or commonalities in geolocation or ports and services used in the samples and also to identify commonalities in targeted CVE threats.

A dropzone is an area of network address which is categorised and grouped by geographical location. Dropzone addresses were identified and categorised through entries noted as being linked to specific data transfer technologies. Target network addresses are listed also. These addresses are then grouped by the family of malware. This helps to identify common Indicators of compromise IoC's and highlights the potential implications that a compromise can have in regard to the scale or severity depending on the system compromised and highlights how large scale distributed and decentralised attacks can be enabled through propagation, amplification or reflection. It is important to identify IOC’s as these can map to suspicious or malicious host, network or file-based behaviours and dictate the level of potential severity an exploitation of these is capable of. Some of the dropzone address are noted as not having current data, this could mean that some of these are networks could have either been taken down or modified due to being previously compromised but also as the study notes this can mean that a dropzones operation can be dynamic or "short-lived - long enough to carry out an attack and short not to be detected". This highlights that the speed of analysis is important to ensure the most complete and accurate understanding of activity and behaviour can be captured.

A large number of target network addresses are noted as being shared between dropzones potentially due to attackers using the same methods of acquiring targets or this could also be possible due to the same malware being hosted or passed from different dropzones. This research provides a good understanding of the types of vulnerability being exploited in IoT endpoints and shows the top 5 dropzones per number of target IP addresses include the UK, US, Canada and France. The results also showed a large distribution of US based target entries pointing to China, Vietnam and Brazil. Research from Imperva Incapsula states that these 3 countries were heavily affected by compromises from the Mirai botnet malware. This is useful as it allows patterns in targeting and deployment used by the 4 malware families to be identified. The analysis is useful but is considered limited due to the restricted and slightly dated collection of variants used.

The broad subject of IoT Attacks and Malware is explored in research by Anand Mudgerikar and Elisa Bertino in [2], the work explores the types of existing malware and the methods of exploitation they use in attack and classifies types of attack

on IoT systems and networks into the categories of Passive/Information Stealing Attacks, Service Degradation Attacks and botnet-based attacks. The study notes the emergence of variants of IoT ransomware or jack-ware and that these variants of malware differ from traditional variants that will simply perform a DoS until the demanded ransom payment is provided. Many of the emerging examples will generally perform full-disk encryption or overwrite critical areas of memory to completely disable the system or service. This is bricker malware, the recent Brickerbot and Silex variants are two of the first examples of this type of variant. The research also provides further analysis of the methods used in the exploitation of IoT targets by malware categorised as Degradation based attacks, Network level attacks and Application-level attacks.

The work presents an informative look at some of the types of existing threat and variants of malware facing IoT systems and networks. Jamming, Node Tampering, Tag cloning, such as Radio Frequency Identification (RFID) and Injection are noted as types of Degradation-based attacks. Insider based attacks, Sinkhole, routing, flooding, injection and authentication-based attacks are listed for Network level attacks and for Application-level based attacks list flooding and types of malware including cryptomining, ransomware and brickers as being common trends. One recommendation is the use of AI based IDS solutions for detection of components or patterns from kill chains and identification of reconnaissance, intrusion, exploitation, lateral movement, obfuscation, or ex-filtration parts of an attack, although this type of capability is not always available.

In "An Analysis of the use of CVE's by IoT Malware" by Raphaël Khoury et al [62], research explores an analysis of 27 variants of IoT malware that have emerged between 2008 to 2019 with the concentration on their use of known or recorded threats known as CVE's. Thirteen of the variants analysed used methods such as dictionary attacks, abuse of insecure development features or default configurations and 1 variant used an unrecorded vulnerability exposure although it may just be that the CVE is not contained in the database or data source used.

The main types of threat recorded as being leveraged against IoT systems are identified as being DoS, sabotage, espionage and cryptomining. A list of botnet malware is also provided with the concerned CVE's that they target. From the results gathered the authors note that it is common for malware developers to consult CVE databases to identify exploitation methods for use in development of IoT malware payloads. This has become more prevalent since 2016 and there appears to be a trend towards the use of less complex CVE's to leverage compromise with just 3 of the samples in analysis having a high complexity score for execution for the Common Vulnerability Scoring System (CVSS). This means more variants are utilising techniques that will allow low to zero touch interaction in order to be successfully deployed against a target. There are 2 versions of the CVSS system that are used, these are V2 introduced in 2007 and V3 introduced in 2015. Out of the samples analysed, 92.1% scored against the V2 system and 93.8% of samples scored against the V3 system show the use of CVE's that do not require user interaction to leverage. A common technique used by hackers is to look for low hanging fruit and to be able to leverage exploitation with the most ease and least noise or interaction with the most expansive coverage. The top Common Weakness Identification (CWE) listed as being compromised by malware include improper input validation, improper control of generation of code, improper neutralization of special elements used in an Operating System (OS) command, improper neutralization of special elements used in a command, improper restriction of operations within the bounds of a memory buffer and improper authentication. These account for 67% of cases showing that there is a significant issue with regard to insecure development and operational practices in the deployment of IoT solutions.

Another analysis of IoT malware threat is provided by Ibrahim Gulatas et al in [63], this provides the analysis of samples of 64 IoT malware families that have been identified between 2008 and 2022 looking at the variance of features including the architectures targeted, deployment methods, vectors of attack and methods of persistence. 80% of the malware samples offered botnet capabilities with the other 20% using sabotage, cryptomining or data exfiltration techniques, 19% of the samples contain multiple threat payloads or have multiple threat capabilities. 49 and 48 of the 64 samples variants target the Advanced RISC Machine (ARM) and Microprocessor without Interlocked Pipe Stages (MIPS) processor architectures with 41 targeting Intel based architecture. The research provides an informative summary of the 64 IoT malware variant families covered organised by the previously mentioned categories and also the types of consumer, commercial and industrial IoT devices that each malware is known to target. This is a valuable piece of research that allows reviewal and comparison of the collection of IoT malware variants covered and their adversary behaviours. Many of the example variants covered deploy botnet or cryptominer threat payload capabilities in compromise of a target, with other variants objectives being focused on espionage or data exfiltration activities against targets and also a few variants identified with bricker payloads. These identified variants are capable of targeting a wide range of types of IoT devices including Digital Video Recorder's (DVR's) and IP or webcams, Routers, Network Attached Storage (NAS) devices, toys and also SCADA control systems. Notably, the Hydra and ChuckNorris malware variants discovered around 2008 were some of the first identified examples of malware targeting IoT devices, these both used Internet Relay Chat (IRC) based, Command and Control (C&C) servers and dictionary attack methods against insecure services present on targets to leverage botnet capabilities including further propagation of threat payloads or deployment of DDoS attacks. Later examples including Gafgyt in 2014 and Mirai in 2016 were also capable of targeting IP cameras, NAS devices and DVR's to leverage botnet compromise.

One of the first IoT cryptominer malware identified around 2013 named Darlloz targeted set top boxes, toys and webcams devices and used a PHP Hypertext Processor (PHP) Common Gateway Interface (CGI) vulnerability to leverage RCE on the target device to mine cryptocurrency. Bricker malware variants, such as the Brickerbot malware identified around 2017, used various threat vectors to target smart bulbs, toys and webcams and are also noted as an emergent trend in more destructive malware. One other variant of note is the VPNFilter malware identified around 2018 that is capable of targeting SCADA control systems in order to leverage hijacking or Man in The Middle (MiTM) capabilities or bricking of the target device by overwriting critical operational areas of memory to leverage Permanent DoS (PDoS). Other interesting findings from the research include

proposal of the identification of four main malware families of Hydra, Tsunami, Gafgyt, and Mirai to be established as initial parent families in the evolution of development of IoT malware and as milestones with many of their behaviours or features being adopted by emerging variants.

A good point noted in the research is the emergence of cross-architecture malware that contain different payloads where required for targeting different Central Processing Unit (CPU) architectures, this presents a significant issue for detection of a signature of the malware as there will essentially be different signatures for the same variant through mutation of the signatures dependent of the CPU architecture of the target environment. This combined with the increasing variance in attack vectors along with the adoption of more advanced methods of obfuscation and communication present significant challenges for future intrusion detection for IoT systems and networks.

A timeline of historical Cyberattack incidents against ICS networks is provided by Kevin Hemsley and Ronald Fisher in [64], this work presents a timeline of significant Cyber incidents against Industrial Control Systems or Industrial IoT (IIoT) between 2010 and 2017, a number of these cases discussed in this following section involved significant or widespread compromise through the use of malware and also provide a good perspective of examples of relevant cases of malware threat against industrial IoT systems.

A. Stuxnet – 2010

One of the first suggested uses of state sponsored Cyber warfare against an industrial facility was reported in 2010, this was an operation that is proposed by many researchers and officials to be attributed to US and Israeli allied forces [68]. This deployed a Cyber-attack operation using the Stuxnet Malware against the Natanz Nuclear facility in Arak, Iran with the aim to disrupt or disable their nuclear weapons production capability, this was also known by the codename Olympic Games.

The attack exploited zero-day vulnerabilities in the Windows 7 Server Message Block (SMB) protocol and Siemens SCADA controller software technologies using a worm malware deployed from a removable Universal Serial Bus (USB) device. The malware established propagation of threat through the deployment of a rootkit and the use of fraudulently obtained digital certificates to allow further propagation of threat to be deployed from a remote C&C server. It also used other methods of evasion including injection of false data to provide legitimate looking readings from the Programmable Logic Controllers (PLC's) to the Human-Computer Interface (HCI) whilst performing covert corruption of the controllers of the facilities uranium hexafluoride centrifuges to instruct them to run a speed's that exceeded their operational capacity [64]. This resulted in reportedly a fifth of the centrifuges being damaged and failure of the facility and in turn the uranium enrichment program and marks one of the first recorded uses of state sponsored cyber threat to cause significant damage to critical infrastructure in a conflict setting [18].

B. Night Dragon – 2010

Also in 2010, a malware named Night Dragon was used to target oil and energy companies through phishing campaigns that deployed compromise of the Windows Active directory and operating system to allow for privilege escalation and propagation of threat through the injection of a Remote Access Trojan (RAT). This enabled further compromise and sensitive data exfiltration through Dutch and US based C&C servers [18]. Whilst this malware did not directly compromise the IoT or industrial control systems it could have allowed hijacking of the Human-Machine Interface (HMI) of the control systems through the remote desktop capabilities using the RAT component and highlights that there are various vectors of attack that can be used in order to gain compromise of such critical systems. A similar example of this type of vector of attack is the Duqu malware that appeared shortly after the Night Dragon variant in 2011 [18] [64].

C. Shamoon – 2012

Another variant similar to the Night Dragon and Duqu malwares was the Shamoon malware that targeted energy industry giants including RasGas and Saudi Aramco in 2012, along with intrusion and compromise to exfiltrate sensitive information the Shamoon variant caused destruction to the Master Boot Record (MBR) partition table and storage space by overwriting them with random data effectively disabling systems [68]. The malware also presented a graphic of a US flag on fire on the compromised system. In August 2012, Saudi Aramco were attacked with around 30,000 systems reported to be compromised. About a week and a half later RasGas were compromised by the malware. Further attacks were reported against Saudi Arabia's civil aviation agency in 2016 which reportedly resulted in the loss of data from thousands of systems [18] [64]. Again, this malware did not provide the direct compromise of ICS or IoT systems although it did provide the potential to be capable of this through an indirect vector of attack.

D. Havex – 2013

Another malware that has targeted ICS systems around 2013 is a RAT malware named Havex. This variant was capable of enumeration of systems, shares and ICS devices through exploitation of the Distributed Component Object Model (DCOM) based version of the Open Platform Communications (OPC) protocol. It was also capable of using a C&C server to propagate further exploitation. A threat actor tracked as EnergeticBear who are linked to Russian state intelligence services are proposed as being connected to the malware campaign. This shows another example of these types of attacks being proposed as being attributed to or deployed by state sponsored or linked actors and the capability to compromise critical infrastructure environments [64].

E. BlackEnergy – 2014

A malware variant named BlackEnergy was identified targeting the HMI's of ICS systems of the Ukrainian utilities provider Prykarpattyaoblenergo in 2015. The malware was proposed to be linked to a threat actor group affiliated with Russian intelligence services tracked as Sandworm and was suggested to have been active since 2011 and targeted multiple ICS vendors including Siemens and General Electric (GE) [64]. The malware carried out enumeration of shares and local or removable storage in order to attempt propagation of threat and DDoS attacks to disrupt services. A further variant of the malware identified as BlackEnergy3 with extended capability was reported to have compromised a further Ukrainian energy facility to cause an outage

resulting in mass blackout [17] [73]. This malware was also reported to have been successful in targeting rail and mining infrastructure in Ukraine [68]. The attack was reported to have lasted a few hours and may not seem long, but it should show that the potential damage that an attack of this type could cause could be catastrophic.

F. Industroyer – 2016

In December 2016 a second attack against another Ukrainian utilities provider occurred using a variant of malware tracked as Industroyer or CRASHOVERRIDE [64] [68]. The malware used a firmware rootkit, hijacking of Virtual Private Network (VPN) connections and modules that target ICS specific protocols including the International Electrotechnical Commission (IEC) 101, 104, 61850 and OPC protocols to leverage compromise and also provided support for targeting Distributed Network Protocol 3 (DNP3) [15]. The malware targeted circuit breakers of Remote Terminal Units (RTUs) in substations with the aim of causing sustained outage to Uninterruptible Power Supply (UPS) controllers by causing circuit breakers in 30 substations to trip reportedly affecting around 225,000 customers resulting in mass outage of services in Kiev. Similar to the BlackEnergy3 attack in 2015, technical help services were targeted with DoS at the same time as the malware deployment to hinder any assistance being acquired and to maximise the effect of the outage which was reported to have lasted a few hours [69].

G. NotPetya – 2017

In 2017, the NotPetya malware was identified as being responsible for one of the most economically destructive Cyber-based attacks in history across the Ukraine with reportedly around 10% of the computer systems in the country being compromised along with economic damage amounting to 0.5% of the Ukraine's Gross Domestic Product (GDP). Similar to the Petya malware the NotPetya variant used the EternaBlue and EternalRomance exploits to leverage access and carried out encryption of target systems however the NotPetya variant differed in that its aim was to corrupt systems by carrying out irreversible encryption of compromised targets MBR's in turn disabling the compromised system from booting [64]. The malware also targeted middle eastern Industrial control safety systems and many others with victims across airline, banking, government, healthcare and utilities sectors identified across 65 countries. Some of the high-profile targets compromised included FedEx, Maersk and Rosneft with damage estimations proposed of around $10 billion [68]. The NotPetya malware was again proposed to be linked to Russian state backed or affiliated threat actors the Sandworm group [48].

H. Triton/Trisis – 2017

Also in 2017, Cyber security analysis firms Symnatec and FireEye along with others reported the emergence of a malware variant known as Triton, Trisis and also HatMan. The threat framework targeted Middle eastern Industrial control safety systems with the aim of compromise of safety instrumented systems of the manufacturer Schneider Electric's Triconex [68] [49].

Triton was capable of modification of the in-memory firmware of the targeted device and injection of further malicious payload allowing access to memory contents, process corruption and RCE through malicious packet injection [70].

Triton is one of the first examples of a payload that targets specific types of industrial safety systems, this is particularly dangerous as it poses a significant threat to ICS systems and the safety systems defending them as well as the critical assets or human lives they are protecting [64]. The fact that more of these examples are being described as frameworks presents that the complexity and capabilities of these types of malware variants is significantly evolving.

Research in [65], by Shalia Sharmeen et al, looks at the security of mobile devices as part of an IoT network in particular the suspicious system and API calls and permissions that can be accessed by Android malware. The work notes various potentially suspicious system calls, permissions and API calls that's presence could be considered suspicious depending on the case. This is useful for developers or security practitioners unfamiliar with this.

Some of the suspicious system calls listed including UMASK, FCHOWN32, FSYNC, SYS224 and SYS248 could be of interest and potentially appear suspicious as it is common for malware to use uncommon or obscure routines or methods to attempt to carry out malicious operations in a stealthy manner. There are however various listed that are of clear commonly legitimate use with examples including MKDIR and CONNECT, RENAME and SOCKET. It also notes various potentially suspect API calls and permissions although many of these are genuinely used but could be of use to be aware of. Overall, the work does present a useful look at potentially suspicious system call presence in Android software.

A comparative analysis of five of the most high-profile malwares capable of targeting ICS systems is provided by Yassine Mekdad et al in [74] with a comparison of the Stuxnet, Havex, BlackEnergy2, CrashOverride, and TRISIS malware. The TRISIS malware is another example of ICS capable targeting malware that uses two CVE's (CVE-2018-7522, CVE-2018-8872) to target exploitation of Triconex safety systems [68]. The paper presents a two-layer approach of analysis of ICS malware with a cyber threat intelligence layer that maps indicators in the ICS kill chain of the example and a hybrid analysis layer of static and dynamic analysis. The solution uses Cuckoo sandbox to perform the automated Static and Dynamic analysis of the malware samples along with a threat analysis gathering stage to identify the "intrusion activities and their complexity" used in the example. This solution could prove to be valuable however the sandbox may present significant issues in versatile analysis of different samples aimed at varied or multiple architectures and may require development of a Sandbox environment specific to this.

Another useful approach for analysis of IoT malware is presented by Gaurav Pramod Kachare et al in [66], the research presents a solution that proposes to address the lack of presence of versatile sandbox environments for performing reverse engineering or analysis of IoT malware. There are some existing sandbox analysis solutions for IoT including v-sandbox, IoTPOT and Executable and Linkable Format (ELF) analyser although these solutions possess shortcomings in capabilities or some kind of constraint, such as being specifically scoped to ELF files, unable to perform a particular part of analysis or unable to address certain Anti-Virtual Machine (Anti-VM), Anti-debugging, evasion or

other advanced or unseen techniques presented by particular malware variants.

The challenge is to create the most legitimate and secure testing and emulation environment that allows a realistic execution environment to trick the malware into running and to allow the most legitimate and effective analysis potential. The research presents a conceptual design for a Sandbox solution for reverse engineering and emulation of IoT malware that allows static, dynamic and network analysis to extract features from the concerned malware sample. This research aims to provide solutions to address some of the previously noted shortcomings in existing solutions including providing the capability to be able to support emulation of multiple CPU architectures and performing advanced analysis of system and network data.

The proposed solution is capable of analysis of a malware sample using various static, network and real time or dynamic analysis techniques to extract features from the example, these features from the malware binary files are converted to 8-bit vector image files then to grayscale images generated from the grayscale vector values provided. Convolutional Neural Networks (CNN) are then used to attempt to provide accurate classification and generate automated reports.

It is arguable that the proposed solution is more effective than other known approaches in analysis, the research has promise in capability and for analysis of large batches of samples and it does appear to be more versatile compared to some existing solutions like v-sandbox, IoTPOT, IoTBOX and ELF analyser. Issues that could present challenges to the proposed solution include evasive or complex malware or zero-day threats and the ever-existing issue of false positive classification. The conceptual solution presented could provide a useful system that can attempt much of the heavy lifting in extraction of interesting or suspicious features from provided suspect malicious samples for further investigation.

A review of some of the recent approaches being explored in the detection of IoT malware is presented in the work by Sangeeta Kakati et al in [67]. The work notes that across IoT environments a significant percentage of devices use Android based operating systems including Electronic Chart Display and Information System (ECDIS) and Automatic Identification System (AIS) maritime systems, automotive solutions and also smartphones, watches, toys, smart television's as well as various other smart appliances.

The survey discusses various detection approaches discussed in recent research including traditional static, dynamic or hybrid analysis using feature extraction or analysis of suspicious Opcode, string patterns or API calls accompanied by machine learning classification techniques like Support Vector Machine (SVM), K-Nearest Neighbours (KNN) and fuzzy and decision tree methods with varying proposed classification accuracies of around 95 to 99%. It also discusses other machine learning assisted methods using Blockchain or CNN techniques. Blockchain technologies can be of use due to the distributed nature of ledgers which could present a useful resource that could assist in ensuring ease of access, portability and integrity of data or authentication in IoT settings. The study cites various methods for using CNN for classification. A method where the malware binary files are converted to 8-bit vector files then to grayscale images similar to the research in [66] is noted. These signature files were then processed with a CNN model with an accuracy of around 95 to 98% classification accuracy. While these methods are useful for batch or high-level analysis there would likely be issues in the analysis of cross platform malware or advanced variants using techniques like staged, polymorphic or metamorphic payloads.

Some of the examples discussed in the related works present useful areas in research and promising opportunities in the potential advancement in classification and detection of IoT malware. However, there remains problematic challenges of cross-platform variants, zero-day threats, false positive classification and the countering of obfuscation, anti-reversal and other deceptive or evasive measures employed by advanced threats.

Feature analysis or identification and classification of IoT malware studies also show that IoT malwares are becoming more complex advancing adversarial behaviours including smart and cross platform threats and poly and metamorphic payloads as the security of IoT systems and networks is beginning to be more considered.

III. CASE ANALYSIS

The following section will present an analysis of the BlackEnergy and Industroyer malwares and aims to provide a technical understanding of the two variants which are two of the most recent and significant malware threats to industrial IoT systems.

A. BlackEnergy

The BlackEnergy malware has evolved from the first variant in 2007 which primarily concentrated on the deployment of DDoS to further spamming and reconnaissance capabilities being provided in the second variant. The third generation has further evolved to support a modular architecture and significant Advanced Persistent Threat (APT) capabilities. Research by K. Stoddart in [68] notes the BlackEnergy2 threat as being "identified in energy-sector systems worldwide" around 2014 and was suggested to be primarily targeted at Ukrainian infrastructure with many intelligence and security researchers suggesting the threat being attributed or connected to the Sandworm group linked to Russian intelligence services.

The BlackEnergy2 variant appeared around 2010 and uses process injection and rootkit techniques to deploy its payload and provides an evolved modular structure with additional enumeration and reconnaissance abilities. This means the malware has expanded capabilities that can be deployed as required by target making the payload more efficient and also more complex to perform analysis for reverse engineers. It was used in an attack against Ukrainian power grid infrastructure in 2014 and was capable of targeting various vendor specific HMI products including Siemens SIMATIC, Advantech/Broadwin WebAccess and GE CIMPLICITY.

BlackEnergy2 is distributed through a malicious email attachment which deploys a Trojan containing 8 imported Dynamic Link Libraries (DLL's) and 164 functions and uses further propagation and privilege escalation to leverage authenticated connection to SCADA HMI's to allow injection of commands to open circuit breakers and cause outages.

The BlackEnergy3 variant employs a method of exploitation that targets abuse of the parsing of INF configuration files through a known CVE (CVE-2014-4114) in the Object Linking and Embedding (OLE) packager held in the Windows packager.dll that allows sharing of media between office and other applications. The vulnerability

allows possible injection of malicious macros to Microsoft Office documents with a potential to leverage RCE against the target. Microsoft has since patched this vulnerability however it is still a relative threat as it is still possible to engineer a target into enabling the macros in a file. BlackEnergy3 was listed as being present in a Ukrainian energy providers infrastructure that was victim to an attack in 2015 causing an outage in a report by the US department of Homeland security. It was used to perform 3 simultaneous attacks against substations of DTEK Kyiv Region Grids (formerly PJSC Kyivoblenergo) which opened breakers, corrupted hardware and performed DoS against response services. The attacks resulted in seven 110 kV and twenty-three 35 kV substations being disconnected for around three hours and caused outages for approximately 225,000 customers across 3 different providers.

An analysis of one of these attacks is provided by the Electricity information sharing and analysis center (ESIC) of SANS in [73] which suggests that a collection of factors contributed to the ease or capability of intrusion or compromise including a lack of 2-factor authentication of VPN connections and a lack of capability in network monitoring facilities, such as IDS or Intrusion Prevention Systems (IPS). The attacks were deployed through spear phishing campaigns to gain access to the IT or business networks of the providers, this was achieved through a payload embedded in a malicious Microsoft Excel or Word office document. On acceptance of a request to enable macros an embedded malicious macro in the document is then executed which will initiate the process of deploying the BlackEnergy payload. The malware then pivoted through the network with harvested credentials, abuse of VPN accounts and use of native tooling or living-off-the-land techniques to access the ICS segments of the network. This then allowed injection of malicious instructions to HMI's in the SCADA network segment to open breakers in substations while also deploying a KillDisk payload to delete the MBR of compromised devices and leveraging corruption of network-connected UPS equipment by injection of malicious bricking firmware to serial to ethernet controller equipment which in turn would disable the equipment raising power outage. An attempt at preventing direct remote response by deploying telephony DoS attacks against call center response services was also carried out. It is suggested that the attackers were knowledgeable of RTU equipment or able to enumerate infrastructure through precursor attacks or persistence to be able to target firmware of the serial to ethernet hardware and also achieve successful interaction with the variance of Distributed Management Systems (DMS) in the targets attacked.

An analysis of a sample of the BlackEnergy3 source is provided by Udi Shamir on behalf of SentinelOne in [73]. A malware author will usually attempt to obfuscate as much of the malicious source as possible however analysis of a sample of the BlackEnergy variant has shown the presence of entries left in the FONTCACHE.DAT file that provides the address location of the sources Program Database (PDB). This allows the program to be analysed with static analysis tools or connected to a debugger to investigate evidence including the addresses of functions, inspection of variables, parameters or pointers or general inspection of source. Further inspection of the malicious samples OLE structure shows an attached macro present, the extracted macro contains the BlackEnergy payload in chunks as arrays, these segments are reassembled then the payload is executed. The beginning of the arrays shows the values 77 and 90 contained, these are 4d 5A in hex which are the magic number identifier for DOS executable. The reassembled source contains two Portable Executables (PE) named rundll32.exe and FONTCACHE.DAT. This is the mechanism the threat will use to deploy.

The payload will run from the macro to deploy an executable which will deploy the rundll32.exe if not present. The rundll32.exe is a native Windows tool for running DLL's. This will then be used to run the desired DLL, in this case the FONTCACHE.DAT file. This file contains a disguised network sniffing utility which is run using rundll from a startup menu lnk shortcut and registry entry with the ShellExecute Windows API to deploy a further malicious payload. This allows the payload to be run on boot.

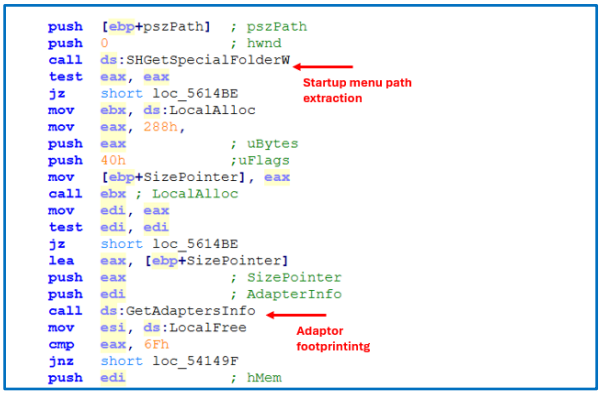

Figure 1: Initial enumeration by source

The sample carries out various actions to attempt evasion and possibly hinder debugging in performing obfuscation through the use of a CryptDecrypt() function and also performing a check using a call to the SetUnhandled ExceptionFilter API to check for the presence of a debugger. The source checks the available network adapters on the target system using an API call to GetAdapterinfo. This call can be seen in Figure 1. This is then provided as a parameter to the previously mentioned startup menu lnk entry to rundll to define the network adapter to use.

An entry is also injected to target system registry at Software\Microsoft\Windows\CurrentVersion\Explorer\Shel l to allow execution on startup. When the rundll call is made on execution of the lnk shortcut entry a process is spawned to kill the original process running the malicious macro and delete the original dropped malicious office file. The attack routine then makes multiple attempts to run the disguised WinPcap service from the FONTCACHE.DAT file using a call to OpenSCManagerA, OpenServiceA, StartServiceA, LoadLibrary or with W appended to the function for wide and also attempts evasion through the use of crypter() and sleep() functions.

This allows the payload to be capable of extensive network sniffing and subversion abilities. Analysis of the source provided in [73] shows the corresponding registry entry of OpenSCManagerW being modified. If successful, this will allow further reconnaissance or control through C&C services. Figure 2 below shows the macros execution, this will be run from the startup registry entry setup in the previous step, once this has executed the macro will deploy the BlackEnergy payload to complete the intrusion kill chain.

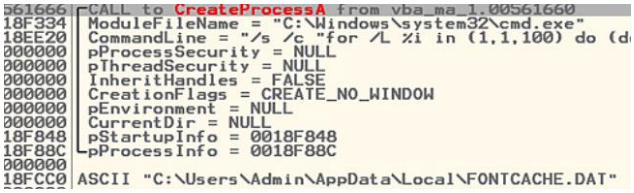

Figure 2: Macro execution

The BlackEnergy payload then will attempt traversal of the network aiming to access the ICS segments to inject malicious commands to the HMI's and open substation breakers while also injecting the KillDisk payload and malicious firmware to brick target devices and their serial to ethernet controllers. This then would cause an outage.

Research in [73] suggests there are similarities between the BlackEnergy payload and other well-known variants like the Sality and Operation Potao Express malware variants [50] identified as being used in attacks around the same time in Estonia and Georgia, this could imply that there is a potential that the same actors may be responsible or that the authors of the Sality and Potao Express variants have modified the payload or borrowed features from it.

B. *Industroyer & Industroyer2*

Industroyer

Another recent example of malware capable of targeting ICS is the Industroyer malware also known as CrashOverride. Research by Dragos in [69] and ESET verify that this variant was responsible for further attacks against Ukrainian power grid infrastructure in December 2016 in Kiev. This has since been attributed to a threat actor group tracked as ELECTRUM who are known to be affiliated with the Sandworm group who are linked to Russian intelligence services. [51].

Dragos researchers note that the Industroyer malware is one of the first malware variants capable of targeting ICS infrastructure along with the Stuxnet, Havex and BlackEnergy variants and also one of the first specifically developed to target electric utilities providers infrastructure.

Industroyer, like BlackEnergy, uses a modular architecture and contains sabotage and wiper modules and modules capable of targeting ICS protocols including IEC-101, IEC-104, IEC-61850 and OPC as well as support for DNP3 meaning the variant has the potential to be highly configurable and adaptable. Its method of compromise abuses DLL's of the concerned protocol for example 101.dll, 104.dll or OPC.dll. Unlike BlackEnergy it is capable of direct interaction with ICS hardware rather than injection of instructions through an HMI.

The attack routine by the malware bears significant similarities to the routine used in the BlackEnergy malware attacks by deployment through a Phishing campaign and opening breakers in substations to cause a significant outage and sabotage of serial to ethernet controllers with malicious firmware, this was also accompanied by a DoS attack against telephony assistance services to hinder response or resolution and sustain the compromise.

The Industroyer source contains 7 imported DLL's and 46 functions and includes launcher and wiper payloads. It also contains a backdoor payload and uses harvested VPN account details to leverage access to the ICS segment of a targeted network through the ICS segments historian database. It then deploys a launcher for propagation of threat through the various ICS protocol targeting modules and creates a malicious service to target corruption of HMI configurations. An overview of the behaviour of the Industroyer malware is provided in [70] by Marcus Geiger et al, their analysis explores the variant's use of native tooling like Powershell to leverage Golden Ticket attacks against the Kerberos service in Windows using Mimikatz or dumping of credentials from the systems memory. These are common exploit routines or techniques used for privilege escalation in Windows operating systems to provide elevated access. This assists with propagation of threat and pivoting to the ICS segment to deploy the Industroyer payload as a service to maximise persistence.

The Industroyer malware is capable of the enumeration of available protocols and configurations used in a target network and the selection of appropriate payloads for use in successful interaction with the target that are then deployed by the launcher payload.

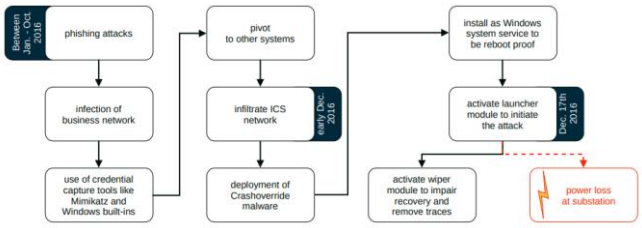

Figure 3: Industroyer compromise routine

As well as this, wiper malware and backdoor payloads are deployed to corrupt entries in the registries of Windows machines with the aim of corrupting the systems from booting successfully and also to attempt to leverage and maintain persistence. An example of the Industroyer malware high level kill chain routine can be seen in Figure 3 above:

Industroyer2

The Industroyer malware has since been evolved by the developers to directly target IEC-104 ICS network protocol rather than targeting multiple.

An overview of attacks involving the variant known as Industroyer2 is provided by K.Stoddart in [68]. The Industroyer2 malware was used in attacks in February, March and April of 2022 carried out against Ukrainain electrical utility infrastructure, this time the attacks were accompanied by the use of a wiper malware named CaddyWiper to attempt to leverage further compromise. These events were inline with the Russian invasion of Ukraine.

The Industroyer2 variant differs from the original Industroyer payload in that it specifically targets the IEC-104 rather than being able to target various ICS protocols with an adaptable modular framework like the first variant [52]. The sabotage modules in the Industroyer2 payload are used to instruct RTU's to open and keep open circuit breakers to leverage a sustained outage. The result of one of the attacks was the temporary disablement of 9 substations supplying around 2 million customers in turn creating significant outage [53].

The source code of Industroyer2 contains a collection of hardcoded configurations of Information Object Address

(IOA) listings which are used for targeting differently configured endpoints in an ICS segment [54]. These IOA listings hold details of the addresses of the Application Service Data Unit (ASDU) or Information Objects and are passed as strings to the module interacting with the IEC-104 protocol [52], this differs from the original strain that uses an Initialisation (.INI) file to store these configurations [55].

Another analysis of two samples of the Industroyer2 variant by Nozomi networks in [71] provides a good discussion of its low-level behaviour. As mentioned previously, the second variant of the Industroyer malware specifically targets the IEC-104 protocol and contains a hardcoded list of unobfuscated string IOA's which are configuration details for different end stations. The hardcoded listings contain entries for 3 separate station configurations providing the ability to target these ranges of station configurations and hold definition for a Station Configuration Header and an IOA Configuration Format.

(1) Station Configuration Header

An example of one of the Station Configuration Headers can be seen below, this contains local IP address and port followed by the ASDU address (in this case 3) then the mode of configuration which can be 0 for use of hardcoded listings or 1 for allowing the specification of two values to be used as a range of hardcoded IOA's to be attempted.

In the following example, we can see a specified address followed by a port and then an ASDU address of 3 and the operation mode set to 0. The header also contains the name of the process to be killed of PService_PPD.exe, the path location where the executable targeted for hijacking is stored of D:\OIK\DevCounter and also other configurable options, such as sleep counter, filename path location and the header number of the following IOA object, this is the end value in the example below of 44.

10.x.y.z 2404 3 0 1 1 PService_PPD.exe 1 "D:\OIK\DevCounter" 0 1 0 0 1 0 0 44

This template of instruction defines the format and configurable options for commands that can be sent to the particular type of station device to be executed. These Station Configuration Headers will be selected as required to target the appropriate station device.

(2) IOA Configuration Format

The IOA Configuration Format holds details of a list of IOA's and there concerned parameters including setting of single or double commands, index number and priority.

The malware begins infiltration by disabling and renaming the PServiceControl.exe and PServicePPD.exe services on the target, this stops the service being restarted. Capture of simulated network behaviour of the malware using Wireshark allowed for analysis of IEC104 protocol and port 2404 specific traffic which is a commonly used port for IEC protocol traffic. Inspection of packets show they contain the values for the IOA being accessed.

The payload then attempts interaction with target substations by initiating a network connectivity test using ***TESTFR act*** packets which are acknowledged by the recipient with ***TESTFR con*** packets. Once this transaction has taken place an attempt to start a data transaction is initiated using ***STARTDT act*** packets which are answered with a ***STARTDT con*** reply if successful, this is followed by an interrogation command C_IC_NA_1. This allows configuration of the type of frames that will be used in communication which can be C_SC_NA_1 for allowance of single command or C_DC_NA_1 double command depending on the endpoints configuration. This transaction can be seen in Figure 4. The malware uses its hardcoded configuration to iterate available IOA's of the target to identify and send the appropriate type of frames. This allows further interaction with the endpoints in the ICS segment of the network and carrying out injection of commands with disruptive intent. The Industroyer2 variant is more complex in nature compared to the first variant and BlackEnergy in that it is capable direct manipulation of ICS devices rather than remote execution and it is also highly configurable or adaptable.

Figure 4: Initial transaction with ICS segment

There are noted to be heavy similarities in source code in the two samples analysed of a sample of Industroyer from 2016 and a sample of Industroyer2 from 2022 [52]. An example of this can be seen in Figure 5. The samples are different in that the execution of the disabling of processes in the main thread of the first Industroyer variant have been transferred into a thread that starts the main thread [71]. However, various other similarities in the code or routines exist in the variants.

Similarities include the use of the same elements and routine to store global data showing an incorporation of this template design. Both samples are also noted as passing this data using the same data structure and similar methods of parsing to various functions and also have a lack of presence of obfuscation.

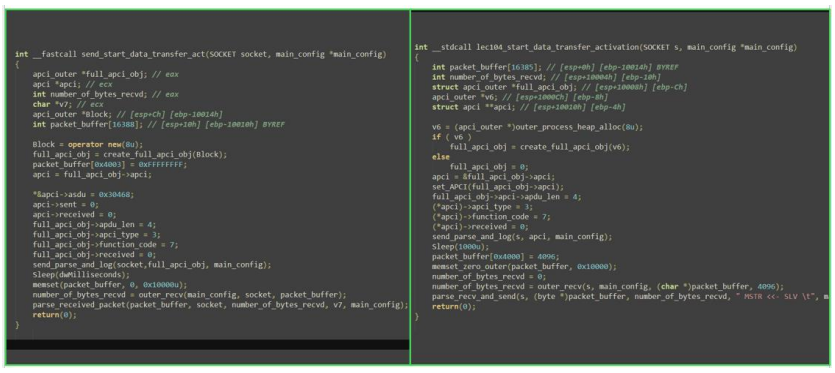

Figure 5: Similarities between Industroyer and Industroyer 2 samples

A report by ESET stated that the attacks targeted against a Ukrainian provider in April 2022 were unsuccessful but aimed to leverage a large-scale outage and deploy the CaddyWiper and other wiper malware to cause further disruption and hinder forensic analysis. It is suggested in some reports that there is a potential that Industroyer or similar types of malware could cause significant and extended outages if there were used in synchronised attacks against various targets. Another factor of note of this analysis is that the authors are highly likely to have been familiar with (or gained familiarity possibly through precursor attacks or insider knowledge of) the Operational Technology environment to achieve the successful design and deployment of the threat operation. This would tie in with reports of the suggested attribution to the Sandworm threat actor group who would likely have substantial knowledge and familiarity with the hardware and software used in the utilities infrastructure of the target [56] [68].

The BlackEnergy and Industroyer malwares mark a new era of threat towards ICS or IIoT systems in the targeting of utilities infrastructure and provide examples of the general advancement of methods and kill chains of attack used to target these types of systems. These cases demonstrate the breadth and variance of potential targets capable and also highlight the potential criticality of severity that a successful attack against certain IoT solutions can imply.

IV. DISCUSSION

Malware threats facing the IoT have shown significant evolvement in the past decade. Many of the early malware threats that emerged leveraged DoS and botnet capabilities, this has evolved into ransomware, bricker, cryptominer and info stealer variants being observed emerging as more recent threat trends.

Two of the first threats of significance discovered, named Hydra and ChuckNorris were first identified around 2008 and 2009 respectively, these were capable of botnet and DoS intents and targeted MIPSel and 32 and 64-bit Intel (x86/x64) architecture modems and routers with the Hydra variant originally targeting D-Link branded routers. The Hydra variant exploits insecure or default credentials in the D-link router authentication mechanism using dictionary cracking attacks or an authentication bypass technique over Secure Shell (SSH) or Hypertext Transfer Protocol (HTTP) with further threat propagated through an IRC based C&C agent for example the downloading of further threat payload, malicious instruction execution or the launching of TCP or User Datagram Protocol (UDP) based DoS flood attacks.
The ChuckNorris variant leverages compromise through the deployment of a Telnet dictionary attack and propagates further threat through a for purpose SSH client downloaded to the target through IRC based botnet control. This can then be used to hijack the device or execute botnet operations including Domain Name System (DNS) spoofing and the deployment of UDP DoS flood attacks.

One of the first cryptominer IoT malware was discovered in 2013 named Darlloz, this targeted tv set top boxes, toys and webcams using ARM, MIPS, MIPSel and Power PC (PPC) architectures and leveraged use of a known CVE tracked as CVE-2012-1823 which is a PHP CGI vulnerability that can allow RCE on the target. This was one of the first identified examples of a malware threat that leveraged the mining of cryptocurrencies and made use of a known CVE in its exploitation of a target IoT system.

Another example of a different type of variant was observed between 2013 and 2016 and involved the use of a trojanised Android application named X-Agent, a good analysis of this is provided in **[72]** by Crowdstrike. This was a trojanised Android application that was disguised as software for the remote configuration and control of howitzer equipment used by Ukrainian forces and hosted on a legitimate or trusted Ukrainian forum. This was used to provide targeting and espionage capabilities against Ukrainian forces and also enumerated and exfiltrated locational and communications data from the compromised devices which was then used to provide information to assist pro-Russian forces in leveraging offensive operations against the targets. The campaign was reported to have resulted in the loss of around 80% of the Howitzer Artillery equipment it was used to target within a period of 1 year. This was attributed by various researchers to the FancyBear threat actor group who are also tracked by the label APT28 and are linked to the Russian GRU intelligence service [18]. While this example seems extreme it highlights the varying potential severity that attacks against an IoT system can result in and also the heterogeneous characteristics and sensitivity of environments that an IoT system can involve. Further examples of botnet capable malware have been identified targeting a number of devices including IP cameras, NAS devices, DVR's and routers. These include the Gafgyt malware in 2014 and the Mirai malware in 2016, both of these used dictionary cracking methods against insecure services present including SSH, Telnet, Microsoft Structured Query Language (SQL) and MYSQL. These were both used to leverage significantly large-scale botnets and DDoS attacks. The Mirai variant was particularly destructive in its intent as once a target is compromised the Mirai malware will instruct the compromised device to refuse any further HTTP, SSH and Telnet connections essentially disabling the device and to hinder any attempt to recover it.

An additional emergent trend identified around 2017 was that of Bricker malware that will sabotage or brick a target device to disable it. One of the first examples of this type of variant was the Brickerbot variant in 2017 that targeted smart bulbs, toys and webcams through known vulnerable vectors in the Busybox OS which is a widely used embedded Linux framework in mobile and IoT or smart devices. It also used Dictionary attacks against HTTP, Simple Object Access Protocol (SOAP), SSH, Telnet and Home Network Administration Protocol (HNAP) protocols and was also capable of targeting a wide range or vendor specific devices with target specific threat payload. Another example of this type of variant is the Silex malware discovered around 2019 which was also capable of targeting a wide range of architectures and devices and used dictionary attack techniques against insecure services present to leverage compromise. Both variants will then overwrite critical areas of memory of the device to attempt to leverage bricking or PDoS against the device or service it is providing.

There is an increase in malware identified that is capable of targeting SCADA control systems since around the time of the Stuxnet incident in 2010. This includes the discovery of the BlackEnergy, Industroyer, LemonDuck, and VPNfilter variants along with others. The VPNFilter variant was discovered around 2018 and targets ARM, MIPS and x86

architecture SCADA control systems and NAS and router devices.

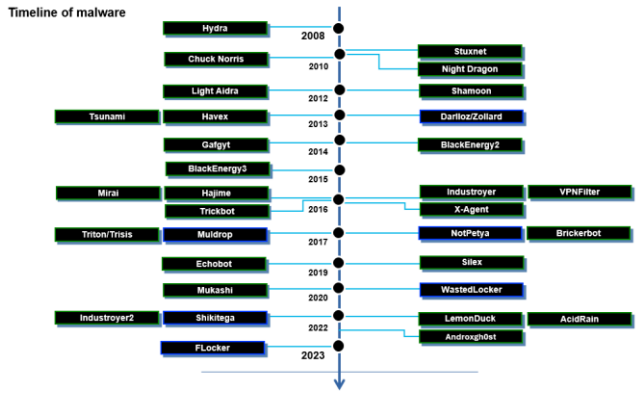

Figure 6: Timeline of significant IoT malware

The variant uses dictionary attack techniques to attempt to leverage hijack or MiTM compromise of the target to further propagate compromise through data exfiltration, DNS poisoning, DDoS or PDoS through the overwriting of critical OS components to render the system inoperable.

The following image in Figure 6 shows a timeline diagram of the 32 of the most significant malware variants targeting IoT solutions over the past fifteen years by the year they were first observed.

These examples show that there is a clear evolution in adversary behaviours and more extensive malware threat campaigns towards IoT systems in recent years. The BlackEnergy and Industroyer variants are examples of malware that are capable of significant and in cases potentially critical threat to the operation and safety of ICS systems. The capabilities of deploying wiper and bricking payloads to corrupt firmware, deletion of critical system data and disruption of operations is a considerable threat to these types of networks, systems, data and operational security. Both cases show that there are often multiple vectors of potential vulnerability or attack in the attempt to compromise IoT or ICS systems which increases the challenges in creating secure while efficient environments.

The BlackEnergy3 and Industroyer2 variants both show evolution in their methods from predecessor counterparts with the BlackEnergy variant originally being used for DoS attacks to using a Trojan and macro as methods of exploitation and further interaction with the target for propagation of compromise. The Industroyer variant transformed from a multiple protocol targeting modular framework to a protocol specific configurable and adaptable threat payload. They are also capable of enumeration of the target, advanced process injection, C&C interaction, espionage and sabotage.

This work along with the studies in various of the referenced research show that there has been an advancement of adversarial routines by malware authors in use of obfuscation, communication techniques and others methods of evasion in malware targeting IoT systems. The adversarial routines of attackers are likely evolving in parallel with improving security practices. There has been an emergence of cross platform or architecture malware along with more target specific or what could be considered a level of smart payloads. Early examples, such as Brickerbot sabotage devices through the compromise of products of insecure development or practice for example insecure default configurations or the Ramnit Trojan that creates a File Transfer Protocol (FTP) network from targets and propagates by malicious links. Others like the Trickbot malware directly exploit CVE's in MikroTik router devices to propagate further botnet threat [43]. More evolved recent examples emerging include the LemonDuck [44] variant that targets industrial & manufacturing systems, this contains payloads to target exploitation through SQL injection or abuse of SMB or other insecure technologies present.

The BlackEnergy and Industroyer malware are examples of some of the most significant malware threats to industrial IoT systems as they are payloads capable of disruption or sabotage of critical facing systems and are a concerning example of what future potential threats could be.

Traditional ICS systems are built with the view of convergence of IT and OT, this with the introduction of IoT creates an architecture that is created to ensure compatibility but may overlook or omit certain aspects of security. As always, an attacker will generally exploit low hanging fruit to gain compromise, there is however a much larger pool of potential threat vectors concerning IoT security.

A shortlist summary of the number of significant variants and types of malwares found to be targeting IoT can be seen in Table 1 on the following page. This shows the malware names, types, year or emergence, architectures and types of devices that they target and the vector of attack that they use in compromise of a target.

The adversarial routines of malicious actors are evolving along with IoT technologies developing and becoming more secure, threat operations are also possibly maturing through experience. There has been a noted increase in the use of CVE's [62] by malware threats to target compromise, the Gafgyt and VPNFilter variants are examples of this and also as mentioned previously the Echobot malware has a range of 71 CVE's that it can use to target vulnerable systems [58] [59]. Malware authors can make use of advanced techniques including fileless threat deployment, covert process injection or hollowing, code caves, zero days, cross platform threats, smart payloads, custom routines, advanced obfuscation or evasion techniques, AI or various others. The advancement of adversary behaviours in subversion and compromise against IoT targets will present further challenges to IoT security, for example when attackers begin to more prevalently utilise advanced techniques including polymorphic, metamorphic, staged or fileless payloads or use of more evasive segmentation or stronger obfuscation and encryption in these payloads there will likely require a parallel advancement in security and analysis practices. This means effective security strategies and practices are fundamental in order to protect IoT technologies from threat of IoT malware.

Some useful directions of research towards the mitigation of IoT malware threat include the design and development of lightweight device side monitoring or altering tools, the use of network-based hardening techniques including periodic authentication or use of forensics artefacts, such as beacons, canary tokens or honey tokens or the development of an analysis methodology and proactive solutions for the effective analysis of mobile and IoT malware.

TABLE I: MALWARE SUMMARY TABLE

Malware	Year	Type	Target	Architecture	Vector
Hydra	2008	Botnet, DDoS	Routers	MIPSel, x86	CVE-2018-7043
ChuckNorris	2009	DDoS, Hijacker	Modems, Routers	MIPSel	Telnet, Dictionary attack
Darlloz	2013	Cryptominer (Dogecoin)	Webcams, Toys, Set top boxes	ARM, MIPS, MIPSel, PPC	Dictionary attack, CVE-2012-1823, instruction injection
Gafgyt	2014	Botnet, DDoS	Routers, IP cameras, DVR's	ARM, MIPS, x86, PPC, Sparc…	RCE, CVE-2014-8361, CVE-2017-17217, CVE-2017-18368, CVE-2018-15887
BlackEnergy3	2015	ICS, Sabotage, DDoS	Siemens, GE HMI equipment	x86/64	Phishing, malicious macro injection, CVE-2014-4114
Trickbot	2016	Botnet, DDoS	Mikrotik routers	ARM	Brute force attack, CVE-2018-14847
Mirai	2016	Botnet, DDoS	Routers, IP cameras, DVR's, NAS, Printers	ARM, MIPS, x64	Dictionary attack
Industroyer	2016	ICS, Sabotage, PDoS	RTU's, UPS	x86, x64	Phishing, direct tampering of ICS equipment using (IEC) 101, 104, 61850 and OPC
Muldrop	2017	Cryptominer	Raspberry Pi	ARM	Default credentials
Brickerbot	2017	Sabotage, DDoS	Webcams, Toys, Smart bulbs	Busybox OS	Dictionary attack
VPNFilter	2018	MiTM, Sabotage	SCADA, NAS, Routers	ARM, MIPS, x86	Dictionary attack, 14 known CVE's
LiquorBot	2019	Cryptominer (Monero)	Routers	ARM, MIPS, x86, x64	Dictionary attack, 12 known CVE's
Silex	2019	Sabotage, DDoS	Any	ARM, MIPS, x86, SH4, Sparc	Dictionary attack
Echobot	2019	Botnet, DDoS, Propagation	Modems, Routers, ECDIS, PLC/RTU's/ NAS, Smart TV, ICS	ARM, MIPS, MIPSel, x86, x64, SH4, Sparc, PPC	71 Known CVE's
WastedLocker	2019	Ransomware	Garmin devices	ARM	Phishing, backdoor injection
Industroyer2	2019	ICS, Sabotage, PDoS	RTU's, UPS	x86, x64	Phishing, direct tampering of ICS equipment using IEC 104, Wiper payload deployment
Mukashi	2020	Botnet, DDoS	NAS (Zyxel)	ARM, MIPS, MIPSel, x86, SH4	Dictionary attack, Pre-authentication command injection, CVE-2020-9054
AcidRain	2022	Botnet, DDoS, Sabotage	KA-SAT Modems, Routers	MIPS	Firmware exploitation, Wiper payload deployment
Androxgh0st	2022	DoS, Hijacking, Info Stealing	Many	ARM, MIPS, x86/64	CVE-2017-9841**,** CVE-2018-15133, CVE-2021-41773
Shikitega	2022	Cryptominer (Monero)	Any	x86, x64	CVE-2021-3493, CVE-2021-4034
Flocker	2023	Ransomware	Smartphones, TV's Tablets, Android IoT devices	ARM, x86, x64	Phishing, Social engineering, trojanised apk

The use of effective network segmentation particularly in appropriate segmentation of IT and OT infrastructure endpoints or components or a zero-trust network strategy is a useful approach but this may not always suit operational requirements. A useful approach in ensuring the most secure practice is the development of zero trust configurations, these would most likely be setting or device specific and could consist of whitelisted definitions of allowed operations and blacklisted definitions of suspected or known malicious actions.

The VPNFilter [79] and AcidRain [80] malwares are more recent examples of this type of variant. Both variants are of particular note. The AcidRain malware was successfully targeted at Satellite router and terminal equipment to cause widespread outages. The VPNFilter malware variant utilises 14 CVE's it can use to target devices. The Echobot malware [57] is one of the more recent good examples of malware incorporating multiple CVE's to target compromise making use of 71 known CVE's.

Another rising trend is in ICS targeting malware including BlackEnergy 3 [17], Industroyer [51], Industroyer 2 [51] and LemonDuck [44] as recent examples. These have shown significant capabilities in disruption with the BlackEnergy 3 and Industroyer 2 variants being used to raise significant outages.

The Androxgh0st malware identified in 2022 was one of the most active variants in 2024 and is a final good example of evolving threat behaviour, this example uses info stealing and hijacking techniques to leverage compromise of Android based devices.

A clear shift in malware threat trend can be observed from the cases reviewed in this paper. There are already examples of malware that contain extensive threat payloads, advanced adversary behaviours and cross-platform targeting capabilities. The advancement of behaviours, increase in

cross-platform threats, ease of deployment through emerging resources like Malware-as-a-Service (MaaS) where malware threat campaigns are deployed from throw away infrastructure, the challenge of timely attribution and also the issue of zero-day threats of which there could arguably be higher potential for presence in an IoT setting mean that malware will remain a significant challenge to the security of IoT systems and networks.

There is requirement for effective resources or solutions that can provide the extensive analysis capabilities required for the analysis of the variance of IoT malware. Not only is there a lack of capable environment to achieve all of the emulation, virtualization or analysis capabilities required, there is also a lack of a standard analysis methodology for application. These are potential areas of valuable future research.

V. CONCLUSIONS AND FUTURE WORK

This paper aims to have provided insight in the review and analysis of IoT malware threats and outlined the variance of threats that exist. The review of related literature looking at these areas and the centralisation of certain relevant research in the investigation and analysis of some of the example variants covered is another value that could provide useful assistance to other researchers.

This paper should assist in providing an understanding of the range of routines or techniques that malware developers can employ to target and leverage compromise or exploitation of IoT solutions. The analysis and comparison of the BlackEnergy and Industroyer variants of malware could also prove to be useful assistance to other researchers or as a basis of research in analysis of or comparison to future variants that may emerge.

Future direction of additional research in this area could include the analysis and comparison of collections of malware variants targeting automotive, healthcare or types of IoT solutions to identify their capabilities, commonalities and unique elements. Also, further analysis of the Industroyer2 malware variant in regard to the low-level analysis of its modular components could provide further understanding of the malware's exploitation routine

It is likely that there will continue to be an increase in the development and adoption of IoT and smart technologies. As new technologies, systems and networks are introduced, IoT malware threat trends are likely to shift in parallel to target exploitation of these. The development of proactive analysis solutions and a standard analysis methodology for the analysis of IoT malware are two areas that would be of useful future research direction and if developed could provide a valuable resource.

REFERENCES

[1] M. Weiser, "The computer for the 21st century," Available at: https://www.cs.cmu.edu/~jasonh/courses/ubicomp-sp2007/papers/02-weiser-computer-21st-century.pdf [retrieved: August, 2025].

[2] Cisco, "Cisco annual internet report (2018–2023) white paper," Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [retrieved: June, 2025].

[3] The Government Office for Science, "The internet of things: Making the most of the second digital revolution," Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf [retrieved: June, 2025].

[4] [Unit 42, "2020 Unit 42 IoT threat report," Available at: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ [retrieved: June, 2025].

[5] A. Gowdiak, "Security vulnerabilities in Telit Cinterion IoT (formerly Thales) devices," Available at: https://seclists.org/fulldisclosure/2023/Apr/11 [retrieved: June, 2025].

[6] Mitre, "OpenSSH CVE list," Available at (cve.mitre.org) [retrieved: June, 2025].

[7] Tenable, "ArubaOS WPA2 key reinstallation vulnerabilities (KRACK)," Available at: https://www.tenable.com/plugins/nessus/103855 [retrieved: June, 2025].

[8] D. Antonioli, "Bluetooth BIAS attacks," Available at: https://francozappa.github.io/project/bias/ [retrieved: June, 2025].

[9] Carnegie Mellon University, "CERT/CC vulnerability note VU#918987: Bluetooth BR/EDR supported devices are vulnerable to key negotiation attacks," Available at: https://www.kb.cert.org/vuls/id/918987/ [retrieved: June, 2025].

[10] Montsecure, "Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE," Available at: https://montsecure.com/research/revolte-attack/ [retrieved: July, 2025].

[11] Radware, "BrickerBot results in permanent denial-of-service," Available at: https://www.radware.com/getattachment/Security/Threat-Advisories-and-Attack-Reports/1418/ERT-Alert-BrickerBot-PDoS-2.pdf.aspx/?lang=en-US [retrieved: June, 2025].

[12] Ilascu, "New Silex malware trashes IoT devices using default passwords," Available at: https://www.bleepingcomputer.com/news/security/new-silex-malware-trashes-iot-devices-using-default-passwords/ [retrieved: June, 2025].

[13] B. Krebs, "Source Code for IoT Botnet 'Mirai' Released," Available at: https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/ [retrieved: June, 2025].

[14] VX-Underground, "Hajime worm battles Mirai for control of the Internet of Things," Available at: https://www.vx-underground.org/malware_defense.html [retrieved: June, 2025].

[15] C. Huey, A. Windsor and E. Brumagin, "Lemon Duck spreads its wings: Actors target Microsoft Exchange servers," Available at: https://blog.talosintelligence.com/lemon-duck-spreads-wings [retrieved: June, 2025].

[16] Cherepanov, ESET, "Win32/Industroyer: A new threat for industrial control systems," Available at: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf [retrieved: June, 2025].

[17] Securelist, Kapersky, "BlackEnergy APT attacks in Ukraine employ spearphishing with Word documents," Available at: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/ [retrieved: June, 2025].

[18] M.B. Gazula, MIT CAMS, "Cyber warfare conflict analysis and case studies," Available at: https://cams.mit.edu/wp-content/uploads/2017-10.pdf [retrieved: June, 2025].

[19] B. Krebs, "Mirai IoT botnet co-authors plead guilty," Available at: https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/ [retrieved: June, 2025].

[20] Rapid7, "Types of cyber attacks: Hacking attacks and techniques," Available at: https://www.rapid7.com/fundamentals/types-of-attacks/ [retrieved: June, 2025].

[21] A.Remillano II, J. Molina, "Mirai botnet attacks IoT devices via CVE-2020-5902," Available at:

https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-iot-devices-via-cve-2020-5902.html [retrieved: June, 2025].

[22] Gulatas, H. Hakan Kilinc, A. Halim Zaim and M. Ali Aydin, "Malware threat on edge/fog computing environments from Internet of Things devices perspective," Available at: https://ieeexplore.ieee.org/document/10083045 *IEEE Access*, vol. 11, pp. 33584–33606, doi:10.1109/access.2023.3262614 [retrieved: June, 2025].

[23] C. Cimpanu, "BrickerBot author retires claiming to have bricked over 10 million IoT devices," Available at: https://www.bleepingcomputer.com/news/security/Brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/ [retrieved: June, 2025/].

[24] NCC Group, "WastedLocker: A new ransomware variant developed by the Evil Corp group," Available at: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-Ransomware-variant-developed-by-the-evil-corp-group/ [retrieved: June, 2025].

[25] Mitnick Security, "An overview of the 2020 Garmin ransomware attack," Available at: https://www.mitnicksecurity.com/blog/2020-garmin-Ransomware-attack [retrieved: June, 2025].

[26] Mitre, "Amazon CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Amazon+fire+alexa [retrieved: July, 2025].

[27] Mitre, "Apple CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=watchOS+%26%26+tvOS [retrieved: July, 2025].

[28] Mitre, "Fitbit CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Fitbit [retrieved: July, 2025].

[29] Mitre, "Google Nest CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Google%2Bnest [retrieved: July, 2025].

[30] J. Stckliey, T. Davis, SOS Daily News, "A whole flock of Google Nest indoor camera issues found," Available at: https://www.sosdailynews.com/?articleid=+305494CF8F5AD05E81214387321385CF [retrieved: July, 2025].

[31] Mitre, "Ring CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Ring%2Bdoorbell [retrieved: July, 2025].

[32] Mitre, "BMW CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=BMW [retrieved: July, 2025].

[33] Mitre, "Chrysler/Jeep CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Chrysler [retrieved: July, 2025].

[34] Mitre, "Ford CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Ford [retrieved: July, 2025]

[35] Mitre, "Honda CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Honda [retrieved: July, 2025].

[36] Mitre, "Tesla CVEs," Available at: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Tesla [retrieved: July, 2025].

[37] JSOF, "RIPPLE20," Available at: https://www.forescout.com/research-labs/ripple20-vulnerability/ [retrieved: July, 2025].

[38] Forescout, "Name:Wreck," Available at: https://www.forescout.com/research-labs/namewreck/ [retrieved: July, 2025].

[39] Forescout, "Nucleus:13," Available at: https://www.forescout.com/research-labs/nucleus-13/ [retrieved: July, 2025].

[40] Forescout, "Amnesia:33," Available at: https://www.forescout.com/research-labs/amnesia33/ [retrieved: July, 2025].

[41] Armis, "Urgent/11," Available at: https://www.armis.com/research/urgent-11/ [retrieved: July, 2025]

[42] B. E. Duan, V. Zhang and K. Ye, "Flocker mobile ransomware crosses to smart TV," Trend Micro, Available at: https://www.trendmicro.com/ru_ru/research/16/f/flocker-Ransomware-crosses-smart-tv.html [retrieved: July, 2025].

[43] D. Atch, N. Frumovich and R.Bevington, Microsoft Threat Intelligence, "Uncovering Trickbot's use of IoT devices in command-and-control infrastructure," Available at: https://www.microsoft.com/en-us/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/ [retrieved: July, 2025].

[44] Microsoft Threat Intelligence, "When coin miners evolve, part 1: Exposing LemonDuck and LemonCat," Available at: https://www.microsoft.com/en-us/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/ [retrieved: July, 2025].

[45] X. Zhang, O. Upton, N. Beebe and K. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," Trend Micro. Available at: https://www.sciencedirect.com/science/article/pii/S2666281720300214 [retrieved: July, 2025].

[46] V. Singhal, R. Nigam, Z. Zhang, and A. Davila, "New Mirai variant targeting network security devices," Unit 42. Available at: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/ [retrieved: July, 2025].

[47] Microsoft Threat Intelligence, "When coin miners evolve, part 2: Hunting down LemonDuck and LemonCat attacks," Available at: https://www.microsoft.com/en-us/security/blog/2021/07/29/when-coin-miners-evolve-part-2-hunting-down-lemonduck-and-lemoncat-attacks/ [retrieved: July, 2025].

[48] R. Holt, ESET Security Community, "Sandworm: A tale of disruption told anew," Available at: https://www.welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/ [retrieved: July, 2025].

[49] CISA, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a [retrieved: July, 2025].

[50] R. Lipovsky, A. Cherepanov, ESET, "Operation Potao Express," Available at: https://web-assets.esetstatic.com/wls/2015/07/Operation-Potao-Express_final_v2.pdf [retrieved: July, 2025].

[51] Hall, CCDCOE, "Industroyer – Crash Override," Available at: https://cyberlaw.ccdcoe.org/wiki/Industroyer_–_Crash_Override_(2016) (cyberlaw.ccdcoe.org in Bing) [retrieved: July, 2025].

[52] D. Zafra et al, Mandiant, "INDUSTROYER.V2: Old malware learns new tricks," Available at: https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks/ [retrieved: July, 2025].

[53] Greenberg, "Russia's Sandworm hackers attempted a third blackout in Ukraine," Wired. Available at: https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/ [retrieved: July, 2025].

[54] Splunk, "Threat update: INDUSTROYER2," Available at: https://www.splunk.com/en_us/blog/security/threat-update-industroyer2.html [retrieved: July, 2025].

[55] ESET Ireland, "Industroyer2: Industroyer reloaded," Available at: https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/ [retrieved: July, 2025].

[56] Microsoft Digital Security Unit, "Special report: Ukraine – An overview of Russia's cyberattack activity," Available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/1212211-ms-ukrainespecialreport-fy23-link-update.pdf [retrieved: July, 2025].

[57] E. Kreminchuker, M. Zavodchik, "Echobot malware now up to 71 exploits, targeting SCADA," F5 Labs. Available at: https://www.f5.com/labs/articles/threat-intelligence/echobot-

malware-now-up-to-71-exploits--targeting-scada [retrieved: July, 2025].

[58] R. Nigam, Unit 42, "Mirai variant Echobot resurfaces with 13 previously unexploited vulnerabilities," Unit 42. Available at: https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/ [retrieved: August, 2024].

[59] J. Choi et al, "IoT malware ecosystem in the wild," *IoT Malware Ecosystem in the Wild*. Available at: https://dl.acm.org/doi/abs/10.1145/3318216.3363379 doi:10.1145/3318216.3363379 [retrieved: August, 2024].

[60] Mudgerikar and E. Bertino, "IoT attacks and malware," in *Cyber Security Meets Machine Learning*, Springer, pp. 1–27. Available at: https://link.springer.com/book/10.1007/978-981-33-6726-5 [retrieved: August, 2024].

[61] R. Khoury, B. Vignau, S. Hallé, A. Hamou-Lhadj, and A. Raz, "An analysis of the use of CVEs by IoT malware," in *Foundations and Practice of Security*, Springer, pp. 47–64. Available at: https://link.springer.com/book/10.1007/978-3-030-70881-8 [retrieved: August, 2024].

[62] FortiGuard Labs, "Linux/Darlloz.A," Available at: https://www.fortiguard.com/encyclopedia/virus/5902488 [retrieved: August, 2024].

[63] K. Hemsley and R. Fisher, "A history of cyber incidents and threats involving industrial control systems," in *Critical Infrastructure Protection XII*, Springer, pp. 222–249. Available at: https://link.springer.com/chapter/10.1007/978-3-030-04537-1_12 [retrieved: August, 2024].

[64] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE Access*, vol. 6, pp. 15941–15957, doi:10.1109/ACCESS.2018.2815660. Available at: https://ieeexplore.ieee.org/document/8315029 [retrieved: August, 2024].

[65] G. P. Kachare, G. Choudhary, S. K. Shandilya, and V. Siha, "Sandbox environment for real-time malware analysis of IoT devices," in *Computing Science, Communication and Security*, Springer, pp. 169–183. Available at: https://link.springer.com/chapter/10.1007/978-3-031-10551-7_13 [retrieved: August, 2024].

[66] S. Kakati, D. Chouhan, A. Nag, and S. Panja, "Survey on recent malware detection techniques for IoT," in *Pattern Recognition and Data Analysis with Applications*, Springer, pp. 647–660. Available at: https://link.springer.com/chapter/10.1007/978-981-19-1520-8_53 [retrieved: August, 2024].

[67] K. Stoddart, "On cyberwar: Theorizing cyberwarfare through attacks on critical infrastructure," in *Cyberwarfare Threats to Critical Infrastructure*, Palgrave Macmillan, pp. 53–145. Available at: https://link.springer.com/chapter/10.1007/978-3-030-97299-8_2 [retrieved: August, 2024].

[68] Dragos, "CRASHOVERRIDE: Analysis of the threat to electric grid operations," Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf [retrieved: August, 2024].

[69] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of BlackEnergy, CrashOverride, and Trisis," in *IEEE ETFA*, pp. 1537–1543, doi:10.1109/ETFA46521.2020.9212128. Available at: https://ieeexplore.ieee.org/document/9212128 [retrieved: August, 2024].

[70] Nozomi Networks, "Industroyer2: Nozomi Networks Labs analyzes the IEC-104 payload," Available at: https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload [retrieved: August, 2024].

[71] CrowdStrike Global Intelligence Team, "Use of FancyBear Android malware in tracking Ukrainian field artillery units," Available at: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf [retrieved: August, 2024].

[72] U. Shamir, SentinelOne, "Analyzing a new variant of BlackEnergy 3 likely insider-based execution," Available at: https://www.scribd.com/document/421931582/BlackEnergy3-WP-012716-1c [retrieved: August, 2024].

[73] Y. Mekdad, G. Bernieri, M. Conti and AE. Fergougui, "The rise of ICS malware: A comparative analysis," Springer. Available at: https://link-springer-com.libproxy.abertay.ac.uk/chapter/10.1007/978-3-030-95484-0_29 [retrieved: August, 2024].

[74] K. Hsu, Z. Z. Zhang and R. Nigam, "New Mirai variant targets Zyxel network-attached storage devices," Unit 42. Available at: https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/ [retrieved: August, 2024].

[75] Famera, B. Hilger, S. Bhunia and P. Heil, "Analyzing the Mirai IoT botnet and its recent variants: Satori, Mukashi, Moobot, and Sonic," arXiv.org. Available at: https://arxiv.org/abs/2508.01909v1 [retrieved: August, 2024].

[76] Checkpoint "November 2024's most wanted malware: Androxgh0st leads the pack, targeting IoT devices and critical infrastructure," Check Point Blog. Available at: https://blog.checkpoint.com/research/november-2024s-most-wanted-malware-androxgh0st-leads-the-pack-targeting-iot-devices-and-critical-infrastructure/ [retrieved: August, 2024].

[77] CISA, "Known indicators of compromise associated with Androxgh0st malware," Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a?=&web_view=true [retrieved: August, 2024].

[78] Picus Labs, "Androxgh0st malware: Unmasking the silent threat to cloud and web security," Available at: https://www.picussecurity.com/resource/blog/androxgh0st-malware-cloud-web-security-threat [retrieved: August, 2024].

[79] CISA, "VPNFilter Destructive malware," Available at: https://www.cisa.gov/news-events/alerts/2018/05/23/vpnfilter-destructive-malware [retrieved: September, 2025]

[80] Mitre, "Acid Rain," Available at: https://attack.mitre.org/software/S1125/ [retrieved: September, 2025].