National Cyber Security Centre
a part of GCHQ

Organisational use of Enterprise Connected Devices

Assessing the cyber security threat to UK organisations using Enterprise Connected Devices.

Contents

4 **Introduction**

Key judgements

How likely is a 'realistic possibility'?

6 **What are enterprise connected devices?**

8 **Why target enterprise connected devices?**

Lateral movement

Data theft

Monetary gain

Attack base / positioning

12 **Who attacks enterprise connected devices?**

Nation state actors

Cyber criminals

14 **How threat actors target enterprise connected devices**

Supply chain

Bots

Unpatched IoT devices on enterprise network

Personal connected devices on enterprise network

18 **Conclusion**

Assessment - what it is

Key judgements

pHIA probability yardstick

Introduction

This paper aims to provide an assessment of the current cyber security threat to Enterprise Connected Devices. This information will be of interest to industry and any person using a connected device.

Devices used and deployed by organisations have changed dramatically in recent years. From enabling remote and flexible working to improving efficiency and productivity, these devices are broad in scope and frequently rely on their ability to be connected; with this comes increased risk.

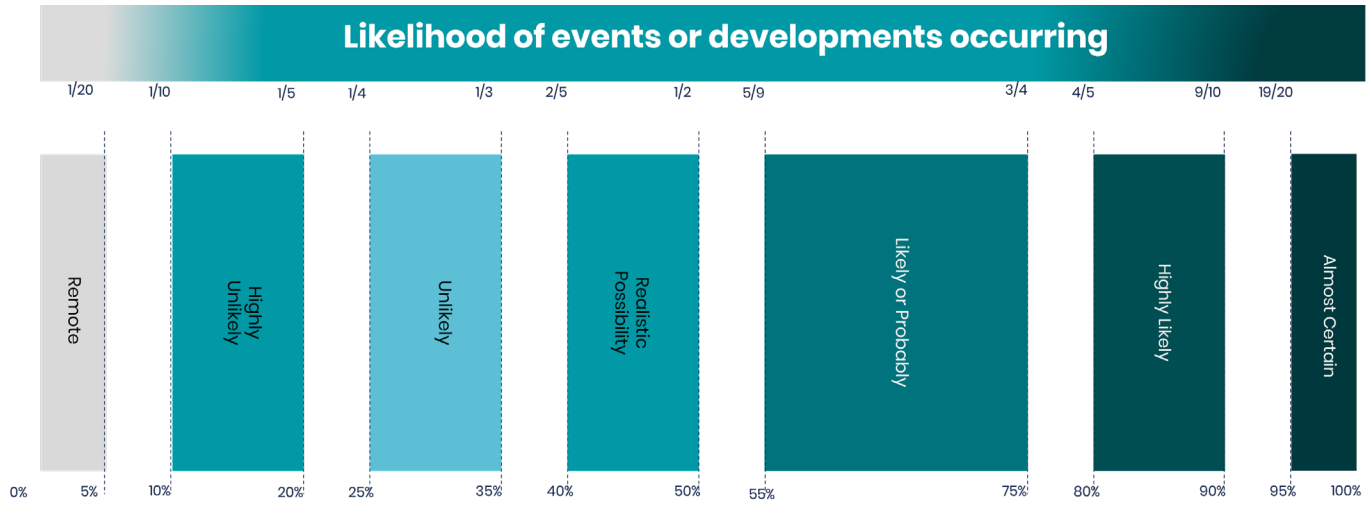
In collaboration with DCMS, NCSC have begun the process of assessing the landscape of these Enterprise Connected Devices and we have launched the Device Security Principles (Beta) as a framework to help drive forward security in this area.

Key judgements

- It is highly likely that the growing number of Enterprise Connected Devices (ECDs) being adopted by enterprises presents an expanding attack surface, with many of these devices being accessible over the public internet, and with cyber security often being an afterthought.
- Following initial compromise, it is highly likely that ECDs will be used as an attack vector or pivot point to enable cyber actors to gain access to an enterprise's corporate network for espionage purposes, disruption, or financial gain.
- Deployments of ECDs within large UK organisations are likely to present a different threat profile from typical consumer use. Organisations often have more knowledge, responsibility and control of networks and cyber security, compared with a typical consumer.

How likely is a ‘realistic possibility’?

NCSC Assessment uses the PHIA probability yardstick every time we make an assessment, judgement, or prediction. The terms used correspond to the likelihood ranges below.



What are Enterprise Connected Devices?

Enterprise Connected Devices (ECDs) are any devices that interact with, hold, or process an organisation's data. ECD is making the fabric of the world around us smarter and more responsive, merging the digital and physical worlds.

Enterprise Connected Devices (ECDs) refer to any device which interacts with, holds, or processes an organisation's data. As a result of the broad range of devices, ECDs can encompass other categories of devices depending on their use and can cross over to multiple other device classes, including:

End user devices

Devices such as laptops and smartphones. Although these are devices designed for both consumers and organisations, if used in the context outlined above, they are classed as ECDs. If a personal device is also used for work purposes (e.g. Bring Your Own Device (BYOD)) or is able to interact with organisation data, for example by being able to connect to an enterprise network, as classed above, it is viewed as an ECD.

Internet of Things (IoT)

IoT refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Connecting all these different devices to the internet and adding sensors and mechanisms to interact with their surrounding environment adds a level of digital intelligence to devices, enabling them to communicate real-time data without involving a human being.

Distinct ECDs

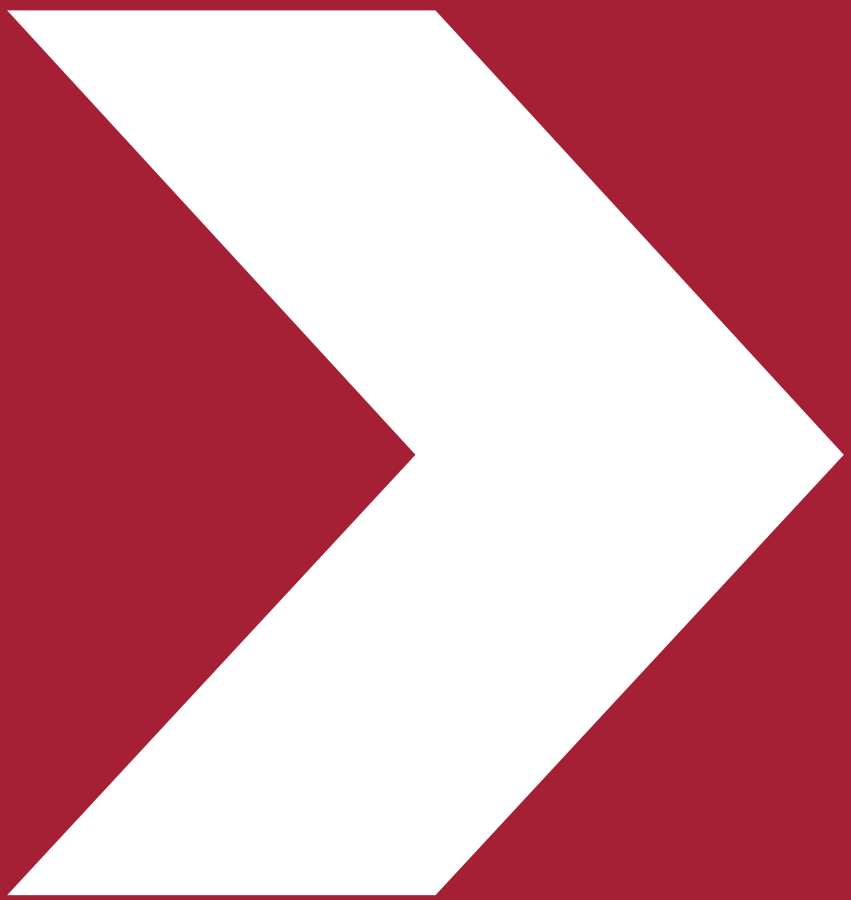
These are devices that are primarily designed for use in an enterprise setting. Whilst they may be available to purchase by consumers, they usually require some form of additional infrastructure or have limited use by the public.

Consumer IoT is now embedded in every part of our lives, with more and more devices becoming connected to the internet each day. Examples include smart kettles, watches, refrigerators, and televisions. As we connect more devices in our homes to the internet, products and appliances that have traditionally been offline are now becoming part of the IoT.

For the purpose of this paper, Enterprise IoT devices and distinct ECDs are defined as devices that are industry-agnostic and are typically not available or intended for consumers to purchase. Operational Technology (OT) is not within scope.

Enterprise IoT is the advancement in technology that enables physical 'things' with embedded computing devices to participate in business processes for reducing manual work and increasing overall business efficiency. Taking advantage of a combination of technologies ranging from embedded devices with sensors and actuators to internet-based communication and cloud platforms, enterprise IoT applications can now automate business processes that depend on contextual information provided by programmed devices such as machines, vehicles, and other equipment.

ECDs, both consumer and enterprise, are used within the daily operation of thousands of organisations around the UK. However, vulnerable devices can provide a route for hostile actors to attack enterprise systems.



Why target Enterprise Connected Devices?

ECDs are a hugely attractive target for different types of threat actor as they can hold and process valuable, sensitive, or personal data. Many categories of ECDs (particularly IoT devices) present an easy target to compromise due to typically limited security efforts by vendors, a large attack *surface* (multiple endpoints for access to wider networks) and attack *base* for lateral movement.

The COVID-19 pandemic has driven a surge in remote working, and ECDs have played a vital role in supporting business continuity. ECD usage has boosted operational efficiency, as seen in the retail industry where some ECDs are used to monitor entire supply chains, from manufacturing to the store. This has improved production quality and ensures that distribution matches demand across retail outlets. Not only has it enabled some tasks to be automated and work to be carried out remotely, but it has also helped prioritise manual work to cope with reduced labour, and protect those employees doing vital work. For example, energy providers can remotely check an organisation's utility installations from a distance rather than going into the field themselves.

This has presented opportunities for organisations to work innovatively but has also created new opportunities for threat actors. The increase in the number of connected services globally and their dependency on ECDs to run and facilitate such services raises concerns over threats like Distributed Denial of Service (DDoS) attacks to potentially cause nationwide failures for businesses and critical systems.

Case Study: Hacking group compromise of VoIP networks

Cyber security researchers have detailed how one hacking group compromised the VoIP networks of almost 1,200 organisations in over 20 countries, with over half the victims in the UK. Industries including government, military, insurance, finance, and manufacturing are believed to have fallen victim to the campaign. The attackers exploited CVE-2019-19006, a critical vulnerability in Sangoma and Asterisk VoIP phone systems that allows outsiders to remotely gain access without any form of authentication. A security patch to fix the vulnerability had been released, but many organisations were yet to apply it, at the time of reporting – and cyber criminals are taking advantage of this by scanning for unpatched systems.

Lateral movement

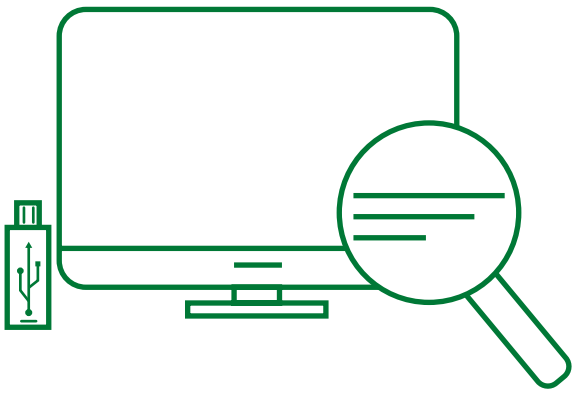
A single exposed ECD has the potential to enable a cyber actor to gain access to an enterprise's corporate network. While the security postures of many ECDs make them easy targets, it is highly likely devices are used as stepping stones in lateral movement to compromise other systems on a network.

Case Study: Internet-connected fish tank

In 2017, cyber actors acquired data from a North American casino by compromising an internet-connected fish tank. The fish tank had sensors connected to a computer, which monitored the temperature, food, and cleanliness of the fish tank. The cyber actor was able to compromise the fish tank, gain access to other areas of the network through lateral movement, and steal data.

Data theft

An ECD can store, process, or stream an abundance of information that can be critical, private, or sensitive, depending on the environment or industry. One of the main ECD challenges is that the devices often record, have access to, and stream sensitive data. Security systems such as cameras and doorbells are increasingly a part of small business networks and can quickly create major issues if compromised by a cyber actor. Office equipment, such as printers, are also potential access points - a compromised printer could easily mean that the attacker can view everything that is printed or scanned in an office.



Why target Enterprise Connected Devices?

Monetary gain

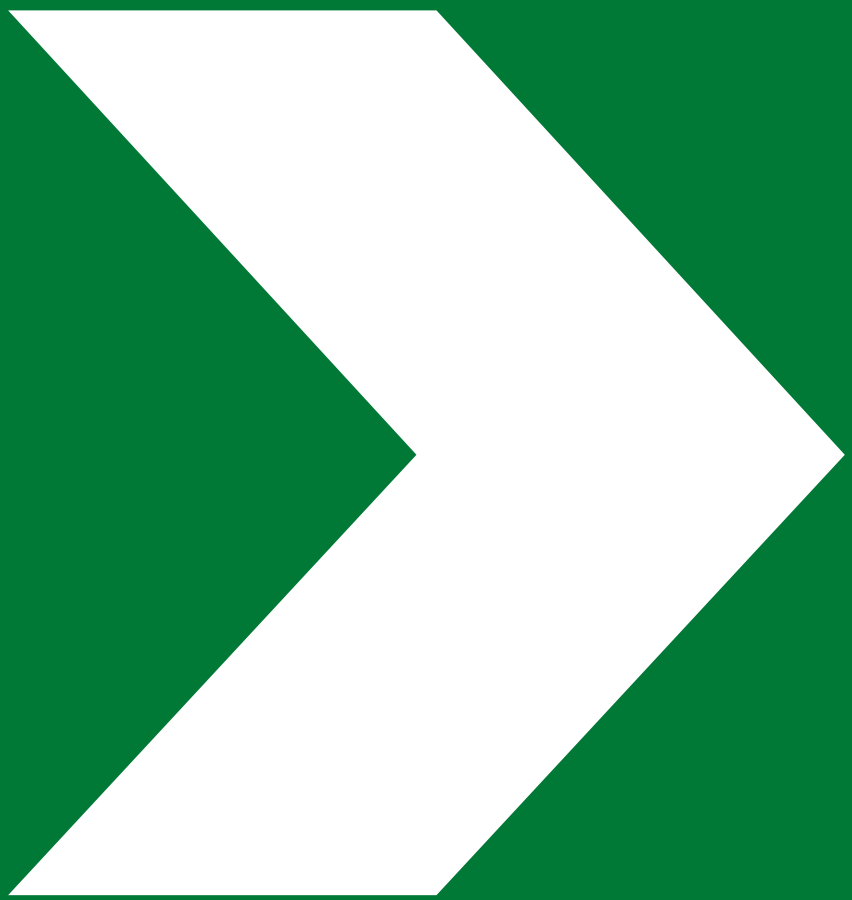
ECD attacks can prove profitable for threat actors. Vulnerable ECDs can enable ransomware attacks against victim networks, providing attackers with the ability to seek payment to relinquish control of compromised assets.

Attack base / positioning

Cyber actors can weaponise ECDs so attacks can be spread outwards or deeper into the main infrastructure. ECDs are also ideal targets to turn into bots for use in further campaigns. A botnet is a collection of internet-connected 'bots' under remote control from malicious actors

Case Study: VPNFilter malware

VPNFilter is a malware type that affects routers and storage devices by using backdoor accounts and exploits of several known vendors, likely to have been developed by a nation state. The botnet, referred to by the FBI and cyber security researchers as VPNFilter, targets small office/home office routers and network-access storage (NAS) devices, which are hardware devices made up of several hard drives used to store data in a single location that can be accessed by multiple users. VPNFilter operates in multiple stages that include initial infection, command-and-control communications, and the third stage, in which the payloads are deployed.



Who attacks Enterprise Connected Devices?

Nation state actors

Nation state cyber actors have reportedly targeted ECDs for espionage purposes. Nation state cyber actors have highly likely taken notice of such ECD vulnerabilities such as default passwords, outdated protocols, the absence of encryption, incorrect configurations, and unpatched devices, to get in the backdoor of enterprise networks.

The goals for cyber espionage campaigns may differ but are often focused on theft of information without the target becoming aware. It is a realistic possibility that nation state actors target the supply chain of ECDs, due to the wide range of ECDs, the access they have, and the size of the user base. Nation states compromising supply chains is nothing new - the 2017 NotPetya attack and the 2020 SolarWinds compromise are both supply chain attacks that have been attributed by the UK to a nation state.

Case Study: APT group compromising popular IoT devices

In April 2020, Microsoft security researchers observed the Russian-backed hacking group STRONTIUM (also known as Fancy Bear or APT28) compromising popular IoT devices (a VOIP phone, an office printer, and a video decoder) across multiple customer locations. Microsoft had more widely observed the group's attacks targeting a range of sectors, including defence, education, engineering, government, IT, medicine, and military.

Case Study: Ransomware and smart TVs

In 2016, there were instances reported of Android malware infecting phones, tablets, and other Android-powered devices, such as smart TVs. LG smart TVs were infected with ransomware, and victims were required to pay the cyber actors to unlock their smart TV. A 2016 report detailed that smart TVs were regularly targeted by ransomware, with the most active threat being Cyber.Police (FLocker).

Cyber criminals

Cyber criminals are financially motivated, and their capabilities vary. They often attempt to disrupt services via DDoS attacks or encrypt data through ransomware and demand payment. Cyber criminals will likely attempt to gain access to insecure ECDs by openly scanning for vulnerabilities that can be exploited.

Case Study: Mirai malware being used by cyber criminals

In 2016, IP cameras and basic home routers were infected with the Mirai malware, creating a botnet that was subsequently abused to take out Domain Name System (DNS) provider Dyn, in an attack that left many high-profile websites inaccessible.

Despite first appearing in 2016, the Mirai malware has continued to be dominant, and a worrying new trend has seen criminals develop variations that are specifically engineered to infect enterprise IoT devices. Digital signage monitors, wireless presentation systems and other such devices present attackers with access to greater bandwidth connections than can be achieved through consumer devices, which enables them to launch stronger DDoS attacks.

The Mirai malware targets IoT devices to turn them into botnets capable of launching DDoS attacks. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware.

How threat actors target Enterprise Connected Devices

ECDs bring great opportunities for organisations but a significant number of devices on the market today have been found to lack basic security measures. Threat actors will seek to take advantage of technical vulnerabilities and poor cyber security to compromise ECDs. This is problematic if manufacturers do not seek to fix the issue, and if users do not apply updates.

Most IoT devices possess fewer processing and storage capabilities than traditional enterprise computing platforms. This makes it difficult to employ security applications that could help protect them, such as antivirus software. Additionally, whilst patches are made available for IoT devices, many older IoT devices were not built with security in mind and do not have capacity to receive remote patches. Some organisations also do not have processes in place to monitor and manage if an ECD is supported or not. At the same time, it has become steadily easier and cheaper for criminals to acquire tools that enable them to launch high-volume, low-sophistication attacks that are ideally suited for compromising large numbers of poorly secured devices.

ECD attack surface areas or areas in ECD systems and applications where threats and vulnerabilities may exist include:

Devices ›

Devices can be the primary means by which attacks are initiated. Parts of a device where vulnerabilities may exist include its storage firmware and application software, physical interface, web interface, and network services. Attackers can also take advantage of insecure default settings, outdated components, and insecure update mechanisms, among others. Vulnerabilities that exist in hardware sometimes cannot be patched, like with software, and would need a complete physical replacement to secure.

Communication channels ›

Attacks can originate from the communication channels that connect ECD components with one another. Protocols used in a range of ECD systems can have security issues that can affect the entire system. Many ECD systems are also susceptible to known network attacks such as denial of service and spoofing.

Applications and software ›

Vulnerabilities in network services and related software for ECDs can lead to compromised systems. Network services can, for example, be exploited to steal user credentials or push malicious firmware updates.

Case Study: Ripple20

In June 2020, researchers announced 19 zero-day vulnerabilities impacting millions of devices, affecting the Treck embedded IP stack. Treck is used by over 50 vendors and millions of devices, including mission-critical devices for healthcare, data centres, and critical infrastructure. This group of vulnerabilities has been named “Ripple20” to reflect the widespread impact the exploitation of these flaws could have on a wide range of products from various industries.

Ripple20 impacts critical IoT devices, including printers, networking equipment, IP cameras, video conferencing systems and building automation devices. By exploiting the software library flaws, attackers could remotely execute code and gain access to sensitive information. The impact of these vulnerabilities is exacerbated by the fact that Ripple20 is a supply chain vulnerability, meaning it is hard to track all the devices that make use of this library.

Supply chain

ECDs exacerbate supply chain vulnerabilities. Supply chain attacks typically occur before devices are deployed onto organisations' networks. However, as seen in the SolarWinds supply chain attack, compromised software updates to devices deployed onto a network can also be a vector.

Supply chain attacks on ECDs often involve compromised software being installed in a certain ECD, such as a router or a camera. However, an ECD supply chain attack can also refer to a piece of hardware that has been implanted or modified to change a device's behaviour.

Supply chain attacks have a significant impact since the compromised software or device can present a single point of failure for the security of several entities.

In 2020, a series of Shodan* searches for 37 specific device models from 18 vendors (including printers, IP cameras, video conferencing systems and networking equipment) revealed that there were around 15,000 internet-connected instances of these affected devices that could potentially be compromised by anybody on the internet.

*Shodan is a search engine that lets users search for internet-connected devices.

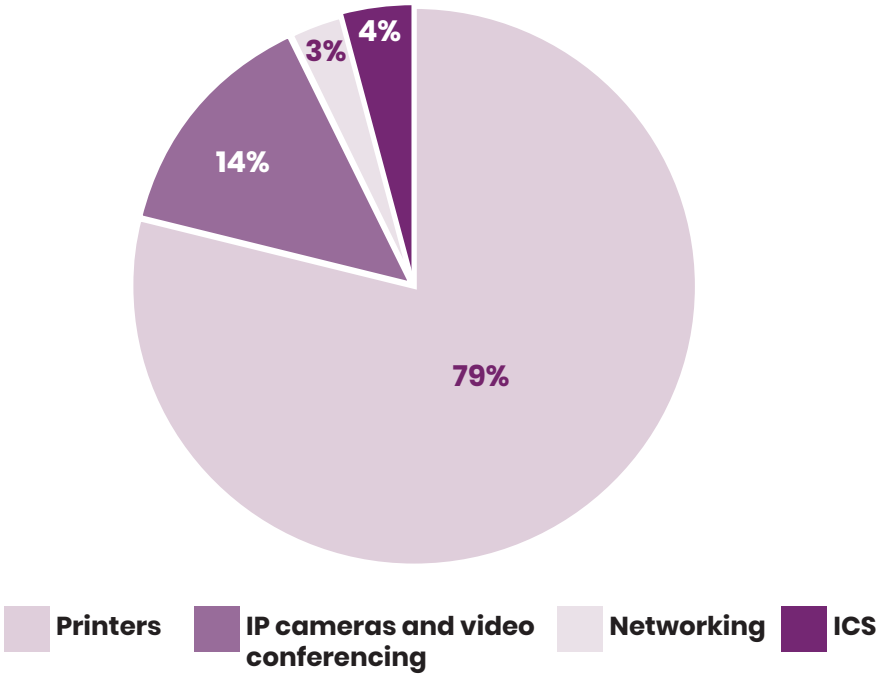


Figure 1: Shodan search results for vulnerable device models, split between printer, IP cameras and video conferencing, networking, and ICS.

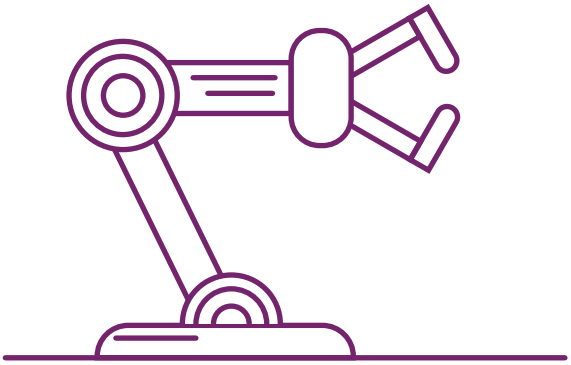
Bots

While threat actors still make ready use of compromised traditional computers, their bot armies are now increasingly composed of IoT.

The majority of IoT botnets have been used for coordinated DDoS attacks, although there are also IoT botnets that have the ability to exfiltrate sensitive information, as seen in the example of the Torri botnet. With the large, and rapidly increasing, number of ECDs, IoT botnets will continue to pose a unique challenge and noteworthy threat.

Case Study: Mirai-inspired IoT botnet

In 2020, a Russian hacking group, dubbed Digital Revolution, leaked documents claimed to be taken from a subcontractor to a company building cyber tools for the FSB, the Russian domestic intelligence agency. According to the documents, the project began in 2017 and looks to create an IoT botnet inspired by the notorious Mirai botnet of 2016. The plans showed that its main targets would be security cameras and network video recorders. Each infected device in the botnet would be reprogrammed to carry out password attacks on other devices in order to keep the botnet alive and growing. With a large enough botnet, attackers can launch powerful DDoS attacks. Both state and non-state actors are likely to exploit vulnerabilities in the IoT, including CCTV cameras, to form botnets for malicious ends including attack infrastructure and DDoS attacks.



Unpatched enterprise connected devices on enterprise networks

The security of common enterprise infrastructure devices such as desktops and laptops has advanced over the years through incremental improvements in operating systems and endpoint security. However, security controls for network devices such as enterprise printers are often ignored and thus present a greater potential for exploitation and compromise by threat actors seeking to gain a persistent foothold on target organisations.

Cyber actors will try to locate any vulnerable ECD to compromise enterprise systems. The use of unpatched devices is a common risk - since they lack the latest security updates, threat actors can use older known vulnerabilities to compromise such devices and gain privileged access to corporate networks. Ultimately, unpatched devices can then lead to data breaches or exposed information, manipulation of other assets, access to servers and systems, deployment of malware, or even physical disruption of operations.

Case Study: Enterprise printer vulnerabilities

In 2019, researchers conducted a six-month project to identify vulnerabilities and exploitations relating to devices made by six of the largest enterprise printer makers in the world. The researchers uncovered weaknesses that opened devices to DDoS attacks, but of much more concern is the potential for those devices to be used as entry points into corporate networks, with remote code execution (RCE) and the bypassing of security layers. According to a leading printer manufacturer, cyber crime represents a $445 billion global crisis for printers, PCs, and other mission-critical IoT endpoints.

Personal connected devices on enterprise networks

Personal IoT devices which are brought into the office environment may be allowed to connect to some enterprise networks. Due to the increased number of personal devices connected to enterprise networks, it is likely these devices will be targeted to gain access to the enterprise network.

Deployments of ECDs within large UK organisations are likely to present a different threat profile from personal consumer-use devices. Organisations often have more knowledge, responsibility and control for networks and cyber security, compared with a typical consumer. On the consumer side, DCMS has been conducting extensive work to improve the security of consumer connected products and brought legislation into Parliament to support this goal in 2021.

Conclusion

ECDs are a hugely attractive target for different types of threat actors as they can hold valuable, sensitive, or personal data. They present an easy target to compromise due to typically limited security efforts by vendors, a large attack surface (multiple endpoints for access to wider networks) and attack base for lateral movement. With the huge scale of ECDs connected to the internet comes a wave of products that are potential targets for both espionage and financially-motivated cyber actors.

The COVID-19 pandemic has driven a surge in remote working, and ECDs have played a vital role in supporting business continuity as the COVID-19 crisis affected companies across the globe. This has presented opportunities for organisations to work innovatively but has also created new opportunities for threat actors.

Organisations increasingly rely on ECDs. Many of these devices are built with poor security which could result in these devices being used as part of DDoS attacks, such as against large organisations and critical national infrastructure.

It is likely that malware which creates IoT botnets poses the greatest threat to ECDs and therefore the wider enterprise. The majority of IoT botnets have been used for coordinated DDoS attacks; however, there are also IoT botnets that have the ability to exfiltrate sensitive information.

Following initial compromise, ECDs can be used as an attack vector or pivot point to enable cyber actors to gain access to an enterprise's corporate network for espionage purposes, disruption, or financial gain. A single exposed ECD has the possibility of enabling a cyber actor to gain access to an enterprise's corporate network and potentially put their supply chain at risk.

All sectors deploying ECDs will be at risk, if these devices are found to be insecure, particularly due to the common uptake of particular devices that help enterprises to run on a day-to-day basis. The growing number of IoT devices being adopted by enterprises presents an expanding attack surface, with many of these devices being accessible over the public internet, and with cyber security often being an afterthought.

Assessment – what it is

NCSC Assessment products are drawn from all-source information. We fuse government, industry, media and open source material with unique classified intelligence to provide assessment on cyber threats to the UK. They are commissioned by NCSC's 'customers', including government and industry, to inform their work. Assessment includes Key Judgements (KJs) and a Probability Yardstick. The purpose of these devices is to provide the reader with the key takeaways from the paper and ensure that the reader interprets any judgements in the way that the analyst intended.

Key judgements

Key Judgements provide answers to the specific questions agreed between NCSC and the sponsor of the paper when it was commissioned. KJs are the most important judgements that an NCSC analyst wants a reader to absorb. KJs relate only to a specific issue and are not a summary of the paper's overall assessment or a summary of all the judgements within a paper. Typically, a paper will contain no more than six or seven KJs and each will be approximately three or four lines long. KJs will generally correspond closely to the language in the main body of the paper.

PHIA probability yardstick

Most judgements have some degree of uncertainty associated with them. The assessment community use terms like unlikely or probable to convey this. These terms are used instead of numerical probabilities (e.g., 55%) to avoid interpretation of judgements as being overly precise, as most judgements are not based on quantitative data. A Yardstick establishes what these terms approximately correspond to in numerical probability. This ensures that readers understand a judgement as the analyst intends. The rigorous use of a Yardstick also ensures that analysts themselves make clear judgements and avoid the inappropriate use of terms that imply a judgement without being clear what it is (e.g., "if X were to occur then Y might happen").

The Professional Head of Intelligence Assessment (PHIA) Probability Yardstick splits the probability scale into seven ranges. Terms are assigned to each probability range. The choice of terms and ranges was informed by academic research, and they align with an average reader's understanding of the terms in the context of what they are reading.

@NCSC

National Cyber Security Centre

@cyberhq