Infoblox

REPORT

What is Lurking on Your Network

Exposing the threat of shadow devices

Foreword by Gary Cox, Technology Director, Western Europe at Infoblox

“For IT departments, the complexities and security issues around managing BYOD schemes and unsanctioned Shadow IT operations have long been a cause for concern.

“In an increasingly complex, connected world, this challenge has now been exacerbated by the explosion in the number of personal devices individuals own, as well as the plethora of new IoT devices being added to the network.

“Due to the poor security levels of many consumer devices, there is a very real threat posed by those connected devices operating under the radar of many organisations’ traditional security policies. These devices present a weak entry point for cybercriminals into the network, and a serious security risk to the company.

“With cybercriminals increasingly exploiting vulnerable devices, as well as targeting employees' insecure usage of these devices, it is crucial for enterprise IT teams to discover what's lurking on their networks and actively defend against the threats introduced.”

Overview

This report has been commissioned to gain a better understanding of the challenges that the IT office faces in securely managing shadow devices on enterprise networks.

With extensive insights provided by IT directors across the US, UK, Germany and UAE, as well as feedback from employees in the US and UK into their usage of non-business devices on enterprise WiFi networks, we investigate the extent to which shadow devices, and their use by employees, pose a security risk.

We also provide practical recommendations on how companies can best manage the rising threat posed by shadow devices.

The Challenge

There has been a massive explosion in the number and types of devices connecting to enterprise networks. Over three quarters of all organisations have more than 1,000 business devices, such as laptops or tablets supplied by or managed by the company, connected to the enterprise network on a typical day, with 10 percent reporting more than 10,000 devices typically connecting.

Even small businesses, those with between 10-49 employees and 50-99 employees, have a significant number of devices connecting – with 25 percent and 52 percent respectively reporting more than 1,000 business devices connecting on an average day.

Further to those devices deployed by the IT team, organisations across the US, UK and Germany have thousands of shadow personal devices, such as personal laptops, kindles and mobile phones, connecting to the network. However, the UAE has a much small number of devices connecting.

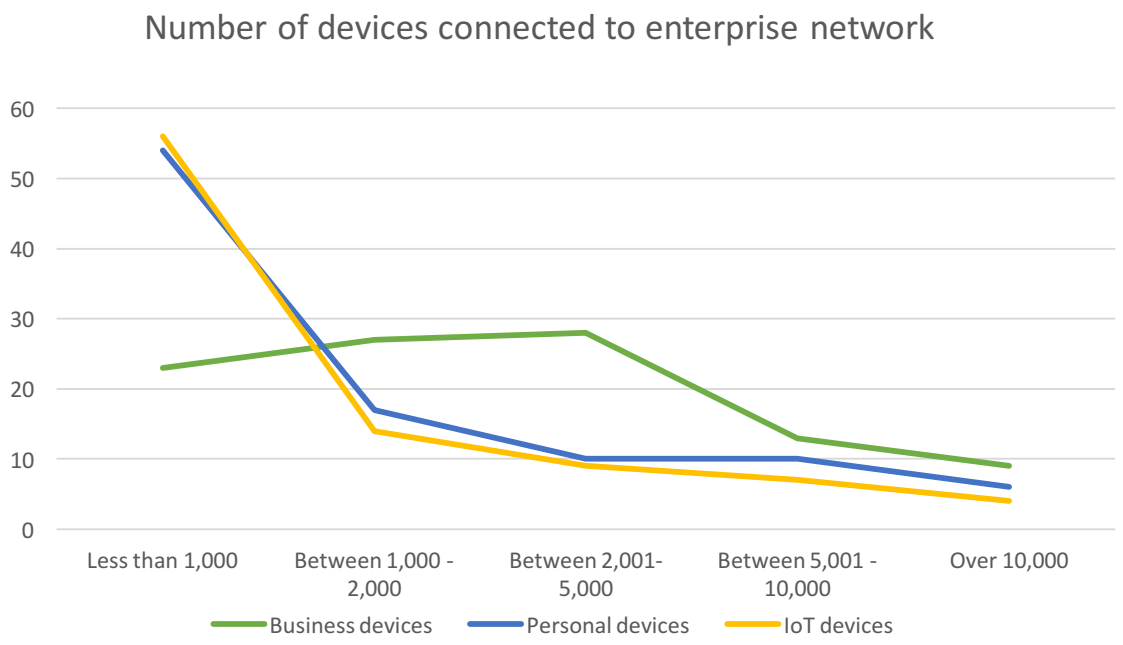
Over a third of companies in the US, UK and Germany (35 percent) reported more than 5,000 non-business devices connecting to the network each day. Conversely, just 16 percent of IT directors in the UAE reported having more than 500 personal devices connecting to their networks.

Employees from the US and UK report using their personal devices while connected to the enterprise network to access social media (39 percent), as well as to download apps, games and films (24 percent, 13 percent and 7 percent respectively).

These practices open enterprise networks up to the risk of malware infection, with social media increasingly being used to spread malware through social engineering, taking advantage of the fact people typically have a low guard and will click on many links with unknown sources. The mega breach of the streaming service Vevo last year, for example, which resulted in the loss of 3.12TB of sensitive internal data, occurred after an employee was compromised via a phishing campaign on LinkedIn.

Applications and media found on legal download sites have been found to contain serious malware. For example, in 2017, McAfee researchers identified 144 apps on the Google Play store that contained a new malware strain, Grabos, in most cases disguised as audio players and apps for downloading MP3 music files. Based on statistics from 34 of these applications, McAfee reported the malicious apps had been downloaded between 4.2 million and 17.4 million times.

IT directors also reported a significant number of non-business IoT devices connected to the enterprise network, such as smart TVs and digital assistants. A third of companies in the US, UK and Germany have more than 1,000 shadow IoT devices connected to their network on a typical day, with 12 percent of UK organisations reporting having more than 10,000.



The most common devices found on enterprise networks included:

- Fitness trackers, such as FitBit or Gear Fit – 49 percent
- Digital assistants, such as Amazon Alexa and Google Home – 47 percent
- Smart TVs – 46 percent
- Smart kitchen devices, such as connected kettles or microwaves – 33 percent
- Games consoles, such as Xbox or PlayStation – 30 percent

A number of exploits are available that enable cybercriminals to exploit these devices' controls. In 2017, for example, WikiLeaks published the details of a CIA tool, dubbed "Weeping Angel" that explains how an agent

can turn a Samsung Smart TV into a live microphone. Consumer Reports also found flaws in popular Smart TVs that could be used to steal data, as well as to manipulate the televisions to play offensive videos and install unwanted apps.

Vulnerable connected devices are easily discoverable online via search engines for internet-connected devices, like Shodan. Even when searching simple terms, Shodan provides details of identifiable devices, including the banner information, HTTP, SSH, FTP, and SNMP services. And, as identifying devices is the first step in accessing devices, this provides even lower level criminals with an easy means of identifying a vast number of devices on enterprise networks that can then be targeted for vulnerabilities.

For example, in March 2018:

- There were 5,966 identifiable cameras deployed in the UK
- There were 2,346 identifiable Smart TVs deployed in Germany

There were 1,571 identifiable Google Home deployed in the US

The Threat

The huge number of shadow personal devices and IoT devices on enterprise networks presents a massive challenge to the IT team – and security professionals in particular.

These devices are often exploited by cybercriminals using a number of different tactics, whether their goal is to steal data or cause disruption. The most common tactics include:

Data Exfiltration

Connected devices can serve as a weak entry point that malicious actors can use to infiltrate a network, from which a command and control (C&C) server can be used to exfiltrate data via DNS port. The technique, known as DNS tunneling, enables cybercriminals to insert malware or pass stolen information into DNS queries, creating a covert communication channel that bypasses most firewalls. While there are semi-legitimate uses of DNS tunnelling, most instances are malicious.

Project Sauron was one particularly advanced threat, which allegedly went undetected for five years at a number of organisations, that used DNS tunnelling for data exfiltration. And the tactic is far from rare. Assessing files containing the recent DNS traffic of 248 participating organisations for the 2016 Infoblox Security Assessment Report, Infoblox found that 40 percent of all files showed evidence of DNS tunnelling in them.

DDoS

Vulnerable connected devices can be hijacked to leverage DDoS attacks by sending repeated and frequent queries that bombard the Domain Name Server (DNS) – the address book of the Internet – slowing the IT network from processing legitimate queries, often to the point that it can no longer function.

Last year, Verizon reported on one such case at a US university campus where over 5,000 systems from its network dedicated IoT infrastructure – including connected vending machines and lightbulbs – were making hundreds of DNS queries every 15 minutes to sub-domains related to seafood. The botnet spread across devices on the network by brute forcing default and weak passwords, creating its own army that launched a DDoS attack on the network, which resulted in slow or inaccessible network connectivity across the campus.

Botnet Army

To harness the most power with which they can wreak havoc, hackers are increasingly targeting weak IoT devices across the world that they can control and use to launch massive DDoS attacks. The 2016 Infoblox Security Assessment Report revealed that 35 percent of all files showed evidence of botnet activity.

In 2016, the Mirai botnet, which leveraged over 600,000 infected IoT devices, targeted DNS service provider Dyn. Under a sustained attack throughout the day, the repeated interruption to Dyn's services resulted in many sites across North America and Europe going down, including Twitter, Netflix, Reddit and CNN.

Ransomware

An increasingly popular tactic, ransomware is a form of malware that, once it takes over a computer or network, threatens to deny access to or destroy your data. Ransomware can easily intercept an enterprise network after being accidently downloaded by an employee on either a business or personal device connected to network, as City University discovered when an administrative assistant downloaded a document from a legitimate educational website that, unbeknownst to her, was infected with ransomware.

IoT devices themselves can also be targeted with ransomware. Two researchers at DefCon demonstrated that they could gain full control of a connected thermostat, opening its users up to ransom demands in order to regain control. In an enterprise, such an attack could result in an office becoming inhabitable.

Confidence in security policies

To manage the security threat posed by shadow personal devices and IoT devices in the network, 82 percent of organisations have introduced a security policy for connected devices. However, our research indicates that IT directors are misguided in their estimation for how effective these policies are.

While 88 percent of the IT leaders that responded to our survey believe that their security policy is either effective or very effective, nearly a quarter of employees from the US and UK that we surveyed (24%) did not know if their organisation had a security policy.

Furthermore, of those that reported that their organisation did have a security policy for connected devices, 20 percent of UK respondents reported either rarely or never following it. And only one fifth of respondents in the US and UK reported that they followed it by the book.

Managing the threat

In response to the growing threat, 85 per cent of healthcare organisations surveyed have increased their cybersecurity spending over the past year; 12 per cent of organisations increased their cybersecurity spending by over 50 per cent.

Of the security investments made, getting the basics right appears to be the priority with traditional security solutions. Anti-virus software and firewalls were the most popular investments for cybersecurity spending in the healthcare industry (60 per cent and 57 per cent respectively).

However, the rise in malicious activity has also led many healthcare organisations to invest in other cybersecurity solutions. Half of organisation have invested in network monitoring to identify malicious activity on the network; one third have invested in DNS security solutions, which can actively disrupt Distributed Denial of Service (DDoS) attacks and data exfiltration; and 37 per cent invested in application security to secure web applications, operating systems and software.

Encryption is being deployed more regularly in the US than UK, with half of US healthcare IT professionals reporting that their company invests in encryption software, compared to 36 per cent of those in the UK.

Similarly, roughly one third of healthcare IT professionals indicated that their company is investing in employee education, email security solutions and threat intelligence (35 per cent, 33 per cent and 30 per cent respectively), with just one in five healthcare organisations investing in biometrics solutions.

Conclusions and recommendations

Whether down to neglect or ignorance, it is clear that organisations cannot rely upon employees to follow their security policy for connected devices. Network and security professionals must actively manage the threat introduced by shadow devices.

What steps should IT teams prioritise to defend their networks?

Restrict access to certain sites

IT administrators should deploy solutions that allow them to build safeguards that will prevent potential dangerous activity occurring on the network. For example, deploying solutions that give security administrators the ability to restrict access to certain types of content (e.g. social media, adult content and other restricted categories) will allow for policy enforcement and review of non-compliant activity in the organisation.

Integrating threat intelligence data into DNS management will also enable security teams to monitor and prevent access to Newly Observed Domains. Many new domains will be set up ahead of a phishing and/or spear phishing campaign, so in preventing access to these sites, organisations can reduce the risk of employees accidently introducing malware through clicking through to insecure links on personal devices connected to the enterprise network.

Achieve full visibility

Adopt a solution that enables you to manage policy and provide unified visibility into all the devices on premise or while roaming, as well as the network context required to prioritise action. For on-premise, IP address management system (IPAM) can enable effective management of devices.

Secure DNS

Most internet communications rely on DNS, although it is often not sufficiently secured, which creates vulnerabilities that can be exploited for data exfiltration and spreading malware. Over 91 percent of malware uses DNS to communicate with C&C servers, lock up data for ransom or exfiltrate data. Existing security controls, such as firewalls and proxies, rarely focus on DNS and associated threats – leaving organisations vulnerable to highly aggressive, rapidly proliferating attacks.

When secured, the DNS can act as an organisation’s first line of defence. The DNS can provide essential context and visibility, so IT admins can be alerted of any network anomalies, report on what assets and/or devices are joining and leaving the network, and resolve problems faster. IT leaders should invest in DNS security solutions that will enable them to identify and block malicious activity.

About Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com

Infoblox