A Trend Micro Research Report

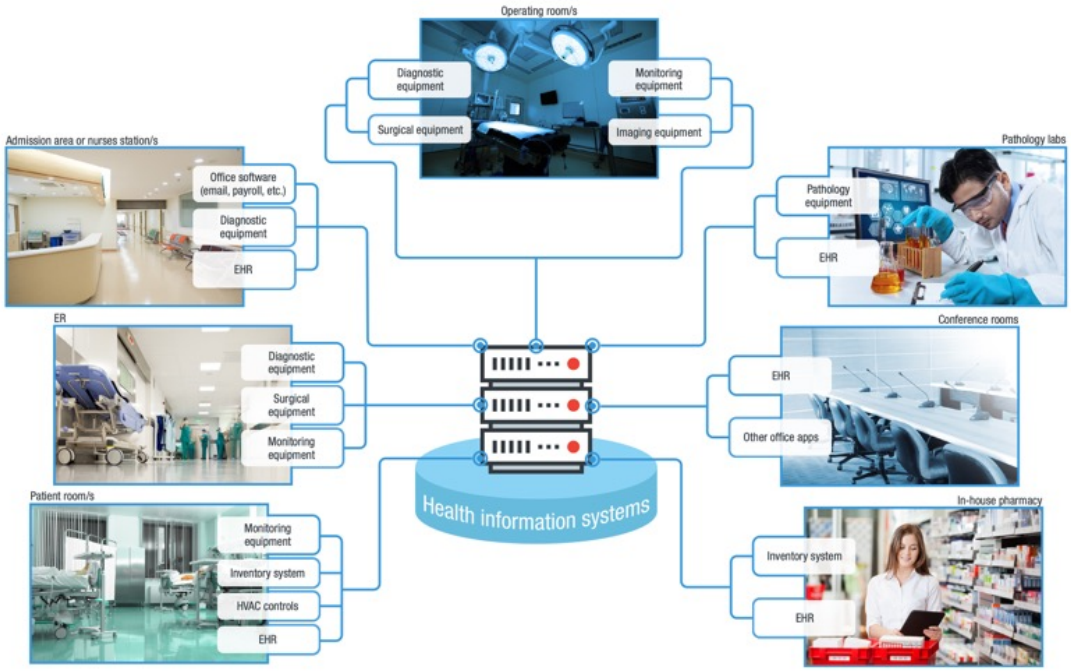
Protecting connected hospitals against cyber risks.

Learn how to defend your internet-enabled medical devices and systems from the most common threats.

INTRODUCTION

Healthcare is becoming an increasingly connected industry. Around the world, hospitals are harnessing internet-enabled medical devices and systems to speed up and improve patient care. But against this backdrop of progress, there's a potential cost — these technologies are advancing faster than they can be secured.

That's a major problem when you consider the array of connected devices and systems within many modern healthcare settings:



The connectedness of devices and systems to the health information system

What is the true nature and scale of this risk?
To answer that question, we conducted a global study that analysed how many healthcare-related cyber assets were exposed on the internet. The results should act as a wake-up call to all healthcare providers.

Read on to learn more, including a summary of our findings, potential implications for your organisation, and our key security recommendations to combat the most common risks we discovered.

FINDING VULNERABILITIES WITH SHODAN – THE WORLD'S MOST DANGEROUS SEARCH ENGINE

Our research involved searching for exposed devices and systems in hospitals and clinics using the Shodan web interface. We then downloaded the raw results for further analysis.

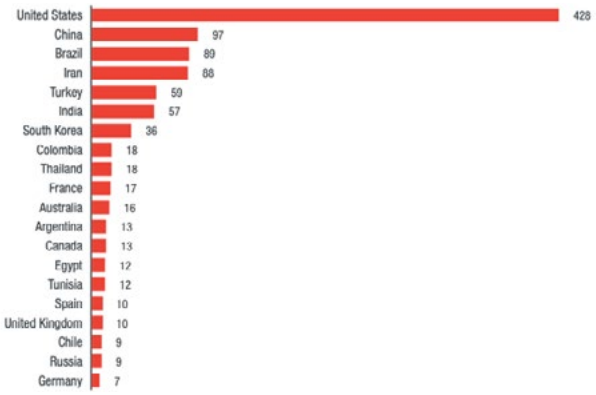
Shodan is a search engine for internet-connected devices. Software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in the exposed cyber assets. However, an adversary can also use Shodan to perform detailed surveillance and gather intelligence about a target – which is why it has been referred to as "the world's most dangerous search engine".

The exposed information we were able to locate in Shodan falls into the following categories:

- Medical images
- Protocols
- Databases
- Industrial controllers
- Healthcare systems software

1. Firmware attacks on devices

Digital Imaging and Communications in Medicine (DICOM®) is a standard for managing and exchanging medical images, and includes any related data shared between connected medical devices and systems. The image on the right shows the exposed DICOM devices/systems they were able to find – plotted against the top 20 countries.



Top 20 countries with DICOM servers exposed

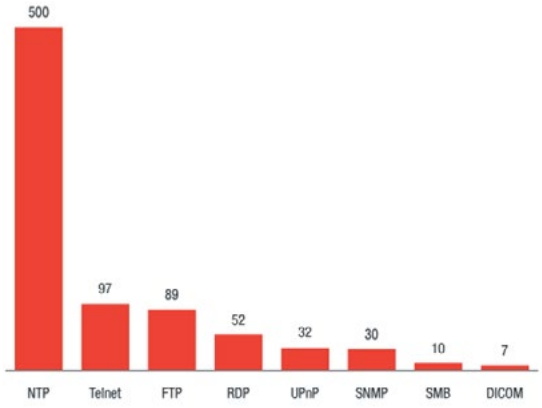
Key takeaways and insights

- The vast majority of DICOM devices were registered to their ISPs. This makes it very difficult to identify the actual owners of the devices.
- When reviewing the raw banner data, we were able to identify the DICOM application names. Perpetrators can use this to find known vulnerabilities and exploit them to compromise the device/system
- Shodan managed to fingerprint the device operating system for only 22 devices. Our assumption is that all the DICOM devices/systems Shodan discovered are application servers that store and process medical images.

2. Exposed protocols

Protocols refer to standards used to define how computers communicate over a network. When we talk about 'exposed protocols' in this research, we mean that we were able to view the port numbers or services that are in use and open on the internet. Vulnerabilities in the related protocols can be exploited to compromise the devices or systems that run them.

As the image on the right shows, **we found a high number of exposed ports/services inside hospitals and clinics.**



Exposed protocols in clinics and hospitals

We then selected the following eight ports/services that, if abused, could introduce the greatest amount of cyber risk for the hospitals and clinics.

NTP (Network Time Protocol) synchronizes time between computers.
Potential threat: Connections between computers and NTP servers are rarely encrypted, enabling hackers to perform man-in-the-middle attacks that reset clocks to months or even years in the past.

Telnet (Teletype Network) is an internet protocol that enables two-way, text-based communication.
Potential threat: In a Telnet session, all data is sent and received in clear text with no end-to-end content encryption, which means it's highly vulnerable to packet sniffing attacks.

FTP (File Transfer Protocol) is an internet protocol that enables two-way, text-based communication.
Potential threat: In a Telnet session, all data is sent and received in clear text with no end-to-end content encryption, which means it's highly vulnerable to packet sniffing attacks.

RDP (Remote Desktop Protocol) provides users with a graphical interface to connect to another computer over a network.
Potential threat: RDP has traditionally been abused to steal data as part of a targeted attack.

UPnP (Universal Plug & Play) enables networked devices (e.g. computers, printers, mobile devices) to discover, connect and share information with one another.
Potential threat: The Metasploit framework (the world's most used penetration testing software) includes many UPnP and SSDP modules that can help exploit devices with UPnP/SSDP enabled.

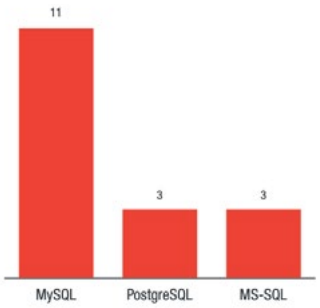
SNMP (Simple Network Management Protocol) is used to collect information and configure network devices (e.g. servers, printers, routers).
Potential threat: Hackers can use SNMP to their advantage in multiple ways, such as gaining control of devices to shut down a network interface.

SMB (Server Message Block) is a network protocol that allows applications (or their users) to share files within a computer network.
Potential threat: The 2017 WannaCry ransomware attack involved hackers exploiting an SMB vulnerability to spread and infect unpatched systems.

DICOM (Digital Imaging and Communications in Medicine) is a standard for storing and transmitting medical images enabling the integration of medical imaging devices from multiple manufacturers.
Potential threat: If DICOM servers are exposed online, perpetrators can potentially jeopardize critical information (such as patients' medical records) and disrupt healthcare operations through various methods, such as corrupting the data or infecting systems with ransomware.

3. Exposed databases

Databases play a critical role in modern hospital operations, and they're also a treasure trove of sensitive data. Suffice to say, that makes them lucrative targets for hackers. On the right, you can see the three most popular databases that we found to be exposed inside hospitals and clinics (MySQL, PostgreSQL and MS-SQL).



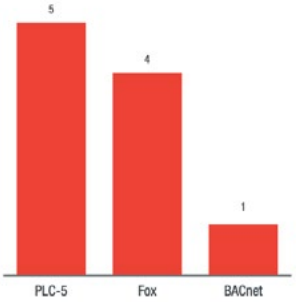
Exposed databases in clinics and hospitals

Key takeaways and insights

- Our Shodan results found that MySQL was the most popular database exposed inside hospitals and clinics.
- MS-SQL and PostgreSQL both had smaller exposure footprints.
- It's fairly safe to assume that hospitals use these three databases as the primary data store for their EHR, EMR and PACS. As a consequence, any breach would pose a serious threat to their day-to-day operations and patient data.

4. Exposed industrial controllers

Within both hospitals and clinics, the Shodan results revealed three types of exposed industrial control systems: PLC-5, Tridium Fox, and BACnet. The fact these systems were exposed is a major risk, as they're used to control a range of critical healthcare infrastructure – from internal networks and smart devices to HVAC, building access and fire detection.



Exposed controllers in clinics and hospitals

Key takeaways and insights

- When exposed building automation controls are compromised, hackers can quite literally "turn off the lights" inside the hospital.
- Compromising exposed building controls might also give hackers access to the backup generators, which they can then disable or sabotage.

5. Exposed healthcare systems software

Shodan has an image search database full of screenshots it has collected. We searched through this database and found several examples of exposed medical systems. These examples came from VNC servers that had authentication disabled, meaning they were accessible to anyone.

Here's a screenshot of one of the EHR/EMR system interfaces we found via Shodan Images:

Exposed graphical user interface (GUI) for patient record maintenance containing various PII

Key takeaways and insights

- We found a patient scheduling/appointment system that contained the patients' diagnosis information exposed.
- We also discovered an exposed graphical user interface for patient record maintenance that contained various Personally Identifiable Information.
- Pharmacy management software was one of the more common medical systems we were able to access online. As hospital pharmacies use similar software (which also integrates with their EHR/EMR system) their own patient data is also at potential risk.

DEFEND YOUR CONNECTED HEALTHCARE ENVIRONMENT

Internet-enabled devices and systems are changing the nature of healthcare – from improving internal efficiencies to speeding up patient diagnosis and treatment. But to prevent these gains from being undermined, robust cybersecurity is essential.

Trend Micro can help you mitigate security threats by protecting internet-enabled devices and systems throughout your healthcare organisation. To learn more, contact our team and ask about taking a **free trial of our industry-leading solutions.**

Speak to the team

Research disclaimer: At no point during this research did we perform any scanning or attempt to access any of the internet-connected devices and systems. All published data, including screenshots, were collected via Shodan. Any mention of brands in this research does not suggest any issue with the related products, only that they are searchable in Shodan. Furthermore, the analysis was carried out using September 2017 data, so given the fluid nature of the internet, the state of exposure may change.