Microsoft Security

Unpatched and exposed

The unique security risk of IoT devices

The increasingly connected world has enabled organizations to benefit from digital transformation, while creating new opportunities for threat actors to forge a multi-billion-dollar cybercrime industry.

What's the difference between IoT and OT?

The Internet of Things (IoT) is a reference to a growing network of physical objects ("things") that possess the sensors, software, and other technologies necessary to connect and exchange data with other devices on the internet. These devices can be medical equipment, embedded systems, sensors, printers, or any smart household or handheld device.

On the other hand, operational technology (OT) defines a specific category of hardware and software that were designed to monitor and control the performance for physical processes, devices, and infrastructure. In essence, OT is hardware or software that can operate independent of internet connectivity. Examples of these kinds of devices could be industrial machinery, robotic arms, turbines, centrifuges, air conditioning systems, and more.

The convergence between the IT world's laptops, web applications, and hybrid workforces and the OT world's factory and facility-bound control systems bring significant risks. Through greater connectivity, attackers can now "jump" air gaps between formerly physically isolated systems.

Similarly, IoT devices like cameras and smart conference rooms can become risk catalysts by creating novel entryways into workspaces and other IT systems.

In terms of impact, threat actors infiltrating an IT network can mean gaining access to critical OT. The implications of this are wide-reaching, from hefty financial losses for the organization and the theft of foundational IP, to onsite safety concerns where uncontrolled operational technology can affect human lives.

Examples of IoTs and OTs

Dedicated IoT	OT/ICS	General-purpose IoT
Sensors, detectors, meters, and purpose-built appliances	PCS/Industrial automation, embedded, proprietary	Cameras, thermostats, smoke alarms, HVAC
Greenfield	Industrial	

Corporate IoT	Network	Endpoints
IP cameras, printers, smart TVs, VoIP phones, smart appliances	Routers, switches, APs	Servers, laptops, tablets, mobile
Enterprise		Traditional

Attacks against remote management devices are on the rise

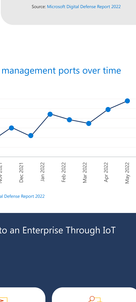
The Microsoft Threat Intelligence Center (MSTIC) observed a variety of IoT/OT attack types through its sensor network. The most prevalent attacks were against remote monitoring and management devices, attacks via the web, and attacks on databases (brute forcing or exploits).

If not secured correctly, an exposed IoT device can be used as a pivot point into another layer of the enterprise network as unauthorized users can remotely access the ports.

Remote Management Devices

Threat actors scan the internet for unpatched or exposed devices by identifying services listening on open network ports. These ports are commonly used for remote management of devices like desktops, tablets, smartphones, and sensors.

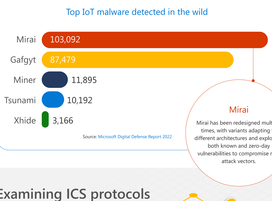
IoT/OT attack types



- 46% Remote management devices
- 30% Web
- 18% Databases
- 4% Email
- 1% Industrial control systems
- 1% Other

Source: Microsoft Digital Defense Report 2022

Increasing attacks on remote management ports over time



Source: Microsoft Digital Defense Report 2022

How an Attacker Can Get Into an Enterprise Through IoT

Attacker wants to sabotage a factory

Reconnaissance

Attacker finds an employee on social media who talks about:

- Their employer.
- The TV they bought a few years ago.
- Of they are working on at home.

Email

Attacker sends email or direct message to the employee. Rather than attaching their laptop or phone, attacker targets the TV on their home network.

Exploit

- IoT, without endpoint protection and auditing, is a safe place for an attacker to hide.
- The attacker searches the employee's home network for the employee's work device or OT device.
- Can downgrade firmware, use exploit and install backdoor/payload.

Lateral Movement

- Attacker moves from TV to the OT device that the employee took home. The OT device is now vulnerable to previously patched vulnerabilities.
- Attacker uses exploit and installs backdoor/payload.
- Payload lies about version.

Work from Home

Employee continues about their business, unaware of the compromise.

Return to Factory

- Employee takes OT device back to their place of work, such as at a factory.
- The factory trusts the hardware/OT device.
- Payload timed to go off (e.g. programmed to the DNS change; no longer on home network).

Revamped malware utility

As cybercrime groups have evolved, so, too, has their deployment of malware and choice of targets.

Cybercrime groups and nation state actors are repurposing botnets. The persistence of malware, such as Mirai, highlights the modularity of these attacks and the adaptability of existing threats.

The revamped utility of malware designed to target vulnerable IoT devices has serious implications for both organizations and nations, as lateral movement can expose backdoors to additional payloads and other devices on networks.

Top IoT malware detected in the wild

Source: Microsoft Digital Defense Report 2022

Mirai

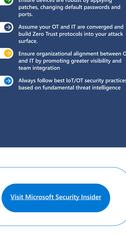
Mirai has been redesigned multiple times, with variants adapting to different architectures and exploiting both known and zero-day vulnerabilities to compromise new attack vectors.

Examining ICS protocols

We investigated OT data from our cloud-connected sensors, revealing the most common industrial control system (ICS) protocols.

Many ICS protocols are unmonitored and therefore vulnerable to OT-specific attacks (Microsoft Digital Defense Report 2022). This can mean increased risk for critical infrastructure.

These protocols provide insights into the nature of these devices and their attack surface. This is especially relevant to the security of critical infrastructure.



Some key learnings are:

Most of the protocols represented are proprietary

This means standard IT monitoring tools won't have adequate security visibility across these devices and protocols. As a result, networks are left unmonitored and therefore more vulnerable to OT-specific attacks.

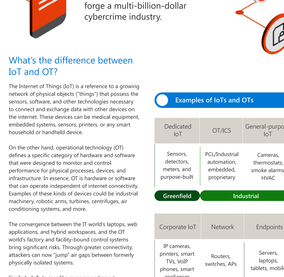
There is a large variety of vendor-specific protocols

This means vendor-specific security solutions won't be able to cover the whole network adequately. Microsoft prioritizes a vendor-agnostic approach to provide security coverage for the broad variety of different devices.

Protocols should not be exposed directly to the internet

Organizations should ensure these protocols are not exposed directly to the internet from their networks. This exposure could pose a major security risk due to vulnerabilities and the unsecure nature of these protocols.

Industrial control system protocol prevalence



Source: Microsoft Digital Defense Report 2022

Actionable Insights

- Use an IoT/OT-aware network detection and response (NDR) solution and a security information and event management (SIEM)/security orchestration and response (SOAR) solution to gain deeper visibility into IoT/OT devices on your network, monitor devices for anomalous or unauthorized behaviors, such as communication with unfamiliar hosts.
- Protect engineering stations by monitoring with endpoint detection and response (EDR) solutions.
- Reduce the attack surface by eliminating unnecessary internet connections and open ports, restricting remote access by blocking ports, denying remote access, and using VPN services.
- Ensure ICS protocols are not exposed directly to the internet.
- Segment networks to limit an attacker's ability to move laterally and compromise assets after initial intrusion. IoT devices and OT networks should be isolated from corporate IT networks through firewalls.
- Ensure devices are robust by applying patches, changing default passwords and ports.
- Assume your OT and IT are converged and build Zero Trust protocols into your attack surface.
- Ensure organizational alignment between OT and IT by promoting greater visibility and team integration.
- Always follow best IoT/OT security practices based on fundamental threat intelligence

Get the latest insights from Microsoft Security:

Visit Microsoft Security Insider

Microsoft Security