

Killware: Understanding the Threat and Protecting Your Assets

A briefing on a next-generation cyberthreat aimed at physical safety and critical infrastructure.

What Is Killware?

Killware is a type of cyberattack designed to cause direct physical harm, severe injury, or death by targeting critical infrastructure and operational systems, rather than simply stealing data or extorting money.

- **Definition:** Unlike standard ransomware or malware that focuses primarily on data theft or financial extortion, killware aims to disrupt physical operations or safety controls.
- **The Goal:** The intent is sabotage, terrorism, or raising the stakes of extortion by threatening human lives.
- **How It Works:** Attackers use phishing, unpatched software, or compromised remote access tools to infiltrate networks, manipulate industrial control devices, or shut down vital community services.

Primary Targets

- **Hospitals and Healthcare:** Crippling internal networks, medical devices, or patient monitoring systems.
- **Water and Wastewater Plants:** Tampering with chemical treatment levels, such as the 2021 incident in Oldsmar, Florida.
- **Power Grids and Energy:** Shutting down electrical power or manipulating oil and gas supply pipelines.
- **Public Transportation:** Halting trains, air traffic control, or municipal transit networks abruptly.

How to Prevent and Defend Against It

- **Network Segmentation:** Isolate critical operational technology (OT) from standard corporate IT networks.
- **Hardware-Enforced Security:** Implement data diodes to allow only one-way data flow out of sensitive networks, blocking external entry points.
- **Strict Access Control:** Enforce multi-factor authentication (MFA) across all administrative and remote access systems.
- **Rapid Patching:** Update firmware and software vulnerabilities promptly to close entry vectors.

Protecting Your Assets: Practical Steps

Killware attacks succeed by exploiting weak points in the systems people and organizations rely on every day. The following steps reduce exposure for individuals, families, small organizations, and larger operators of critical systems.

For Individuals and Families

- **Strong Credentials:** Use unique, strong passwords for every account and a password manager to keep track of them.
- **Enable Multi-Factor Authentication:** Turn on MFA wherever it is offered, especially for email, banking, and any “smart home” or utility account.

- **Patch Everything:** Keep phones, computers, routers, and any internet-connected home devices (thermostats, cameras, medical devices) updated with the latest security patches.
- **Recognize Phishing:** Be skeptical of unexpected emails, texts, or calls asking for credentials or urging immediate action — phishing is the most common entry point for these attacks.
- **Secure Home Networks:** Change default router and device passwords, segment smart-home devices onto a separate guest network, and disable remote access features you don't use.
- **Have an Emergency Plan:** Keep several days of water, non-perishable food, medication, cash, and a battery/solar power source on hand in case a utility or grid outage results from an attack.
- **Know Your Device Backups:** If you rely on internet-connected medical devices, know the manual backup or override procedure and keep it accessible.

For Businesses and Organizations

- **Network Segmentation:** Separate operational technology (OT) and industrial control systems from the general corporate IT network so a breach in one cannot reach the other.
- **Hardware-Enforced Boundaries:** Use one-way data diodes or similarly strict boundary controls for the most sensitive control systems.
- **Access Control and Audits:** Require MFA for all administrative, remote, and vendor access; audit who has access on a regular schedule and remove what is no longer needed.
- **Patch Management:** Apply firmware and software updates promptly, and maintain an inventory of every connected device so nothing is patched by accident of omission.
- **Backups and Recovery Testing:** Maintain tested, offline backups of critical configurations and data, and rehearse restoring from them.
- **Incident Response and Manual Fallback:** Regularly test how systems fail and confirm that manual overrides and safety interlocks still work if digital controls are compromised.
- **Employee Training:** Train staff to recognize phishing and social engineering, since attackers frequently gain initial access through a person rather than a technical flaw.
- **Third-Party Risk Management:** Vet the security practices of vendors and contractors with remote access to your systems, and limit that access to what is strictly necessary.

For Critical Infrastructure Operators

- **Follow Regulatory Guidance:** Follow sector-specific guidance from agencies such as CISA (Cybersecurity and Infrastructure Security Agency) and, for water systems, the EPA.
- **Participate in Information Sharing:** Share threat indicators with industry groups (ISACs) and law enforcement so attacks on similar systems elsewhere become early warning.
- **Independent Security Audits:** Bring in outside experts to test for exploitable weaknesses in both IT and OT environments before an attacker finds them.
- **Physical Safety Interlocks:** Ensure that safety-critical processes (chemical dosing, valve controls, grid switching) have physical or analog safeguards that cannot be overridden by a remote digital command alone.

This document is for general awareness and preparedness purposes and is not a substitute for a formal risk assessment or guidance from qualified cybersecurity and emergency management professionals.