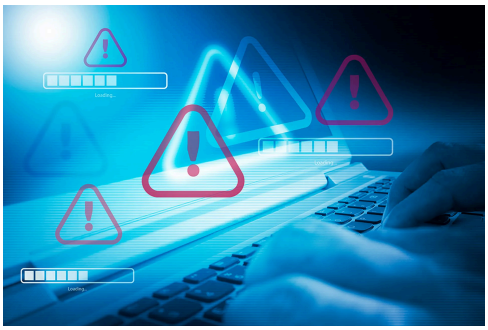
# Malware Incident Report

**Topic:** Three Recent Malware Attacks and Precautions Taken

**Prepared by:** Raseena. R

**Date:** August 11, 2025

## 1. PXA Stealer - Information-stealing Malware


- ☐ **Date:** August 8, 2025
- ☐ **Incident:** A new Python-based infostealer called *PXA Stealer* was detected, targeting over 200,000 user accounts worldwide. It spread through phishing websites and malicious ZIP archives pretending to be legitimate tools like PDF readers or Microsoft Word installers. Once executed, it stole browser cookies, saved passwords, autofill data, cryptocurrency wallet keys, and credit card details. The malware maintained persistence by adding entries to the Windows Registry and sent stolen data to attackers over Telegram channels, where it was later sold on dark web marketplaces.
- ☐ **Precautions Taken:**
  - ☐ Security advisories urged users to avoid clicking unknown links or opening suspicious email attachments.
  - ☐ Organizations pushed for disabling browser password storage and moving to encrypted password managers.
  - ☐ Endpoint security tools updated signatures to detect the malware.
  - ☐ Awareness campaigns highlighted safe downloading practices.

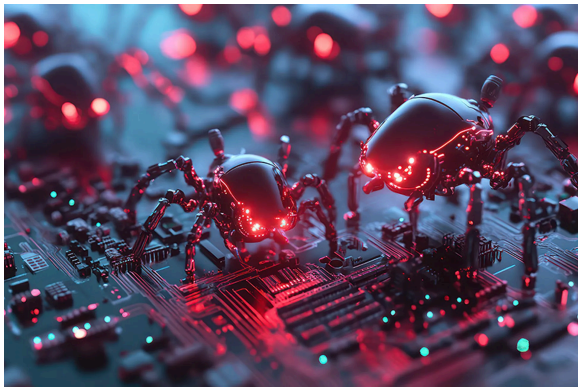
## 2. Akira Ransomware - SonicWall SSL VPN Exploit

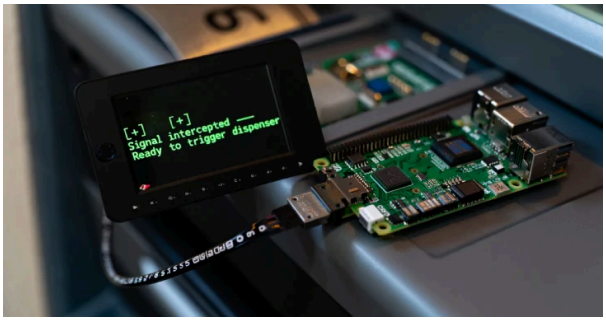




- ☐ **Date:** July 16, 2025 (attacks began mid-July)
- ☐ **Incident:** The Akira ransomware group began exploiting a suspected zero-day vulnerability in SonicWall SSL VPN appliances. By exploiting this flaw, they gained remote access to networks without valid credentials, deployed ransomware, and encrypted critical files. This campaign targeted enterprises using outdated or unpatched SonicWall devices, leading to operational disruptions and ransom demands in Bitcoin.
- ☐ **Precautions Taken:**
  - ☐ Organizations were instructed to immediately disable SSL VPN services if not essential.
  - ☐ Restrict access to VPN portals using IP allowlists.
  - ☐ Apply firmware updates and enable SonicWall's built-in security features.
  - ☐ Remove unused VPN user accounts and enforce multi-factor authentication (MFA) for all remote logins.
  - ☐ Incident response teams isolated infected systems to prevent lateral spread.

## 3. ATM Network Breach - Raspberry Pi Implant






- ☐ **Date:** August 9, 2025
- ☐ **Incident:** A targeted attack on a bank's ATM infrastructure involved physically installing a Raspberry Pi with a 4G modem inside a network switch connected to ATMs. This covert device bypassed the bank's firewall and intrusion prevention systems by operating inside the internal network. The attackers used a hidden remote shell tool (*TinyShell*) to send commands, aiming to deploy a rootkit named CAKETAP, which could alter ATM transaction authorizations for fraudulent cash withdrawals. Fortunately, security teams detected unusual network activity before the attack was completed.
- ☐ **Precautions Taken:**
  - ☐ The physical device was immediately removed from the network.
  - ☐ Forensic analysis identified and removed a compromised internal mail server used for persistence.
  - ☐ Additional physical security controls were added to network hardware.
  - ☐ Internal network segmentation and monitoring were tightened to detect similar intrusions in the future.