Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

The News



Active ScreenConnect campaign targets MSPs and downstream customers

ConnectWise is investigating unauthorised access to partner ScreenConnect environments, with current evidence pointing to possible abuse of independently developed RMM+ extensions rather than a vulnerability in ScreenConnect itself.

Huntress observed attackers deploying rogue ScreenConnect clients and malicious tooling to affected systems. The tooling could also target technicians connecting to infected devices, increasing the risk of compromise spreading through trusted remote-support relationships.

The campaign is particularly relevant to MSPs because compromised remote-management access can create downstream exposure across customer environments.

Defender focus: disable the identified RMM+ extensions, review unexpected remote commands and client deployments, revoke active sessions, enforce MFA and investigate technician systems connected to affected hosts.

Read more ›

Other news highlights

Critical Apache HTTP/2 Flaw Could Let Unauthenticated Attackers Execute Code Remotely

–

Critical Red Hat Quay Flaw Lets Attackers Read and Overwrite All Private Container Images in a Registry

–

Massive Microsoft 365 outage disrupts Outlook, Teams, Copilot worldwide

–

Citrix Patches 12 NetScaler and Secure Access Client Flaws, Including Authentication Bypass

The News

Top of the news



Fireworks AI breach exposes customer datasets and downstream services

Fireworks AI disclosed further impact from its security incident after attackers reached development systems through a third-party cloud provider.

Potentially affected information includes resource metadata, billing information and, for some customers, subsets of datasets and incomplete model weights. Payment card numbers were not affected.

The impact also extended downstream. Notion confirmed that AI chat transcripts associated with fewer than 1% of its customer workspaces were exposed through Fireworks. Notion said its own systems were not breached and disconnected from the provider while investigating the exposure.

The incident highlights how organisations can inherit security risk through infrastructure supporting trusted AI services, particularly where prompts, datasets, credentials and other sensitive information are processed externally.

Defender focus: identify third-party AI services and subprocessors, understand where organisational data is processed, minimise sensitive information shared with external services, review retention arrangements and rotate credentials where supplier exposure is identified.

Read more ›

Other news highlights

Attackers abuse Qubole's trusted AWS access to reach customer accounts and steal secrets and data.

–

AI agents used to target emergency services, banks and universities across multiple countries.

–

Default credentials exposed connected-vehicle identity systems at two automakers.

–

C***isco BroadWorks flaw added to CISA's Known Exploited Vulnerabilities catalogue.***

Geo-Politics



France attributes supermarket refrigeration attacks to Iran-linked cyber unit

French authorities have attributed the October cyberattacks against refrigeration systems at approximately 700 French retail sites to Shahid Kaveh, a cyber unit linked to Iran's Islamic Revolutionary Guard Corps.

The attribution is a significant update to the attacks covered in last week's Threat Pulse, when responsibility remained unconfirmed. French authorities said the attacks caused substantial food losses, material damage and fires. Similar refrigeration incidents later affected organisations elsewhere in Europe, but France has not attributed those attacks to the same group.

The incident shows how attacks against connected operational technology can move beyond IT disruption and create physical, financial and business-continuity consequences.

Read more ›

Other news highlights

China-nexus espionage campaigns target government, telecoms and critical infrastructure

–

Russia-aligned Turla uses new malware to target government Exchange servers

Breaches

Security Breaches this week



Maersk confirms data theft from legacy system

Shipping and logistics group Maersk confirmed that an attacker gained unauthorised access to a local legacy system inherited through a previous acquisition and extracted data.

The WhiteArmor ransomware group has claimed responsibility and says it stole around 100GB of information. Maersk has not confirmed the group's identity or its claims about the stolen data, and currently says its findings strongly suggest no sensitive data has been disclosed.

Maersk says the incident is isolated to the affected local system, with no indication of impact to its wider systems or customer and partner connections through APIs or EDI. It does not currently expect operational disruption.

The incident highlights the importance of maintaining visibility and consistent security controls across inherited technology following acquisitions.

Defender focus: inventory legacy and acquired systems, apply consistent identity and access controls, review unusual access and data-transfer activity, and validate attacker claims against confirmed company disclosures.

Read more ›

Other news highlights

–

Baker Tilly notifies clients after data held by third-party provider is compromised.

–

European telecom data exposure reportedly exposes 125 million text messages.

–

SEGA confirms data breach exposing 2.2 million email addresses.

–

Node.js Fixes 16 Flaws, Including HTTP/2 Bugs That Crash Servers and Leak Other Connections' Data

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-116606 & CVE-2026-111560 | Barracuda ESG
Barracuda confirmed exploitation affecting a small number of organisations. The flaws can be chained to bypass authorisation and gain root access where an affected administrative interface is reachable. Apply current security patches, update firmware and restrict administrative access to trusted networks.

CVSS score: 9.3

THIS WEEK | CVE-2026-125350 | Google Chromium
Google patched an actively exploited use-after-free vulnerability in Chromium's XML component. Successful exploitation could allow arbitrary code execution inside the browser sandbox through malicious web content. Upgrade Chrome to a fixed stable release and update other Chromium-based browsers as their vendors release fixes.

CVSS score: 8.8

Last week’s recaps

CVE-2026-76418
Cisco ASA and FTD

CVSS 8.6. Cisco reported active exploitation of an unauthenticated SSL VPN flaw that can reload affected firewalls when secondary authentication is configured. Apply the fixed ASA or FTD release, restrict remote access and review tunnel-group settings.

CVE-2026-28336
SolarWinds Dameware

CVSS 9.9. SolarWinds disclosed a command-injection vulnerability that can compromise the remotely controlled host; authentication is required. Upgrade Dameware 2026.3 and earlier to fixed version 2026.3.1.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's November PixelLeaks profile records five disclosed or published victim listings since the group first appeared on 3 November. A further 15 listings remained under Upcoming Disclosures at the time of capture. All victim and capability assertions are source claims and have not been independently verified.

Target industries

Technology and IT services account for three of the five disclosed or published listings (60%), with healthcare and general trading/textiles accounting for one each (20%). The sample remains too small to establish a consistent targeting preference.

Target country

The five disclosed or published listings span Saudi Arabia, Peru, Vietnam, China and Italy, with one claimed victim in each country. Fifteen upcoming disclosures are excluded because they remain unnamed and unverified.

Top Group

PixelLeaks uses staged leak-site listings and countdown deadlines to pressure victims before publishing data. No encryptor, ransom note, ransom amount or initial-access method has been confirmed. Validate leak-site claims against internal evidence, monitor for data exfiltration and prepare for phishing or business-email-compromise activity using exposed correspondence.

Top Threat Actors

PixelLeaks

5 disclosed/published listings
Nov 3–9

15 upcoming disclosures

Claims remain unverified

5 countries

1 disclosed/published listing each

Phishing

Phishing news this week



BluePhishing demonstrates emerging Entra AI-agent consent risk

Proofpoint researchers have demonstrated a technique dubbed BluePhishing that applies established OAuth consent-phishing concepts to Microsoft Entra AI agent identities.

The proof of concept shows how an attacker could socially engineer a victim into approving a malicious agent blueprint. Successful consent could allow attacker-controlled agent identities to be created in the victim tenant and operate using the permissions subsequently granted to them.

Proofpoint has not identified exploitation in the wild. The research instead highlights an emerging identity risk as organisations begin adopting AI agents alongside traditional applications and service principals.

Defender focus: restrict who can approve applications and agent identities, enforce least privilege, review consent and role grants, monitor newly created agent identities and maintain accountable ownership of non-human identities

Read more ›

Other news highlights

Microsoft patches exploited Outlook flaw that can expose NTLM authentication data.

–

Microsoft Teams begins rollout of AI-powered contextual phishing detection.

–

Stolen GitHub credentials target more than 61,000 repositories in secret-stealing campaign.

–

Microsoft records 7.3 billion email-based phishing threats during Q3 2026.