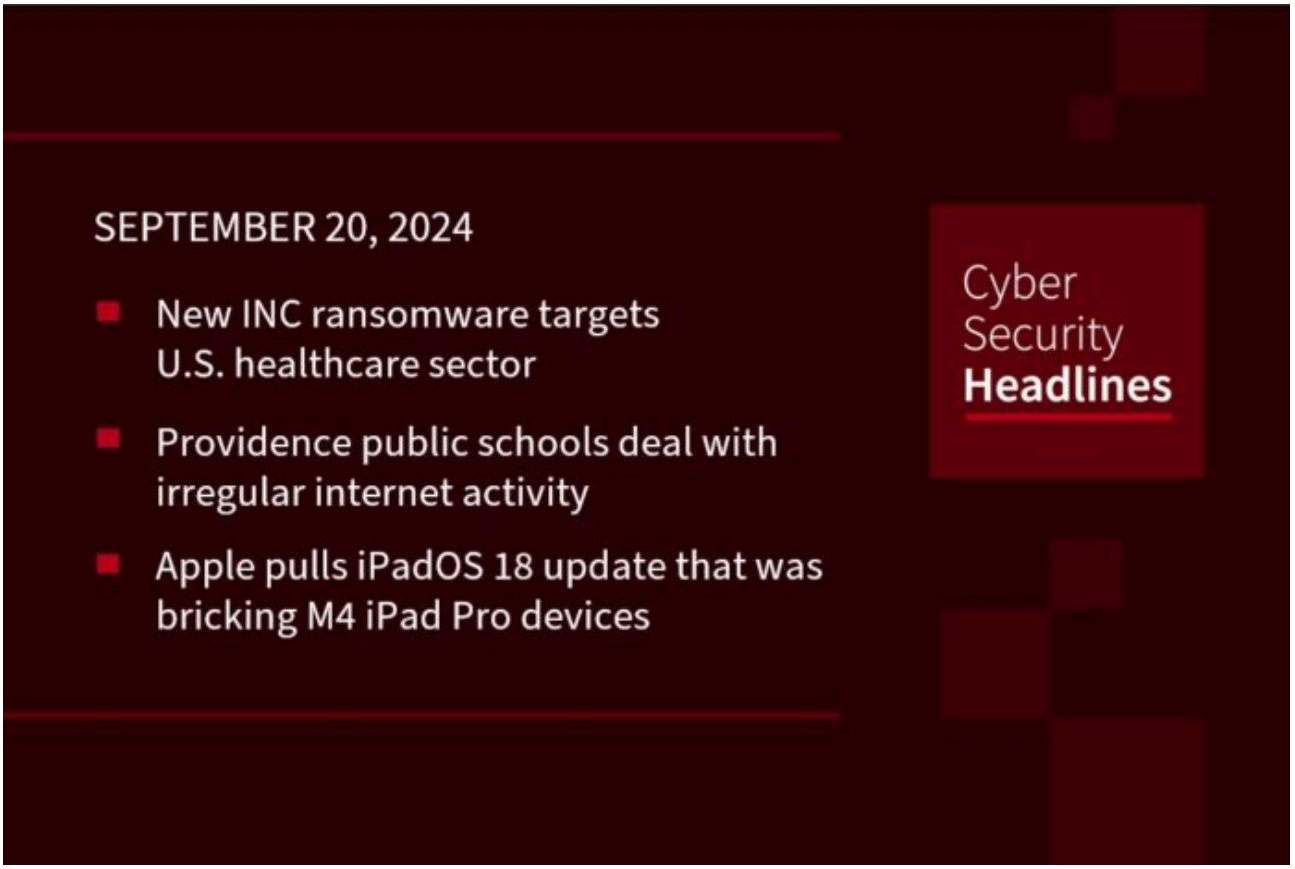
Cybersecurity News: INC targets healthcare, Providence schools cyberattack, Apple iPads bricked

By Steve Prentice

Published: 2024-09-20 · Archived: 2026-05-01 02:15:39 UTC



In today's cybersecurity news…

New INC ransomware targets U.S. healthcare sector

A warning from Microsoft about a financially motivated threat actor who is using INC ransomware against the U.S. health sector for the first time. The group has been given the name Vanilla Tempest. In a series of posts on X, Microsoft describes its campaign as "receiving hand-offs from GootLoader infections by the threat actor Storm-0494, before deploying tools like the Supper backdoor, the legitimate AnyDesk remote monitoring and management (RMM) tool, and the MEGA data synchronization tool." Following this, "the attackers proceed to carry out lateral movement through Remote Desktop Protocol (RDP) and then use the Windows Management Instrumentation (WMI) Provider Host to deploy the INC ransomware payload."

(The Hacker News)

Providence public schools deal with “irregular” internet activity

The Providence Public School District (PPSD) is working to handle issues caused by the shutdown of their network following an incident that occurred on September 11. The district serves more than 20,000 students across 37 schools. The PPSD is not saying if this was a ransomware attack or a cyberattack, but Rhode Island State Police and the Department of Homeland Security have been called in. The Medusa ransomware gang has claimed responsibility – this is the same group who last year attacked the Minneapolis Public School system and leaked student data. Classes remain open at PPSD schools.

(The Record)

Apple pulls iPadOS 18 update that was bricking M4 iPad Pro devices

Following complaints from some users about their devices turning into bricks without even the ability to be turned back on, Apple has paused the rollout of iPadOS 18 on iPad Pro tablets with the M4 chip. Regular recovery methods such as a force restart or recovery mode are not working, requiring owners to visit their local Apple store for evaluation. Apple says the problem appears to impact only a small number of devices, but did not provide actual numbers, nor any information on what the problem might be.

(BleepingComputer)

GitHub Scanner campaign pushes malware

A new and creative campaign is using GitHub repositories to send malware to users who visit an open source project repository or who are subscribed to email notifications from it. The threat actor opens a new issue on an open source repository claiming that there is a security vulnerability. The message then asks other users to visit a counterfeit GitHub Scanner domain, which, of course, tricks them into installing Windows malware. Users and contributors to these repositories receive email alerts from legitimate GitHub servers each time a threat actor files a new issue on a repository, which makes the campaign and its sense of urgency more convincing.

(BleepingComputer)

Thanks to today’s episode sponsor, Conveyor

Hadooken malware strikes Oracle servers

According to researchers from Aqua Security Nautilus, Hadooken is a Linux malware that targets Oracle WebLogic servers and has been linked to several ransomware families. Upon execution, the malware drops a Tsunami malware and deploys a cryptominer. Its target, the Oracle WebLogic Server is "an enterprise-level Java EE application server developed by Oracle, designed for building, deploying, and managing large-scale, distributed applications." The researchers suggest that the threat actors behind this campaign are targeting Windows endpoints for ransomware attacks, and Linux servers to deploy backdoors and cryptominers.

(Security Affairs)

Credential Flusher steals login credentials directly from browser

Researchers at OALABS describe this new technique as using an AutoIt script to "force users to enter their credentials in a browser operating in kiosk mode. This mode limits the user's ability to close the browser or access other applications, making it easier for hackers to obtain the desired information." The script does not steal the credentials but works with other stealer malware to do so. The attackers are taking advantage of the service provided by browsers to save user's passwords securely. The researchers state that standard security hygiene such as updated software, 2FA and avoiding re-use of passwords will help protect against this new technique.

(Security Affairs)

UK Pegasus spyware victims ask police to charge NSO Group

Four UK-based human rights advocates who are also critics of Middle Eastern states have requested that London's Metropolitan Police lay charges against NSO Group, the manufacturer of Pegasus spyware. The complainants state that their communications were spied on and they accuse NSO and its associates of being behind alleged spyware infections dating back to 2018. They say also that "the use of Pegasus against targets inside the UK has threatened the country's sovereignty and security," and point out that the UK government has not taken any legal action to date against the spyware maker.

(The Register)

Knowledge bases at risk due to ServiceNow misconfigurations

According to researchers Aaron Costello of AppOmni and Dan Meged of Adaptive Shield, thousands of companies are "potentially leaking secrets from their internal knowledge base (KB) articles via ServiceNow misconfigurations." The researchers, working separately and publishing separate reports, suggested that "pages set to 'private' could still be read by tinkering with a ServiceNow customer's KB widgets." This applies to cases where an organization' s KB is set to 'public,' but the pages inside it are set to 'private.' Meged estimates 30 percent of ServiceNow customers have this faulty configuration and could be "unwittingly exposing secrets held in their KB, such as first-time-access passwords for new starters connecting to a company VPN.

(The Register)
