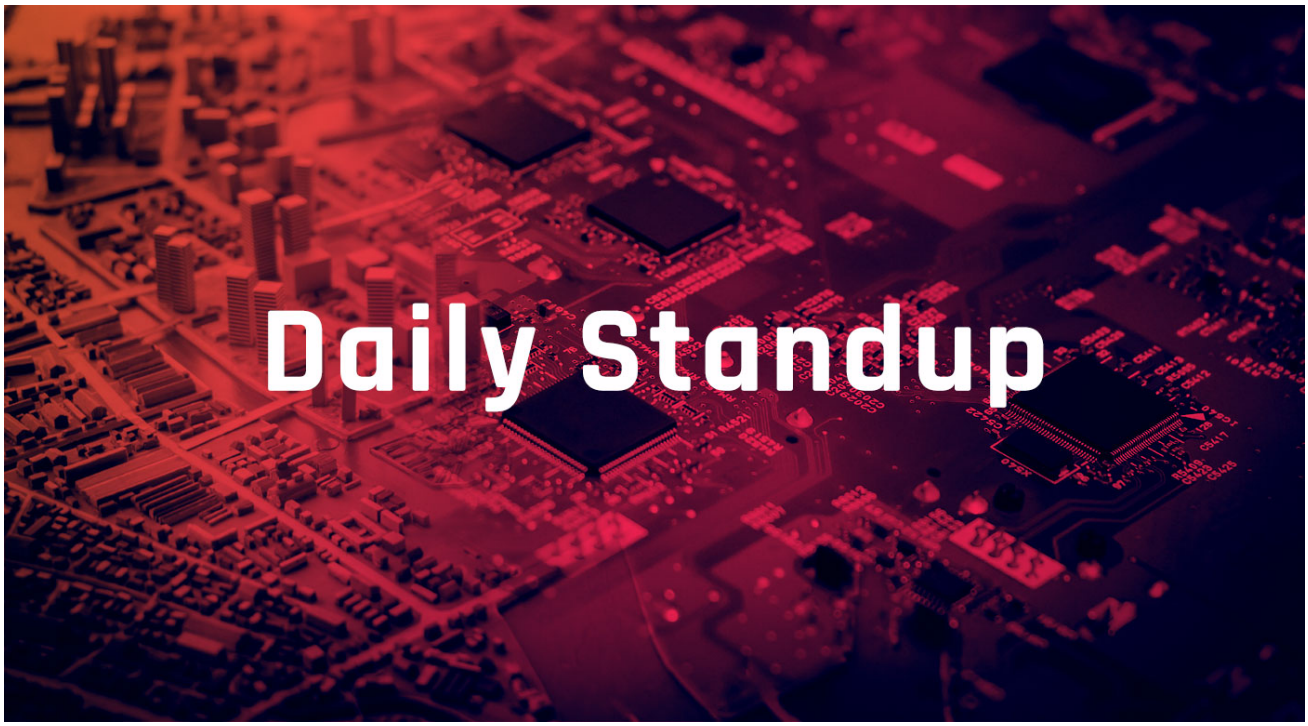
FLASHPOINT

Intelligence Report

Daily Standup

November 20, 2023



Yamaha Motor Confirms Data Breach Following Ransomware Attack (SecurityWeek)

Target audience: CISO, CIO, Incident Response, Security Architects, Security Engineers, Security Ops, Threat Intel/CTI, Windows or Unix Admin Teams

Summary: *The personal information of employees was stolen in a ransomware attack targeting a Philippines subsidiary of Yamaha Motor. The incident, the Japanese mobility and industrial giant says, occurred on October 25, and only impacted one server managed by Yamaha Motor Philippines, the company's motorcycle manufacturing and sales subsidiary in the country. The server, Yamaha Motor says, "was accessed without authorization by a third party and hit by a ransomware attack, and a partial leakage of employees' personal information stored by the company was confirmed." The company says it has restored all Yamaha Motor Philippines servers and systems that were not impacted in the attack. The incident did not affect the headquarters and other companies in the Yamaha Motor group, the motorcycle maker says. While Yamaha did not name the ransomware group responsible for the attack, the INC Ransom gang has claimed responsibility for the incident. According to SentinelOne, INC Ransom has been observed exploiting CVE-2023-3519, a critical-severity Citrix NetScaler ADC and Gateway vulnerability that came to light in July, when it was exploited as a zero-day by both financially motivated and state-sponsored threat actors.*

Analyst comment: Yamaha Motor Philippines was infected by an "INC" ransomware attack recently, but its operations seem unaffected. If that is the case, Yamaha Motor would be lucky, as companies with production lines that are victims of ransomware attacks often experience severe disruptions during the encryption process. Additionally, the INC ransomware gang is relatively new, with their first victim being posted in June. They have reportedly been exploiting the critical Citrix vulnerability CVE-2023-3519 in their attacks.

See also:

"Yamaha Motor Confirms Ransomware Attack on Philippines Subsidiary" (BleepingComputer)

"Inc ransomware blog" (Flashpoint)

"CVE-2023-3519" (Flashpoint Ignite)

Russian Hackers Use Ngrok Feature and WinRAR Exploit to Attack Embassies (BleepingComputer)

Target audience: CISO, Fraud Teams, Incident Response, Security Architects, Security Engineers, Security Ops, Threat Intel/CTI, Windows or Unix Admin Teams

Summary: *After Sandworm and APT28 (known as Fancy Bear), another state-sponsored Russian hacker group, APT29, is leveraging the CVE-2023-38831 vulnerability in WinRAR for cyberattacks. APT29 is tracked under different names (UNC3524,/NobleBaron/Dark Halo/NOBELIUM/Cozy Bear/CozyDuke, SolarStorm) and has been targeting embassy entities with a BMW car sale lure. The CVE-2023-38831 security flaw affects WinRAR versions before 6.23 and allows crafting .RAR and .ZIP archives that can execute in the background code prepared by the attacker for malicious purposes. In a report this week, the Ukrainian National Security and Defense Council (NDSC) says that APT29 has been using a malicious ZIP archive that runs a script in the background to show a PDF lure and to download PowerShell code that downloads and executes a payload. NDSC says that the Russian hackers used a Ngrok free static domain (a new feature Ngrok announced on August 16) to access the command and control (C2) server hosted on their Ngrok instance. By using this method, the attackers managed to hide their activity and communicate with compromised systems without being the risk of being detected.*

Analyst comment: APT29 has been seen actively exploiting vulnerability CVE-2023-38831 against international embassies. Many other threat actors have been leveraging the vulnerability since April. The WinRAR vulnerability allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. Attackers are incorporating this zero-day with older techniques through a diversification of attack methods.

See also:

"APT29 Pivots to Open Source Tools" (Flashpoint)

"CVE-2023-38831" (Flashpoint)

Canadian Armed Forces, Mounties Exposed in Data Breach (DarkReading)

Target audience: CISO, CIO, Incident Response, Security Ops, Threat Intel/CTI,

Summary: *Data breaches on Brookfield Global Relocation Services (BGRS) and SIRVA Canada systems have likely exposed everyone who has used relocation services within the Canadian government since 1999. Both BGRS and SIRVA Canada were contracted by the Canadian government to provide relocation support to government employees. Such services include financial, logistical, and other support for employees changing work locations. "Preliminary information indicates that breached information could belong to anyone who has used relocation services as early as 1999 and may include any personal and financial information that employees provided to the companies," reads the government's statement. Theoretically, attackers could access information about every CAF troop on NATO's eastern flank. While it's unclear how many people were impacted by the cyberattack, authorities vouched to provide credit monitoring services and cover the costs of "reissuing valid passports that may have been compromised."*

Analyst comment: The Canadian government confirmed a third-party breach occurred at Brookfield Global Relocation Services (BGRS). The breach contains information about Canadian government employees, the Canadian Armed Forces, and the Royal Canadian Mounted Police. This makes the data breach very sensitive, especially because it dates back to 1999. Threat actors will likely target affected individuals to gain account access.

See also:

"Incident 72033" (Cyber Risk Analytics)

"Incident 71431" (Cyber Risk Analytics)

Additional stories are included below, as they are of interest to threat intelligence teams:

"Welltok MOVEit Hack Impacts 1.6M Individuals" (Cybernews)

"FCC Adopts New Rules to Protect Consumers from SIM-Wwapping Attacks" (BleepingComputer)

"Exploit for CrushFTP RCE Chain Released, Patch Now" (BleepingComputer)

"Russia's LitterDrifter USB Worm Spreads Beyond Ukraine" (SecurityWeek)

"Shadowy Hack-for-Hire Group Behind Sprawling Web of Global Cyberattacks" (DarkReading)

"LummaC2 Malware Deploys New Trigonometry-Based Anti-Sandbox Technique" (Hacker News)

"Poloniex Confirms Hackers Identity, Offers $10M White Hat Reward to Return Stolen Funds" (CryptoSlate)

Please find past standups at https://fp.tools/home/intelligence/standup.