



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

7 Apr 25

## Cyber Threat Roundup

*A collection of recent open-source items of interest to the Defense Industrial Base*

### Contents

Articles .....	2
A Flaw in Verizon's iOS Call Filter App Exposed Call Records of Millions .....	2
Microsoft Credits EncryptHub, Hacker Behind 618+ Breaches, for Disclosing Windows Flaws .....	2
North Korean Hackers Deploy BeaverTail Malware via 11 Malicious npm Packages .....	2
Port of Seattle Says Ransomware Breach Impacts 90,000 People .....	2
WinRAR Flaw Bypasses Windows Mark of the Web Security Alerts .....	3
E-ZPass Toll Payment Texts Return in Massive Phishing Wave .....	3

## Articles

### **A Flaw in Verizon's iOS Call Filter App Exposed Call Records of Millions**

Verizon's Call Filter app allows users to identify and manage unwanted calls, such as spam and robocalls. It offers features like spam detection, automatic blocking of high-risk spam calls, and the ability to report unwanted numbers. A vulnerability affects the Verizon Call Filter app's /clr/callLogRetrieval endpoint. Although authentication is enforced via JWT tokens, the server failed to verify that the phone number in the header matched the token's user ID (sub). As a result, attackers could retrieve call histories for arbitrary numbers. The issue likely affected most Verizon Wireless users, as the service is often enabled by default. "While there was no indication that the flaw was exploited, the issue was resolved and only impacted iOS devices. Verizon appreciates the responsible disclosure of the finding by the researcher and takes the security very seriously," Verizon said in a statement.

<https://securityaffairs.com/176217/hacking/verizon-s-ios-call-filter-app-flaw.html>

### **Microsoft Credits EncryptHub, Hacker Behind 618+ Breaches, for Disclosing Windows Flaws**

Microsoft credited the discovery of multiple vulnerabilities to a party named "SkorikARI with SkorikARI," which has been assessed to be another username for EncryptHub. The flaws in question, CVE-2025-24061 (CVSS score: 7.8) and CVE-2025-24071 (CVSS score: 6.5) were fixed by Redmond as part of its Patch Tuesday update last month. EncryptHub, also tracked under the monikers LARVA-208 and Water Gamayun, was spotlighted in mid-2024 as part of a campaign that leveraged a bogus WinRAR site to distribute various kinds of malware hosted on a GitHub repository named "encrypthub." According to PRODAFT, EncryptHub is estimated to have compromised over 618 high-value targets across multiple industries in the last nine months of its operation.

<https://thehackernews.com/2025/04/microsoft-credits-encrypthub-hacker.html>

### **North Korean Hackers Deploy BeaverTail Malware via 11 Malicious npm Packages**

The North Korean threat actors behind the ongoing Contagious Interview campaign are spreading their tentacles on the npm ecosystem by publishing more malicious packages that deliver the BeaverTail malware, as well as a new remote access trojan (RAT) loader. The end goal of the campaign is to infiltrate developer systems under the guise of a job interview process, steal sensitive data, siphon financial assets, and maintain long-term access to compromised systems. The findings illustrate the persistent nature of Contagious Interview, which, besides posing a sustained threat to software supply chains, has also embraced the infamous ClickFix social engineering tactic to distribute malware.

<https://thehackernews.com/2025/04/north-korean-hackers-deploy-beavertail.html>

### **Port of Seattle Says Ransomware Breach Impacts 90,000 People**

Port of Seattle, the US government agency overseeing Seattle's seaport and airport, is notifying roughly 90,000 individuals of a data breach after their personal information was stolen in an August 2024 ransomware attack. The agency disclosed the attack on 24 Aug 25, saying the resulting IT outage disrupted multiple services and systems, including reservation check-in systems, passenger display boards, the Port of Seattle website, the flySEA app, and delayed flights at Seattle-Tacoma International Airport. After the incident, the Port also decided not to give in to the cybercriminals' demands to pay for a decryptor even though they threatened

to publish stolen data on their dark web leak site.

<https://www.bleepingcomputer.com/news/security/port-of-seattle-says-ransomware-breach-impacts-90-000-people/>

### **WinRAR Flaw Bypasses Windows Mark of the Web Security Alerts**

A vulnerability in the WinRAR file archiver solution could be exploited to bypass the Mark of the Web (MotW) security warning and execute arbitrary code on a Windows machine. The CVE-2025-31334 vulnerability can help a threat actor bypass the MotW security warning when opening a symbolic link (symlink) pointing to an executable file in any WinRAR version before 7.11. An attacker could execute arbitrary code by using a specially crafted symbolic link. It should be noted that a symlink can be created on Windows only with administrator permissions. Threat actors, including state-sponsored ones, have exploited MotW bypasses in the past to deliver various malware without triggering the security warning.

<https://www.bleepingcomputer.com/news/security/winrar-flaw-bypasses-windows-mark-of-the-web-security-alerts/>

### **E-ZPass Toll Payment Texts Return in Massive Phishing Wave**

An ongoing phishing campaign impersonating E-ZPass and other toll agencies has surged recently, with recipients receiving multiple iMessage and SMS texts to steal personal and credit card information. The messages embed links that, if clicked, take the victim to a phishing site impersonating E-ZPass, The Toll Roads, FasTrak, Florida Turnpike, or another toll authority that attempts to steal their personal information including names, email addresses, physical addresses, and credit card information. The volume of texts being sent in this scam is so large that users have been expressing their frustration over the frequency and persistence of the particular scam attempts, sometimes reaching up to 7 messages in a day.

<https://www.bleepingcomputer.com/news/security/toll-payment-text-scam-returns-in-massive-phishing-wave/>