

LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 18:51:26 UTC



[Threat Research | FireEye Inc](#)

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers



[CISA Alert \(AA20-239A\) Joint Technical Alert: FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks](#)

CISA Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks This joint advisory is the result of analytic efforts among the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury), the Federal Bureau of Investigation (FBI) and U.S. Cyber Command (USCYBERCOM). Working with U.S. government partners, CISA, Treasury, FBI, and USCYBERCOM identified malware and indicators of compromise (IOCs) used by the North Korean government in an automated teller machine (ATM) cash-out scheme—referred to by the U.S. Government as “FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks.” CISA, Treasury, FBI, and USCYBERCOM highlight the cyber threat posed by North Korea—formally known as the Democratic People’s Republic of Korea (DPRK)—and provide recommended steps to mitigate the threat. Refer to the following Malware Analysis Reports for associated IOCs: CROWDEDFLOUNDER, ECCENTRICBANDWAGON, ELECTRICFISH, FASTCash for Windows, HOPLIGHT, and VIVACIOUSGIFT.

- 108 Subscribers

 Author Url

[New ElectricFish samples from USCYBERCOM](#)

FileHash-MD5: 2 | FileHash-SHA1: 2 | FileHash-SHA256: 2

New ElectricFish samples uploaded to VT by USCYBERCOM. Check <https://otx.alienvault.com/pulse/5cd45f00ae1a8e3cb266c520> for previous activity and Yara rule.

- 373,973 Subscribers

Source: <https://otx.alienvault.com/browse/pulses?q=tag:ElectricFish>