TO: All MS-ISAC Members

DATE: August 26, 2020

SUBJECT: CISA Joint Technical Alert (TA) and Malware Analysis Reports (MAR) - North
Korean Remote Access Tools - TLP: WHITE

On August 26, 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) issued a joint Technical Alert (TA) that is the result of collaborative analytic
efforts by each agency.

The CISA Malware Analysis Reports (MAR) are the result of analytic efforts between the
Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the
Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD
identified Remote Access Tool (RAT) malware variants used by the North Korean government.
This malware variants have been identified as ECCENTRICBANDWAGON, VIVACIOUSGIFT,
and FASTCASH for Windows. The U.S. Government refers to malicious cyber activity by the
North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA
activity, visit https://www.us-cert.gov/hiddencobra.

Information on these variants including screenshots, md5’s, and recommendations can be found
at the links below.

ECCENTRICBANDWAGON - https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a
VIVACIOUSGIFT - https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239b
FASTCASH for Windows - https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239c

USCYBERCOM uploaded associated malware samples of the reports on its VirusTotal account
that can be found here. Previously reported North Korean malicious cyber activity and important
mitigation recommendations can be found here.

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Subject to standard copyright rules, TLP:WHITE information may be distributed without
restriction.
https://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.