North Korea Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the North Korean government's malicious cyber activities. The U.S. Government (USG) refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a complete list of related CISA publications, many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to North Korean government actors). Additionally, this page provides instructions on how to report related threat activity.

The North Korean government—officially known as the Democratic People's Republic of Korea (DPRK)—employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.[1],[2] Recent advisories published by CISA and other unclassified sources reveal that North Korea is conducting operations worldwide. According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "North Korea's cyber program poses a growing espionage, theft, and attack threat." Specifically, the Assessment states, "North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs."[3]

Latest U.S. Government Report on North Korean Malicious Cyber Activity

On February 17, 2021, CISA, the Federal Bureau of Investigation (FBI), and the Department of the Treasury identified malware and other indicators of compromise (IOCs) used by the North Korean government to facilitate the theft of cryptocurrency—referred to by the USG as "AppleJeus." See the Joint FBI-CISA-Treasury Cybersecurity Advisory: AppleJeus: Analysis of North Korea's Cryptocurrency Malware for details, including Malware Analysis Reports (MARs) on AppleJeus malware versions: Celas Trade Pro, JMT Trading, Union Crypto, Kupay Wallet, CoinGoTrade, Dorusio, and Ants2Whale.

The North Korean Malicious Cyber Activity section below lists all CISA Advisories, Alerts, and MARs on North Korea's malicious cyber activities.

Expand All Sections

North Korean Malicious Cyber Activity —

The information contained in the Alerts, Advisories, and MARs listed below is the result of analytic efforts between CISA, FBI, the U.S. Departments of Homeland Security (DHS), Defense (DoD), and Treasury; and U.S. Cyber Command; to provide technical details on the tools and infrastructure used by cyber actors of the North Korean government. The publications below include descriptions of North Korean malicious cyber activity, technical details, and recommended mitigations. Users and administrators should flag activity associated with the information reported in the publications listed in table 1 below, report the activity to CISA or FBI Cyber Watch (CyWatch) , and give the activity the highest priority for enhanced mitigation.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
February 17, 2021	- Joint FBI-CISA-Treasury CSA: AppleJeus: Analysis of North Korea's Cryptocurrency Malware - MAR 10322463-1.v1: AppleJeus – Celas Trade Pro - MAR 10322463-2.v1: AppleJeus – JMT Trading - MAR 10322463-3.v1: AppleJeus – Union Crypto - MAR 10322463-4.v1: AppleJeus – Kupay Wallet - MAR 10322463-5.v1: AppleJeus – CoinGoTrade - MAR 10322463-6.v1: AppleJeus – Dorusio - MAR 10322463-7.v1: AppleJeus – Ants2Whale	CISA, FBI, and the Department of the Treasury released a Joint Cybersecurity Advisory and seven MARs on the North Korean government's dissemination of malware that facilitates the theft of cryptocurrency—referred to by the U.S. Government as "AppleJeus."
October 27, 2020	- Joint CISA-CNMF-FBI CSA: North Korean Advanced Persistent Threat Focus: Kimsuky	CISA, FBI, and the U.S. Cyber Command Cyber National Mission Force (CNMF) released a new Joint Cybersecurity Advisory on TTPs used by North Korean APT group Kimsuky.
August 26, 2020	- Joint CISA-Treasury-FBI-USCYBERCOM CSA: FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks - MAR 10301706-1.v1: North Korean Remote Access Tool: ECCENTRICBANDWAGON - MAR 10301706-2.v1: North Korean Remote Access Tool: VIVACIOUSGIFT - MAR 10257062-1.v2: North Korean Remote Access Tool: FASTCASH for Windows	CISA, the Department of the Treasury, FBI, and U.S. Cyber Command released a joint Technical Alert and three MARs on the North Korean government's ATM cash-out scheme—referred to by the U.S. Government as "FASTCash."
August 19, 2020	- MAR 10295134.r1.v1: North Korean Remote Access Trojan: BLINDINGCAN	CISA and FBI have identified a malware variant—referred to as BLINDINGCAN—used by North Korean actors. FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. A threat group with a nexus to North Korea targeted government contractors early this year to gather intelligence surrounding key military and energy technologies.
May 12, 2020	- MAR 1028834-1.v1: North Korean Remote Access Tool: COPPERHEDGE - MAR 1028834-2.v1: North Korean Trojan: TAINTEDSCRIBE - MAR 1028834-3.v1: North Korean Trojan: PEBBLEDASH	CISA, FBI, and DoD identified three malware variants used by the North Korean government. - COPPERHEDGE is Manuscrypt family of malware is used by APT cyber actors in the targeting of cryptocurrency exchanges and related entities. Manuscrypt is a - TAINTEDSCRIBE and PEBBLEDASH are full-featured beaconing implants.
May 12, 2020	- U.S. Government Advisory: Top 10 Routinely Exploited Vulnerabilities	CISA, FBI, and the broader U.S. Government authored a Joint Alert with details on vulnerabilities routinely exploited by foreign cyber actors, including North Korean cyber actors.
April 15, 2020	- U.S. Government Advisory: Guidance on the North Korean Cyber Threat	The U.S. Departments of State, Treasury, and Homeland Security and FBI issued this Advisory as a comprehensive resource on the North Korean cyber threat for the international community, network defenders, and the public. The Advisory highlights the cyber threat posed by North Korea and provides recommended steps to mitigate the threat.
February 14, 2020	- MAR 10265965-1.v1: North Korean Trojan: BISTROMATH - MAR 10265965-2.v1: North Korean Trojan: SLICKSHOES - MAR 10265965-3.v1: North Korean Trojan: CROWDEDFLOUNDER - MAR 10271944-1.v1: North Korean Trojan: HOTCROISSANT - MAR 10271944-2.v1: North Korean Trojan: ARTFULPIE - MAR 10271944-3.v1: North Korean Trojan: BUFFETLINE - MAR 10135536-8.v4: North Korean Trojan: HOPLIGHT ***Note:*** *this version of HOPLIGHT MAR updates the October 31, 2019 version, which updated April 10, 2019 version.*	CISA, FBI, and DoD identified multiple malware variants used by the North Korean government. - BISTROMATH looks at multiple versions of a full-featured Remote Access Trojan implant executable and multiple versions of the CAgent11 GUI implant controller/builder. - SLICKSHOES is a Themida-packed dropper that decodes and drops a Themida-packed beaconing implant. - CROWDEDFLOUNDER looks at Themida packed Windows executable. - HOTCROSSIANT is a full-featured beaconing implant. - ARTFULPIE is an implant that performs downloading and in-memory loading and execution of a DLL from a hardcoded URL. - BUFFETLINE is a full-featured beaconing implant. - HOPLIGHT looks at multiple malicious executable files. Some of which are proxy applications that mask traffic between the malware and the remote operators.
September 9, 2019	- MAR 10135536-21: North Korean Proxy Malware: ELECTRICFISH ***Note:*** *this version of the ELECTRICFISH MAR updates the* May 9, 2019 version. - MAR 10135536-10: North Korean Trojan: BADCALL ***Note:*** *this version of the BADCALL MAR updates the* February 6, 2018 version: and STIX file.	CISA, FBI, and DoD identified multiple malware variants used by the North Korean government. - ELECTRICFISH implements a custom protocol that allows traffic to be tunneled between a source and a destination Internet Protocol (IP) address. - BADCALL malware is an executable that functions as a proxy server and implements a "Fake TLS" method.
October 2, 2018	- CISA Alert TA18-275A - HIDDEN COBRA FASTCash Campaign - MAR 10201537: HIDDEN COBRA FASTCash-Related Malware	CISA, Treasury, FBI, and U.S. Cyber Command identified malware and other IOCs used by the North Korean government in an ATM cash-out scheme—referred to by the U.S. Government as "FASTCash." The Joint Technical Alert provides information on FASTCash and the MAR provides information on 10 malware samples related to this activity.
August 9, 2018	- MAR 10135536-17: North Korean Trojan: KEYMARBLE	DHS and FBI identified a Trojan malware variant—referred to as KEYMARBLE—used by the North Korean government. KEYMARBLE is a RAT capable of accessing device configuration data, downloading additional files, executing commands, modifying the registry, capturing screen shots, and exfiltrating data.
June 14, 2018	- MAR 10135536-12: North Korean Trojan: TYPEFRAME	DHS and FBI identified a Trojan malware variant—referred to as TYPEFRAME—used by the North Korean government. DHS and FBI distributed this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity. This malware report contains an analysis of multiple malware samples consisting of 32-bit and 64-bit Windows executable files and a malicious Microsoft Word document that contains Visual Basic for Applications macros.
May 29, 2018	- CISA Alert TA18-149A: HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm - MAR 10135536-3: HIDDEN COBRA RAT/Worm	This Joint Technical Alert and MAR authored by DHS and FBI provides information, including IOCs associated with two families of malware used by the North Korean government: - A remote access tool, commonly known as Joanap; and Server Message Block worm, commonly known as Brambul.
March 28, 2018	- MAR 10135536.11: North Korean Trojan: SHARPKNOT - STIX file for MAR 10135536.11	DHS and FBI identified a Trojan malware variant—referred to as SHARPKNOT—used by the North Korean government. SHARPKNOT is a 32-bit Windows executable file. When executed from the command line, the malware overwrites the Master Boot Record and deletes files on the local system, any mapped network shares, and physically connected storage devices.
February 13, 2018	- MAR 10135536-F: North Korean Trojan: HARDRAIN - STIX file for MAR 10135536-F	DHS and FBI identified a Trojan malware variant—referred to as HARDRAIN—used by the North Korean government.
December 21, 2017	- MAR 10135536: North Korean Trojan: BANKSHOT - STIX file for MAR 10135536	DHS and FBI identified a Trojan malware variant—referred to as BANKSHOT—used by the North Korean government. This MAR analyzes three malicious executable files. - Two files are 32-bit Windows executables that function as Proxy servers and implement a "Fake TLS" method. - The third file is an Executable Linkable Format file designed to run on Android platforms as a fully functioning Remote Access Trojan.
November 14, 2017	- CISA Alert TA17-318A: HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL - CISA Alert TA17-318B: HIDDEN COBRA – North Korean Trojan: Volgmer	These Joint Technical Alerts provide information and IOCs on malware variants used by the North Korean government to maintain a presence on victims' networks and to further network exploitation. DHS and FBI distributed these alerts to enable network defense and reduce exposure to any North Korean government malicious cyber activity.
August 23, 2017	- MAR 10132963: Analysis of DeltaCharlie Attack Malware - STIX file for MAR 10132963	This MAR examines the functionality of the DeltaCharlie malware variant to manage North Korea's distributed denial-of-service (DDOS) botnet infrastructure (refer to TA17-164A). DHS distributed this MAR to enable network defense and reduce exposure to any North Korean government malicious cyber activity.
June 13, 2017	- CISA Alert TA17-164A: HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure	This Joint Technical Alert provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. Working with U.S. government partners, DHS and FBI identified Internet Protocol addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's DDoS botnet infrastructure.
May 12, 2017	- CISA Alert TA17-132A: Indicators Associated With WannaCry Ransomware	This DHS-FBI Joint Technical Alert provides information, including IOCs on the ransomware variant known as WannaCry. The U.S. Government publicly attributed this WannaCry ransomware variant to the North Korean government.

Report Activity Related to This Threat +

Mitigate and Detect this Threat +

Respond to an Incident +

References +

Contact Us

(888)282-0870

Send us email

Download PGP/GPG keys

Submit website feedback

Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

HSIN

Report

Home Site Map FAQ Contact Us Traffic Light Protocol PCII Accountability Disclaimer Privacy Policy FOIA No Fear Act Accessibility Plain Writing Plug-ins Inspector General The White House USA.gov

CISA is part of the Department of Homeland Security