


EMERGENCY COMMUNICATIONS COORDINATOR REPORT MAY 2024



Joint Cybersecurity Advisory (CSA): Akira

- Released by FBI, CISA, Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL).
- Akira Ransomware has affected a wide range of businesses, critical infrastructure and government agencies.
- New CSA has information on tactics and mitigation steps:
 - Defense evasion.
 - Prioritize remediating known exploited vulnerabilities.
 - Enable multifactor authentication (MFA) for all services to the extent possible (webmail, VPN, and access critical systems).
 - Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

JOINT CYBERSECURITY ADVISORY

Co-Authored by:    

Product ID: A124-1034
April 18, 2024

#StopRansomware: Akira Ransomware

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The United States' Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) are releasing this joint CSA to disseminate known Akira ransomware IOCs and TTPs identified through FBI investigations as recently as February 2024 and trusted third party reporting.

Since March 2023, Akira ransomware has impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia. In April 2023, following an initial focus on Windows systems, Akira threat actors deployed a Linux variant targeting VMware ESXi virtual machines. As of January 1, 2024, the ransomware group has impacted over 250 organizations and claimed approximately \$42 million USD in ransomware proceeds.

Early versions of the Akira ransomware variant were written in C++ and encrypted files with a .akira extension; however, beginning in August 2023, some Akira attacks began deploying Megazord, using Rust-based code which encrypts files with a .powerranges extension. Akira threat actors have continued to use both Megazord and Akira, including Akira_v2 (identified by trusted third party investigations) interchangeably.

Actions to take today to mitigate cyber threats from Akira ransomware:

- Prioritize remediating [known exploited vulnerabilities](#).
- Enable [multifactor authentication \(MFA\)](#) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your [local FBI field office](#) or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.


This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see cisa.gov/tlp.




TLP:CLEAR



Joint CSA: North Korean Spearphishing

- Released by FBI, State Dept., & National Security Agency (NSA).
- Exploiting improperly configured DNS Domain-based Message Authentication, Reporting and Conformance (DMARC) record policies to conceal social engineering attempts.
- Creating fake usernames and using legitimate domain names to impersonate individuals from trusted organizations.
- Red Flag Indicators include but are not limited to awkward English in emails, documents with macros, follow-up emails 2-3 days after initial contact, emails claiming to be from official sources but from unofficial email services.



JOINT CYBERSECURITY ADVISORY
Do-Authored by:    TLP:CLEAR Product ID: JCSA-20240502-001 May 2, 2024

North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts

SUMMARY

The Federal Bureau of Investigation (FBI), the U.S. Department of State, and the National Security Agency (NSA) are jointly issuing this advisory to highlight attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) Kimsuky cyber actors to exploit improperly configured DNS Domain-based Message Authentication, Reporting and Conformance (DMARC) record policies to conceal social engineering attempts. Without properly configured DMARC policies, malicious cyber actors are able to send spoofed emails as if they came from a legitimate domain's email exchange. The North Korean cyber actors have conducted spearphishing campaigns posing as legitimate journalists, academics, or other experts in East Asian affairs with credible links to North Korean policy circles. North Korea leverages these spearphishing campaigns to collect intelligence on geopolitical events, adversary foreign policy strategies, and any information affecting North Korean interests by gaining illicit access to targets' private documents, research, and communications. This Joint Cybersecurity Advisory (CSA) includes indicators of North Korean social engineering (page 4) for potential victims receiving spearphishing emails as well as mitigation measures (page 9) for organizations who could be victims of North Korean impersonation. For additional information on state-sponsored North Korean malicious cyber activity, see the June 2023 Kimsuky CSA, "[North Korea using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media](#)."

Actions to take today to mitigate malicious activity:

- Update your or your organization's DMARC security policy to one of the two configurations found below.


To report suspicious or criminal activity related to information found in the Joint Cybersecurity Advisory, contact your local FBI field office or submit a report to the [FBI Internet Crime Complaint Center \(IC3\)](#). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is distributed as TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tlp](#).



Directory Traversal Vulnerability Alert

- Released by CISA and the FBI.
- Directory traversal—or path traversal—vulnerabilities remain a persistent class of defect in software products.
- Directory traversal vulnerabilities involve a user manipulating inputs (i.e., input parameters or file paths) to illicitly access application files and directories that the developer did not intend for users to access.
- Secure by Design initiative to bring awareness to this vulnerability & remediation by manufacturers.
- <https://www.cisa.gov/resources-tools/resources/secure-design-alert-eliminating-directory-traversal-vulnerabilities-software>



Secure by Design Alert
Eliminating Directory Traversal Vulnerabilities in Software

TLP: CLEAR

Secure by Design

Malicious Cyber Actors Use Directory Traversal To Compromise Systems

Directory traversal—or path traversal—vulnerabilities remain a persistent class of defect in software products. The software industry has documented directory traversal vulnerabilities, along with effective approaches to eliminate these vulnerabilities at scale, for over two decades.¹ Yet software manufacturers continue to put customers at risk by developing products that allow for directory traversal exploitation. CISA and the FBI are releasing this Secure by Design Alert in response to recent well-publicized threat actor campaigns that exploited directory traversal vulnerabilities in software (e.g., [CVE-2024-1708](#), [CVE-2024-20345](#)) to compromise users of the software—impacting critical infrastructure sectors, including the Healthcare and Public Health Sector.

Additionally, this Alert highlights the prevalence, and continued threat actor exploitation of, directory traversal defects. Currently, CISA has listed 55 directory traversal vulnerabilities in our [Known Exploited Vulnerabilities \(KEV\) catalog](#). Approaches to avoid directory traversal vulnerabilities are known, yet threat actors continue to exploit these vulnerabilities which have impacted the operation of critical services, including hospital and school operations. CISA and the FBI urge software manufacturer executives to require their organizations to conduct formal testing (see OWASP testing guidance)² to determine their products' susceptibility to directory traversal vulnerabilities.

CISA and the FBI also recommend that software customers ask manufacturers whether they have conducted formal directory traversal testing. Should manufacturers discover their systems lack the appropriate mitigations, they should ensure their software developers immediately implement mitigations to eliminate this entire class of defect from all products. Building security into products from the beginning can eliminate directory traversal vulnerabilities.

Secure by Design Lessons to Learn

A core tenet of [secure by design](#) software development is that manufacturers create safe and secure behavior in the products they provide to customers. "Secure by Design" means that manufacturers design and build their products in a way that reasonably protects against malicious cyber actors successfully exploiting product defects. Incorporating this risk mitigation at the outset—beginning in the design phase and continuing through product release and updates—reduces both the burden of cybersecurity on customers and risk to the public. Vulnerabilities like directory traversal have been called "unforgivable" since at least 2007. Despite this finding, directory traversal vulnerabilities (such as CWE-22 and CWE-23) are still prevalent classes of vulnerability. For example, CWE-22 is listed in the top 25 lists for both the "most dangerous" and "stubborn" software weaknesses in 2023.³ Note: CWE-22 is a parent of several child weaknesses that involve directory traversal variations.

¹ Steve Christey and The MITRE Corporation, "Unforgivable Vulnerabilities," August 2, 2007, https://www.mitre.org/documents/unforgivable_vulns/unforgivable.pdf. In 2007, MITRE deemed directory traversal as one of the "unforgivable" vulnerabilities (i.e., "unforgivable" that the developer allowed it to exist in their product) yet exploitation continues today.

² "Testing Directory Traversal File Include," OWASP Web Security Testing Guide (WSTG) GitHub. Last modified July 2023. https://github.com/OWASP/wstg/blob/master/DOCUMENTS/4-Web_Application_Security_Testing/03-Authentication_Testing/01-Testing_Directory_Traversal_File_Include.md

³ "2023 CWE Top 25 Most Dangerous Software Weaknesses, Stubborn Weaknesses in the CWE Top 25," MITRE's CWE Top 25, 2023. https://www.mitre.org/top25/archive/2023/2023_top25_list.html, https://www.mitre.org/top25/archive/2023/2023_stubborn_weaknesses.html

CISA.gov | central@cisa.dhs.gov | @CISAcyber | @FBI | [CISA](#) | [FBI](#) | [OSG](#) | [EPA](#)

As of May 2024



Regional News of Note

- CR911 Symposium – May 14-15 in Kansas City, MO.
- FIFA World Cup Cities Meeting – May 14-15 in Dallas, TX
- Communications Exercises:
 - Kansas COMMEM – Wichita on June 11, 2024
 - Central States COMMEM – Joplin (MO)/Quapaw (OK) from September 10-13, 2024
- Other SIGBs/SIECs & Councils
 - SIAC Meeting on May 9, 2024, in Salina, KS
- Interoperability Markers update meeting requests will go out for the July timeframe.





For more information:

Chris Maiers

Christopher.Maiers@cisa.dhs.gov

202-701-3235