EMBER BEAR: Threat Actor Profile

March 30, 2022

Who is EMBER BEAR?

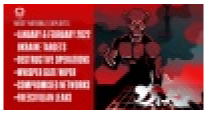
March 30, 2022

CrowdStrike Threat Intel Team Executive Viewpoint Research & Threat Intel

4/4/22 Editor's note: The hearing described below has been rescheduled for 10 a.m. EST on Tuesday, April 5.

On Wednesday, March 30, 2022, Adam Meyers, CrowdStrike Senior Vice President of Intelligence, will testify in front of CHS (House Committee on Homeland Security) on Russian cyber threats to critical infrastructure. Within his testimony, Adam will speak publicly for the first time about a Russia-nexus state-sponsored actor that CrowdStrike Intelligence tracks as EMBER BEAR.

EMBER BEAR (aka UAC-0056, Lorec53, Lorec Bear, Bleeding Bear, Saint Bear) is an adversary group that has operated against government and military organizations in eastern Europe since early 2021, likely to collect intelligence from target networks. EMBER BEAR appears primarily motivated to weaponize the access and data obtained during their intrusions to support information operations (IO) aimed at creating public mistrust in targeted institutions and degrading government ability to counter Russian cyber operations.



Meet the Adversary: EMBER BEAR

CrowdStrike Intelligence attributes destructive activity against Ukrainian networks using the WhisperGate wiper to EMBER BEAR, assessed at moderate confidence. Additionally, CrowdStrike Intelligence assesses with low confidence that data obtained through EMBER BEAR operations are used to support data leak operations conducted by multiple attribution fronts.

While other Russia-state nexus adversaries have also been implicated in the dissemination of stolen data for similar motivations — particularly FANCY BEAR and VOODOO BEAR, both operated by Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) — EMBER BEAR does not present known links with previously tracked adversaries. EMBER BEAR is not currently attributed to a specific Russian organization, although the adversary's target profile, assessed intent, and their technical tactics, techniques and procedures (TTPs) are consistent with other GRU cyber operations.

CrowdStrike Intelligence Confidence Descriptions

High Confidence – Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence – Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence – Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *To watch Adam Meyers' CHS testimony, visit the Committee on Homeland Security website.*
- *Learn how to incorporate intelligence on dangerous threat actors into your security strategy by visiting the CrowdStrike Falcon X™ product page.*

- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*

Related Content

CrowdStrike Delivers Adversary-Focused, Platform Approach to CNAPP and Cloud Security

“CrowdStrike Dominates in EDR...”

FORRESTER WAVE FOR ENDPOINT DETECTION AND RESPONSE

CrowdStrike “Dominates” in Endpoint Detection and Response

MITRE Engenuity ATT&CK®

ENTERPRISE EVALUATION

#1 in Prevention

#1 in Stopping Breaches

The leader in XDR

CrowdStrike leads the latest MITRE ATT&CK Evaluations with 100% automated prevention

Leading visibility

Leading analytic coverage

The **ONLY** platform with native Zero Trust & Identity Protection

CROWDSTRIKE

CrowdStrike Achieves 100% Prevention in Recent MITRE Engenuity ATT&CK Evaluation Emulating Russia-based Threat Groups