FEB 2022

Russia Update: ATIP Shield

IMMEDIATE ACTION REQUIRED

In response to the Ukrainian conflict, Adlumin recommends you immediately configure ATIP Shield.

Following the initial buildup and now invasion of Russian forces into Ukraine, the possibilities of a cyber conflict have significantly increased. Adlumin strongly recommends integrating ATIP Shield, which has a direct threat intelligence link with the Department of Homeland Security's CISA intelligence operation, an organization in the best position to distribute valuable insights on escalating cyber operations.

If your firewall or IDS/IPS device supports external blocklists, Adlumin recommends integrating our ATIP Shield threat intelligence feed. Many of the Indicators of Compromise (IoC) for these new attacks are actively being gathered by FBI, DHS, and other U.S. Intelligence sources. The U.S. Cybersecurity and Infrastructure and Security Agency (CISA) have issued a warning to all organizations in the United States, titled Shields Up, recommending the adoption of "heightened posture when it comes to cybersecurity" and making sure to protect their most critical assets. ATIP Shield is a dynamic feed that helps to defend against these IoCs.

Automated Indicator Sharing (AIS), a CISA capability, enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect AIS community participants and ultimately reduce the prevalence of cyberattacks. The AIS community includes private sector entities; federal departments and agencies; state, local, tribal, and territorial governments; information sharing and analysis centers, information sharing and analysis organizations, and foreign partners and companies.

ATIP Shield is Adlumin's publicly accessible threat intelligence feed, containing IP address indicators of compromise sourced from several industry-leading private sector companies and US government entities, including CISA DHS. The ATIP Shield feed is updated every 2 hours and is intended for automated ingest by firewalls, IDS/IPS, and other devices that can import external IP blocklists. Documentation and integration information for select vendors can be found in the platform by navigating to ***Threat Intel > ATIP Shield***. The feed is available at: **https://shield.adlumin.com/ip_indicators.txt**.

Copyright © 2022 Adlumin Inc. All rights reserved.