mvelazc0 / **PurpleSharp**   Public

Notifications   Fork 110   Star 774

<> Code   Issues   Pull requests 4   Actions   Projects   Wiki   Security   Insights

master

Go to file   <> Code

PurpleSharp

.gitignore

LICENSE

PurpleSharp.sln

README.md

azure-pipelines.yml

README   BSD-3-Clause license

PurpleSharp

Open Threat Research Community   Black Hat Arsenal USA 2021
Black Hat Arsenal Asia 2023

About
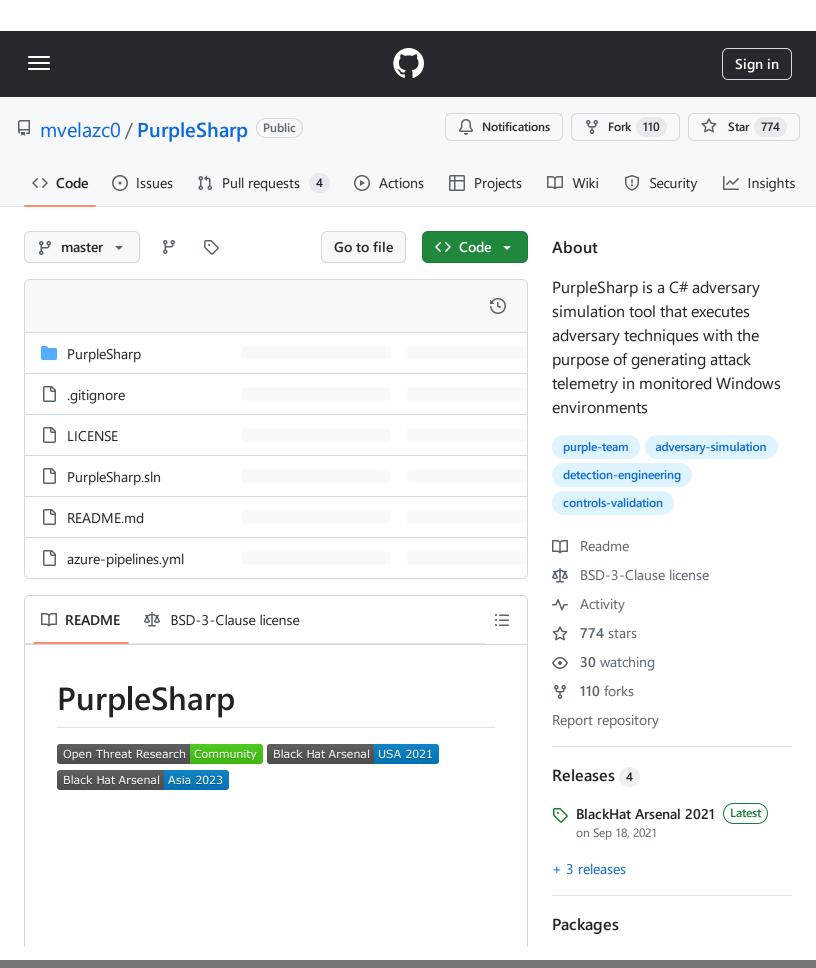
PurpleSharp is a C# adversary simulation tool that executes adversary techniques with the purpose of generating attack telemetry in monitored Windows environments

purple-team   adversary-simulation

detection-engineering

controls-validation

Readme

BSD-3-Clause license

Activity

774 stars

30 watching

110 forks

Report repository

Releases 4

BlackHat Arsenal 2021   Latest
on Sep 18, 2021

+ 3 releases

Packages

No packages published

Languages

● **C#** 100.0%

PurpleSharp

Defending enterprise networks against attackers continues to present a difficult challenge for blue teams. Prevention has fallen short; improving detection & response capabilities has proven to be a step in the right direction. However, without the telemetry produced by adversary behavior, building new and testing existing detection capabilities will be constrained.

PurpleSharp is an open source adversary simulation tool written in C# that executes adversary techniques within Windows Active Directory environments. The resulting telemetry can be leveraged to measure and improve the efficacy of a detection engineering program. PurpleSharp leverages the MITRE ATT&CK Framework and executes different techniques across the attack life cycle: execution, persistence, privilege escalation, credential access, lateral movement, etc. It currently supports 47 unique ATT&CK techniques.

PurpleSharp was first presented at Derbycon IX on September 2019.

An updated version was released on August 6th 2020 as part of BlackHat Arsenal 2020. The latest version was released on August 2021 as part of BlackHat Arsenal 2021

Visit the [Demos](#) section to see PurpleSharp in action.

Goals / Use Cases

The attack telemetry produced by simulating techniques with PurpleSharp aids research & detection teams in:

- Building new detecttion analytics
- Testing existing detection analytics
- Validating detection resiliency
- Identifying gaps in visibility
- Identifing issues with event logging pipeline

Quick Start Guide

Build from Source

PurpleSharp can be built with Visual Studio Community 2019 or 2020.

Download Latest Release

[Download](#) the latest release binary ready to be used to execute TTP simulations.

.NET Framework 4.5 is required.

Simulate

The PurpleSharp assembly is all you need to start simulating attacks.

For simulation ideas, check out the [Active Directory Purple Team Playbook](#), a repository of ready-to-use JSON playbooks for PurpleSharp.

Documentation

https://www.purplesharp.com/

Authors

- **Mauricio Velazco** - @mvelazco

Acknowledgments

The community is a great source of ideas and feedback. Thank you all.

- Olaf Hartong
- Roberto Rodriguez
- Matt Graeber
- Jonny Johnson
- Keith McCammon
- Andrew Schwartz