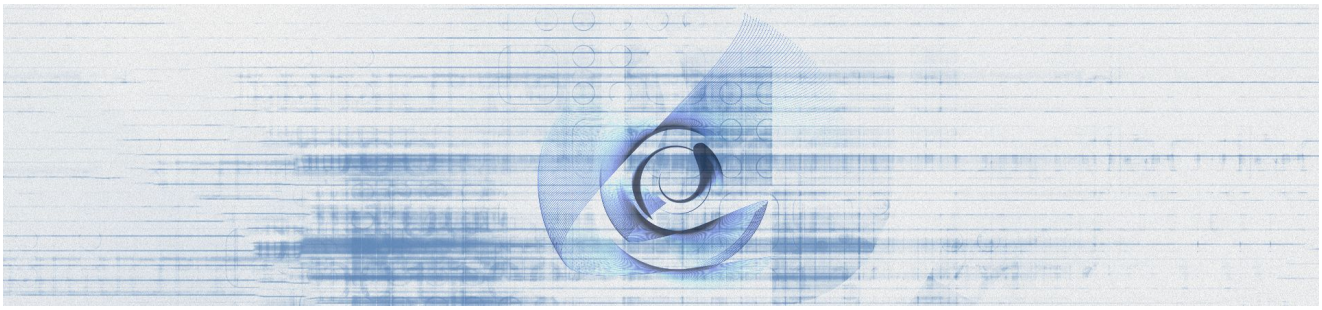
Full Spectrum Detections for 5 Popular Web Shells: Alfa, SharPyShell, Krypton, ASPXSpy, and TWOFACE

recordedfuture.com/full-spectrum-detections-five-popular-web-shells



Blog

Posted: 14th December 2021

By: INSIKT GROUP

Insikt Group®

Editor's Note: *The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

This report provides a technical overview of 5 prominent web shells: Alfa, Krypton, SharPyShell, ASPXSpy, and TWOFACE. It contains details on the capabilities of the web shells and host-based and network-based detections. This report is intended for security operations audiences who focus on detection engineering. Sources include the Recorded Future Platform®, GreyNoise, Shodan, and BinaryEdge.

Executive Summary

Web shells are common and powerful tools used by threat actors to maintain access to public-facing web servers. They are lightweight, sometimes containing as few as 4 lines of code, and let threat actors execute secondary payloads, escalate privileges, exfiltrate data, and move laterally within the compromised network. Web shells often go undetected due to the small footprint left during their use, an organization's limited visibility of their public-facing servers, and the ability for web shell-associated network traffic to blend

in with normal web server activity. Our research provides a full-spectrum approach to detecting web shells, combining log analysis, network analysis, and web shell scanning techniques. We focus on a subset of web shells recently used by state-sponsored and criminal threat actors: Alfa, SharPyShell, Krypton, ASPXSpy, and TWOFACE. Our methodology and detections can be applied internally for defenders but also by security researchers hunting for the presence of web shells on externally facing servers.

Key Judgments

- Web shells will continue to be used by both APTs and financially motivated threat actors, primarily due to their ease of use and their difficulty in being detected.
- We identified 4 techniques to detect web shells that can be used together: YARA rules, Sigma rules, network traffic patterns, and internal/external scanning. While these methods are not foolproof, they provide diverse opportunities for defenders to look for web shells on their systems.
- Security teams with limited host and network visibility can still detect web shells on their systems using HTTP scanning techniques.
- As long as threat actors can viably exploit public-facing servers, they will continue to use web shells to maintain persistence and provide additional capabilities.

Editor's Note: *This post was an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*