Hunting Webshells: Tracking TwoFace - SANS Threat Hunting Summit 2018

Published: 2019-02-13 · Archived: 2026-04-05 17:37:56 UTC

Microsoft Exchange Servers are a high-value target for many adversaries, which makes the investigation of them during Incident Response vital. Backdoor implants in the form of webshells and IIS modules on servers are on the rise. Find out how to hunt webshells and differentiate between legitimate use and attacker activity, using default logging available on every exchange server. The presentation will feature real-world examples carried out by an adversary group using web-based backdoors to breach and maintain access to networks of targeted organizations in the Middle East. Josh Bryant (@FixtheExchange), Director of Technical Account Management, Tanium Josh Bryant is currently a Director of Technical Account Management at Tanium where he helps customers conduct rapid Threat Hunting data collection on a very large scale. Prior to joining Tanium, he was a Cybersecurity Architect at Microsoft where he focused on delivering Cybersecurity services ranging from Tactical and Strategic Recovery to Advanced Threat Analytics implementations, Risk Assessments, and more, to customers in a variety of industries around the world. Josh is also a Master Sergeant in the Illinois Air National Guard, where he manages a team of Systems Administrators that maintain an Air Operations Center. He has over 19 years in IT specializing in Cybersecurity and Messaging, and spent some of his Active Duty U.S. Air Force time as a Network Security Manager, performing vulnerability assessments and penetration testing. Robert Falcone, Threat Researcher, Palo Alto Unit 42 Robert is a Threat Intelligence Analyst with Palo Alto Networks' Unit42 focusing on malware analysis, reverse engineering, and tracking advanced threat actors. Prior to joining Unit42, he was a Malware Research Engineer at iDefense focusing primarily on malware analysis and tracking threat actors associated with cyber espionage activity. He also worked as a Security Engineer within a Security Operations Center for a managed security service provider focused on intrusion detection and prevention.
