Rule of the Week: Possible Malicious File Double Extension

By Eugene Tkachenko

Published: 2020-05-01 · Archived: 2026-04-05 19:57:28 UTC

Adversaries can mask malicious executables as images, documents or archives, replacing file icons and adding fake extensions to the file names. Such “crafted” files are often used as attachments in phishing emails, and this is a fairly effective way to infect Windows systems due to “Hide known file types extensions” option enabled by default for Windows XP and newer systems. The real file extension is hidden by the system in the file browser and most applications following the system’s file browser policies. If the phishing email convinces the user to open the “document”, the malware is installed on the system, and then the lure document is often downloaded and run so that the user does not suspect anything.

Our SOC Team released an exclusive Sigma rule that detects suspicious use of an .exe extension after a non-executable file extension like .pdf.exe, a set of spaces or underlines to cloak the executable file in spear phishing campaigns: https://tdm.socprime.com/tdm/info/2FWv97nWNL5L/iea3vHEBv8lhbg_iMXqH/?p=1

Threat Detection is supported for the following platforms:

SIEM: Azure Sentinel, ArcSight, QRadar, Splunk, Graylog, Sumo Logic, ELK Stack, RSA NetWitness, Logpoint, Humio, RSA NetWitness

EDR: CrowdStrike, Carbon Black, Elastic Endpoint

MITRE ATT&CK:

Tactics: Initial Access

Technique: Spearphishing Attachment (T1193)

Please find hereby the top-5 community rules released last week by participants in Threat Bounty Program: https://socprime.com/en/blog/rule-digest-fresh-content-to-detect-trojans-and-ransomware/
