Unmasking Windows Advanced Persistent Threat Execution

Title	Unmasking Windows Advanced Persistent Threat Execution
Publication Type	Conference Paper
Year of Publication	2020
Authors	Coulter, Rory, Zhang, Jun, Pan, Lei, Xiang, Yang
Conference Name	2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)
Date Published	Jan. 2021
Publisher	IEEE
ISBN Number	978-1-6654-0392-4
Keywords	advanced persistent threat, APT, APT Execution, Collaboration, collaboration agreements, composability, Conferences, cyber security, data privacy, dataset, feature extraction, Industries, Manuals, policy-based governance, pubcrawl, Sandboxing, Scalability, security, statistical analysis
Abstract	The advanced persistent threat (APT) landscape has been studied without quantifiable data, for which indicators of compromise (IoC) may be uniformly analyzed, replicated, or used to support security mechanisms. This work culminates extensive academic and industry APT analysis, not as an incremental step in existing approaches to APT detection, but as a new benchmark of APT related opportunity. We collect 15,259 APT IoC hashes, retrieving subsequent sandbox execution logs across 41 different file types. This work forms an initial focus on Windows-based threat detection. We present a novel Windows APT executable (APT-EXE) dataset, made available to the research community. Manual and statistical analysis of the APT-EXE dataset is conducted, along with supporting feature analysis. We draw upon repeat and common APT paths access, file types, and operations within the APT-EXE dataset to generalize APT execution footprints. A baseline case analysis successfully identifies a majority of 117 of 152 live APT samples from campaigns across 2018 and 2019.
URL	https://ieeexplore.ieee.org/document/9343214
DOI	10.1109/TrustCom50675.2020.00046

Citation Key coulter_unmasking_2020

advanced persistent threat APT APT Execution collaboration collaboration agreements composability Conferences cyber security data privacy dataset feature extraction Industries Manuals policy-based governance pubcrawl sandboxing Scalability security statistical analysis