NAME: Amin Kharraz
AFFILIATION: Northeastern University
WEBSITE: http://www.ccs.neu.edu/home/mkharraz/
EMAIL:
PHONE NUMBER:
PUBLICATION DETAIL:
Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda, UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware, USENIX SECURITY 2016. Austin, Texas, August 2016.

TITLE: An automated Approach to Detect Ransomware Attacks

SESSION ABSTRACT: Today, an important enabler for malware detection is dynamic analysis which executes a malware sample in a controlled environment, and records its behavior. The presentation focuses on an automated system that is designed to detect ransomware with zero false positive. We show that the system significantly improves the state of the art, and is able to identify a previously unknown family that was not detected by the antimalware industry.

SESSION DETAIL: In this presentation, hear the findings of new academic research into ransomware in which we analyzed 148,223 recent general malware samples in the wild. We present a novel dynamic analysis system, called UNVEIL, that is designed to analyze and detect ransomware attacks and model their behaviors. We implemented a prototype of our approach in Windows through custom Windows kernel drivers that provide monitoring capabilities for the filesystem. In our approach, the system automatically creates an artificial, realistic execution environment and monitors how ransomware interacts with that environment. The presentation consists of the following parts: First, learn how we prepare the execution environment in our analysis system by generating an artificial user environment which serves as an “enticing target” to encourage ransomware to attack the user’s data. Second, see a comparison of different classes of ransomware on how they attack user’s data. For example, by analyzing the filesystem activity of a wide range of ransomware families, we extracted the I/O access sequences generated by ransomware. Our analysis shows that although these attacks can be very different in their attack strategies (e.g., evasion techniques, key generation, key management, connecting to C&C servers), they can be categorized into three main classes of attacks based on their access requests. Third, delve into how the system monitors the interaction of the malicious process by intervening the access requests to the filesystem. Hear about how we tested the system with real-world malware samples to automatically detect unknown (i.e., zero-day) ransomware. For example, our analysis shows that 72% of the ransomware samples detected by the system were not detected by any of the 55 VirusTotal scanners. Finally, get insight into the new ransomware family, called SilentCrypt, that we detected during our large-scale experiment. After our system detected the samples from this family and submitted them to VirusTotal, several AV vendors picked up on them and also started detecting them a couple of days later, confirming the malice of the sample that we automatically detected. Multiple online malware analysis systems such as malwr.com, Anubis, and a modern sandboxing technology provided by a well-known, anti-malware

company did not register any malicious activity for this sample. However, the sample showed heavy encryption activity when analyzed by UNVEIL.