Malware Analysis

Overview

The cyber threat landscape continues to evolve into an environment where attackers use ever-more-sophisticated tools and tactics to target government, private industry, and commercial enterprise systems and networks. With malware circulating in cyberspace at an all-time high, it continues to be the primary tool for conducting these attacks. Using a variety of threat vectors, including socially engineered e-mails, compromised web sites leading to drive-by web attacks, and infected media, cyber criminals routinely employ malware to breach enterprise security controls to conduct cyber espionage, data destruction, and denial-of-service attacks.

Having a detailed understanding of malicious threats is a critical requirement for protecting the enterprise. This requirement must be supported by a malware forensics function that can rapidly collect and analyze the malicious tools used in cyber attacks. Comprehensive analysis of the attacker’s malware can reveal infection vectors, attack sources, payloads, and attribution. Such information provides crucial threat intelligence to aid those responsible for protecting the network in remediating the threat, improving its security posture, and identifying new defensive strategies.

The Parsons Solution

To meet today’s threats, Parsons employs a malware analysis service that provides detailed damage assessment, mitigation, remediation, and reporting services for cyber attack incidents involving malware. We develop detailed analysis of malware code using a combination of static and dynamic techniques and tools. We perform deep-dive code forensics analysis and reverse engineering of malicious artifacts using state-of-the-art tools, techniques, and methods. Our malware analysis service can analyze a wide variety of current threats, including malicious office documents, viruses, bots, rootkits, keyloggers, trojans, and advanced persistent threats.
Parsons' malware analysis capability is based on more than 12 years of experience, resulting in the development of broad expertise in performing in-depth code analyses using both manual and automated approaches. Our manual approach includes analysis of binary executable construction, code deobfuscation, behavioral analysis, code attribution, and trend analysis using feature clustering techniques.

Parsons supports automated malware analysis processing using our proprietary Automated Malware Analysis and Storage System (AMASS). AMASS implements custom-developed analyzers and uses open source analysis tools to provide fast static and dynamic inspection of binary files across four distinct analytical functions: binary unpacking, signature identification, triage analysis, and dynamic analysis. These functions include static analysis processes for performing antivirus (AV) scanning, strings extraction, binary section hashing, and entropy analysis. Dynamic processing includes capturing of file, registry, and network behaviors exhibited by the executing malware. The systems analysis processing functions use an extensible design, enabling operators to add new analysis tools to the system with minimal effort.

Parsons maintains a secure, scalable malware laboratory and infrastructure for collecting, storing, cataloging, and analyzing malicious code samples. The malware lab's infrastructure leverages virtual machine technology for simulating Internet services and vulnerable operating system platforms with varying patch levels to support secure interactions with live malware. The malware lab currently houses tens of thousands of samples, including viruses, bots, rootkits, keyloggers, malicious office documents, and toolkits. The samples in the lab are obtained from a variety of feeds, including Parsons' honey pot, actual cyber incidents, and research repositories.