Analysis and Detection of Modern Cyber Payloads

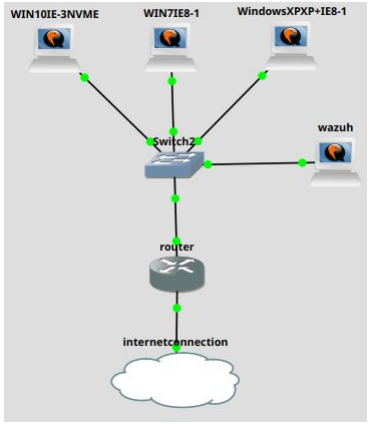
Justin Van Der Sluys, Emily West, Elang Sisson, Lyric Hathcock

Introduction

The barrier to deploying sophisticated malware has been progressively lowering year after year. Readily available toolkits and exploit frameworks place advanced attack capabilities in the hands of low level threat actors, while continuously mutating payloads render traditional signature detection increasingly obsolete.

SIEM platforms offer real time visibility into network infections, yet fall short of addressing the true challenge posed by samples explicitly designed to resist analysis. Detecting virtual machines, fingerprinting hypervisor artifacts, and refusing to execute their true payload in scripted or instrumented environments remains a consistent problem for SIEM toolchains. To address this, our research leverages **GNS3** for realistic network simulation and **Wazuh** as a SIEM and host monitoring platform to capture authentic malware behavior in real time. Rather than relying solely on existing detection libraries, this work also introduces **custom virus** detection signatures derived directly from observed real world malware samples demonstrating detection logic that can be tailored to specific payloads and bridging the gap between generic rulesets and the complicated signals produced by modern malwares.

Diagram



Explanations

- Experiments can be setup for any machine entirely virtualized while simulating theoretically any network conditions.
- Wazuh and other SIEM tools can be virtualized alongside infected machines to simulate and test real world responses to infections across a network.

Sample Analysis

Analyzed three modern samples that used three distinct evasion strategies. Performed static and dynamic analysis in isolated VMs.

Themida packed trojan masquerading as Kingsoft WPS Office with high entropy code and data segments, expired signing certificate, hardcoded C2 in Hong Kong.

Inno Setup Dropper that installs a malicious Electron app. Deobfuscation of app.asar reveals reveals more obfuscation in the javascript payload.

UPX packed loader that whitelists itself in Windows Defender before staging from sa1atik[.]cn. Originates from a Russian based maas (Malware as a service).

Detection Engineering

Translated analysis findings into a deployable detection logic using yara rules. Authored three rules using static artifacts such as packer signatures and embedded strings and also used behavioral indicators such as C2 domains and suspicious API calls that were discovered during sample analysis.

Further work

The primary constraint encountered was the resource overhead of GNS3 at scale. Simulating larger, more realistic network topologies quickly became untenable. Future work should explore distributed simulation architectures or containerization engines like kubernetes or containerlab to solve this.

Additionally the development of automated activity scoring (similar in concept to VirusTotal) would significantly increase the utility of this system. Automatically correlating system behaviors against known threat intelligence would drastically reduce reliance and dependance on human log reading and analysis and filter actually novel or important samples to the top of the queue.

Acknowledgement

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.