SPLUNK DELIVERY 2025/12/16

Delivery

Attackers create malware and infect devices to gain initial access or evade defenses and find ways to deliver it through different means. We have identified various IP addresses, domains and Email addresses associated with this adversary. Our task for this lesson would be to use the information we have about the adversary and use various Threat Hunting platforms and OSINT sites to find any malware linked with the adversary.

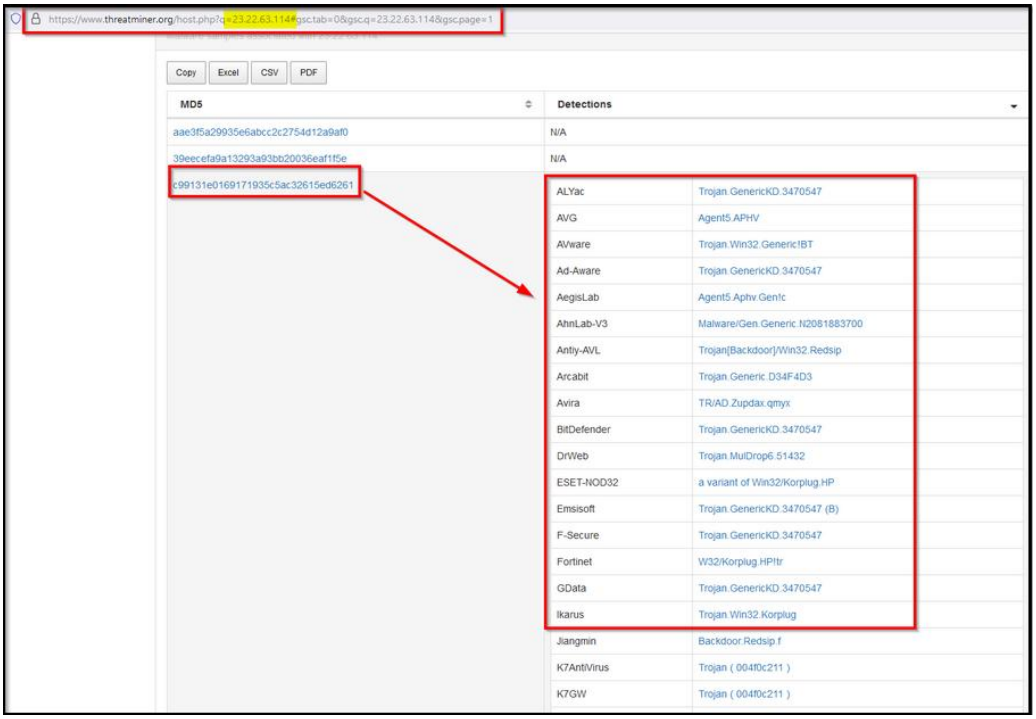
Threat Intel report suggested that this adversary group Poison lvy appears to have a secondary attack vector in case the initial compromise fails. Our objective would be to understand more about the attacker and their methodology and correlate the information found in the logs with various threat Intel sources.

OSINT sites

- Virustotal
- ThreatMiner
- Hybrid-Analysis

STEP 1: What is the HASH of the Malware associated with the APT group?

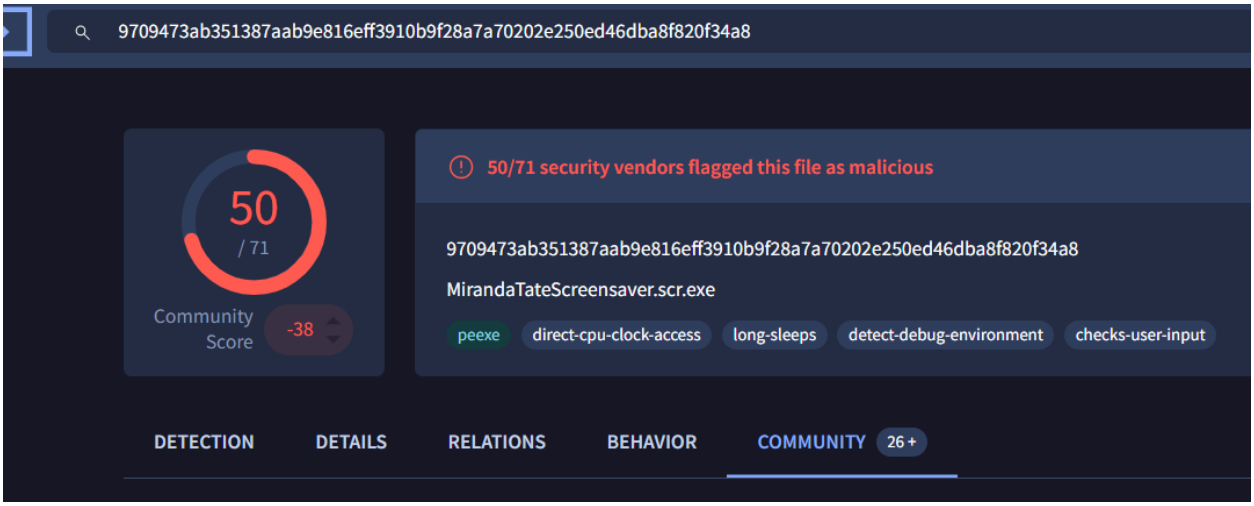
Let's start our investigation by looking for the IP 23.22.63.114 on the Threat Intel site [ThreatMiner.]



We found three files associated with this IP, from which one file with the hash value c99131e0169171935c5ac32615ed6261 seems to be malicious and something of interest.

ALL OF THE ABOVE SOURCED FROM TRYHACKME PLATFORM(2025,12)

STEP 2: What is the name of the Malware associated with the Poison Ivy Infrastructure?



The answer here is – **MirandaTateScreensaver.scr.exe.**

Conclusion Summary

In the Delivery phase, the investigation focused on identifying malware linked to the Poison Ivy adversary by correlating log data with external threat intelligence and OSINT platforms. Using ThreatMiner, the attacker IP address 23.22.63.114 was analysed, revealing multiple associated files. One file stood out as malicious, with the hash c99131e0169171935c5ac32615ed6261. Further intelligence confirmed the malware name as MirandaTateScreensaver.scr.exe. These findings demonstrate how adversaries prepare secondary delivery mechanisms and highlight the importance of correlating internal telemetry with threat intelligence sources to detect and understand malware delivery methods.