



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.

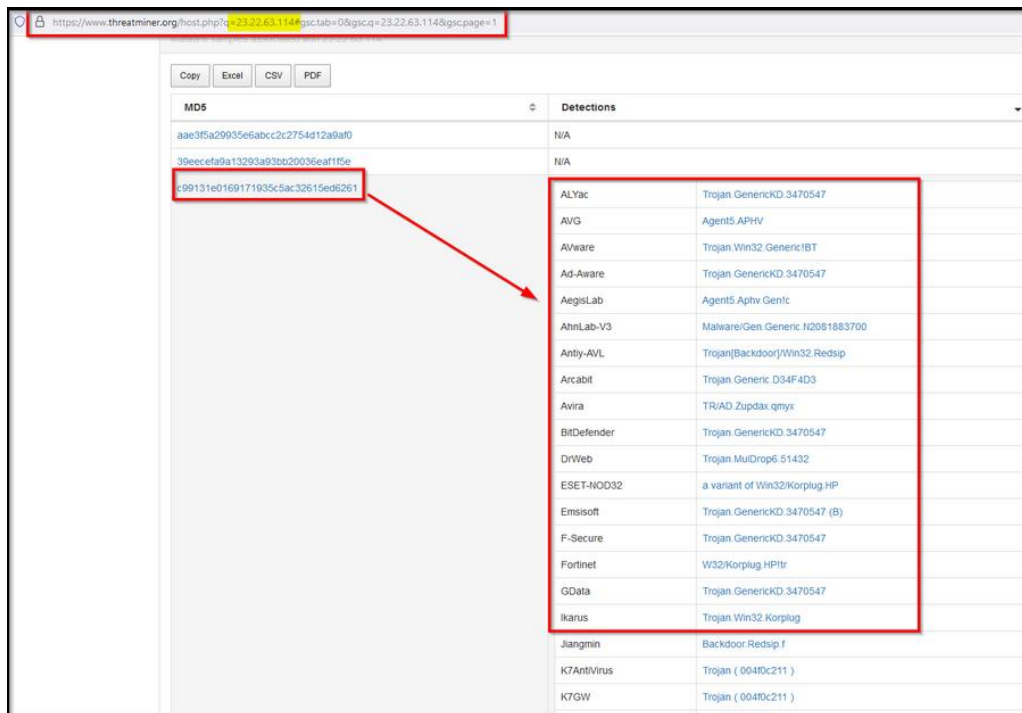
Threat Intel report suggested that this adversary group Poison Ivy appears to have a secondary attack vector in case the initial compromise fails. Our objective would be to understand more about the attacker and their methodology and correlate the information found in the logs with various threat Intel 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](https://www.threatminer.org/).

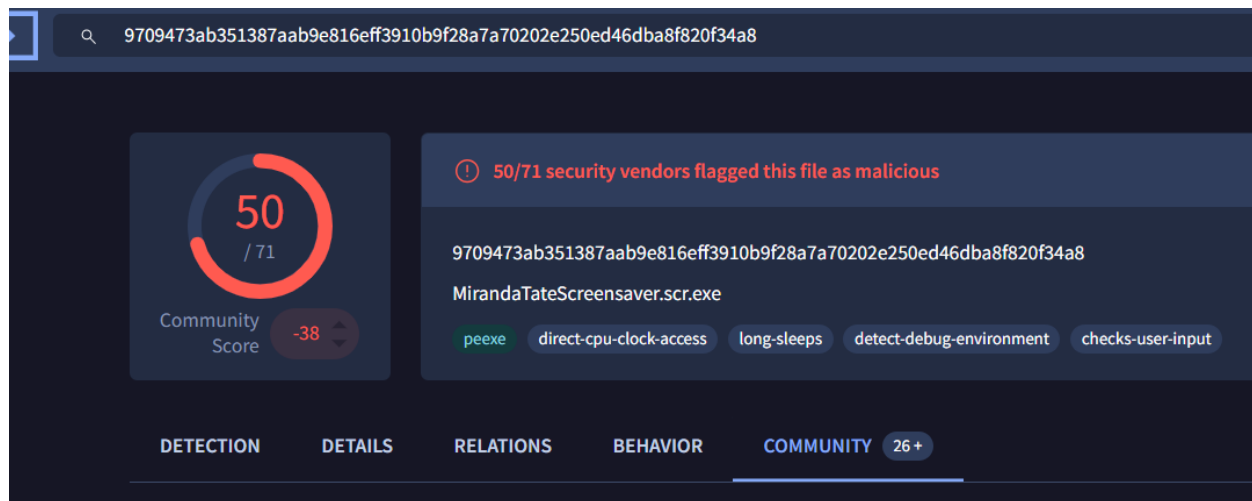


MD5	Detections																																								
aae3f5a29935e6abcc2c2754d12a9a0	N/A																																								
39eecefa0a13293a93bb2005eaf1f5e	N/A																																								
c99131e0169171935c5ac32615ed6261	<table border="1"><tbody><tr><td>ALYac</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>AVG</td><td>Agent5.APHV</td></tr><tr><td>AVware</td><td>Trojan.Win32.Generic18T</td></tr><tr><td>Ad-Aware</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>AegisLab</td><td>Agent5.Aphv.Gen!c</td></tr><tr><td>AhnLab-V3</td><td>Malware/Gen.Generic.N2081883700</td></tr><tr><td>Antiy-AVL</td><td>Trojan.Backdoor/Win32.Redsip</td></tr><tr><td>Arcabit</td><td>Trojan.Generic.D34F4D3</td></tr><tr><td>Avira</td><td>TR/AD.Zupdax.qmyx</td></tr><tr><td>BitDefender</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>DrWeb</td><td>Trojan.MulDrop6.51432</td></tr><tr><td>ESET-NOD32</td><td>a variant of Win32/Korplug.HP</td></tr><tr><td>Emsisoft</td><td>Trojan.GenericKD.3470547 (B)</td></tr><tr><td>F-Secure</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>Fortinet</td><td>W32/Korplug.HP!tr</td></tr><tr><td>GData</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>Ikarus</td><td>Trojan.Win32.Korplug</td></tr><tr><td>Jiangmin</td><td>Backdoor.Redsip.f</td></tr><tr><td>K7AntiVirus</td><td>Trojan (0040c211)</td></tr><tr><td>K7GW</td><td>Trojan (0040c211)</td></tr></tbody></table>	ALYac	Trojan.GenericKD.3470547	AVG	Agent5.APHV	AVware	Trojan.Win32.Generic18T	Ad-Aware	Trojan.GenericKD.3470547	AegisLab	Agent5.Aphv.Gen!c	AhnLab-V3	Malware/Gen.Generic.N2081883700	Antiy-AVL	Trojan.Backdoor/Win32.Redsip	Arcabit	Trojan.Generic.D34F4D3	Avira	TR/AD.Zupdax.qmyx	BitDefender	Trojan.GenericKD.3470547	DrWeb	Trojan.MulDrop6.51432	ESET-NOD32	a variant of Win32/Korplug.HP	Emsisoft	Trojan.GenericKD.3470547 (B)	F-Secure	Trojan.GenericKD.3470547	Fortinet	W32/Korplug.HP!tr	GData	Trojan.GenericKD.3470547	Ikarus	Trojan.Win32.Korplug	Jiangmin	Backdoor.Redsip.f	K7AntiVirus	Trojan (0040c211)	K7GW	Trojan (0040c211)
ALYac	Trojan.GenericKD.3470547																																								
AVG	Agent5.APHV																																								
AVware	Trojan.Win32.Generic18T																																								
Ad-Aware	Trojan.GenericKD.3470547																																								
AegisLab	Agent5.Aphv.Gen!c																																								
AhnLab-V3	Malware/Gen.Generic.N2081883700																																								
Antiy-AVL	Trojan.Backdoor/Win32.Redsip																																								
Arcabit	Trojan.Generic.D34F4D3																																								
Avira	TR/AD.Zupdax.qmyx																																								
BitDefender	Trojan.GenericKD.3470547																																								
DrWeb	Trojan.MulDrop6.51432																																								
ESET-NOD32	a variant of Win32/Korplug.HP																																								
Emsisoft	Trojan.GenericKD.3470547 (B)																																								
F-Secure	Trojan.GenericKD.3470547																																								
Fortinet	W32/Korplug.HP!tr																																								
GData	Trojan.GenericKD.3470547																																								
Ikarus	Trojan.Win32.Korplug																																								
Jiangmin	Backdoor.Redsip.f																																								
K7AntiVirus	Trojan (0040c211)																																								
K7GW	Trojan (0040c211)																																								

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.