redsense
INTELLIGENCE OPERATIONS

Lionkebab

During the final week of June 2022, Red Sense adversary space operations acquired a large victim list relating to criminal activities centered around a recent Confluence 0-Day, CVE-2021-26084. This list contains not just vulnerable servers, but also machines that have been actively exploited and backdoored by an emerging Iranian ransomware group, which we have tagged as LionKebab.

Quick Facts

- Name: LionKebab
- Origin: Iran
- Space: Ransomware
- Threat: Low-Moderate
- Targeting: Opportunistic

MITRE ATT&CK

- T1486 - Data Encrypted for Impact
- T1106 - Native API
- T1083 - File and Directory Discovery
- T1140 - Deobfuscate/Decode
- Files or Information
- T1489 - Service stop
- T1490 - Inhibit System Recovery

Red Sense is making this data available to any vetted entity, who may have exposure and/or the ability to notify other exposed entities. These files also contains victims different from the current OSINT lists being distributed in trust groups and on github.[1]

Details

LionKebab, isn’t a completely new group; instead, the group has traditionally worked behind Redline stealer logs and available ‘exploits en vogue’ to establish and sell accesses across a number of crimeware forums and markets. While the group has occasionally deployed other groups' payloads, they really have minimal history in active operations to recon and exploit victim infrastructures.

Based on current observations, it is evident that the group’s range of operations has now expanded to recon, exploitation, and potentially their own ransomware delivery. The image below depicts the group’s use of a remote administration tool and clear escalation of illicit cyber activities (figure 1).

In multiple observed victims, LionKebab is implanting a netcat payload on the exploited server, if the confluence process is running with sufficient rights. Netcat is a common cross platform remote administration tool. Entities identified within shared Red Sense intelligence,have been successfully and actively exploited. These attacks occured over the weekend (June 24-25) and are continuing into this week.

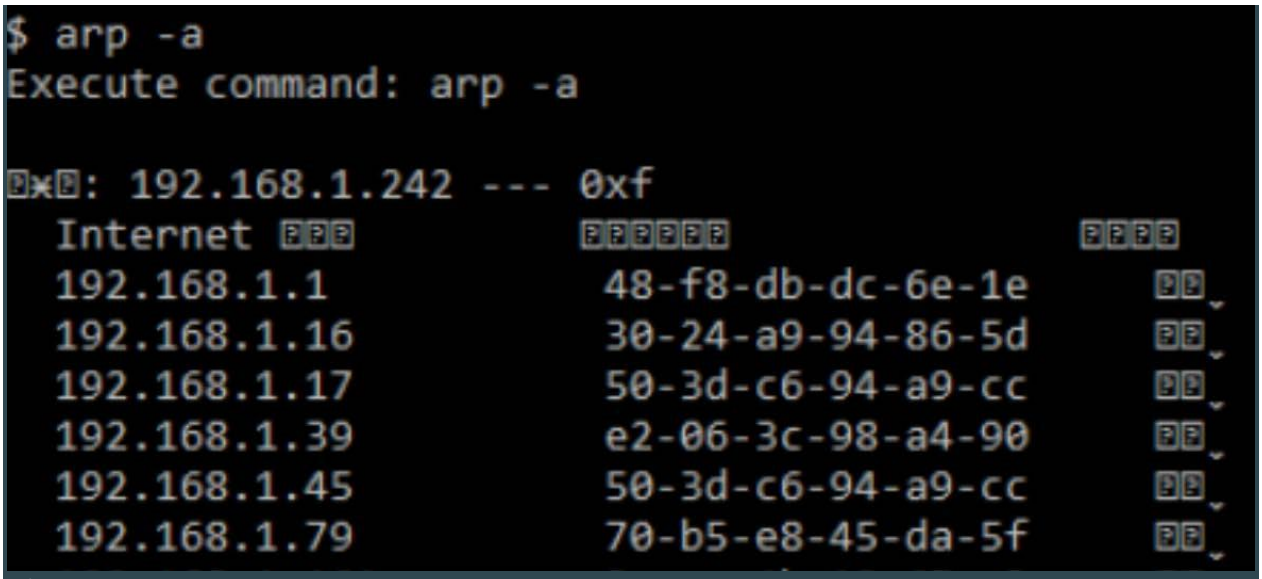

Figure 1

Being somewhat inexperienced here, LionKebab appears to be testing various open source penetration and red team tools, such as mimikatz (i.e., to enumerate and gain elevated permissions). Additionally, Red Sense observed the attackers looking for and exporting any exposed database(s) within the victim network.

Additionally, Red Sense observed the attackers looking for and exporting any exposed database(s) within the victim network.

Maintaining a backup copy of the unencrypted information bolsters criminal success within the negotiation phase of the attack, and demonstrates that LionKebab intends to extort companies with this data even if the full scale ransomware deployment is unsuccessful.

Red Sense analysts assess with moderate-to-high confidence that LionKebab actors will further evolve and escalate their Tactics, Techniques, and Procedures (TTPs) and emerge as an active threat to watch in the Ransomware space.

Figure 2

[smadi0x01/CVE-2021-26084]