
LEAFMINER
AXIAL

# A SURVEY ON LEAFMINER: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

## I. ABOUT

Leafminer a.k.a. FlashKitten or Raspite is a threat group from Iran that has been active since 2017.Like other Iran-based actors, the target scope for FlashKitten appears to be focused on the MENA region and EU using tools like Sorgu, Lazagne, Imecab, etc. Their prime motivation is Information Theft and Cyber-Espionage.

## II. TARGET SECTORS

This threat actor targets government organizations and entities in the financial, petrochemical, and transportation sectors for espionage purposes.

## III. METHODS USED

Leafminer leverages strategic website compromise to gain initial access to target networks. Leafminer uses the same methodology as Berserk Bear, Dragonfly 2.0 and Allanite in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to Leafminer -controlled infrastructure, allowing the adversary to remotely access the victim machine.Leafminer leverages strategic website compromise to gain initial access to target networks. Leafminer uses the same methodology as Berserk Bear, Dragonfly 2.0 and Allanite in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to Leafminer -controlled infrastructure, allowing the adversary to remotely access the victim machine.

## V. OPERATIONS

Since 2017, It was uncovered that Operations of this threat actor was targeting a broad list of government organizations and business verticals in Middle East. According to Symantec, the group tends to adapt publicly available techniques and tools for their attacks and experiments with published proof-of-concept exploits. It was also noted that at the same time Raspite overlapped significantly with Leafminer in Operations against electric utility organizations in US.

AX1AL

# IV. IOC

## SHA256

- 09653415084e64caed272f089610c5218a60372e17755ba71176785736e71c0d
- 09a20ca2db5b75f4ee55874929dec64acfffa46d54a4ed561b9c3f04baa91d52
- 1e4f56a1999ffa5376ef0acaaa5da0993f07e9c5aa1c222e297db7a4117d04b1
- 200ec4e8f16ed205cf94c02fcd73ee43ee511fa44ce34c458a1fca195c4bc737
- 2591b50355ed8053c8ed2e122f0b5769dd52c6d0b658cd0f2847f39056c6ac8c
- 3373d81a74c1ea75c794244b2c6d4e5fb246224128412b9348291e2f68994d83
- 332762804dd17f9b81620ea60ca8962daa493df24f6d98799d784d50fd4d0108
- 36e9c95b65692b110f4fe2ed27aa6066368c07525c020ec081b59bad272e6172

## DOMAINS

1. adobe-flash.us
2. ilhost.in
3. iqhost.us
4. offiice365.us
5. adobe-plugin.bid
6. microsoft-office-free-templates.in
7. microsoft-office-free-templates-download.btc-int.in

# VIII. REFERENCES


- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Leafminer%2C Raspite&n=1
- https://www.dragos.com/threat/raspite/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/leafminer-espionage-middle-east