BLACKSWAN CYBERSECURITY

THREAT ADVISORY

August 27, 2024

PEAKLIGHT Dropper Exploits Windows Systems via Pirated Movie Downloads to Deliver Malware

SUMMARY

A novel dropper that launches PowerShell-based malware to infect Windows systems has been identified, which is distributed through pirated movie downloads. The dropper delivers various malware strains, including Lumma Stealer and CryptBot, via a multi-stage attack chain.

TECHNICAL DETAILS

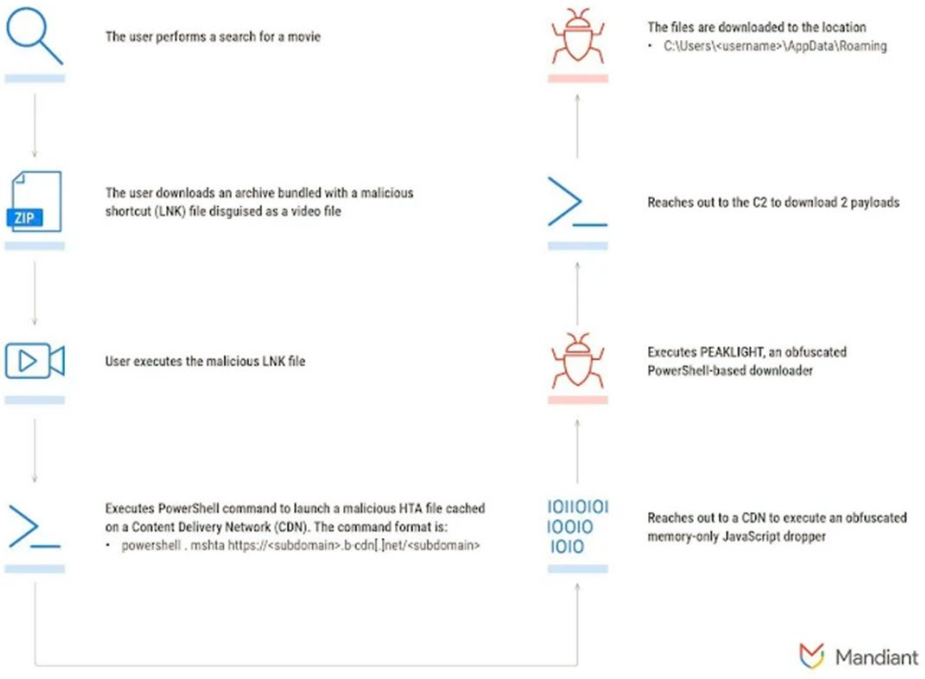
Mandiant identified the dropper that delivers various malware strains, including Lumma Stealer, Hijack Loader, and CryptBot, by leveraging a memory-only PowerShell-based downloader known as PEAKLIGHT. The attack starts when users download a Windows shortcut (LNK) file disguised as a pirated movie via drive-by downloads.

The LNK file, hidden within a ZIP archive, connects to a content delivery network (CDN) hosting an obfuscated JavaScript dropper. This dropper then runs the PEAKLIGHT PowerShell script, which contacts a command-and-control (C2) server to retrieve and execute additional malware payloads. The dropper is also capable of embedding hex-encoded and Base64-encoded PowerShell payloads, which are unpacked to deploy the malware.

Mandiant noted that this method has been used in various attack chains, with LNK files using wildcards to trigger the execution of the mshta.exe binary, discreetly running the malicious code.

Infection Chain

Source: Mandiant



INDICATORS OF COMPROMISE (IOCs)

Domains:

- relaxtionflouwerwi[.]shop
- deprivedrinkyfaiir[.]shop
- detailbaconroollyws[.]shop
- messtimetabledkolvk[.]shop
- considerrycurrentyws[.]shop
- understanndtytonyguw[.]shop
- patternapplauderw[.]shop
- horsedwollfedrwos[.]shop
- tropicalironexpressiw[.]shop

URLs:

- hxxp://gceight8vt[.]top/upload.php
- hxxps://brewdogebar[.]com/code.vue
- hxxp://62.133.61[.]56/Downloads/Full%20Video%20HD%20(1080p).lnk
- hxxps://fatodex.b-cdn[.]net/K1.zip
- hxxps://fatodex.b-cdn[.]net/K2.zip
- hxxps://forikabrof[.]click/flkhfaiouwrqkhfasdrhfsa.png
- hxxps://matodown.b-cdn[.]net/K1.zip
- hxxps://matodown.b-cdn[.]net/K2.zip
- hxxps://nextomax.b-cdn[.]net/L1.zip
- hxxps://nextomax.b-cdn[.]net/L2.zip
- hxxps://potexo.b-cdn[.]net/K1.zip
- hxxps://potexo.b-cdn[.]net/K2.zip
- hxxps://fatodex.b-cdn[.]net/fatodex
- hxxps://matodown.b-cdn[.]net/matodown
- hxxps://potexo.b-cdn[.]net/potexo

MD5:

CRYPTBOT:

- erefgojgbu (MD5: d6ea5dcdb2f88a65399f87809f43f83c)
- L2.zip (MD5: 307f40ebc6d8a207455c96d34759f1f3)
- Setup.exe (MD5: d8e21ac76b228ec144217d1e85df2693)

LUMMAC.V2:

- oqnhustu (MD5: 43939986a671821203bf9b6ba52a51b4)
- WebView2Loader.dll (MD5: 58c4ba9385139785e9700898cb097538)

PEAKLIGHT:

- Downloader (MD5: 95361f5f264e58d6ca4538e7b436ab67)
- Downloader (MD5: b716a1d24c05c6adee11ca7388b728d3)

SHADOWLADDER:

- Aaaa.exe (MD5: b15bac961f62448c872e1dc6d3931016)
- bentonite.cfg (MD5: e7c43dc3ec4360374043b872f934ec9e)
- cymophane.doc (MD5: f98e0d9599d40ed032ff16de242987ca)
- K1.zip (MD5: b6b8164feca728db02e6b636162a2960)
- K1.zip (MD5: bb9641e3035ae8c0ab6117ecc82b65a1)
- K2.zip (MD5: 236c709bbcb92aa30b7e67705ef7f55a)
- K2.zip (MD5: d7aff07e7cd20a5419f2411f6330f530)
- L1.zip (MD5: a6c4d2072961e9a8c98712c46be588f8)
- LiteSkinUtils.dll (MD5: 059d94e8944eca4056e92d60f7044f14)
- toughie.txt (MD5: dfdc331e575dae6660d6ed3c03d214bd)
- WCLDll.dll (MD5: 47eee41b822d953c47434377006e01fe)

RECOMMENDATIONS

- Do not download pirated content or software from untrusted sources.
- Ensure that antivirus and anti-malware solutions are current and capable of detecting PowerShell-based threats.
- Monitor for unusual activities such as the execution of mshta.exe or unexpected network connections to CDN sites.
- Implement security measures that can detect and block obfuscated scripts and LNK file-based attacks.
- Educate users about the risks associated with downloading files from unreliable websites, especially those offering pirated content.

REFERENCES

- https://thehackernews.com/2024/08/new-peaklight-dropper-deployed-in.html
- https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/