# CARBANAK (aka ANUNAK) Distributed via IDATLOADER (aka HIJACKLOADER)

By Dave Truman

Published: 2024-11-18 · Archived: 2026-04-05 14:17:20 UTC

IDATLOADER (aka HIJACKLOADER, GHOSTPULSE) has become prevalent in 2024, using advanced and new techniques such as BPL Sideloading, which Kroll reported on in June. Kroll observes IDATLOADER distributing malware such as ASYNCRAT, PURESTEALER, REMCOS, STEALC and what some might describe as a recent epidemic in LUMMASTEALER infections.

IDATLOADER received its name because of how it stores its malicious payload in the IDAT chunk of the portable network graphics (PNG) file format. First discovered in 2023, Kroll has seen IDATLOADER used by numerous cybercrime actors across a range of technical abilities and objectives. These include initial access brokers, data brokers and more advanced actors associated with ransomware such as KTA106 (Shathak, GOLD CABIN).

## Evidence of CARBANAK

In Kroll's tracking of IDATLOADER, analysts identified one sample that stuck out from the rest. Analysis of the sample indicated that it was a recent version of the remote access trojan CARBANAK (aka ANUNAK), a malware initially used by and named after the infamous cyber-crime group Carbanak (KTA008), which is widely regarded as an advanced persistent threat (APT).

The malware itself is referred to as ANUNAK by its developer. The activity associated with Carbanak is often tracked as interlinked subgroups, such as FIN7 and Cobalt Gang, by sections of the information security community. Regardless of operational nuance, all this activity falls under the sophisticated, financially motivated APT disposition.

Groups associated with the KTA008 cluster have been active since 2012,
and they have shifted focus from financial fraud and point-of-sale malware to ransomware attacks. In doing so, they have coordinated with many well-known ransomware families, such as LOCKBIT, DARKSIDE, REVIL and BLACKSUIT.

The groups often target large corporations in sectors such as retail, hospitality, finance, construction and defense. The groups have also recently used numerous watering hole lures to download LUMMASTEALER, which further links them to our findings.

## Malware Analysis

Kroll Cyber Threat Intelligence team's generative intelligence pipeline, the malware and group monitoring platform (MGMP), detected an anomalous malicious sample dropped by IDATLOADER and flagged it for further

analysis.

A sample found inside the IDATLOADER payload was itself encapsulated in a PNG file in a basic form of stenography. The original file appeared to be a screenshot of a window from the Italian version of the open-source program Scribus. The file was modified such that it maintained the PNG header. However, when opened in an image viewer, it was easy to see that its pixel data had been corrupted, indicating that the purpose of this stenography was likely to bypass automated security tooling.

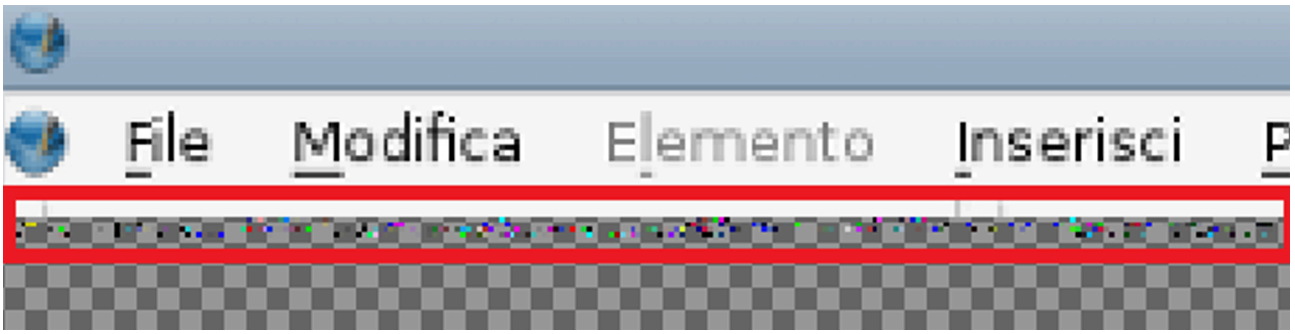


Figure 1: Section of the image showing corrupted pixel data where payload was encapsulated

The sample itself exhibits behaviors as previously noted for CARBANAK. In particular, the collection of processes and services on the system, multiple threads, and use of named pipes for inter-thread communication.

| | | |
|---|---|---|
| 2600 | RegCloseKey | HKLM\System\CurrentControlSet\Services\LanmanWorkstation |
| 2600 | RegQueryKey | HKLM |
| 2600 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Services\lfsvc |
| 2600 | RegOpenKey | HKLM\System\CurrentControlSet\Services\lfsvc |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\lfsvc\ImagePath |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\lfsvc\ImagePath |
| 2600 | RegCloseKey | HKLM\System\CurrentControlSet\Services\lfsvc |
| 2600 | RegQueryKey | HKLM |
| 2600 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Services\LicenseManager |
| 2600 | RegOpenKey | HKLM\System\CurrentControlSet\Services\LicenseManager |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\LicenseManager\ImagePath |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\LicenseManager\ImagePath |
| 2600 | RegCloseKey | HKLM\System\CurrentControlSet\Services\LicenseManager |
| 2600 | RegQueryKey | HKLM |
| 2600 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Services\ltdsvc |
| 2600 | RegOpenKey | HKLM\System\CurrentControlSet\Services\ltdsvc |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\ltdsvc\ImagePath |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\ltdsvc\ImagePath |
| 2600 | RegCloseKey | HKLM\System\CurrentControlSet\Services\ltdsvc |
| 2600 | RegQueryKey | HKLM |
| 2600 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Services\lmhosts |
| 2600 | RegOpenKey | HKLM\System\CurrentControlSet\Services\lmhosts |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\lmhosts\ImagePath |
| 2600 | RegQueryValue | HKLM\System\CurrentControlSet\Services\lmhosts\ImagePath |

Figure 2: Output of process monitor showing services information gathering

```
RAX     0000000000000001
RBX     0000000000000000
RCX     0000000000000009
RDX     0000000004A511BC
RBP     00000000027EFE99     "\\.\\pipe\\RdXGBcnuqiPYrznpviCkVWkPEleZNVK"
RSP     00000000027EFDF8
RSI     00000000001E13B0
RDI     00000000001E13B8

R8      00007FFA4C637570     <advapi32.InitializeSecurityDescriptor>
R9      0000000000000000
```

Figure 3: Malware accessing named pipe usage

When debugging the sample, indicators were present that linked this to CARBANAK malware. For example, a string matching a format commonly used as an ID by the malware.

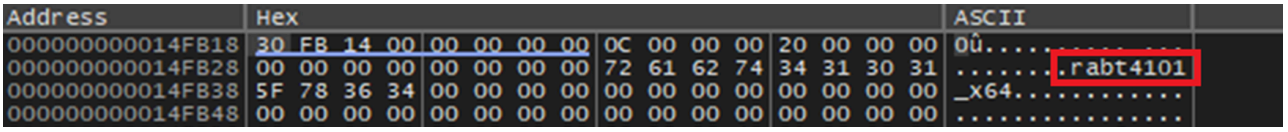


Figure 4: CARBANAK identification string present in memory

Additionally, in-memory references to the malware's internal name (ANUNAK) and configuration can be found.

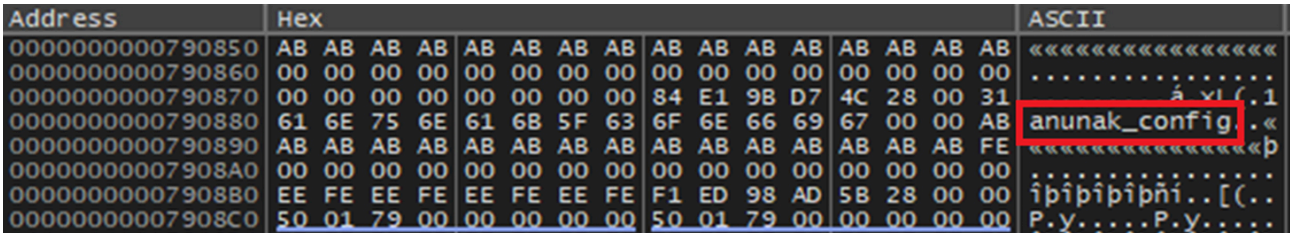


Figure 5: CARBANAK configuration and internal name present in process memory

Because of this, Kroll assesses with high confidence that this sample is CARBANAK/ANUNAK malware.

The presence of the CARBANAK malware inside of a IDATLOADER payload could indicate that some or all of the Carbanak cluster of APT groups are preparing for or participating in a new campaign using IDATLOADER to load their malicious payloads.

Kroll is tracking this new activity cluster as KTAC005.

It should be noted that the source code for CARBANAK was leaked in 2019, so it cannot be ruled out that a new actor could be utilizing the remote access trojan RAT. However, due to the complexity of the malware and the nature of the leak, Kroll assesses that this is less likely to be the case.

Based on KTA008's previous behavior, we could now be witnessing IDATLOADER being adopted in targeted attacks by sophisticated threat actors alongside its abundant use in the propagation of commodity malware.

---