Malware Analysis Report

Sample: Trojan.GenericKD.12661722

Hash: bb82bcef4bfcb5b06a6f8e2de74321468212feea31ec2f132fa842271f045071

1. Overview

The sample analyzed is detected as Trojan.GenericKD.12661722. This detection name is a generic heuristic

2. Static Analysis

- File identified by SHA256 hash.
- Likely packed or obfuscated.
- Potential suspicious imports include networking and process injection APIs.
- Strings may reveal URLs, IPs, or dropped file paths.

3. Dynamic Analysis

- In sandbox environments, GenericKD samples often:
  - • Drop additional files.
  - • Create persistence via registry keys or scheduled tasks.
  - • Connect to remote C2 servers.
  - • Potentially send spam or download further payloads.

4. Indicators of Compromise (IOCs)

- Hash: bb82bcef4bfcb5b06a6f8e2de74321468212feea31ec2f132fa842271f045071
- Possible IOCs include domains, IPs, mutexes, registry keys (to be confirmed via sandbox).

5. YARA Detection Rule (Template)

```
rule Trojan_GenericKD_custom {
    meta:
        description = "Detects Trojan.GenericKD.12661722 sample"
        sha256 = "bb82bcef4bfcb5b06a6f8e2de74321468212feea31ec2f132fa842271f045071"
    condition:
        sha256(@file) == sha256
}
```

6. Mitigation Recommendations

- Quarantine detected file immediately.
- Block suspicious domains/IPs.
- Scan endpoints for persistence mechanisms.
- Submit the file to AV vendor if false positive is suspected.
- Reset credentials if exfiltration activity is suspected.