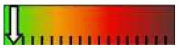
# EXHIBIT 18

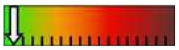
**PE sections with suspicious entropy found** Show sources

**Spreading:**



**Contains functionality to enumerate / list files inside a directory** Show sources

**System Summary:**



**Creates files inside the user directory** Show sources

**Anti Debugging:**

**Contains functionality for execution timing, often used to detect debuggers** Show sources
**Found dropped PE file which has not been started or loaded** Show sources

**Virtual Machine Detection:**

**Contains functionality to enumerate / list files inside a directory** Show sources
**Queries a list of all running processes** Show sources
**Contains capabilities to detect virtual machines** Show sources

## Screenshot

## Startup

- **system is xp**
- cc9fab2465a279b9424da3a09df7c8d5_undefined.exe (PID: 1840 MD5: CC9FAB2465A279B9424DA3A09DF7C8D5)
- **cleanup**

## Created / dropped Files

| File Path | Hashes |
|---|---|
| C:\Documents and Settings\All Users\svchost.exe | • MD5: CC9FAB2465A279B9424DA3A09DF7C8D5<br>• SHA: DE0FCA6F868D48CCF6B5580301D73A44EBE07669<br>• SHA-256: 45C0598E3DB3B7A0A194BF6DE78C8454BCA2B5895A1BC511665D0E22243397E4<br>• SHA-512: FDC478B37449AD98609FE311A86053AC107D1C76BE6F2062386F0BED2696FFF38675C80773693AAC846E138D29238BD01F79D0D189AE |

## Contacted Domains

**No contacted domains info**

## Contacted IPs

**No contacted IP infos**

### Static File Info

| | |
|---|---|
| File type: | Users\admin\Desktop\34362\sample/cc9fab2465a279b9424da3a09df7c8d5_undefined.exe; PE32 executable for MS Windows (GUI) Intel 80386 32-bit |
| File name: | cc9fab2465a279b9424da3a09df7c8d5_undefined.exe |
| File size: | 17920 |
| MD5: | cc9fab2465a279b9424da3a09df7c8d5 |
| SHA1: | de0fca6f868d48ccf6b5580301d73a44ebe07669 |
| SHA256: | 45c0598e3db3b7a0a194bf6de78c8454bca2b5895a1bc511665d0e22243397e4 |
| SHA512: | fdc478b37449ad98609fe311a86053ac107d1c76be6f2062386f0bed2696fff38675c80773693aac846e138d29238bd01f79d0d189aed66720fa1aba9fd07b29 |

## Static PE Info

**General**

| | |
|---|---|
| Entrypoint: | 0x401b0e |
| Entrypoint Section: | .text |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |