

malware_analysis/turla_carbon at master · sisoma2/malware_analysis

By sisoma2

Archived: 2026-04-05 21:53:52 UTC

Turla Carbon System

The Carbon System or Project Cobra is a malware framework developed by the actors identified as Turla. It's a sophisticated backdoor used to steal sensitive information from high valuable targets like diplomats or foreign affairs ministries.

IOCs

Samples

Carbon Dropper

```
a6efd027b121347201a3de769389e6dd
```

Carbon Service

```
957930597221ab6e0ff4fd7c6f2ee1cc
```

Carbon Orchestrator

```
3b10f20729d79ca3a92510674ff037c2  
78cadb0a538105f2fdc42f9956e49b5
```

Carbon Comms x86

```
c9c819991d4e6476e8f0307beed080b7  
1a2372b990a7ff7efd991707d52a13e6  
0868a27ef0aa512cbae82f4251767f4b
```

Carbon Comms x64

```
e5a90e7e63ededbdd5ee13219bc93fce  
7ec8a9641d7342d1a471ebcd98e28b62  
efcfff316e9cf183ca1cd619968cd11c
```

C&C

- [www.berlinguas\[.\]com:443:/wp-content/languages/index.php](http://www.berlinguas[.]com:443:/wp-content/languages/index.php)
- [www.balletmaniacs\[.\]com:443:/wp-includes/fonts/icons/](http://www.balletmaniacs[.]com:443:/wp-includes/fonts/icons/)
- [pastebin\[.\]com:443:/raw/5qXBPmAZ](http://pastebin[.]com:443:/raw/5qXBPmAZ)

Content

[Carbon_decrypt_config.py](#)

ESET Python script to extract encrypted configuration from Carbon

[a6efd027b121347201a3de769389e6dd_Config.txt](#)

Carbon configuration file extracted from the dropper with hash [a6efd027b121347201a3de769389e6dd](#)

Yara Rules

[apt RU Turla Carbon Dropper.yar](#)

YARA Rule to detect the Carbon dropper

[apt RU Turla Carbon ServiceDLL.yar](#)

YARA Rule to detect the Carbon Service DLL

[apt RU Turla Carbon CommunicationLibrary.yar](#)

YARA Rule to detect the Carbon Comms Library

[apt RU Turla Carbon Orchestrator.yar](#)

YARA Rule to detect the Carbon Orchestrator

Source: https://github.com/sisoma2/malware_analysis/tree/master/turla_carbon