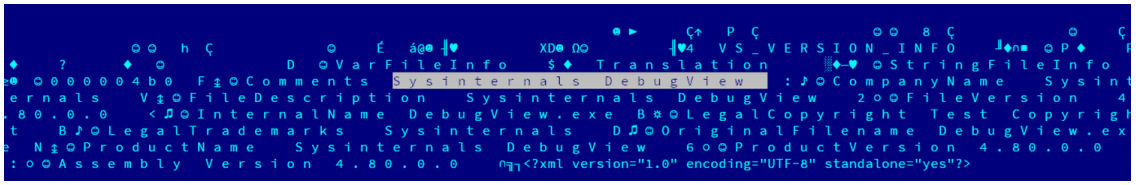
SysInTURLA — The Lost Reports

By May 27 Written By J A G-S

Published: 2001-05-27 · Archived: 2026-04-05 19:00:26 UTC

Cassowary – ‘The World’s Most Dangerous Bird’



PE Version Info for 2019 Kazuar (1749c96cc1a4beb9ad4d6e037e40902fac31042fa40152f1d3794f49ed1a2b5c)

PE Version Info for Legitimate SysInternals DebugView (Left) and Kazuar 2019 (Right)

As you can see, the brand abuse is quite crude and inconsistent and lends itself to easy sigging. As of writing, I’ve stumbled upon four samples. Hashes, partial IOCs, and YARA rules available in the technical appendix below.

A Special Note: As I was wrapping up this writeup, I found partial overlaps with an excellent private report released this month by PwC’s threat intel researchers. For a detailed breakdown of the new Kazuar variants, refer

to PwC's 'Blue Python – Kazuars cryptic strings' report (May 2020). That includes a better handling of their new obfuscator.

Technical Indicators

Kazuar DebugView (2019-2020) Samples

1749c96cc1a4beb9ad4d6e037e40902fac31042fa40152f1d3794f49ed1a2b5c
44cc7f6c2b664f15b499c7d07c78c110861d2cc82787ddaad28a5af8efc3daac
1fca5f41211c800830c5f5c3e355d31a05e4c702401a61f11e25387e25eeb7fa
2d8151dabf891cf743e67c6f9765ee79884d024b10d265119873b0967a09b20f

In-the-Wild Filenames

dbgsview.exe
DebugView.exe
adflctlmon.exe
PSExtendPrivacy.exe
Agent.exe

Command-and-Control Servers

Note: Expect some false positives as it appears these are **compromised wordpress sites**.

echange-afrique-insa[.]fr
afci-newsoft[.]fr
antoniosalieri[.]es <— (**Update 05.28.2020**: Thank you, Christiaan Beek)

Remediated: aviatnetworks[.]com <— (**Update 06.11.2020**: Confirmed remediated by the diligent folks at Aviat Networks)

.NET Module Version IDs

7c1a417d-961e-4fbd-9df7-7b99994eaec7
2cde886e-ee24-496a-bb31-1ced6b766ced
76b7b11a-4124-448b-9903-15524e321f3f
d3429016-d029-45b8-b260-85221265838e

YARA Rules available here
