May 27

SysInTURLA

Update 05.28.2020: Added a missing C&C contributed by Christiaan Beek

Update 06.11.2020: Diligent security folks at Aviat Networks have remediated any potential issues with their site and it should no longer be considered a C&C for Kazuar SysInTurla.

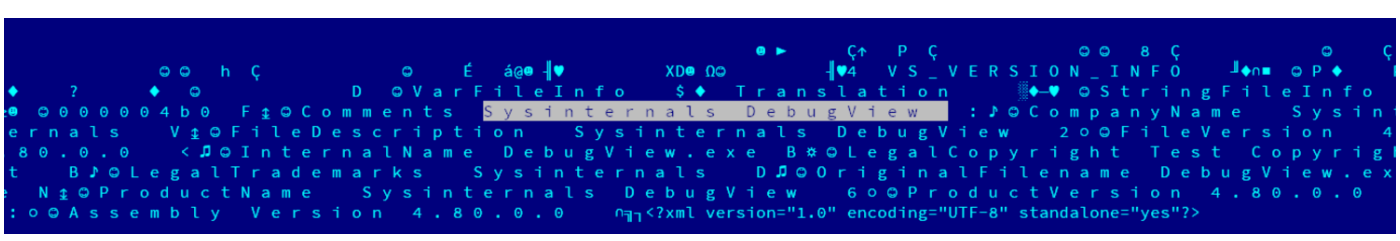
Note 06.11.2020: The researchers at Leonardo described gave a great talk on Penquin Turla x64 at OPCDE.

Today's threat actor of choice is one of my favorites, Turla (namesake of this blog). This prolific threat actor relies on a variety of toolkits (including Skipper, IcedCoffee, KopiLuwak among others). In the past two weeks alone, two distinct clusters of their activities piqued the interest of multiple research groups (see: Leonardo's 'Penquin_x64' and ESET's COMrat v4 reports), but their bag of tricks is hardly exhausted. This short 'tipper' will discuss Kazuar and a universal love for Mark Russinovich's SysInternal Tools.

A Dangerous Bird with Odd Plumage

Cassowary – 'The World's Most Dangerous Bird'

neither were found in-the-wild as far as I know. The Palo Alto report is excellent and can be relied upon for a breakdown of the malware's behavior. Sporadic samples of Kazuar were reported in 2017-2018.



PE Version Info for 2019 Kazuar (1749c96cc1a4beb9ad4d6e037e40902fac31042fa40152f1d3794f49ed1a2b5c)

As of 2019, it appears that Turla operators decided to apply different 'window dressing' to their Kazuar deployments. –one with security appeal at that. Mark Russinovich's SysInternal Suite of tools is a favorite among system administrators, malware analysts, and security researchers alike. It turns out, the infamous Turla shares our love for Mark's handy tools.

SHA256	1749c96cc1a4beb9ad4d6e037e40902fac31042fa40152f1d3794f49ed1a2b5c
SHA1	27002628fe06bb3d5fe180b35313e75b35c5e5fe
MD5	1f70bef5d79efbdac63c9935aa353955
Compilation Timestamp	2012-11-12 21:05:06
First Submission	2019-07-23 14:11:49
Size	135.00KB
ITW Name(s)	'DebugView.exe' 'adflctlmon.exe'
Module Version Id	d3429016-d029-45b8-b260-85221265838e

Newer Kazuar samples are (poorly) branded to look like a SysInternal tool called 'DebugView'. While the original enables users to monitor debug output from local and remote systems, Turla's new Kazuar samples enable a far more nefarious remote monitoring. Apart from cosmetic changes, the new Kazuar samples no longer rely on ConfuserEx. The new .NET obfuscator is a *pain in the ass* and defied my google dorking method of identification. However, it appears to continue to rely on the DLL injection mechanism into explorer.exe described in the Palo Alto blog.

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)

7c1a417d-961e-4fbd-9df7-7b99994eaec7

2cde886e-ee24-496a-bb31-1ced6b766ced

76b7b11a-4124-448b-9903-15524e321f3f

d3429016-d029-45b8-b260-85221265838e

YARA Rules available here

〈 ACIDBOX Clustering Nazar: A Lost Amulet 〉