SysKit (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 03:15:11 UTC

win.syskit (Back to overview)

SysKit

aka: IvizTech, MANGOPUNCH

Actor(s): APT35, Tortoiseshell

There is no description at this point.

References

2021-07-28 · Proofpoint · Crista Giering, Joshua Miller, Michael Raggi
I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona
Liderc SysKit

2021-07-15 · Facebook · David Agranovich, Mike Dvilyanski
Taking Action Against Hackers in Iran
Liderc SysKit

2019-09-25 · Twitter (@QW5kcmV3) · Andrew Thompson
Tweet on APT35 activity
SysKit

2019-09-24 · Cisco Talos · Jungsoo An, Paul Rascagnères, Warren Mercer
How Tortoiseshell created a fake veteran hiring website to host malware
Liderc SysKit

2019-09-24 · DARKReading · Kelly Jackson Higgins
Iranian Government Hackers Target US Veterans
SysKit Tortoiseshell

2019-09-18 · Symantec · Security Response Attack Investigation Team
Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks
SysKit Tortoiseshell

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.syskit