

FunnySwitch (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:55:12 UTC

FunnySwitch

aka: RouterGod

Actor(s): [Earth Lusca](#), Winnti Umbrella

There is no description at this point.

References

2023-08-07 · [Recorded Future](#) ·

RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale

[Winnti Brute Ratel C4 Cobalt Strike FunnySwitch PlugX ShadowPad Spyder Earth Lusca](#)

2022-05-12 · [TEAMT5](#) · [Leon Chang](#), [Silvia Yeh](#)

The Next Gen PlugX/ShadowPad? A Dive into the Emerging China-Nexus Modular Trojan, Pangolin8RAT (slides)

[KEYPLUG Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad Winnti SLIME29 TianWu](#)

2022-01-17 · [Trend Micro](#) · [Cedric Pernet](#), [Daniel Lunghi](#), [Gloria Chen](#), [Jaromír Hořejší](#), [Joseph Chen](#), [Kenney Lu](#)

Delving Deep: An Analysis of Earth Lusca's Operations

[BIOPASS Cobalt Strike FunnySwitch JuicyPotato ShadowPad Winnti Earth Lusca](#)

2021-12-16 · [TEAMT5](#) · [Aragorn Tseng](#), [Charles Li](#), [Peter Syu](#), [Tom Lai](#)

Winnti is Coming - Evolution after Prosecution

[Cobalt Strike FishMaster FunnySwitch HIGHNOON ShadowPad Spyder](#)

2021-01-14 · [PTSecurity](#) · [PTSecurity](#)

Higaisa or Winnti? APT41 backdoors, old and new

[FunnySwitch](#)

2021-01-14 · [PTSecurity](#) · [PT ESC Threat Intelligence](#)

Higaisa or Winnti? APT41 backdoors, old and new

[Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.funnyswitch>