# vOPCDE #6 - The Penquin is in da house (Dr. Silvio La Porta Leonardo, Dr. Antonio Villani Leonardo)

Published: 2020-06-08 · Archived: 2026-04-05 16:15:14 UTC

The Penquin is in da house We'll describe a recently discovered variant of “Penquin“, a stealth backdoor for Linux attributed to the Turla group and dubbed “Penquin_x64”. We'll detail the capabilities of this stealth backdoor, comparing it to the older known versions and providing hints on the possible build dates of these samples. “Penquin_x64” tries to hide itself from the eyes of the system administrators mimicking the “cron” binary, a widespred utility of Linux servers and clients used to manage scheduled tasks.In this talk we shed light on the malware capabilities and on the communication protocol, a component where the threat actor put in place a considerable amount of effort to avoid the improper activation of the backdoor. Also, during the demo session we'll show how to detect a running instance of Penquin_x64 crafting a proper packet that triggers a reverse-connection to a designated host. Dr. Silvio La Porta, Leonardo Dr. Antonio Villani, Leonardo Dr. Silvio La Porta is a Senior Cyber Security Architect in Leonardo's Cyber Security Division. He works in the Cyber Security Research Centre (CSRC) designing security products and researching advanced detection technology for complex malware/APT. Silvio previously was a lead research scientist with EMC Research Europe based in the Centre of Excellence in Cork, Ireland. His primary research focus areas were real-time network monitoring and data analysis in smart grids to detect malware activity in SCADA systems and corporate networks. He was also leading Security Service Level Agreement (Sec-SLA) and end user security/privacy protected data store projects for hybrid Cloud environment. He is a frequent speaker in professional and industry conferences. Before joining EMC, Silvio worked as a Malware Reverse Engineer in Symantec’s Security Response team in Dublin, Ireland. Silvio holds a PhD in Computer Network Security from the University of Pisa, Italy. He is theco-author of the training ‘Modern Malware OPSEC & Anti-Reverse Techniques Implementation and Reversing’ Dr. Antonio Villani is a security expert working for the Cyber Security Research Centre (CSRC) in the Leonardo's Cyber Security Division with the role of Senior Cyber Security Architect. As a researcher he published in top tier conferences and journals and he partecipated to european research projects in the field of cyber resilience and data security. During the final steps of its PhD he worked in the field of malware research and digital forensic starting his path toward the blackmagic of reverse-engineering. In his neverending quest in discovering how deep the rabbit hole goes, he spent the past years analyzing high level implants for top tier customers and providing detailed implementation information to support cyber-defense and cyber threat intelligence teams. He is the co-author of the training ‘Modern Malware OPSEC & Anti-Reverse Techniques Implementation and Reversing’.

---