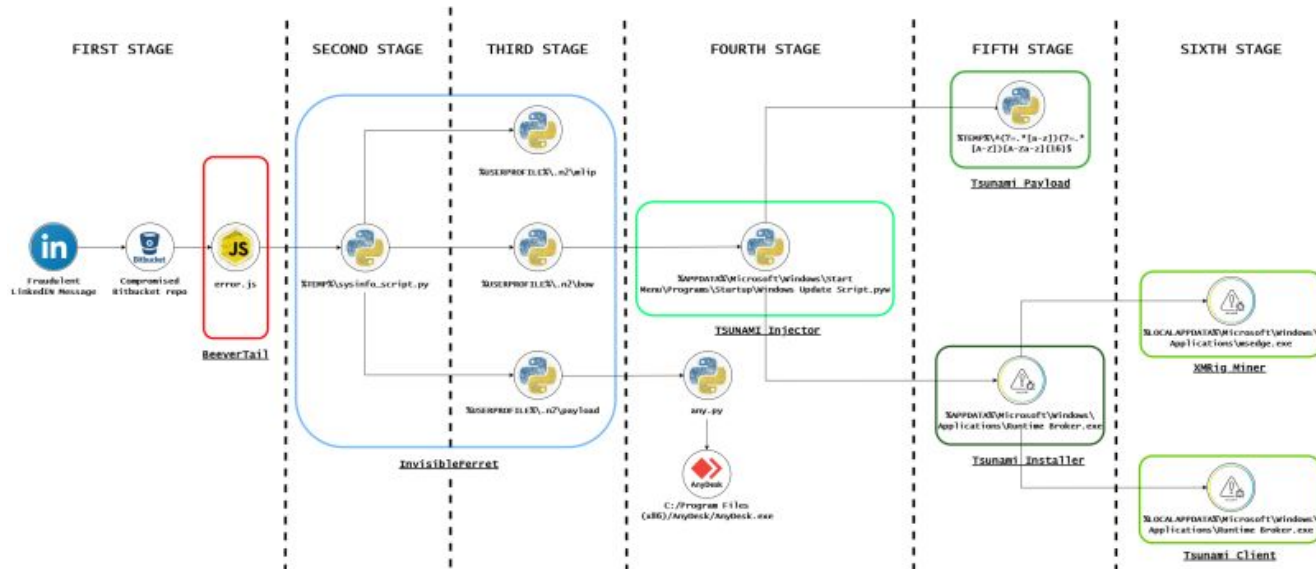


# #iocs #ttps #lazarusgroup #objective #anydesk #cryptominers #xmrigminer...

[in linkedin.com/posts/alessio-di-santo-712348197\\_iocs-ttps-lazarusgroup-activity-7263976334807220224-N6Ue/](https://www.linkedin.com/posts/alessio-di-santo-712348197_iocs-ttps-lazarusgroup-activity-7263976334807220224-N6Ue/)



[View profile for Alessio Di Santo](#)

Alessio Di Santo

GCFA | GDAT | GCTI | GREM | eJPT | Ph.D. Student | Ufficiale della Riserva Selezionata @ Arma dei Carabinieri

4mo Edited

👍 Thanks to the Article shared by [Luca Di Domenico](https://lnkd.in/dT5-sKwG) (<https://lnkd.in/dT5-sKwG>) it has been possible for me to deeply investigate the threat he highlighted. ✨ Based on the acquired **#IoCs** and **#TTPs** it is possible to associate it, with a discrete level of confidence, to the DPRK State-Sponsored Threat Actor **#LazarusGroup**. Their main **#Objective** is to steal Crypto-Wallets information from victims' Assets (even from Browser's Plugins). Additionally, Credentials and Credit Card Numbers are exfiltrated as well. Compromised assets are also backdoored and keylogged. The attacker may eventually deploy also additional payloads, based on their needs, e.g. an **#AnyDesk** instance to increase their Remote Access capabilities or **#Cryptominers** (e.g. **#XMRigMiner**). !! Furthermore, this new attack has shown a new **#Tradecraft** employed by this **#ThreatActor**: **#TSUNAMI** (Injector, Installer, Payload and Client). As it is possible to see from the attached **#InfectionChain**, instead of terminating its activities with its well-known **#Python**-based Third-Stage, it continues by deploying another suite and adding an additional Three-Layers to their compromising activity. 🖼️ Python Scripts are also well-obfuscated with a routine of: Reverse a strings, Base64-Decode and Zlib Decompress, repeated for 50 times. 🟠 IoCs and some useful YARA-rules are available here: <https://lnkd.in/d8VWqfCS>

 diagram

   40 2 Comments

 Luca Di Domenico,.graphic

To view or add a comment, [sign in](#)