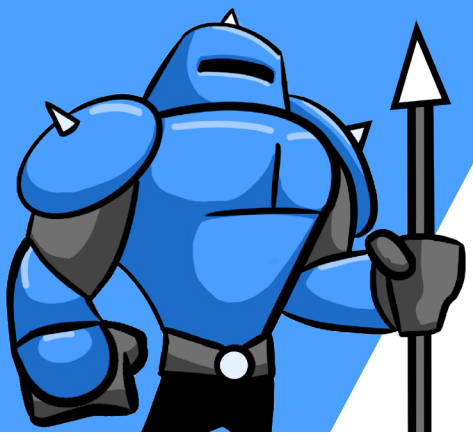
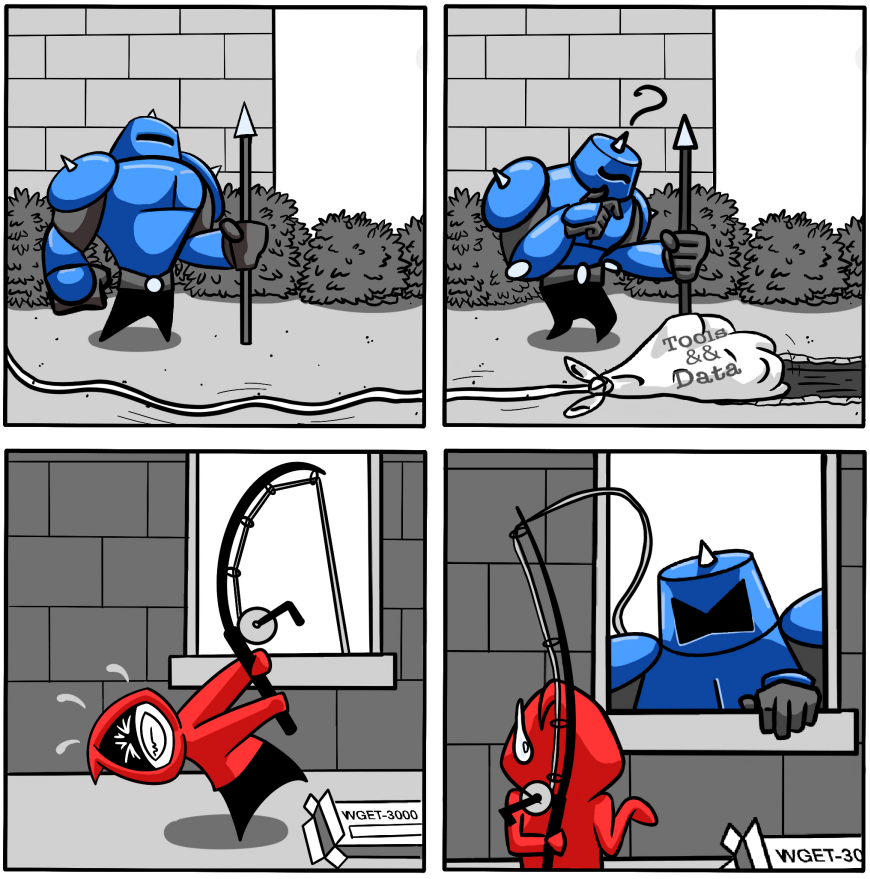


SUDO SCIENCE

AN UPTYCS COMYCS PROJECT



Scenario

This comic has Linus, our Blue Team character, standing guard as they protect the outer castle walls. He begins to notice a suspicious line dragging a bag across the ground. They aren't quite sure what is inside the bag as it is tied quite tightly. Somehow, something inside the castle is dragging it through the window.

Linus begins to investigate and follows the line towards the castle. Inside the castle, on a higher floor, is Curly (our Red Team character) straining to reel him something from the window. It turns out that he has somehow gotten into the castle and is using his new WGET-3000 fishing pole to download some external data. Likely, it is a bag of malicious tools for him to wreck havoc inside the castle. However, as he continues to reel, he is shocked to find Linus show up at the window.

He tries to hide his tool, but it's too late; he's caught red handed once again!

Deep Dive

`curl` and **`wget`** can be quite the security headache for Linux defenders. While these commands are commonly used by attackers to download malicious tools, user agents, and more, they are also quite useful to Linux users to download completely benign data.

This technique is known as T1105 - Ingress Tool Transfer where "adversaries may transfer tools or other files from an external system into a compromised environment". The tools reside on an external system controlled by the adversary and are brought into the network via protocols such as **FTP** or **SFTP**. According to MITRE ATT&CK, this technique is incredibly common and used through a variety of methods. For example, APT41 will use **`certutil`** while CoinTicker executes a Python script.

To detect this technique, we can monitor for file creation and files transferred into the network. While we should not rely on this method, we can look for signatures of what is being downloaded (attackers will likely change the signatures over time to evade detection, so this is not a fool proof method). On the behavioral side, we can detect uncommon data flows or transfers. For example, we can analyze network data to see if the client is sending more data than it receives from a server.