chokepoint/azazel: Azazel is a userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit. It is more robust and has additional features, and focuses heavily around anti-debugging and anti-detection.

github.com/chokepoint/azazel

chokepoint

chokepoint/**azazel**

Azazel is a userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit. It is more robust and...

3 Contributors · 6 Issues · 707 Stars · 179 Forks

Azazel

V 0.1

> The whole earth has been corrupted through the works that were taught by Azazel: to him ascribe all sin. -- 1 Enoch 2:8

Azazel is a userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit. It is more robust and has additional features, and focuses heavily around anti-debugging and anti-detection.

Features

- Anti-debugging
- Avoids unhide, lsof, ps, ldd detection

- Hides files and directories
- Hides remote connections
- Hides processes
- Hides logins
- PCAP hooks avoids local sniffing
- Two accept backdoors.
- Crypthook encrypted accept() backdoor -- Full PTY
- Plaintext accept() backdoor -- Full PTY
- PAM backdoor for local privesc and remote entry
- Log cleanup for utmp/wtmp entries based on pty

Using netcat to communicate with a remote PTY isn't the best idea. See below for a better PTY client written by InfoDox, or use socat with a command similar to the following and then just paste the password into the session, otherwise socat send the first char making the passwords not match.

> socat -,raw,echo=0 TCP:target:port,bind=:61040

Links

Better PTY Client

Disclaimer

The authors are in no way responsible for any illegal use of this software. It is provided purely as an educational proof of concept. We are also not responsible for any damages or mishaps that may happen in the course of using this software. Use at your own risk.