

Indicators of Compromise (IoC)

| IOC | Detection | Description |
|--|----------------------------|--|
| 2a5e003764180eb3531443946d2f3c80ffcb2c30 | Ransom.Linux.PLAYDE.YXEE3T | ELF Binary |
| hxxp://108.61.142[.]190/FX300.rar | 95 - Ransomware | Hosting URL for Play Ransomware Binary |
| 108.61.142[.]190 | Untested | Observed IP address |
| hxxp://108.61.142[.]190/1.dll.sa | 79 - Disease Vector | Hosting URL for Coroxy Backdoor |
| hxxp://108.61.142[.]190/64.zip | 79 - Disease Vector | Hosting URL for NetScan |
| hxxp://108.61.142[.]190/winrar-x64-611.exe | Untested | Hosting URL for WinRAR |
| hxxp://108.61.142[.]190/PsExec.exe | Untested | Hosting URL for PsExec |
| hxxp://108.61.142[.]190/host1.sa | 78 - Malware Accomplice | Hosting URL for Coroxy Backdoor |