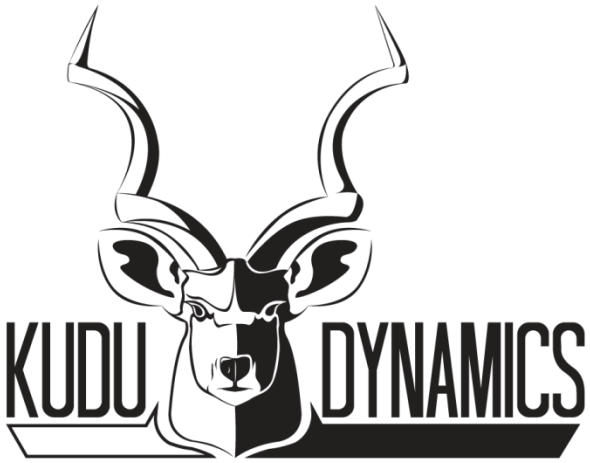
E2 Hotwash: June 2017

TA5.1 TRADECRAFT



Overview

- Simple APT Simulacrum
- Micro APT Simulacrum
- Drakon APT Simulacrum
- GatherApp
- Webshell
- Metasploit

KUDU DYNAMICS

Simple APT Simulacrum

- Same as APT simulacrum from E1
- Mostly downloaded and executed
- File dropper
- getfile, putfile, execfile, shell

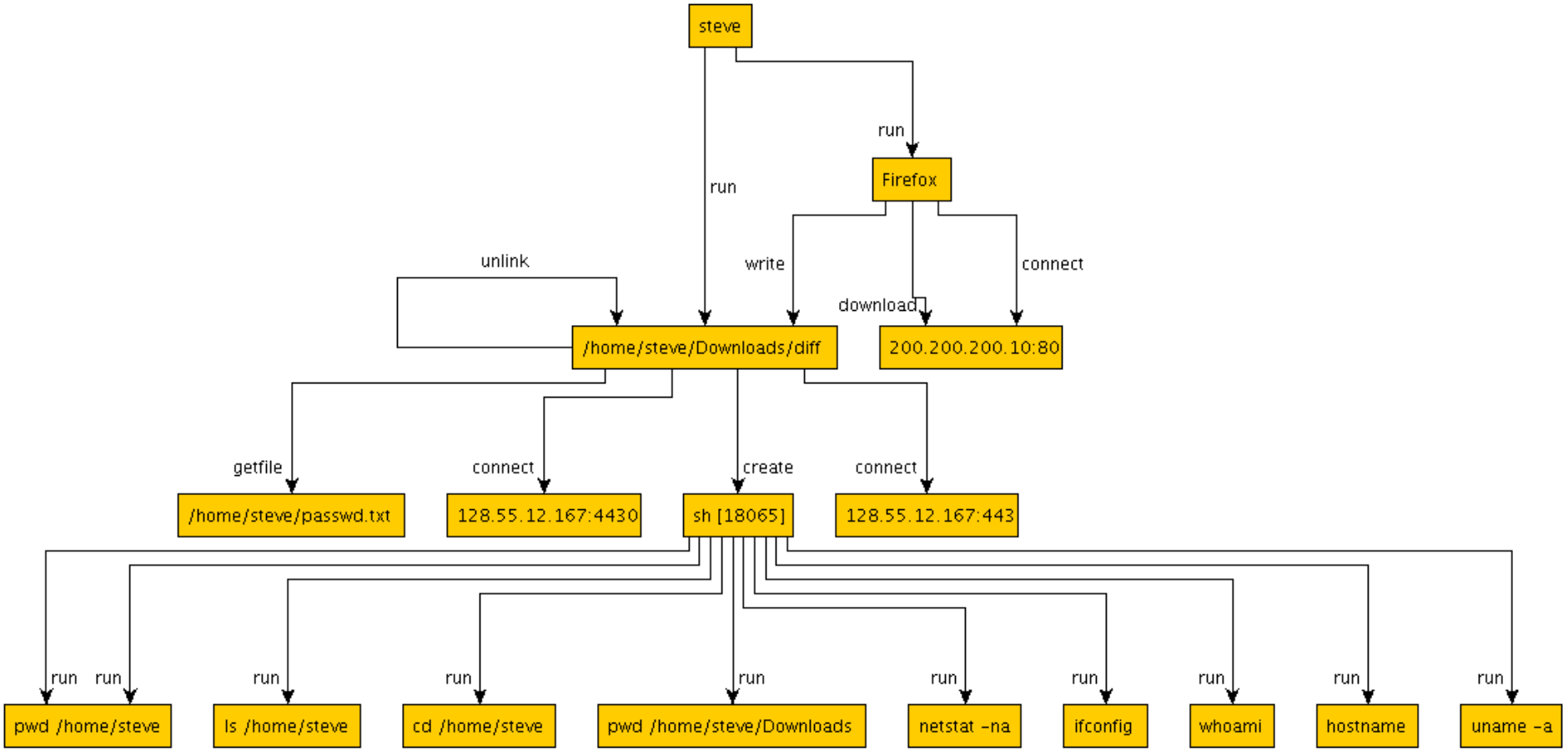
KUDU DYNAMICS

Simple APT Simulacrum

- User steve downloaded program diff from 200.200.200.10
- User steve ran diff
- diff connected out to 128.55.12.167:443 for C2
- diff created a new sh process
- diff connected out to 128.55.12.167:4430 for sh commands
- Adversary ran sh commands uname, hostname, whoami, ifconfig, netstat
- Adversary getfile exfil of passwd.txt
- diff unlinked itself

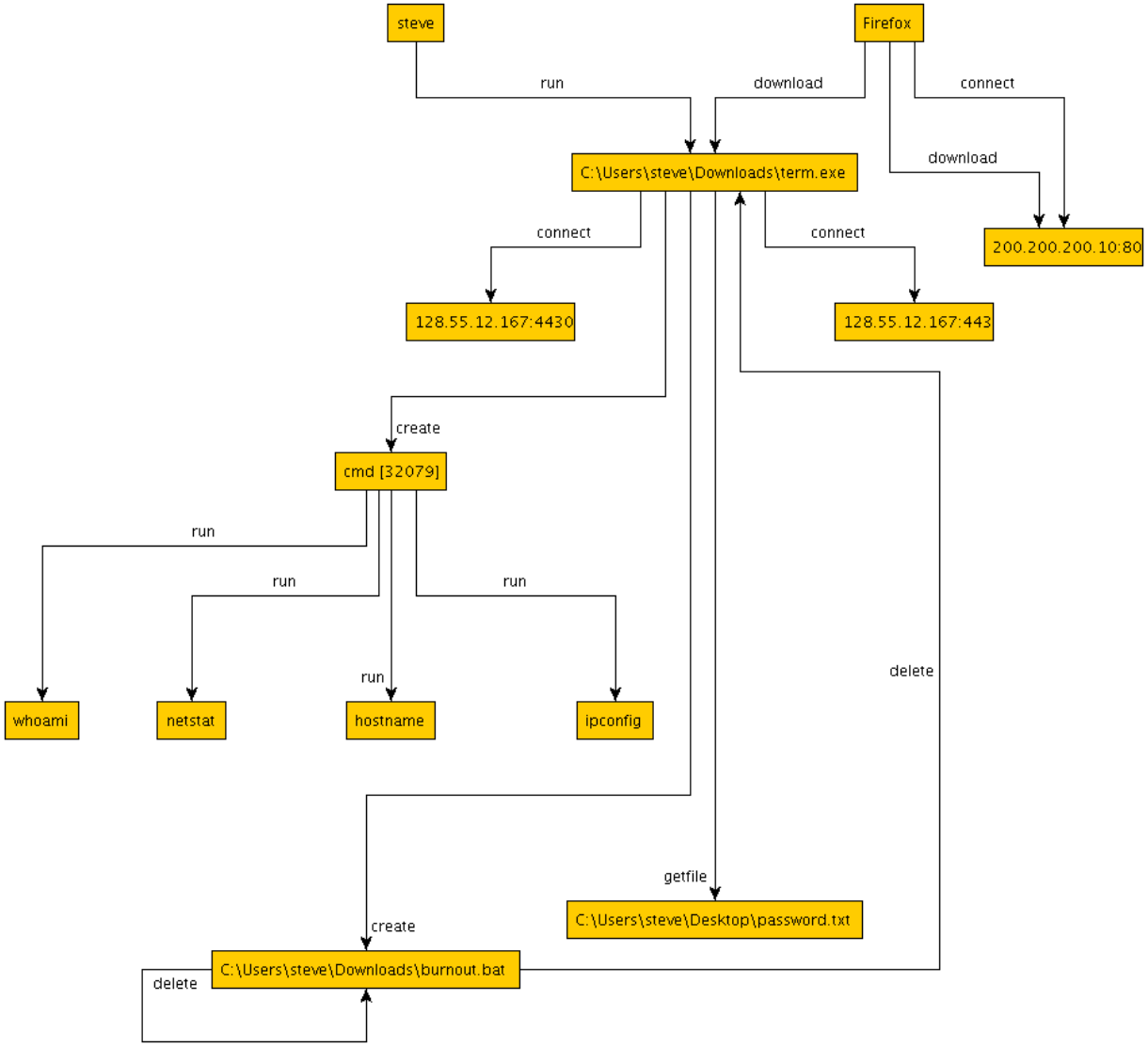
KUDU DYNAMICS

BOVIA – THEIA – Simple



KUDU DYNAMICS

PANDEX – FAROS – Simple



Micro APT Simulacrum

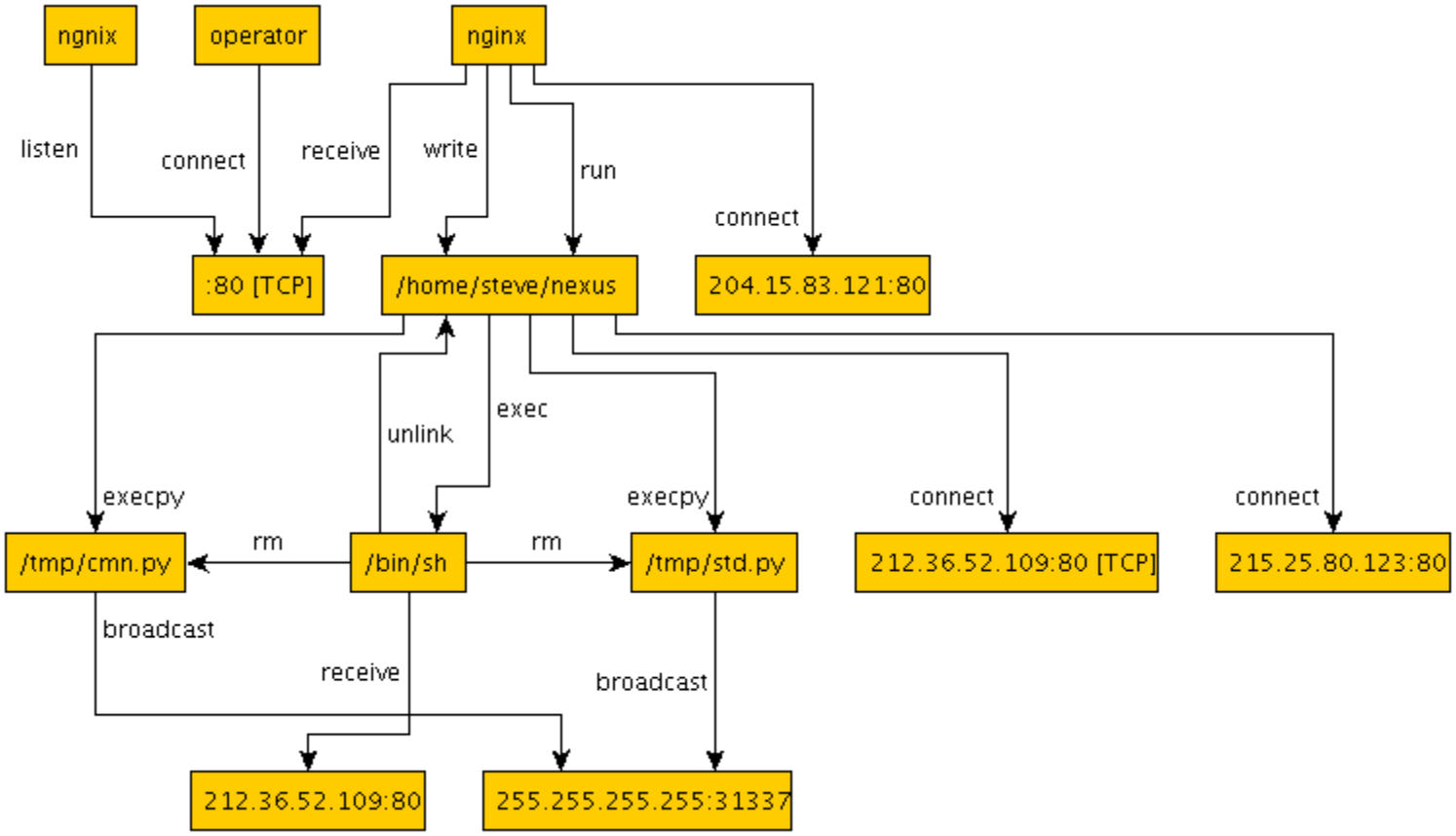
- Started as minimal version of Simple APT
- Downloaded and executed
- File dropper
- getfile, putfile, execfile, shell, execpy
- Support for executing Python scripts

Micro APT Simulacrum

- Adversary exploited Nginx server on port 80
- Nginx server connected out to 204.15.83.121
- Nginx server downloaded micro to /home/steve/nexus
- nexus connected to 212.25.80.123 for C2
- nexus downloaded /tmp/cmn.py and /tmp/std.py
- /tmp/cmn.py and tmp/std.py exfil UDP broadcast 31337
- nexus created a new sh process
- nexus connected to 212.36.52.109 for sh commands
- sh deleted /tmp/cmn.py and /tmp/std.py

KUDU DYNAMICS

PANDEX– CADETS– Micro



Drakon APT Simulacrum

- Simple APT Revision 2
- Privilege escalation
- Reflective self-loading
- Loading of modules in memory
- getfile, putfile, execfile, shell
- OS commands like ps, hostname, whoami, cat

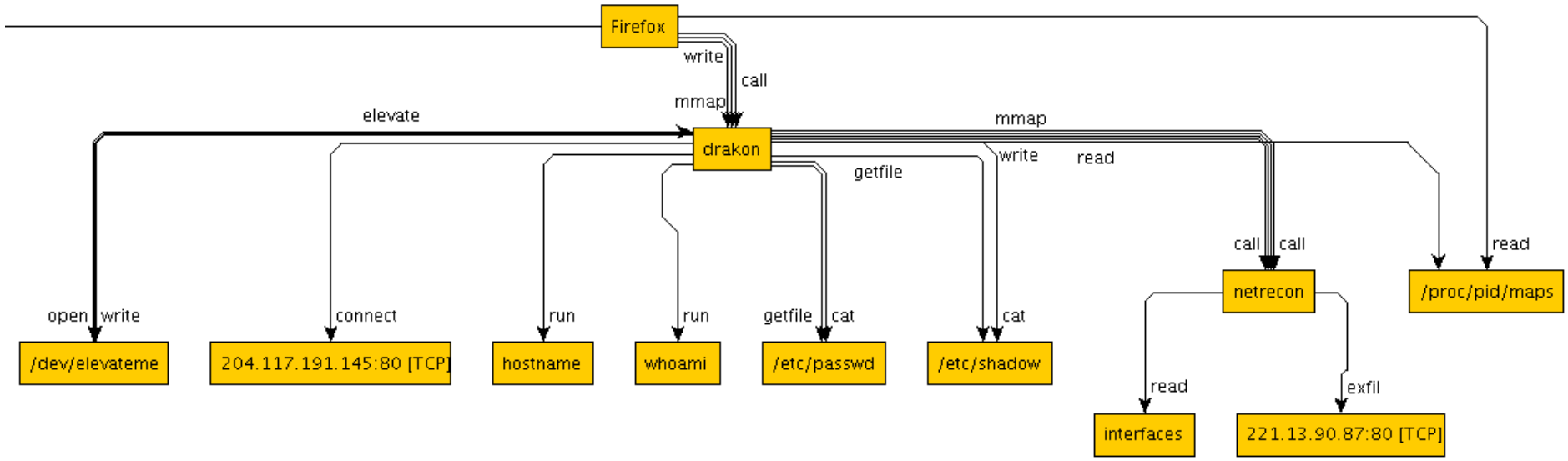
KUDU DYNAMICS

Drakon APT Simulacrum

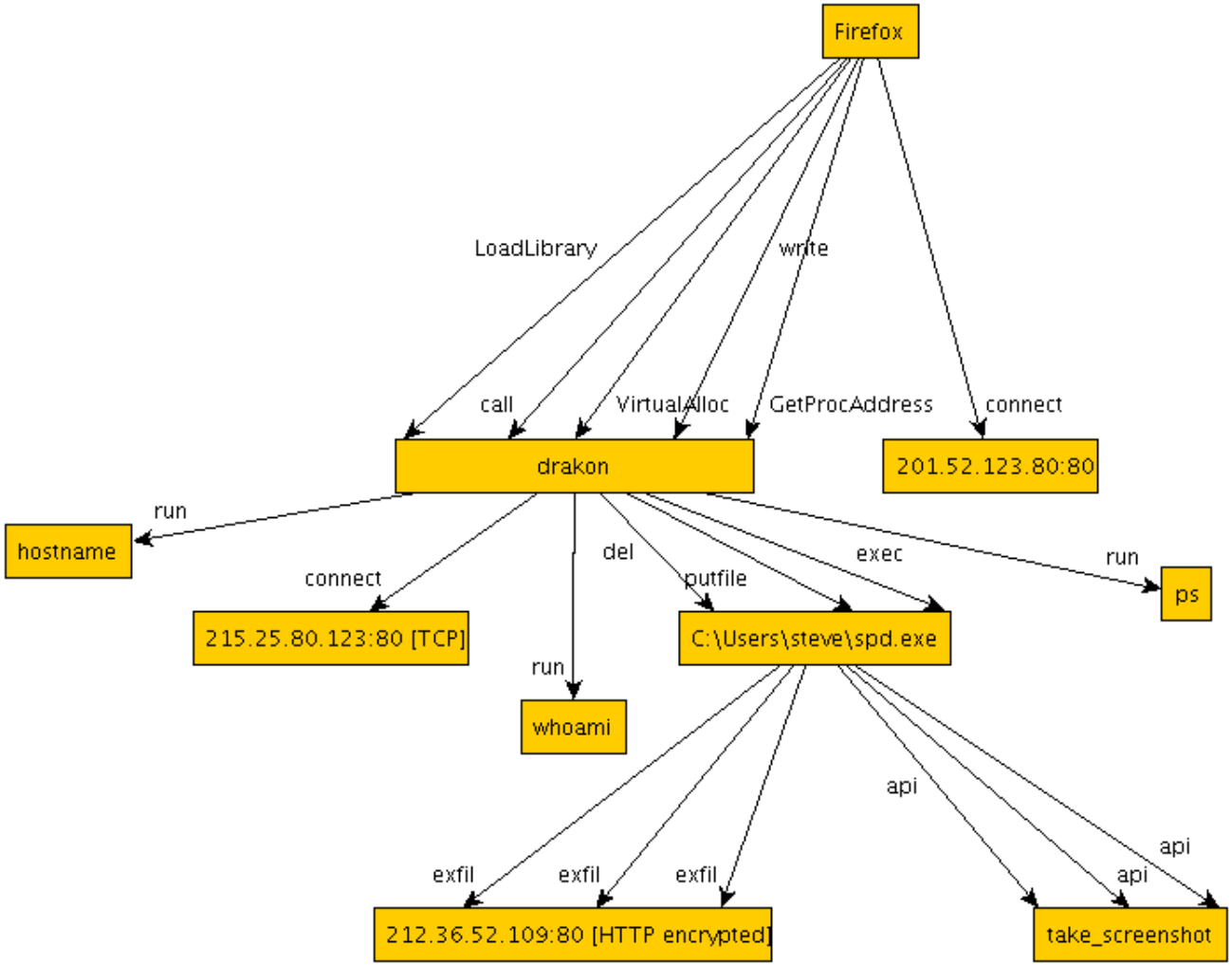
- Firefox read from /proc/pid/maps
- Firefox mmap memory, wrote drakon to it, and called it
- drakon wrote to /dev/elevateme
- /dev/elevateme elevated drakon
- drakon connected to 204.117.191.145 for C2
- drakon ran hostname and whoami
- drakon exfil /etc/passwd and /etc/shadow
- drakon loaded netrecon module in memory
- netrecon read network interfaces
- netrecon exfil to TCP 221.13.90.87

KUDU DYNAMICS

PANDEX – TRACE – Drakon



PANDEX – FiveDirections – Drakon



KUDU DYNAMICS

GatherApp

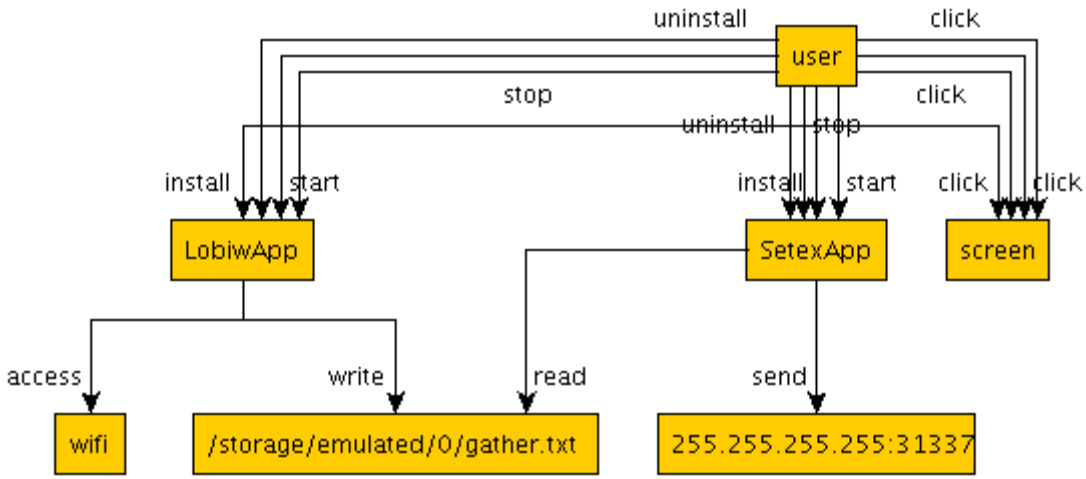
- Multiple variations
  - Same as GatherApp from E1
  - GatherApp with native library

GatherApp

- User installs and runs LobiwApp
- LobiwApp accesses WiFi information
- LobiwApp writes to /storage/emulated/0/gather.txt
- User stops and uninstalls LobiwApp
- User installs and runs SetexApp
- SetexApp reads /storage/emulated/0/gather.txt
- SetexApp exfils via UDP broadcast 31337
- User stops and uninstalls SetexApp

KUDU DYNAMICS

BOVIA – ClearScope – GatherApp

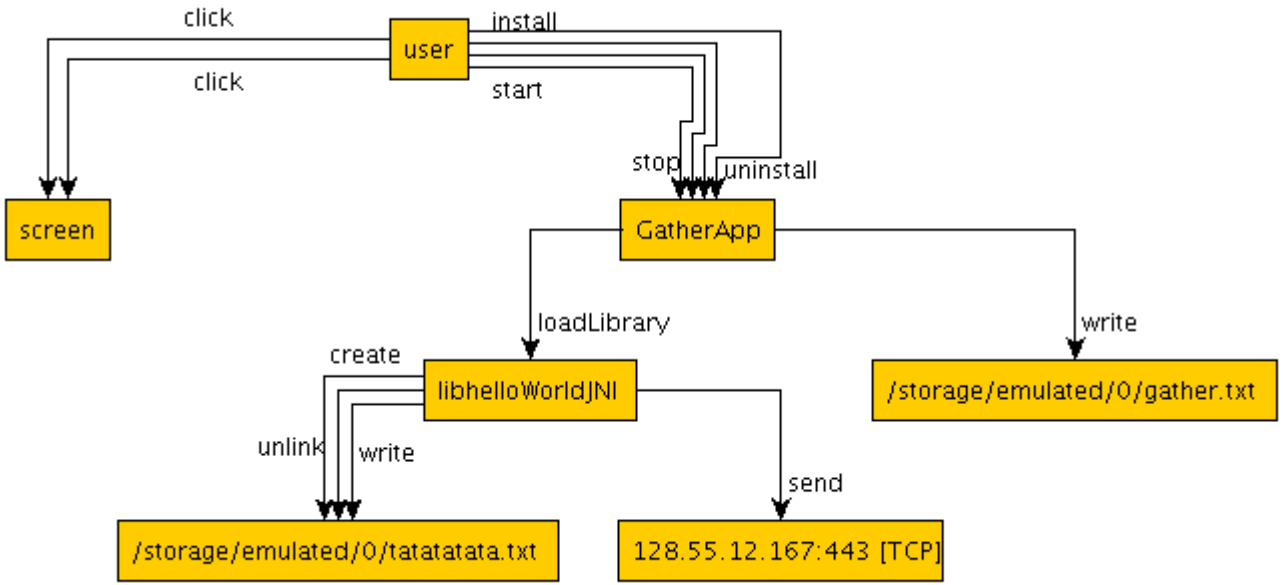


GatherApp with HelloWorld

- User installs and runs GatherApp
- GatherApp collects info
- GatherApp writes to /storage/emulated/0/gather.txt
- GatherApp loads libhelloWorldJNI native library
- libhelloWorldJNI writes to /storage/emulated/0/tatatatata.txt
- libhelloWorldJNI collects info
- libhelloWorldJNI exfils to TCP 128.55.12.167:443
- User stops and uninstalls GatherApp

KUDU DYNAMICS

PANDEX – ClearScope – GatherApp

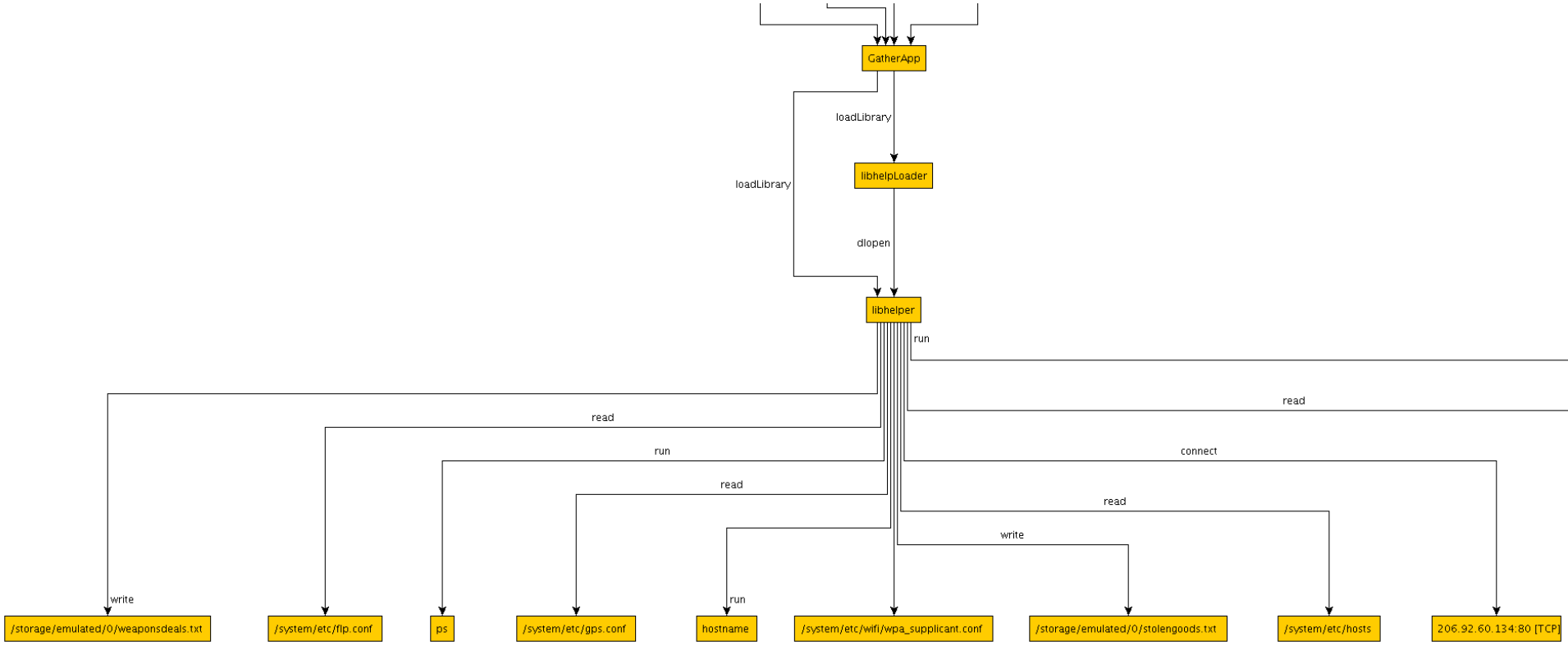


GatherApp with Libhelper

- User installs and runs GatherApp
- GatherApp loads libhelploader which loads libhelper
- Libhelper connects to 206.92.60.134 for C2 comms
- Libhelper runs commands hostname, ps
- Libhelper reads files like /system/etc/hosts and /system/etc/gps.conf
- Libhelper writes to /storage/emulated/0/stolengoods.txt and /storage/emulated/0/weaponsdeals.txt
- User stops and uninstalls GatherApp

KUDU DYNAMICS

PANDEX – ClearScope – GatherApp



Webshell

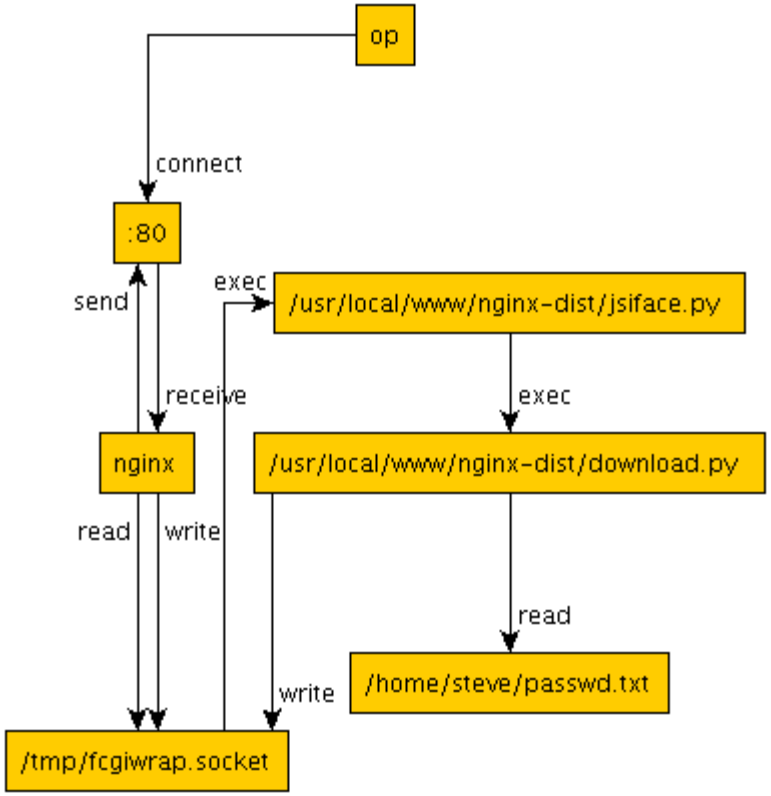
- Target hosts malicious webpage
- Hosted by Nginx web server
- Uses CGI to run Python script
- Remote access to recon system

Webshell

- Adversary connects to webshell diag.html on port 80
- Nginx receives C2 commands
- Nginx writes to /tmp/fcgiwrap.socket
- fcgiwrap.socket executes /usr/local/www/nginx-dist/jsiface.py
- jsiface.py executes /usr/local/www/nginx-dist/download.py
- download.py reads /home/steve/passwd.txt
- download.py writes to /tmp/fcgiwrap.socket
- Nginx reads from /tmp/fcgiwrap.socket
- Nginx sends results back to adversary

KUDU DYNAMICS

BOVIA – CADETS – Webshell



KUDU DYNAMICS

Metasploit

- Used Metasploit to add variety
- Suggested performers test with it leading up to E2
- Used it in a few different ways, depending on the operating system

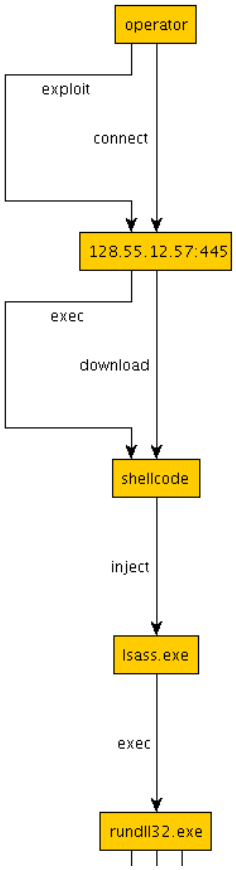
KUDU DYNAMICS

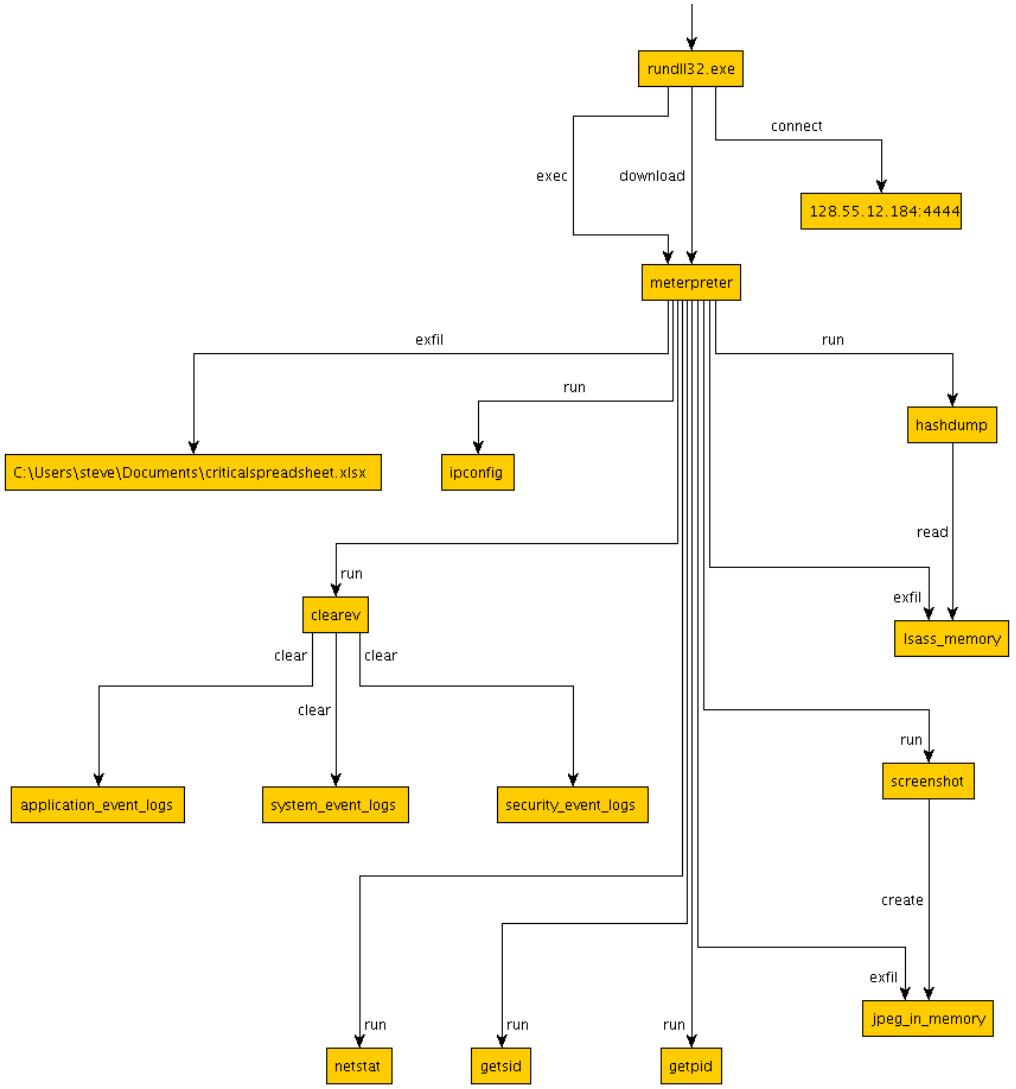
Metasploit

- Adversary exploited target port :445 to run shellcode
- Shellcode injected into lsass.exe process
- lsass.exe executed rundll32.exe to connect to 128.55.12.185:4444
- rundll32.exe downloaded and ran meterpreter
- meterpreter ran recon commands like ipconfig, netstat
- meterpreter took screenshots in memory and exfil'ed them
- meterpreter dumped the SAM password hash database
- meterpreter exfil'ed criticalspreadsheet.xslx
- meterpreter cleared the Windows Event Logs

KUDU DYNAMICS

PANDEX – FiveDirections – Metasploit





Questions?