A Roaming Threat to Telecommunications Companies

crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

Jamie Harries and Dan Mayer

October 19, 2021

- LightBasin (aka UNC1945) is an activity cluster that has been consistently targeting the telecommunications sector at a global scale since at least 2016, leveraging custom tools and an in-depth knowledge of telecommunications network architectures.
- Recent findings highlight this cluster's extensive knowledge of telecommunications protocols, including the emulation of these protocols to facilitate command and control (C2) and utilizing scanning/packet-capture tools to retrieve highly specific information from mobile communication infrastructure, such as subscriber information and call metadata.
- The nature of the data targeted by the actor aligns with information likely to be of significant interest to signals intelligence organizations.
- CrowdStrike Intelligence assesses that LightBasin is a targeted intrusion actor that will continue to target the telecommunications sector. This assessment is made with high confidence and is based on tactics, techniques and procedures (TTPs), target scope, and objectives exhibited by this activity cluster. There is currently not enough available evidence to link the cluster's activity to a specific country-nexus.

Background

CrowdStrike Services, CrowdStrike Intelligence and Falcon OverWatch™ have investigated multiple intrusions within the telecommunications sector from a sophisticated actor tracked as the LightBasin activity cluster, also publicly known as UNC1945. Active since at least 2016, LightBasin employs significant operational security (OPSEC) measures, primarily establishing implants across Linux and Solaris servers, with a particular focus on specific telecommunications systems,[1] and only interacting with Windows systems as needed. LightBasin's focus on Linux and Solaris systems is likely due to the combination of critical telecommunications infrastructure running on those operating systems, in addition to the comparatively lax security measures and monitoring solutions on Linux/Solaris systems that are typically in place on Windows operating systems within an organization.

LightBasin managed to initially compromise one of the telecommunication companies in a recent CrowdStrike Services investigation by leveraging external DNS (eDNS) servers — which are part of the General Packet Radio Service (GPRS) network and play a role in roaming between different mobile operators — to connect directly to and from other compromised telecommunication companies' GPRS networks via SSH and through previously established implants. CrowdStrike identified evidence of at least 13 telecommunication companies across the world compromised by LightBasin dating back to at least 2019.

GPRS eDNS Servers

LightBasin initially accessed the first eDNS server via SSH from one of the other compromised telecommunications companies, with evidence uncovered indicative of password-spraying attempts using both extremely weak and third-party-focused passwords (e.g., `huawei`), potentially helping to facilitate the initial compromise. Subsequently, LightBasin deployed their SLAPSTICK PAM backdoor on the system to siphon credentials to an obfuscated text file. As part of early lateral movement operations to further their access across the network, LightBasin then pivoted to additional systems to set up more SLAPSTICK backdoors.

Later, LightBasin returned to access several eDNS servers from one of the compromised telecommunications companies while deploying an ICMP traffic signalling implant tracked by CrowdStrike as PingPong under the filename `/usr/bin/pingg`, with persistence established through the modified SysVinit script `/etc/rc.d/init.d/sshd` through the following additional line:

```
cd /usr/bin && nohup ./pingg >/dev/null 2>&1 &
```

This implant waits for a magic ICMP echo request, which, when sent to the system, established a TCP reverse shell to an IP address and port specified within the magic packet. The `/bin/bash` process spawned by PingPong masquerades under the process name `httpd`.

eDNS servers are usually protected from general external internet access by firewalls; the magic packet that PingPong listens for would most likely have to be sent from other compromised GPRS network infrastructure. CrowdStrike Services observed reverse shells that had been spawned from this implant, which communicated with a server owned by a different compromised telecommunications company in another part of the world — typically connecting to the remote system on TCP port 53, which is the port primarily used for DNS. These efforts further indicate the actor's continued attempts to disguise their activity as legitimate traffic.

Alongside the deployment of the PingPong implant, LightBasin added `iptables` rules to the eDNS server that ensured SSH access to the server from five of the compromised telecommunications companies. The actor also replaced the legitimate `iptables` binary with a trojanized version (SHA256: `97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb`) that would filter out output from `iptables` that included the first two octets of the IP addresses belonging to the compromised telecommunications companies. These actions make it more difficult for administrators and analysts to identify the firewall rules through review of `iptables` output alone. Indicators relating to this utility are highlighted in Table 1.

File Path	Description
`/usr/local/sbin/iptables`	Trojanized `iptables` binary that replaced legitimate version – SHA256: `97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb`

`/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`
	Legitimate `iptables` binaries in a non-standard directory that are invoked by the trojanized version

Table 1. Trojanized and legitimate iptables file details

Serving GPRS Support Node (SGSN) Emulation

LightBasin uses a novel technique involving the use of SGSN emulation software to support C2 activities in concert with TinyShell. SGSNs are essentially GPRS network access points, and the emulation software allows the adversary to tunnel traffic via this telecommunications network.

TinyShell is an open-source Unix backdoor used by multiple adversaries; however, LightBasin uniquely combined this implant with the publicly available SGSN emulator `sgsnemu`[2] through a bash script. This script constantly ran on the system, but only executed certain steps between 2:15 and 2:45 UTC each day. This window was specified via command-line arguments. During this window, the script performed the following steps in a loop:

1. Execute TinyShell to communicate with an actor-controlled C2 IP address hosted by the virtual private server (VPS) provider Vultr.
2. Add a route to the TinyShell C2 on the interface `tun0`.
3. Check for connectivity to the TinyShell C2 via `ping`.

4. If connectivity to the IP address fails, the script executes the SGSN emulator in a loop, attempting to connect to a set of nine pairs of International Mobile Subscriber Identity (IMSI) and Mobile Subscriber Integrated Services Digital Network (MSISDN) numbers that are used as arguments to the SGSN emulator. These numbers are required to generate Packet Data Protocol (PDP) context requests for connection to a Gateway GPRS Support Node (GGSN), which will then forward traffic to the C2 IP address. Once a connection is established, the SGSN emulator creates a connection to the GGSN via the GPRS Tunnelling Protocol (GTP), and utilizes the interface `tun0` for the connection. The TinyShell implant then uses `tun0`, as mentioned above.[3]
5. If a successful connection has not been made by the end of the 30-minute window, the script kills both the SGSN emulator and the TinyShell implant.

In short, the SGSN emulator is used to tunnel TinyShell C2 traffic between the C2 server and the infected host via GTP through a GGSN.[4] The script is used as a persistence mechanism; it runs continually, but attempts to establish a tunnel to each of the specified mobile stations, which, in turn, act as tunnels to the TinyShell C2 server. The script runs for only 30 minutes each day, culminating in a similar effect to a scheduled job.

CrowdStrike Intelligence assesses that this sophisticated form of C2 is likely an OPSEC measure. This assessment carries moderate confidence, as GTP-encapsulated TinyShell C2 traffic is less anomalous within the environment of a global mobile communications network due to its use of a protocol native to the telecommunications infrastructure that is compromised. Additionally, GTP-encapsulated traffic is potentially subject to less inspection and restrictions by network security solutions.

Additional Malware and Utilities

CordScan: This executable is a network scanning and packet capture utility that contains built-in logic relating to the application layer of telecommunications systems, which allows for fingerprinting and the retrieval of additional data when dealing with common telecommunication protocols from infrastructure such as SGSNs. SGSNs could be targets for further collection by the adversary, as they are responsible for packet data delivery to and from mobile stations and also hold location information for registered GPRS users. CrowdStrike identified multiple versions of this utility, including a cross-compiled version for systems running on ARM architecture, such as Huawei's commercial CentOS-based operating system EulerOS.

LightBasin's ability to fingerprint various brands of telecommunications products and compile tools for various architectures likely indicates robust research and development capabilities to target vendor-specific infrastructure commonly seen in telecommunications environments. This range of capability would also be consistent with a signals intelligence organization with a need to respond to collection requirements against a diverse set of target environments.

SIGTRANslator: This executable provides LightBasin with the ability to transmit data via telecommunication-specific protocols, while monitoring the data being transmitted. SIGTRANslator is a Linux ELF binary capable of sending and receiving data via various SIGTRAN protocols, which are used to carry public switched telephone network (PSTN) signaling over IP networks. This signaling data includes valuable metadata such as telephone numbers called by a specific mobile station. Data transmitted to and from SIGTRANslator via these protocols is also sent to a remote C2 host that connects to a port opened by the binary. This allows the remote C2 server to siphon data flowing through the binary and send data to SIGTRANslator from the C2 to be re-sent via a SIGTRAN protocol.

Notably, data that is sent to and from the remote C2 is encrypted with the hard-coded XOR key `wuxianpinggu507`. This Pinyin translates to "unlimited evaluation 507" or "wireless evaluation 507." "Wireless evaluation" is likely the correct translation, as the malware is targeting telecommunications systems. The identification of a Pinyin artifact indicates the developer of this tool has some knowledge of the Chinese language; however, CrowdStrike Intelligence does not assert a nexus between LightBasin and China.

Fast Reverse Proxy: This open-source utility is a reverse proxy used by LightBasin to permit general access to the eDNS server via an actor-controlled C2 IP address hosted by the VPS provider Vultr.

Microsocks Proxy: This open-source utility is a lightweight SOCKS5 proxy server, typically used by LightBasin to pivot to systems internally.

ProxyChains: This open-source utility is capable of chaining proxies together and forcing network traffic through said chain of proxies, even if the program generating the traffic does not have proxy support. It utilizes a configuration file to specify proxies in use. The recovered configuration file contained a mixture of local IP addresses, IP addresses belonging to Vultr, and IP addresses belonging to eight different telecommunication organizations from around the world.

Some of the tools and TTPs observed by CrowdStrike Services during investigations deviate from the more sophisticated, OPSEC-aware behavior of LightBasin observed in the past, such as by not encrypting binaries using LightBasin's binary packer publicly known as STEELCORGI. The tools and TTPs cataloged in this blog post were observed in congruence with the the usage of SLAPSTICK on select eDNS servers at the start of the intrusion, as well as during periods of strong time correlation, when SSH access from multiple compromised telecommunications company and artifacts indicative of LightBasin tool usage overlapped.

Recommendations

It is not surprising that servers would need to communicate with one another as part of roaming agreements between telecommunications companies; however, LightBasin's ability to pivot between multiple telecommunications companies stems from permitting all traffic between these organizations without identifying the protocols that are actually required. As such, the key recommendation here is for any telecommunications company to ensure that firewalls responsible for the GPRS network have rules in place to restrict network traffic to only those protocols that are expected, such as DNS or GTP.

If already the victim of a LightBasin intrusion, simply restricting network traffic will not solve the problem as LightBasin has displayed the ability to utilize common telecommunications protocols such as GTP for command and control. In this event, CrowdStrike recommends an incident response investigation that includes the review of all partner systems alongside all systems managed by the organization itself. Similarly, if an organization wishes to determine whether they've fallen victim to LightBasin, any compromise assessment must also include a review of all of the aforementioned systems.

Further, as it is a common situation where parts of the network may in fact be managed by a third-party managed service provider as opposed to the telecommunications company itself, an evaluation of security controls in place with the partner should be undertaken to ensure that the systems are sufficiently protected. CrowdStrike Services investigations commonly reveal a lack of any monitoring or security tooling on telecommunications core network systems. While the deployment of security tooling to real-time operating systems is generally limited, other Unix-based operating systems that support the core telecommunications network services are typically targeted by LightBasin and should have some basic security controls and logging in place (e.g., SSH logging forwarded to a SIEM, endpoint detection and response (EDR) for process execution, file integrity monitoring (FIM) for recording file changes of key configuration files). It is also important to ensure that appropriate incident response plans are in place that take into account situations involving partner-managed systems within the network in the event that such an incident is identified. This incident response plan should contain the roles and responsibilities of third-party managed service providers to ensure acquisition of forensic artifacts from third-party equipment not directly under the management of the telecommunication operator themselves.

Finally, given that companies within the telecommunications vertical are extensively targeted by highly advanced state-sponsored adversaries on a constant basis, these organizations need to have access to up-to-date and comprehensive threat intelligence resources so they can understand the threats facing the industry. This intelligence should also provide insights into the TTPs of adversaries that telecommunications companies are likely to encounter, across both the corporate network and critical telecommunications infrastructure, so that these insights can then be used to further augment detection mechanisms and inform on decisions regarding existing security controls.

Conclusion

Securing a telecommunications organization is by no means a simple task, especially with the partner-heavy nature of such networks and the focus on high-availability systems; however, with the clear evidence of a highly sophisticated adversary abusing these systems and the trust between different organizations, focusing on improving the security of these networks is of the utmost importance. Given the significant intelligence value to any state-sponsored adversary that's likely contained within telecommunications companies, CrowdStrike expects these organizations to continue to be targeted by sophisticated actors, further underscoring the criticality of securing all aspects of telecommunications infrastructure beyond simply focusing on the corporate network alone.

Indicators of Compromise

Indicator	SHA256 Hashes	Descripti

`/usr/bin/pingg`	`e9c0f00c34dcd28fc3cc53c9496bff863b81b06723145e106ab7016c66581f72`
	`4668561d60daeb7a4a50a9c3e210a4343f92cadbf2d52caab5684440da6bf562`
		PingPong

`/usr/lib/om_proc`	`3a259ad7e5c19a782f7736b5ac50aac4ba4d03b921ffc6a3ff6a48d720f02012`
	`65143ccb5a955a22d6004033d073ecb49eba9227237a46929495246e36eff8e1`
		Microsock

`/usr/lib/frpc`	`05537c1c4e29db76a24320fb7cb80b189860389cdb16a9dbeb0c8d30d9b37006`
	`16294086be1cc853f75e864a405f31e2da621cb9d6a59f2a71a2fca4e268b6c2`
		Fast Reve

`/usr/lib/frpc.ini`	N/A	Fast Reve Configura

`/usr/lib/cord.lib`
`/usr/lib/libcord.so`
`/usr/bin/libcord.so`
	`6d3759b3621f3e4791ebcd28e6ea60ce7e64468df24cf6fddf8efb544ab5aec0`
	`c5ddd616e127df91418aeaa595ac7cd266ffc99b2683332e0f112043796ede1d`
	`9973edfef797db84cd17300b53a7a35d1207d166af9752b3f35c72b4df9a98bc`
	`4480b58979cc913c27673b2f681335deb1627e9ba95073a941f4cd6d6bcd6181`
	`ad9fef1b86b57a504cfa1cfbda2e2ac509750035bff54e1ca06f7ff311d94689`
		CordScar Telecomm Scanning

/home/**REDACTED**/cordscan_raw_arm	`cdf230a7e05c725a98ce95ad8f3e2155082d5a6b1e839c2b2653c3754f06c2e7`	CordScar Telecomm Scanning (ARM Arc
`/usr/lib/javacee`	`917495c2fd919d4d4baa2f8a3791bcfd58d605ee457a81feb52bc65eb706fd62`	SIGTRAN

/usr/lib/sgsnemu /usr/bin/sgsnemu /usr/lib/sgsnemu_bak	bf5806cebc5d1a042f87abadf686fb623613ed33591df1a944b5e7879fb189c8 78c579319734a81c0e6d08f1b9ac59366229f1256a0b0d5661763f6931c3b63c b06f52e2179ec9334f8a3fe915d263180e538f7a2a5cb6ad8d60f045789123b6	SGSN En
/usr/lib/tshd	a388e2ac588be6ab73d7e7bbb61d83a5e3a1f80bf6a326f42b6b5095a2f35df3	TinyShell
/home/**REDACTED**/win7_exp/proxychains.conf /usr/lib/win7_exp/proxychains.conf	N/A	ProxyCha Configura
/var/tmp/.font-unix	N/A	SLAPSTI Credentia File
/usr/local/sbin/iptables	97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb	Trojanize
/usr/sbin/iptablesDir/ /sbin/iptablesDir/	N/A	Threat Ac created di containing legitimate iptables u following i of trojaniz
45.76.215.0/24	N/A	Vultr IP ra by LightBa
167.179.91.0/24	N/A	Vultr IP ra by LightBa
45.32.116.0/24	N/A	Vultr IP ra by LightBa
207.148.24.0/24	N/A	Vultr IP ra by LightBa
172.104.79.0/24	N/A	Linode IP used by L
45.33.77.0/24	N/A	Linode IP used by L
139.162.156.0/24	N/A	Linode IP used by L
172.104.236.0/24	N/A	Linode IP used by L
172.104.129.0/24	N/A	Linode IP used by L

Table 2. LightBasin indicators of compromise

Endnotes

1. Key examples of telecommunications-specific systems targeted include systems involved in the GPRS network such as External DNS (eDNS) servers, Service Delivery Platform (SDP) systems, and SIM/IMEI provisioning, as well as Operations Support Systems (OSS), and Operation and Maintenance Units (OMU).
2. https[:]//osmocom[.]org/projects/openggsn/wiki/Sgsnemu
3. Correction at 3 p.m. EST 10/20/2021: Clarified the methodology through which an SGSN emulator creates a GTP-encapsulated connection to an IP address.
4. Ibid.

Additional Resources

- *Read How CrowdStrike Falcon Stops REvil Ransomware Used in the Kaseya Attack in the CrowdStrike blog.*
- *Download the CrowdStrike 2021 Global Threat Report for more information about adversaries tracked by CrowdStrike Intelligence in 2020.*
- *See how the powerful, cloud-native CrowdStrike Falcon® platform protects customers from DarkSide ransomware in this blog: DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*