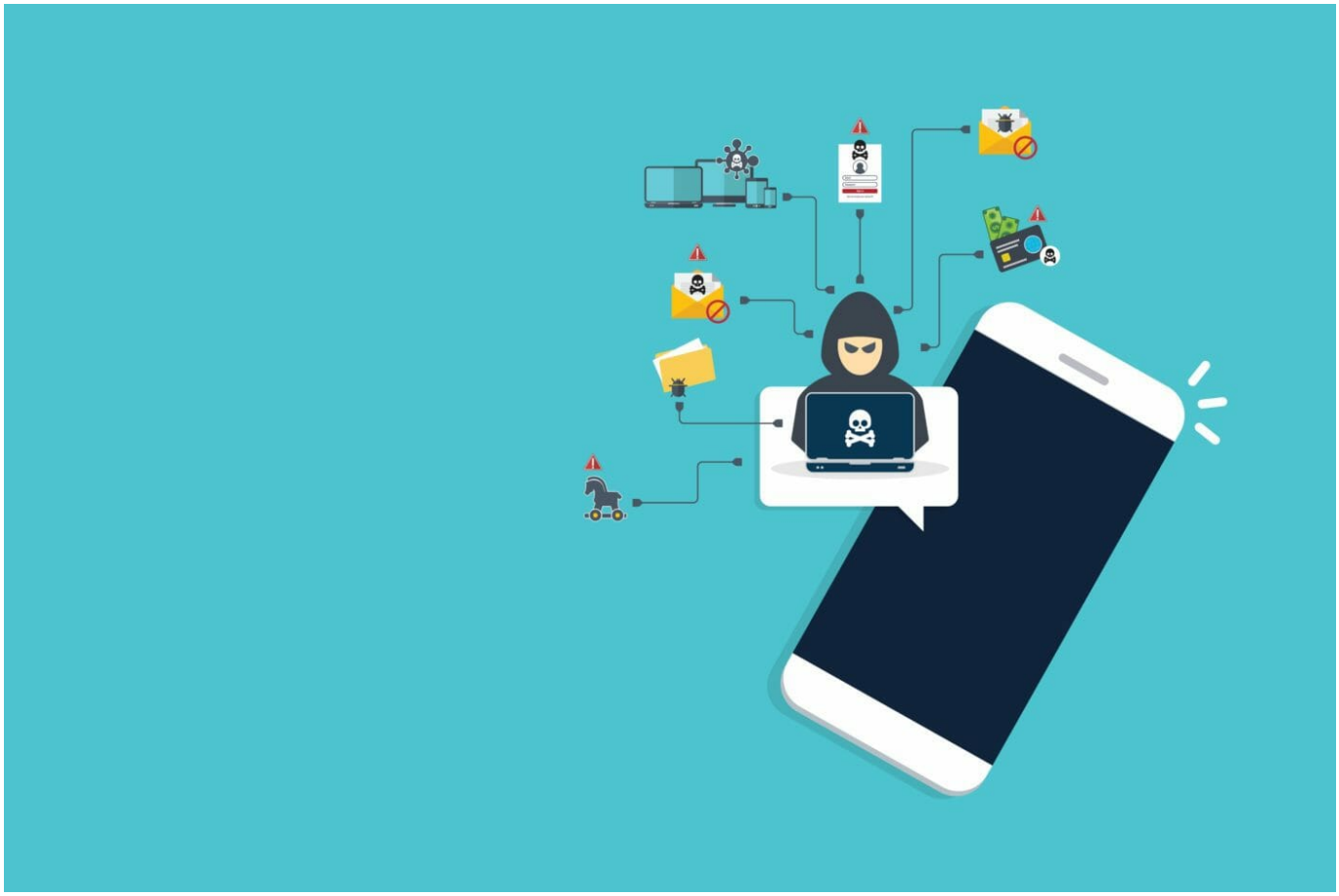
Telecom Networks Are Challenged by Ransomware Attacks



Telecom and cable networks are among the largest and most complex networks in the world. The conditions they operate in and the nature of their business make them prime targets for ransomware:

- **The attack surface is huge.** Carrier networks support millions of end-point devices, including cell phones, wifi routers, devices used in industry and commerce, and so on. Every end point represents a potential entry point to be guarded. Think of it like a castle with a million drawbridges.
- **The hardware mix is extensive.** While carriers have been trying to consolidate network functions onto a smaller range of commodity hardware via Network Function Virtualization, they're a long way from complete. The networks still consist of dozens of unique device types. Each requires its own security management and expertise. There are also many older systems still in use, such as Solaris servers. Patch and password management are full-time tasks.
- **The network is shared.** As core networks, carriers must interconnect at the edge with thousands of other networks. Each of these can become a point of entry.
- **So many connected "things"!** The internet of things is constantly adding more and more

autonomous devices that have no human users and are often left unattended and potentially vulnerable. These devices are often not under the control of the telecom carrier, yet the devices use their networks for data transport.

But there's another trend threatening telecom networks: career hackers. Hacking groups are upping their game and going after larger, more revenue-rich targets. As the telecom website Light Reading reported:

> *Online ransom isn't new. What is new is the scale and sophistication. Groups like DarkSide and their collaborators are what are termed big-game hunters that are going after deep-pocketed corporations with increasing frequency.*

Telecom Ransomware Attacks Are Happening

This shift toward "big-game hunting" attacks makes telecoms prime hacker targets. And this is more than just theoretical. It was recently revealed that a hacking group called LightBasin infiltrated at least 13 different telecom networks. As security firm CrowdStrike noted, this group had expertise with "telecommunications-specific systems … 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)."[1]

This focus on systems specific to an industry represents yet another uptick in the ongoing battle against hackers. Every industry has its unique systems and applications that offer potential exploits. The LightBasin hackers also took advantage of the interconnectedness of telecom networks.[2]

> *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.*

In addition to the LightBasin hacks, there have been other high-profile ransomware attacks on telecom networks. Protecting systems from ransomware is challenging even in a small network. Telecom providers are sophisticated network operators with a strong focus on security, but their task is daunting.

How Pure Storage Can Help

The goal of ransomware infiltration is to encrypt data and use it to extract a financial payment in exchange for a decryption key. This is where Pure can help. Pure SafeMode™ snapshots secure backup data and metadata by creating a secure copy. Ransomware can't eradicate, modify, or encrypt SafeMode snapshots, even when admin credentials are compromised. With just a few clicks, you can restore business-critical data quickly and at scale.

SafeMode can be used with FlashArray™ snapshots to protect primary data sets. Both FlashArray and FlashBlade® can function as backup targets. Pure has partnered with numerous backup providers to certify solutions and provide best practices, including Commvault, Veeam, and Veritas.

With telecom networks increasingly the target of hackers and ransomware, there's no time to lose locking down as much data as possible. For telecoms with existing Pure assets, you can contact your account rep for a SafeMode advisory workshop. SafeMode technology is included with your Pure gear at no additional cost, although it will consume additional storage space depending on snapshot retention times.

For telecoms that aren't currently Pure users, please explore our telecom solutions and learn why nine of the top 10 global telecom providers use Pure.

Learn more about safeguarding your network from ransomware in the "Hacker's Guide to Ransomware Mitigation and Recovery," featuring Hector Monsegur—a former black hat and member of the LulzSec and Anonymous hacking collectives—who shares his insights and tips to help you safeguard your data.

---

[1] https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

[2] https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/