How Telos Ghost® helped a global financial services firm to proactively fight cybercrime.

Truly anonymous virtual private lines connecting locations around the world to a state-of-the-art threat intelligence center — with no discernable latency.

One of the world's largest multinational financial services corporations with over $10 billion in annual revenue faced increasingly sophisticated threats from cyber criminals. These escalating cybersecurity threats put millions of dollars in transactions at risk each day.

To thwart criminals, the company had two choices: one, lock down their system to make it safer, but less functional. Given the competitive nature of the financial services industry, less functionality and flexibility would be corporate suicide — a move their competitors would celebrate. Their second choice? Maintain their open system and their competitive edge — but stay one step ahead of the criminals.

Building a Proactive Threat Intelligence Center

In order to mitigate the significant risk posed by cybercriminals in the more than 200 countries where they do business, the company decided to build a state-of-the-art threat intelligence fusion center with very specific technical needs and requirements. However, they faced two major challenges in bringing this center to life.

Challenge #1: Finding an Affordable Solution

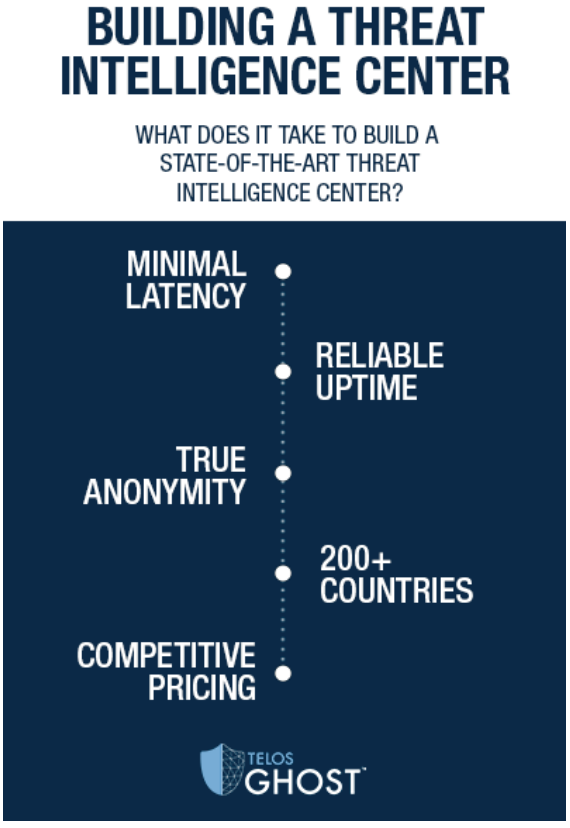
If you want to beat your enemy, you need to understand them. This means making sure you can gather real-time, uncompromised data — anonymously. Malware and attacks need to be studied and analyzed quietly without tipping off the enemy. Data needs to be returned to analysts quickly, without being traced.

However, doing this on a corporate network is risky. To mitigate risks, **any environment used to study malware needs to be completely technically and commercially separate from the corporate network**. This distinct network must also be set up quickly, with nodes available in short notice within any of hundreds of countries across the globe. Nodes that may ultimately be compromised and discarded, while new nodes are quickly created elsewhere.

However, the traditional way of setting up this kind of network – using private leased lines – is incredibly cost-prohibitive, making it impractical for all but the largest organizations.

Challenge #2: Uptime, Latency, Anonymization Requirements

Not only does this network need to be separate and distinct, it also must meet **stringent performance requirements for uptime and minimal latency**. It must also be completely anonymous. Latency tips off the enemy. Downtime costs money. Easily traced sacrificial nodes compromise investigations and expose organizations and their computing assets. Because of this, traditional means of anonymization like Tor or one-hop proxies are inadequate. Why?



Whether you are sending or receiving data, **Tor and similar products are notorious for latency, uptime issues, and identifiable nodes.** Identifiable nodes makes it obvious that you aren't where you claim to be, while network latency and uptime issues slow your investigation to a crawl. This isn't acceptable in a business where time can mean the difference between thwarting an attack and cleaning up after one.