



Barry Cryer
President

TSC's Technology Thwarts Cryptojacking

CARBONDALE, CO – June 14, 2018 - TSC a leading managed technology services provider, is helping small to mid-sized businesses (SMBs) to prevent cryptojacking attacks from damaging their organizations. Cryptojacking attacks, are derived from the widely popular cryptocurrencies, such as Bitcoin and Ethereum, and occurs when a corporate server is hijacked in order to facilitate cryptocurrency transactions by leveraging the inherent power of high-performance servers. As cryptocurrencies rely on an enormous amount of server power in order to facilitate transactions, many of the corporate servers that power small to mid-sized businesses have become an obvious target of cryptojacking attacks, as they are simply the most efficient vehicle for cryptojackers to exploit. TSC is currently protecting SMBs from this threat.

“Businesses that are under attack are often unaware of this threat because these attacks are specifically designed to be minimally intrusive and hard to trace,” stated Barry Cryer, President at TSC. “Typically, cyber criminals set up their malware to run quietly in the background during daytime hours, only to extract maximum power during off-hours. It’s one of the telltale signs, yet this is rarely monitored by organizations that aren’t working

with a reputable managed technology services provider. The result is that most businesses are flying blind and unaware that their security has been compromised, which doesn’t seem very dangerous on the surface. However, this leaves many cryptocurrency hackers with access to very sensitive points within an organization that can be taken advantage of later.”

Most attacks take place when businesses are most vulnerable; after-hours and during migration to cloud-based solutions. During off-hours, cryptocurrency mining software can be installed quickly and without detection, creating a pivot-point where hackers can later install even more malware. Another vulnerable moment is when businesses are migrating their network to the cloud. The vulnerability here is because of the complexity and level of detailed attention required to successfully navigate these kinds of infrastructure transitions. Where most business owners simply add technology piece-by-piece, this fails to address the gaps in the network that arise glomming one solution onto another. Networks can quickly become messy and this is how organizations get exposed to hackers. In the case, of cryptojacking, it’s no different.

“Business owners can protect themselves by taking the following actions, commented Mr. Cryer. “As

a first step, they need to diagnose their network and segment the utilization of their data. By doing this, business owners or CTOs can see which devices, servers, and endpoints are performing optimally and which are underperforming. Underperforming servers can provide a hint that the organization may have been cryptojacked. Another action they can take is to make sure that they aren’t vulnerable to exploit kits, which are tools hackers use to infiltrate networks via common business software. Lastly, businesses can direct their attention to systems that expose the network, like VPNs (Virtual Private Networks) or other cloud-based technology. While there are many more steps to take, these are very effective first steps to protect any organization from cryptojacking.”

ABOUT TECHNOLOGY SYSTEMS CONSULTANTS

Founded in 1992, Technology Systems Consultants is committed to establishing and maintaining a dynamic partnership with every customer. Extensive technology and service experience allows the TSC team to develop an understanding of each customer’s unique telecommunications requirements, and to respond to those requirements quickly and effectively.

TSC's local dispatch center delivers round-the-clock service to ensure system reliability. TSC also

offers comprehensive service 24 hours a day, 7 days a week and

emergency service guaranteed within 4 hours.