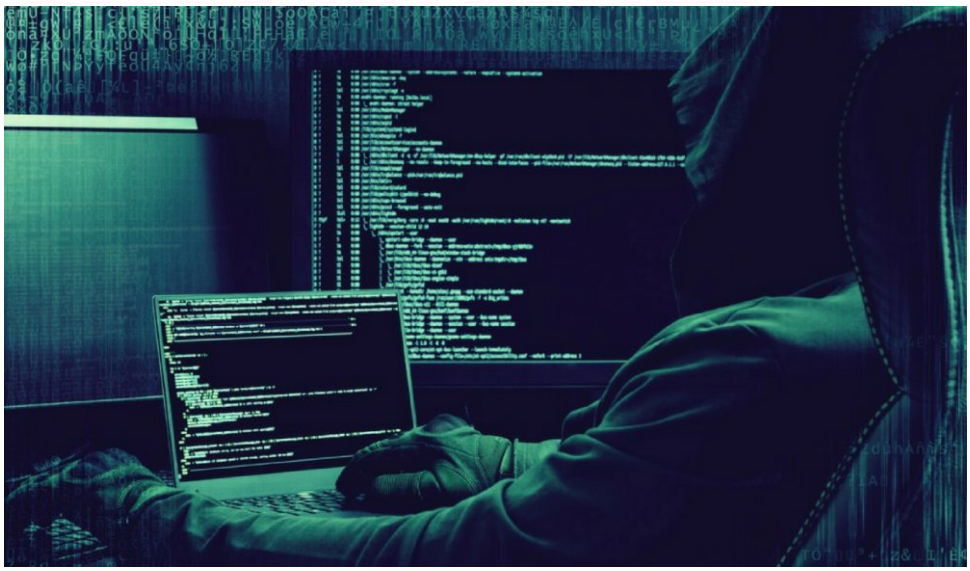
News

“The cybersecurity gap is growing”, says ComNet GTS Specialist



Cybersecurity has again been firmly in the news with a spate of high-profile attacks in recent months. None more so than the SolarWinds cyberattack of 2020, which has been cited by security experts as “one of the potentially largest penetrations of Western governments” since the Cold War.

The attack's most prominent target was the US government, with multiple office networks reported to have been compromised, including the treasury and commerce departments and Homeland Security.

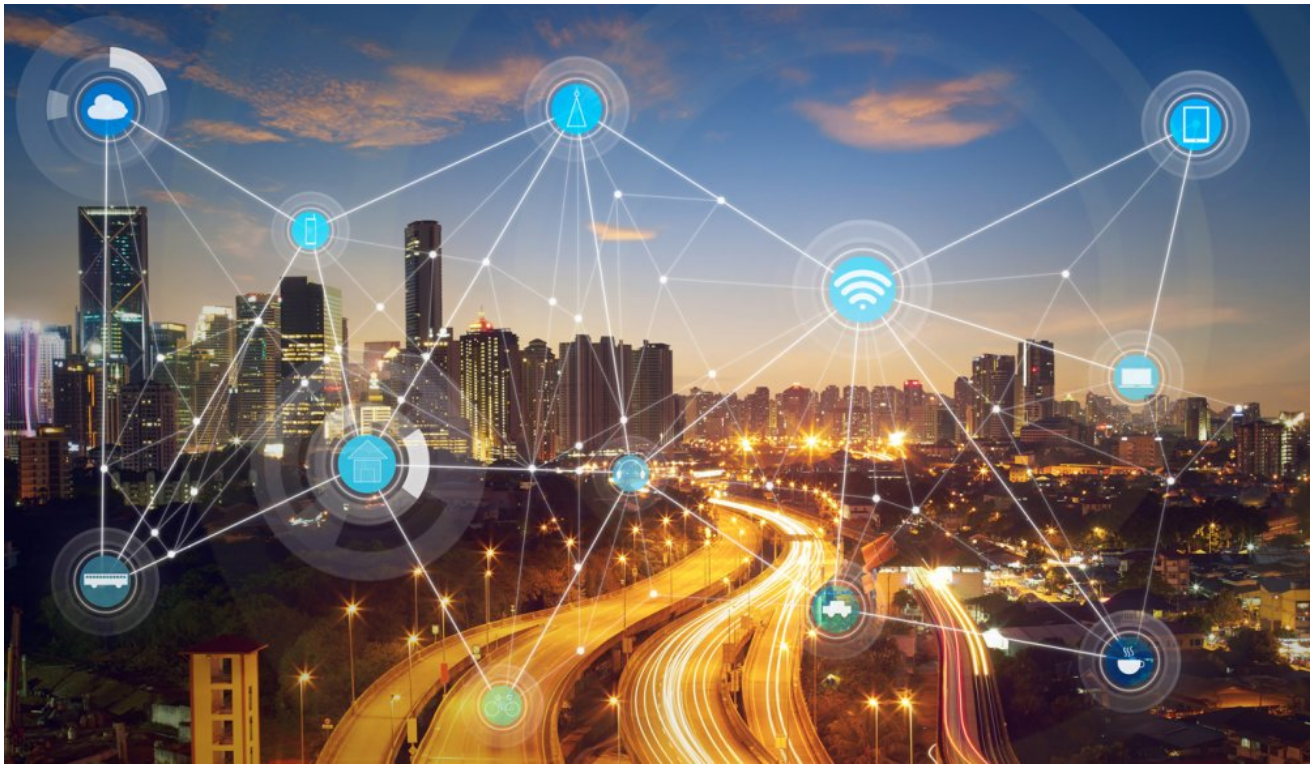
Fraser Johnston, Layer 3 Expert – Network Specialist on ComNet’s GTS team, states that despite the devastating effects of the SolarWinds cyberattack, it was likely caused by something as simple as the exploitation of a “hacker injected backdoor communications

protocol.”

Months ahead of the attack, hackers broke into SolarWinds systems and added malicious code into the companies software development system. This meant that later on, updates being pushed out included the malicious code. This created a backdoor communication for the hackers to use. Once you hack one body, you can then gain access to many.

Johnston asserts that Razberi Monitor™ devices, **newly acquired by ComNet**, can easily protect from these types of attacks by stopping ports talking with routable internet addresses and alerting on a later violation of this protection.

Johnston explains how cyberattacks' threat has increased due to IT's growth in the last 20 years.



“For instance, **IoT devices** have become cheaper and led to an explosion of network devices,” **Johnston** begins. “However, the problem arises where, in my view, while IT hardware and software has grown, spending on IT staff has never matched this pace. This inevitably leads to vulnerabilities when you have limited IT resources to respond to the increase in IoT devices that now get more attention from would-be hackers.”

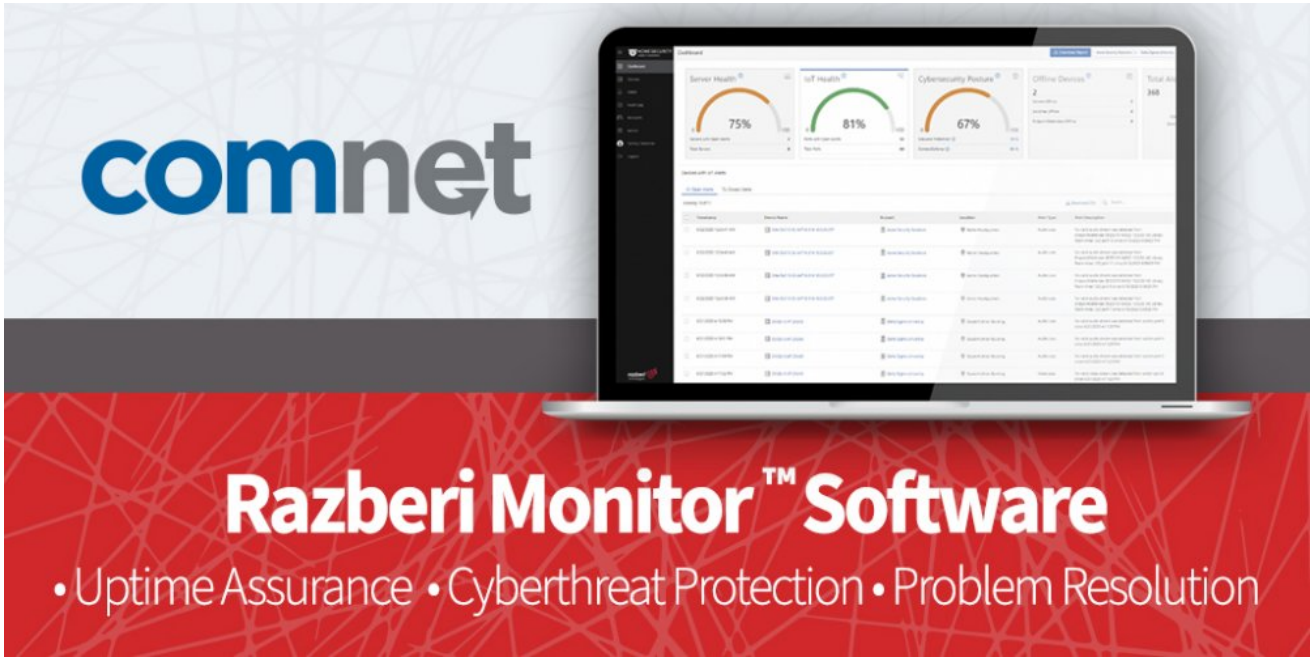
Johnston continues: “The cybersecurity gap is growing. This is because we’re in a world where it's counter versus counter in terms of IT teams plugging gaps and hackers finding new ones. And that is never going to stop. From an IT point of view, we continue fighting cyber threats by developing new ways of protecting through inhouse testing, market leads, and customer leads.”

The key to this battle is the education of end-users. On this point, Johnston says that end-users level and awareness of cybersecurity is increasing. However, Johnston cites this as a double-edged sword, crediting this with the explosion of IoT products in recent years and the following cybersecurity vulnerabilities that many IoT devices can bring.

“For end-users, education is key. When it comes to **cybersecurity**, you need to educate on what’s available, how it is configured, and how to enable your system effectively. In IoT, when you give them a platform, you also have to teach them how to use it correctly. And that can be a constant battle.”

One such product in the ComNet portfolio that is cybersecurity conscious is Razberi Monitor™. This software platform provides a top-down view of the physical security network and ecosystem without IT resources. It monitors and manages all the system components for both cybersecurity and system health. Razberi Monitor™ is a small agent communicating with Razberi Monitor™ cloud. It is also compatible as on-premise with Milestone alert server, SolarWinds API, and MS Syslog (SPLUNK implementations).

Monitor™ provides secure visibility into the availability, performance, and cyber posture of servers, storage, cameras, and networked security devices. Not only that, but it predicts and prevents problems while providing a centralized location for IT departments to view video data.



Johnston describes Razberi Monitor™ as software that enables problem resolutions before becoming more significant problems with proactive maintenance. He explains, “when you don’t see video is when you need the video. So, Razberi Monitor™ identifies issues before they fail and become an outage, which is key to good **cybersecurity** and is a significant cost saving.

“For example, if there is an incident in a supermarket, checking your camera data and realize they have been unavailable/not recording for some time. Suppose your cameras are failing or are compromised in any way. In that case, Monitor™ will pick that up and inform you well in advance of it becoming a problem.”

Countermeasures are also automatically implemented, such as port shutdown for intrusion detection or PoE power cycle for cameras that are offline or not streaming video/audio.

ComNet’s new Razberi Monitor™ software is coming soon. For more information, stay tuned to:

www.vanderbiltindustries.com/comnet

By David Prendergast

David Prendergast is the Content Creation Manager at Vanderbilt International.