# CYBER BODYGUARDS - AIRBUS PROVIDE PEACE OF MIND DURING THE COVID-19 PANDEMIC

**News / Manufacturer**


Difficult situations – such as the current coronavirus pandemic – often bring out the best in people, as exemplified by the global outpouring of support for heroic healthcare and medical professionals in recent weeks. Unfortunately, these situations also can accentuate the worst – which is why the Airbus CyberSecurity team hasn't skipped a beat since the COVID-19 outbreak began, preventing adversaries from stealing valuable data and crippling essential systems at an unprecedented time for governments, agencies, corporations and individuals alike.

According to Nicolas Audiot, the Deputy Head of the Airbus Security Operations Centre (SOC) in Elancourt, France, regular operations are continuing while half of his 40 colleagues now contribute remotely – with one team physically present at the SOC for two weeks while the other team works from home, then switching – to reduce the risk of coronavirus infection.

This setup is essential to maintain the quality of operations 24/7, especially in times where cyber-criminals are trying to exploit the public's fear of COVID-19.


**Resisting ransomware and other malware**

One such scam being perpetuated is called “waterholing,” in which adversaries disguise their intentions by registering internet addresses referring to the coronavirus to build fake websites. The aim is to attract as many followers as possible, and then launch ransomware or other kinds of malware.

In ransomware attacks, adversaries infiltrate networks and encrypt important data – from hospitals, for instance – and demand a ransom before releasing the data again. “Many victims just pay,” said Audiot, adding that most simply can’t afford to shut down. But even after paying a ransom, there is no guarantee the victims will return to a functioning system.

**Phishing prevention**

Phishing email attacks also are on the rise. If recipients click on links or attachments, malware is deployed which hackers then utilise to steal business-critical information. Both ransomware and phishing have been increasingly afflicting companies and institutions since the spread of COVID-19 began, Audiot added.

Airbus’ cyber experts also have observed an uptake of Virtual Private Network (VPN)-related exploits. Here, adversaries are scanning VPN servers to take advantage of systems that companies have set up to enable their employees to work from home, but which were poorly configured or have vulnerabilities.

According to Audiot, the SOC has responses for all such threats. "We have deployed so-called Indicators of Compromise or IOCs and provided our customers with tactical instructions – helping to protect them from harm,” he explained.

**On the alert for new threats**

In constantly assessing the risks, Airbus’ SOC teams design and implement detection means,

 

analyse potential attacks, define adequate remediation measures; repeating this cycle indefinitely, taking the intelligence provided and shared by their colleagues into account.

“Not only do we cover ‘simple’ threats such as malware and ransomware, we’re also focussed on attacks that come from nation-state actors who attempt to steal valuable data or cripple essential systems,” added Audiot.

During the Airbus cyber security operations, Level 1 colleagues identify and evaluate suspicious activities and notify customers in case of a real threat. If it is an attack, Level 2 personnel continue to investigate and define measures. Level 3 colleagues and Incident Response Teams come into play when more complex attacks are to be fended off. The Service Delivery Managers act as an interface between SOC teams and customers, coordinating all measures.

**28 APRIL 2020**

**ARTICLE LINK:**
https://50skyshades.com/index.php/news/manufacturer/cyber-bodyguards-airbus-provide-peace-of-mind-during-the-covid-19-pandemic