



## TECHNOLOGY

Cyber threats against ICS systems most prominent

# Kuwait sees large spike in malware attacks ... up 64%

By Marlon Aquino Malinao  
Arab Times Staff

At GITEX Technology Week 2021, which opened Sunday October 17 at the World Trade Center in Dubai, Kaspersky research highlights that malware is widespread across the Middle East. Accounting for 161 million of attacks and growing by 17% when compared to the last year figure – 138 million. “Kuwait has seen a large spike in malware attacks increasing by 64%,” said Emad Haffar, Head of Technical Experts for the Middle East, Turkey and Africa at Kaspersky.

Cyber threats against ICS systems stand out as the most prominent. The UAE experienced a 4% increase in attacks against ICS computers during the first half of 2021 when compared to the same period last year. This stands higher than the global average which only increased by 1.2% for the same period.

Industrial control system (ICS) security oversees the safeguarding and protection of control systems used for monitoring industrial processes. Such systems are critical in keeping essential infrastructure functioning and they are increasingly under attack. The potential for critical system breakdown, production accidents, and even city-wide or national impact is increasing.

In Kaspersky’s “Threat Landscape for Industrial Automation Systems Report”, spyware, which is mostly deployed to steal money and information, are up by 0.6 percentage points in UAE. Simultaneously, malicious scripts grew



Emad Haffar, Head of Technical Experts — Kaspersky

by 2.7 percentage points. Threat actors use such scripts on various websites hosting pirated content to redirect users to sites that distribute spyware or malware designed to mine cryptocurrency without the user’s knowledge.

“The global trajectory is to move to digital services across the board. This also includes Industrial Control systems which today are increasingly connected. For many, this has translated in increased convenience and efficiency, but it also exposes them to cyberattacks. A worst-case scenario can result in total disruption of industrial processes. Depending on the criticality of an industrial object, the results can mean a loss of money, halt a global supply chain or even lead to real-world, physical damages,” Haffar added.

ICS security is often overlooked because the devices fall somewhere in between ICT and engineering. Cyber Security today is everyone’s concern, it is no longer an option for the responsibility to lie with one department alone but rather across a few departments.

Based on their report’s findings, Kaspersky’s research team outlines a few steps organizations can take to ensure a secure ICS environment:

Conduct ICS assessment: An ICS security assessment will identify security flaws on all layers, starting from physical and network security.

Through the various tests that mimic common attacks, experts will separately analyse the software and hardware solutions used to control the industrial process and the systems connected to it – and most importantly, their vulnerabilities.

Choose the correct product: Security needs to evolve quicker than attackers, to protect industrial environments from cyber threats. As the number of threats targeting critical infrastructure increases, choosing the right advisor and technology partner to secure your systems becomes even more important. Kaspersky ICS products are purpose-built so that the organisation is secured and are designed to protect industrial operator panels, workstations, and servers.

Employee training is a critical part of ICS security: Human error due to a lack of cybersecurity knowledge and awareness is the leading cause of cyber-incidents. Training can be short and intensive, tailored for everyday users of computer-based systems as well as more in-depth for IT/OT security experts, ICS operators and engineers especially ones that do not have an IT background.

Private ICS Intelligence is essential: Intelligence services help ICS operators stay safe in the face of constantly emerging threats, and assists them in developing defensive strategies. Analytics, collected especially for a customer’s region will enhance cyber protection from targeted industrial cyber-attacks.

A service like Kaspersky’s ICS Hash Data Feed offers threat intelligence for the benefit of security operations, incident investigations and responses that are relevant to industrial control systems. It helps to focus on mitigating threats that are most relevant to the user’s industrial infrastructure and pose the most risk to the business.

While this provides a broad strategic approach to ICS security, the fact remains that a customised consultation, testing, and roadmap is absolutely essential. As with any mission-critical consideration, it is sound business sense to be prepared and equipped in advance.



Avaya stand at the GITEX Technology Week Dubai

Ecosystem designed to help firms build better experiences for employees, customers

## Avaya unveils ‘Avaya Experience Builders’

By Marlon Aquino Malinao  
Arab Times Staff

Avaya (NYSE:AVYA), a global leader in solutions to enhance and simplify communications and collaboration, at GITEX Technology Week Dubai unveiled Avaya Experience Builders™, globally aligning Avaya’s services, partners and developers into an ecosystem designed to help enterprises build better experiences for employees and customers, wherever and whenever communications and collaboration happen. The needs of customers have changed dramatically, and this ecosystem is uniquely positioned to deliver next-generation customer and employee experiences through the Avaya OneCloud™ AI-powered experience platform.

“How people feel about their interactions with companies is now more important than the products and services they buy, and every business must orchestrate memorable moments that shape customer and employee engagement, satisfaction and loyalty,” said Jim Chirico, CEO, Avaya. “Enterprises are looking to Avaya for specific expertise in building those better experiences. They can’t be delivered with monolithic apps in a cloud world. They must be composable. Experience Builders can deliver the tailored, engaging and effortless communications and collaboration that enable businesses to create deeper relationships with customers and drive new sources of revenue.”

Avaya Experience Builders makes it easier for businesses to build and deliver these experiences across their limited or siloed development functions by providing the right amount of co-development support each company needs, whether that’s simply subscribing to tailored existing experiences, developing completely new experiences, or leveraging AI technology to enable end users to self-compose their experiences.

“Building the future requires a new way of thinking about experience design and development,” said Simon Harrison, CMO, Avaya. “Avaya is committed to continue empowering our customers to address new, flexible work challenges with best-in-class innovation. Avaya Experience Builders as a community provides them with unparalleled ‘Total Experience’ development and deployment capabilities. It enables them to better navigate uncharted waters as we all move forward into new realities.”

“With the introduction of Avaya Experience Builders, Avaya is recognizing the need for businesses to expand their capabilities beyond their corporate walls to include partners, developers and even customers in an ecosystem creating AI-powered experiences,” said Zeus Kerravala, ZK Research. “Avaya’s unique expertise, large set of technology partners, significant channel reach, and huge global customer base represents one of the largest such ecosystems available today.”

### Avaya Experience Builders Components

#### People:

- Over 250 technology partners, including AI technology vendors
- Over 32,000 companies in Avaya DevConnect
- Over 154,000 registered developers – 24,000 of them using Avaya OneCloud CPaaS

- 7,200 channel partners and agents

#### Solutions and Tools:

- Avaya Hybrid Cloud Services, Omnichannel Services and AI Services – Powerful tools, including frameworks, connectors and pre-built workflows to solve complex problems and use cases. This includes over 40 APIs (and growing) to connect existing Avaya systems with new cloud applications that address today’s new Hybrid Work use cases.

■ Avaya OneCloud, the award-winning, communications and collaboration platform that provides the foundation to compose new experiences. Avaya OneCloud includes Avaya OneCloud UCaaS, Avaya OneCloud CCaaS, and Avaya OneCloud CPaaS – which recently won Best CPaaS of 2021 by UC Today (panel of industry analysts).

■ A vision for AI – Avaya recently won Best Use of AI for 2021 by UC Today (panel of industry analysts).

Here is what some Avaya Experience Builders™ have to say:

■ Darryl Jackman, Business Automation Developer, Marine Rescue Technologies: “We use Avaya for a multitude of applications, including cloud-powered self-service to significantly reduce the number of calls staff are required to handle. Having a scaling cloud infrastructure allows for these use cases in parallel, even during higher load times.”

■ Venkatesh Krishnaswamy, CEO and Founder, Koopid: “We use Avaya OneCloud CPaaS as a preferred provider, streamlining communications and collaboration for our clients to engage with their customers. Our clients run the gamut, from mid-market businesses to large enterprises, and a variety of use cases, to address a broad range of needs across their organizations.

Avaya is providing demos of some of the Avaya Experience Builders™ creations at GITEX this week. For more information, go to [Avaya.com/AvayaExperienceBuilders](https://www.avaya.com/AvayaExperienceBuilders).

#### Additional Resources

- Avaya Experience Builders™ Blog
- Avaya Experience Builders™ Video with Konexios
- Avaya.com website (TBA)
- Experience Builder customers: <https://www.trustradius.com/products/avaya-onecloud-cpaas/reviews>

editor’s choice

