Forbes Middle East

Can we ever defeat the malware maker?

Trend Micro's regional VP discusses the looming threat landscape, common errors that precede digital incursions, and misconceptions about cloud protection

The Middle East has long had an uneasy relationship with cybersecurity. More than 3.2 million clicks led unwary GCC Internet users to malicious websites in the first quarter of this year alone. Those clicks – solicited by malicious emails or SMS messages, through the sly application of social-engineering techniques – were discovered by just one company, so the scale of the phishing problem is many times greater.

Trend Micro's ecosystem of sensors and data is spread across MENA and allows the firm's specialists to gauge the progress of the ever-burgeoning threat landscape.

"During the past couple of years, we have seen a huge escalation in the scale and complexity of cyberattacks in the Middle East," said Dr. Moataz Binali, Vice President, Middle East and North Africa, Trend Micro. "If you look at email attacks, you see more than 53 million that we have managed to detect and block throughout the past quarter alone and more than 1 million malware threats detected and blocked in the same period."

While demonstrating preferences for the government and education sectors, "bad actors" have also shown interest in manufacturing companies and critical infrastructure, including telecoms and the petrochemical industry. Binali believes the Middle East's appetite for digital transformation has played a key role in the escalation, establishing the region as one well-known for having higher-than-average attack numbers.

Backdoors and backstops

"The region is more prone to attacks because, as the recent digital transformation trend took hold, organisations exposed more attack vectors to malicious parties through automation," Binali said. "Consider the manufacturing industry, which has to accommodate two kinds of security – IT and OT [operational technology]. Historically, companies are very good when they are trying to protect themselves from the IT perspective, but not so much from OT, because the OT component is surprisingly simple and outdated compared to the IT, and easy to penetrate. So, IT is left vulnerable because of under-protected OT. And this is an even bigger problem now that the two are connected openly through IoT [Internet of Things]."

Indeed, attackers now have at their disposal the very digital-transformation arsenal that has made their victims increasingly vulnerable. From advanced analytics to remote-sensor technologies, the global technology corpus is expanding. And as it grows, it is simultaneously swelling the attack surface.

"These innovations are global," Binali said. "So, there is no real way to stop hackers from obtaining these innovations and utilising them. The approach in dealing with this is to ensure cybersecurity companies and technology companies are armed with the same innovations, and that they include them in their products and platforms."

Clouds… and silver linings

Cloud – perpetually “the next big thing”, according to Binali – is also an issue with which regional organisations must grapple, especially when it comes to misconceptions about how, and by whom, it is secured.

“A recent Microsoft survey shows 51% of Gulf organisations investing in cloud, but Gartner says cloud spending in the wider Middle East is actually among the lowest in the world,” he pointed out. “But this, I believe, has to do with regulatory straitjackets involving data residency, which may become less acute, now that Google, Microsoft, AWS and SAP are opening data centres in the region. This will allow governments, healthcare, telecoms and banking entities to migrate to the cloud. However, those entities must rid themselves of the notion that security in their new cloud home is incumbent upon the service provider. Cloud has a shared model of security, with the vendor protecting the infrastructure.”

The responsibility for protecting applications and data in the cloud, Binali explained, lies with the customer, just as it would if they had retained their legacy, on-premises architecture. But those customers, because they have moved to the cloud, will also have access to pay-as-you-go software-as-a-service (SaaS) models for cybersecurity. Such models provided by cloud vendors also, traditionally, mitigate cost. This is because economies enjoyed by the vendor can be passed onto customers while converting the costs of procurement cycles from up-front capital outlays (CAPEX) to ongoing, and more predictable, operational spending (OPEX).

“Definitely cloud is a cost-saving model and cybersecurity is part of that saving,” Binali said.

Patrolling the landscape

Trend Micro takes a broad perspective in dealing with cybersecurity, with a portfolio that covers endpoint, cloud and network defences. Binali sees the global market for the company’s offerings as being populated with two main types of competitor.

“The first type is the dedicated cybersecurity company that matches what we do; big portfolio,” he said. “For these companies, we don’t deviate from our core cybersecurity offerings. As a Japanese company, innovation is part of our DNA and we try to spread the connected-threat-defence story as the digital transformation of the security industry, because we connect security products in a new model of protection through Trend Micro Enterprise. The other competitors are the start-ups, a lot of which might have strong, innovative offerings. But we bring the big portfolio.”

At the local level, Trend Micro brings out its CCC (“committed”, “connected”, “complete”) vision.

“The commitment we bring to the Middle East varies from that of other vendors in that we have three separate offices across the region – Dubai, Saudi Arabia and Egypt – offering technical and business resources,” said Binali. “We are also establishing incident-response centres in strategic locations, as well as data labs and mentoring programmes for cybersecurity start-ups. ‘Connected’ comes from the power of the connected-threat defence and ‘complete’ refers to our capability to cover end-point protection, hybrid cloud and network defence.”

In the past year, Trend Micro has struck partnership deals across the region, including one with Saudi education-technology company TETCO, which will cover 28 universities and more than 30,000 schools across the kingdom. Other Saudi engagements include those with the Federation for Cybersecurity, Programming and Drones, the Ministry of Information Technology and Communications and the National Cyber Security Centre.

“We have replicated these relationships with similar organisations across the GCC,” said Binali. “This is part of our commitment – to work with organisations that seek to protect others from digital threats.”

-ENDS-

https://forbesmiddleeast.com/can-we-ever-defeat-the-malware-maker