BIZCOMMUNITY

Ransomware activity doubles in transportation and shipping industry

The Trellix Advanced Research Center has released its latest Threat Report, covering insights into trends and developments in the global cybersecurity landscape in Q3 2022, how it's doubled in the transportation and shipping industry, and how this relates to the South African market.

Source: Supplied

"Interestingly, the trends observed in South Africa are pretty much in line with what is happening globally," says Carlo Bolzonello, country lead for Trellix South Africa. "In the last 12 months, we have seen an uptick in activity from cybercrime actors targeting South Africans, and while the actors may be different, the attacks are the same, in terms of global presence.

"South African companies are indeed taking the necessary steps to protect against cyber threats, but the financial investment this requires is substantial. This is especially challenging considering the exchange rate with the dollar, which has an impact on the ability of some organisations to fully stay abreast of the most relevant technologies from overseas vendors.

Ransomware is a business resilience issue, not an IT problem

Kate Mollett 16 Sep 2022

"Also, human capacity in cyber security resources is still a major problem, as there is a huge dearth of knowledge in South Africa. This doesn’t even account for the steady exodus of these already rare skills from the country, with people being driven by better salaries and work-from-home offerings from international companies, who are more progressive when it comes to remote working," Bolzonello says.

He adds that in order to adequately protect themselves and their customers' information, South African companies need to make aggressive investments in both areas simultaneously, acquiring the best-of-breed technologies and continuously equipping people (both users and security personnel) with globally relevant capabilities.

The report includes evidence of malicious activity linked to ransomware and nation-state-backed advanced persistent threat (APT) actors. It examines malicious cyber activity including threats to email, the malicious use of legitimate third-party security tools, and more.

Image source: Gallo/Getty

Key findings

US ransomware activity leads the pack: In the U.S. alone, ransomware activity increased 100% quarter over quarter in transportation and shipping. Globally, transportation was the second most active sector (following telecom). APTs were also detected in transportation more than in any other sector.

Germany saw the highest detections: Not only did Germany generate the most threat detections related to APT actors in Q3 (29% of observed activity), but they also had the most ransomware detections. Ransomware detections rose 32% in Germany in Q3 and generated 27% of global activity.

Emerging threat actors scaled: The China-linked threat actor, Mustang Panda, had the most detected threat indicators in Q3, followed by Russian-linked APT29 and Pakistan-linked APT36.

Ransomware evolved: Phobos, a ransomware sold as a complete kit in the cybercriminal underground, has avoided

public reports until now. It accounted for 10% of global detected activity and was the second most used ransomware detected in the US. LockBit continued to be the most detected ransomware globally, generating 22% of detections.

Old vulnerabilities continued to prevail: Years-old vulnerabilities continue to be successful exploitation vectors. Trellix observed Microsoft Equation Editor vulnerabilities comprised by CVE-2017-11882, CVE-2018-0798, and CVE-2018-0802 to be the most exploited among malicious emails received by customers during Q3.

Malicious use of Cobalt Strike: Trellix saw Cobalt Strike used in 33% of observed global ransomware activity and in 18% of APT detections in Q3. Cobalt Strike, a legitimate third-party tool created to emulate attack scenarios to improve security operations, is a favorite tool of attackers who repurpose its capabilities for malicious intent.

"So far in 2022, we have seen unremitting activity out of Russia and other state-sponsored groups," said John Fokker, head of threat intelligence, Trellix."This activity is compounded by a rise in politically motivated hacktivism and sustained ransomware attacks on healthcare and education. The need for increased inspection of cyber threat actors and their methods has never been greater."