Companies still hobbled from fearsome cyberattack

July 1 2017, by Frank Bajak And Raphael Satter

Trucks loaded with containers are lined up outside a terminal at the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)

Many businesses still struggled Friday to recover hopelessly scrambled computer networks, collateral damage from a massive cyberattack that targeted Ukraine three days ago.

The Heritage Valley Health System couldn't offer lab and diagnostic imaging services at 14 community and neighborhood offices in western Pennsylvania. DLA Piper, a London-based law firm with offices in 40 countries, said on its website that email systems were down; a receptionist said email hadn't been restored by the close of business day.

Dave Kennedy, a former Marine cyberwarrior who is now CEO of the security company TrustedSec, said one U.S. company he is helping is rebuilding its entire network of more than 5,000 computers.

"It hit everything, their backups, servers, their workstations, everything," he said. "Everything was just nuked and wiped."

Kennedy added, "Some of these companies are actually using pieces of paper to write down credit card numbers. It's crazy."

The cyberattack that began Tuesday brought even some Fortune 1000 companies to their knees, experts say. Kennedy said a lot more "isn't being reported by companies who don't want to say that they are hit."

The malware, which security experts are calling NotPetya, was unleashed through Ukraine tax software, called MeDoc. Customers' networks became infected downloading automatic updates from its maker's website. Many customers are multinationals with offices in the eastern European nation.

Containers are piled up at a terminal at the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)

The malware spread so quickly, worming its way automatically through interconnected private networks, as to be nearly unstoppable. What saved the world from digital mayhem, experts say, was its limited business-to-business connectivity with Ukrainian enterprises, the intended target.

Had those direct connections been extensive—on the level of a major industrial nation—"you are talking about a catastrophic failure of all of our systems and environments across the globe. I mean it could have been absolutely terrifying," Kennedy said.

Microsoft said NotPetya hit companies in at least 64 nations, including Russia, Germany and the United States. Victims include drug giant Merck & Co. and the shipping company FedEx's TNT subsidiary. Trade in FedEx stock was temporarily halted Wednesday.

One major victim, Danish shipping giant A.P. Maersk-Moller, said Friday that its cargo terminals and port operations were "now running close to normal again." It said operations had been restored in Spain, Morocco, India, Brazil, Argentina and Lima, Peru, but problems lingered in Rotterdam, the Netherlands; Elizabeth, New Jersey; and Los Angeles.

An employee at an international transit company at Lima's port of Callao told The Associated Press that Maersk employees' telephone system and email had been knocked out by the virus—so they were "stuck using their personal cellphones." The employee spoke on condition of anonymity because he's not authorized to speak to reporters.

Back in Ukraine, the pain continued. Officials assured the public that the outbreak was under control, and service has been restored to cash machines and at the airport.

But some bank branches remain closed as information-technology professionals scrambled to rebuild networks from scratch. One government employee told the AP she was still relying on her iPhone because her office's computers were "collapsed." She, too, was not authorized to talk to journalists.

Trucks loaded with containers are lined up outside a terminal at the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)

Security researchers now concur that while NotPetya was wrapped in the guise of extortionate "ransomware"—which encrypts files and demands payment—it was really designed to exact maximum destruction and disruption, with Ukraine the clear target.

Computers were disabled there at banks, government agencies, energy companies, supermarkets, railways and telecommunications providers.

Ukraine's government said Thursday that the FBI and Britain's National Crime Agency were assisting in its investigation of the malware.

Suspicion for the attack immediately fell on hackers affiliated with Russia, though there is no evidence tying Vladimir Putin's government to the attack.

Relations between Russia and Ukraine have been tense since Moscow annexed the Crimean peninsula from Ukraine in 2014. Pro-Russian fighters still battle the government in eastern Ukraine.

U.S. intelligence agencies declined to comment about who might be responsible for the attack. The White House did not immediately respond to questions seeking its reaction to the attack.

Experts have blamed pro-Russian hackers for major cyberattacks on the Ukrainian power grid in 2015 and 2016, assaults that have turned the eastern European nation into the world's leading cyberwarfare testing ground.

The main entrance of the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)

A disruptive attack on the nation's voting system ahead of 2014 national elections is also attributed to Russia.

Robert M. Lee, CEO of Dragos Inc. and an expert on cyberattacks on infrastructure including Ukraine's power grid, said the rules of cyberespionage appear to be changing, with sophisticated actors—state-sponsored or not—violating what had been established norms of avoiding collateral damage.

Besides NotPetya, he pointed to the May ransomware dubbed "WannaCry," a major cyberassault that some experts have blamed on North Korea.

"I think it's absolutely reprehensive if we do not have national-level leaders come out and make very clear statements," he said, "that this is not activity that can be condoned."