Global cyberattack seems intent on havoc, not extortion (Update)

June 29 2017, by Raphael Satter, Jan M. Olsen And Frank Bajak

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)

A cyberattack that caused indiscriminate economic damage around the world was apparently designed to create maximum havoc in Russia's neighbor and adversary Ukraine, security researchers said.

While the rogue software used in the attack was configured as extortionate "ransomware," that may have just been a ruse.

"It is clear that this was targeted indiscriminately at Ukrainian businesses, and the Ukrainian government," Jake Williams, president of the security firm Rendition Infosec and a former member of the U.S. National Security Agency's elite cyberwarfare group, told The Associated Press in an online chat. "The 'ransomware' component is just a smokescreen (and a bad one)."

UKRAINE IN PAIN

Although the attack was global in its reach, Ukraine bore the brunt. Computers were disabled at banks, government agencies, energy companies, supermarkets, railways and telecommunications providers. Many of these organizations said they had recovered by Thursday, although some experts suspected that work was incomplete.

"There is still a lot of damage, especially in banks," said Victor Zhora, CEO of the Kiev cybersecurity firm InfoSafe. "ATMs are working (again) but some bank operations are still limited." He estimated damage in "the millions of dollars, perhaps tens of millions."

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)

And that's just in Ukraine. Microsoft said the malware hit at least 64 nations, including Russia, Germany and the United States. "I expect that we will see additional fallout from this is the coming days," said Williams.

In Ukraine, suspicion immediately fell on hackers affiliated with Vladimir Putin's regime, although there is no direct, public evidence tying Russia to the attack. Relations between the two nations have been tense since Moscow annexed the Crimean peninsula from Ukraine in 2014. Pro-Russian fighters are still battling the government in eastern

Ukraine.

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

THE MOSCOW CONNECTION

The malicious program, which researchers are calling NotPetya, initially appeared to be ransomware. Such malware locks up victims' files by encrypting them, then holds them hostage while demanding payment—usually in bitcoin, the hard-to-trace digital currency.

But researchers said the culprits would have been hard-pressed to make money off the scheme. They appear to have relied on a single email address that was blocked almost immediately and a single bitcoin account that collected the relatively puny sum of $10,000.

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)

Firms including Russia's anti-virus Kaspersky Lab, said clues in the code indicate that the program's authors would have been incapable of decrypting the data, further evidence that the ransom demands were a smoke screen.

The timing was intriguing, too. The attack came the same day as the assassination of a senior Ukrainian military intelligence officer and a day before a national holiday celebrating the new Ukrainian constitution signed after the breakup of the Soviet Union.

"Everything being said so far does point to Russia being a leading candidate for a suspect in this attack," said Robert M. Lee, CEO of Dragos Inc. an expert who has studied the attacks on Ukraine's power grid.

What's most worrisome and reprehensible, said Lee, is that whoever was behind the attack was unconcerned about the indiscriminate, collateral damage it caused—much of it within Russia itself. That's highly atypical behavior for nation-states.

ACCOUNTING FOR MALWARE

Williams and other researchers said all evidence indicates that NotPetya was introduced via Ukrainian financial software provider MeDoc. It is one of just two companies in the eastern European nation that supplies required tax software, Zhora said.

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)

Security experts believe MeDoc was the unwitting victim of something akin to a "watering-hole attack," where a malicious program surreptitiously planted at a popular destination infects parties that visit. The method was previously uses to infect industrial control systems operators through software updates in a cyberespionage campaign dubbed "'Dragonfly' that was widely attributed to Russia ," said Williams.

MeDoc's user base is heavily financial—and includes multinational corporations with offices in Ukraine.

NotPetya was cleverly engineered to spread laterally within Windows networks and across the globe via private network connections. Globally, dozens of major corporations and government agencies have been disrupted, including FedEx subsidiary TNT.

Danish shipping giant A.P. Moller-Maersk, one of the global companies hit hardest, said Thursday that most of its terminals were running again, though some are operating in a limited way or more slowly than usual.

Problems have been reported across the shippers' global business, from Mobile, Alabama, to Mumbai in India. At Mumbai's Jawaharlal Nehru Port, several hundred containers could be seen piled up at just two of more than a dozen yards.

"The vessels are coming, the ships are coming, but they are not able to take the container because all the systems are down," trading and clearing agent Rajeshree Verma said. "We are actually in a fix because of all this."