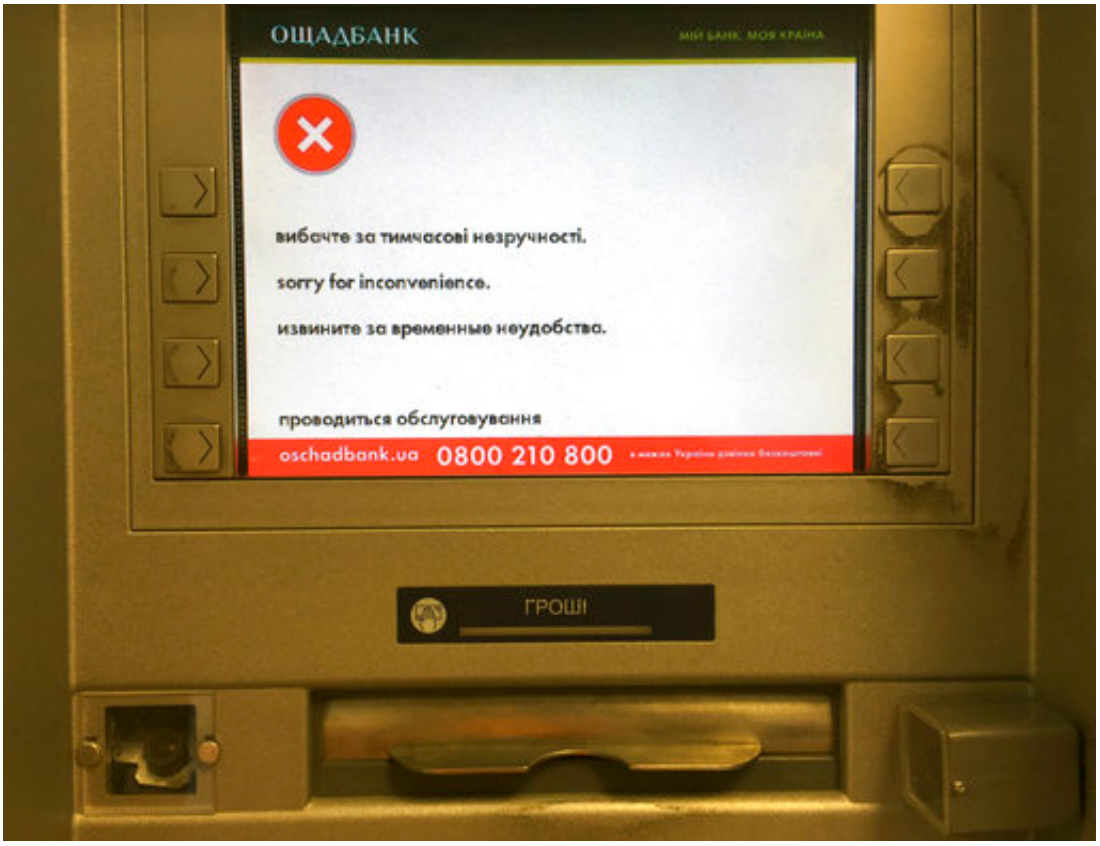
# Companies, governments assess damage from latest malware (Update)

June 28 2017, by Raphael Satter And Frank Bajak




A screen of an idle virus affected cash machine in a state-run OshchadBank says "Sorry for inconvenience/Under repair" in Kiev, Ukraine, Wednesday, June 28, 2017. The cyberattack ransomware that has paralyzed computers across the world hit Ukraine hardest Tuesday, with victims including top-level government offices, energy companies, banks, cash machines, gas stations, and supermarkets. (AP Photo/Efrem Lukatsky)

Companies and governments around the world on Wednesday counted the cost of a software epidemic that has disrupted ports, hospitals and banks.

Logistics firm FedEx says deliveries by its TNT Express subsidiary have been "slowed" by the cyberattack, which had "significantly affected" its systems.

Ports operated by the Danish shipping giant A.P. Moller-Maersk are still crippled. An Alabama port official, James K. Lyons, said crews at Maersk's APM terminal in Mobile, Alabama, have been loading and unloading containers in manual mode, without the normal computerized coordination. The company's operations were shuttered in Mumbai, India, Port Elizabeth, New Jersey, and Los Angeles, among others.

In a statement, Moller-Maersk acknowledged that its APM Terminals had been "impacted in a number of ports" and that an undisclosed number of systems were shut down "to contain the issue." The company declined to provide further detail or make an official available for an interview.

Ukraine, which was hardest hit and where the attack likely originated, said it had secured critical state assets—though everyday life remained affected, with cash machines out of order and airport displays operating manually.


Airport employees work use a laptop computer at Boryspil airport in Kiev, Ukraine, Tuesday, June 27, 2017. A new and highly virulent outbreak of malicious data-scrambling software appears to be causing mass disruption across Europe, hitting Ukraine especially hard, with company and government officials reporting serious intrusions at the Ukrainian power grid, banks and government offices. (AP Photo/Sergei Chuzavkov)

As the impact of the cyberattack that erupted Tuesday was still being measured at offices, loading docks and boardrooms, the Ukrainian Cabinet said that "all strategic assets, including those involved in protecting state security, are working normally."

But that still left a large number of non-strategic assets—including dozens of banks and other institutions—fighting to get back online. Cash machines in Kiev seen by an Associated Press photographer were still out of order Wednesday, and Ukrainian news reports said that flight information at the city's Boryspil airport was being provided in manual

mode.

A local cybersecurity expert discounted the Ukrainian government's assurances.

"Obviously they don't control the situation," Victor Zhora of Infosafe in Kiev told the AP.

At the very least, cybersecurity firms say thousands of computers worldwide have been struck by the malware, which goes by a variety of names, including ExPetr.


People queue for their turn to pay at a slowly working cash desk in a building supermarket in Kiev, Ukraine, Wednesday, June 28, 2017. The cyberattack ransomware that has paralyzed computers across the world hit Ukraine hardest Tuesday, with victims including top-level government offices, energy companies,

banks, cash machines, gas stations, and supermarkets. (AP Photo/Efrem Lukatsky)

In Pennsylvania, lab and diagnostic services were closed at the satellite offices of the Heritage Valley Health System. In Tasmania, an Australian official said a Cadbury chocolate factory had stopped production after computers there crashed. Other organizations affected include U.S. drugmaker Merck, food and drinks company Mondelez International, global law firm DLA Piper, and London-based advertising group WPP.

But most of the damage remains hidden away in corporate offices and industrial parks.

As IT security workers turned their eye toward cleaning up the mess, others wondered at the attackers' motives. The attack has the telltale signs of ransomware, which scrambles a computer's data until a payment is made, but some experts believe this attack was less aimed at gathering money than at sending a message to Ukraine and its allies.

That hunch was buttressed by the way the malware appears to have been seeded using a rogue update to a piece of Ukrainian accounting software—suggesting an attacker focused on Ukrainian targets.

And it comes on the anniversary of the assassination of a senior Ukrainian military intelligence officer and a day before a national holiday celebrating a new constitution signed after the breakup of the Soviet Union.


A woman passes by cash machines that do not work in a city supermarket in Kiev, Ukraine, Wednesday, June 28, 2017. The cyberattack ransomware that has paralyzed computers across the world hit Ukraine hardest Tuesday, with victims including top-level government offices, energy companies, banks, cash machines, gas stations, and supermarkets. (AP Photo/Efrem Lukatsky)

"The threat we're talking about looks like it was specially developed for Ukraine because that was the place it created most of the damage," said Bogdan Botezatu, of Romanian security firm Bitdefender, calling it a case of "national sabotage."

Suspicions were further heightened by the re-emergence of the mysterious Shadow Brokers group of hackers, whose dramatic leak of powerful NSA tools helped power Tuesday's outbreak, as it did a previous ransomware explosion last month that was dubbed WannaCry.

In a post published Wednesday, The Shadow Brokers made new threats,

announced a new money-making scheme and made a boastful reference to the recent chaos.

The malware didn't appear to make a lot of money for its creators. A bitcoin wallet used to collect ransoms showed only about $10,000. And some analysts going through the malware's code said that the ransomware may not even operate as ransomware at all; victims' data appear to be hopelessly scrambled, rather than recoverable after the payment of ransom.

Matthieu Suiche, the founder of Dubai-based Comae Technologies, said the ransom demand was merely "a mega-diversion." In a blog post, he wrote that the code pointed not to criminals, but "in fact a nation state attack."

Researchers at Kaspersky Lab echoed the findings, saying in a statement, "Our analysis indicates there is little hope for victims to recover their data."