New highly virulent strain of ransomware cripples networks (Update 3)

June 27 2017, by Raphael Satter And Frank Bajak

In this in this Jan. 1, 2008 file photo a flag files over the headquarters of shipping company A.P. Moller-Maersk in Copenhagen, Denmark. Hackers Tuesday June 27, 2017 caused widespread disruption across Europe, hitting Ukraine especially hard. Russia's Rosneft energy company also reported falling victim to hacking, as did shipping company A.P. Moller-Maersk, which said every branch of its business was affected. (Jens Dresling/AP via Ritzau, File)

A new, highly virulent strain of malicious software that is crippling

computers globally appears to have been sown in Ukraine, where it badly hobbled much of the government and private sector on the eve of a holiday celebrating a post-Soviet constitution.

The fresh cyber-assault Tuesday leveraged the same intrusion tool as a similar attack in May and proved again just how disruptive to daily life sophisticated cyber-assaults can be in this age of heavy reliance on computers.

Hospitals, government offices and major multinationals were among the casualties of the ransomware payload, which locks up computer files with all-but-unbreakable encryption and then demands a ransom for its release.

Ukraine and Russia appeared hardest hit. In the United States, it affected companies such as the drugmaker Merck and Mondelez International, the conglomerate of food brands such as Oreo and Nabisco. Multinationals, including the global law firm DLA Piper and Danish shipping giant A.P. Moller-Maersk, were also affected.

The virus' pace appeared to slow by Wednesday, in part because the malware appeared to require direct contact between computer networks, a factor that may have limited its spread in regions with fewer connections to Ukraine.

Its origins and the motive for its release remained unclear, and financial gain may not have been a big reason. The time and place of release could have been a clue.

It was loosed on the eve of a national holiday marking Ukraine's 1996 constitution—its first after independence from Soviet rule.

In this Jan. 31, 2014, file photo of A.P. Moller-Maersk containers on a ship in the Panama Canal. Hackers Tuesday June 27, 2017 caused widespread disruption across Europe, hitting Ukraine especially hard. Russia's Rosneft energy company also reported falling victim to hacking, as did shipping company A.P. Moller-Maersk, which said every branch of its business was affected. (Thomas Borberg/Polfoto via AP,file)

Ukraine has been a persistent target of pro-Russia hackers in recent years. They have been blamed for twice shutting down large swaths of its power grid and sabotaging its elections network in a bid to disrupt a May 2014 national vote.

Researchers picking the program apart found evidence its creators had borrowed from leaked National Security Agency code, raising the possibility that the digital havoc had spread using U.S. taxpayer-funded tools.

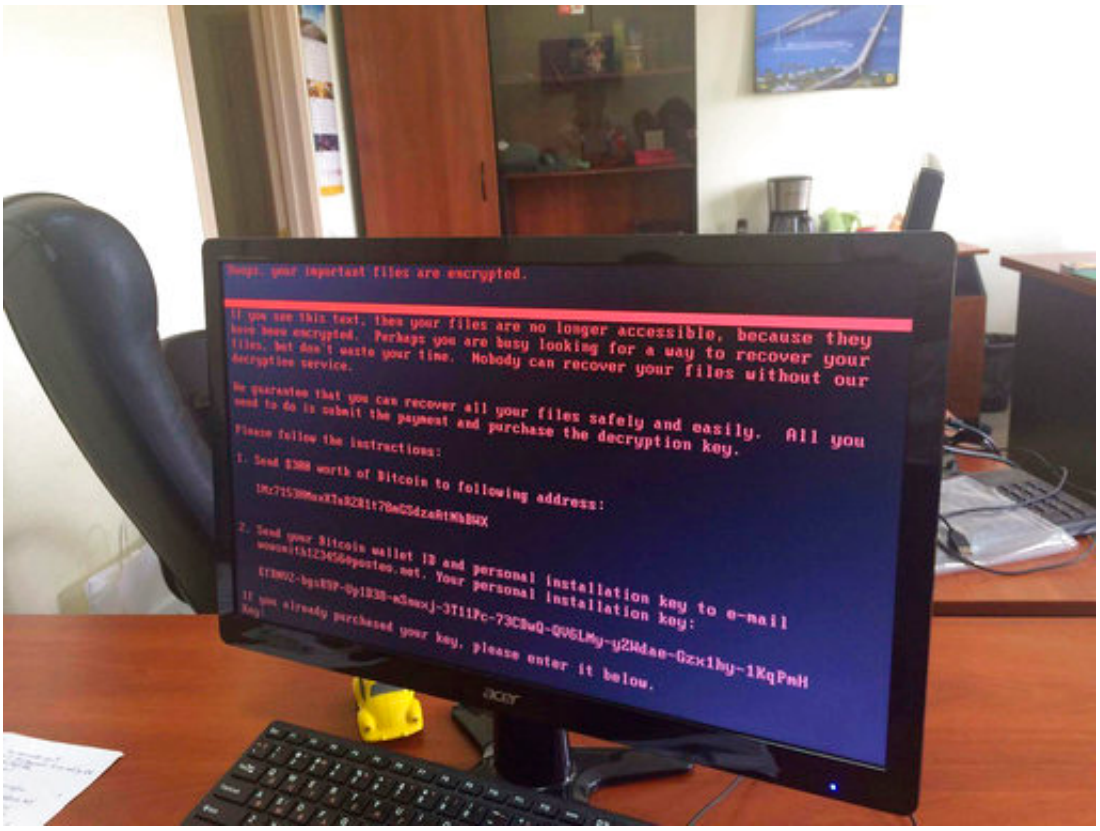
"The virus is spreading all over Europe, and I'm afraid it can harm the whole world," said Victor Zhora, the chief executive of Infosafe IT in Kiev, where the first reports of it emerged early Tuesday afternoon.

Stricken in Ukraine were government offices, where officials posted photos of darkened computer screens, as well as energy companies, the country's biggest airport, the post office, banks, cash machines, gas stations and supermarkets. Ukrainian Railways and the communications company Ukrtelecom were among major enterprises hit, Infrastructure Minister Volodymyr Omelyan said in a Facebook post . Omelyan also wrote: "It's no coincidence that the word 'virus' ends in RUS."

The virus hit the radiation monitoring at Ukraine's shuttered Chernobyl power plant, site of the world's worst nuclear accident, forcing it into manual operation.

The full scope of damage wouldn't be known until Thursday when everyone gets back to work, Zhora said.

Ukraine suffered more than 60 percent of the attacks, followed by Russia with more than 30 percent, according to initial findings by researchers at the cybersecurity firm Kaspersky Lab. It listed Poland, Italy and Germany, in that order, as the next-worst affected.



A computer screen cyberattack warning notice reportedly holding computer files to ransom, as part of a massive international cyberattack, at an office 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. Image used with permission of the account holder facebook.com/olejmaa checked and consistent with independent AP reporting. (Oleg Reshetnyak via AP)

In the U.S, two hospitals in western Pennsylvania were hit; patients reported on social media that some surgeries had to be rescheduled. A spokeswoman for Heritage Valley Health System would say only that operational changes had to be made. A Wellsville, Ohio, woman at one of its hospitals to have her gallbladder removed said she noticed computer monitors off and nurses scurrying around with stacks of paperwork.

Like last month's outbreak of ransomware, dubbed WannaCry , the new attack spread by using digital lock picks originally created by the NSA and later published to the web by a still-mysterious group known as the Shadowbrokers.

Security vendors said the NSA exploit, known as EternalBlue, lets malware spread rapidly across internal networks at companies and other large organizations. Microsoft issued a security fix in March, but Chris Wysopal, chief technology officer at the security firm Veracode, said it would only be effective if every single computer on a network were patched—otherwise, a single infected machine could infect all others.

"Once activated, the virus can automatically and freely distribute itself on your network," Ukraine's cyberpolice tweeted.

Such self-spreading programs are known as "worms."

The attacks appeared to slow down in part because the ransomware appears to spread only when a direct contact exists between two networks—such as when a global company's Ukraine office interacts with headquarters, said Ryan Kalember, a security expert at Proofpoint.

"It's not randomly spreading over the internet like WannaCry. It's somewhat contained to the organizations that were connected to each other," he said.

Bogdan Botezatu, an analyst with Bitdefender, compared the new program to a contagious disease. It appeared nearly identical to GoldenEye, a variant of a known family of hostage-taking programs known as "Petya," he said.

It demanded $300 in Bitcoin. But unlike typical ransomware, which merely scrambles personal data files, this program does more. It

overwrites a computer's master boot record, making it tougher to restore even a machine that has been backed up, Kalember said.

It may have first spread through a rogue update to a piece of Ukrainian accounting software called MEDoc, according to tweets by the country's cyberpolice unit. It said a rogue update seeded the infection across Ukraine. On Facebook, MEDoc acknowledged having been hacked.

Emails sent Tuesday to an address posted to the bottom of ransom demands went unreturned. That might be because the email provider hosting that address, Berlin-based Posteo, pulled the plug on the account before the infection became widely known.

In an email, a Posteo representative said it had blocked the email address immediately after learning that it was associated with ransomware. The company added that it was in contact with German authorities "to make sure that we react properly."