The Washington Post

National Security

Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes

By Ellen Nakashima January 12

The CIA has attributed to Russian military hackers a cyberattack that crippled computers in Ukraine last year, an effort to disrupt that country’s financial system amid its ongoing war with separatists loyal to the Kremlin.

The June 2017 attack, delivered through a mock ransomware virus dubbed NotPetya, wiped data from the computers of banks, energy firms, senior government officials and an airport.

The GRU military spy agency created NotPetya, the CIA concluded with “high confidence” in November, according to classified reports cited by U.S. intelligence officials.

The CIA declined to comment.

Ukraine has been a significant target of GRU cyberattacks coinciding with Russia’s annexation of Crimea and aggression elsewhere. The NotPetya assault was launched on Ukraine’s Constitution Day, a public holiday.

The virus also affected computer systems in Denmark, India and the United States, but more than half of those victimized were in Ukraine.

The attacks reflect Russia’s mounting aggression in cyberspace as part of a larger “hybrid warfare” doctrine that marries traditional military means with cyber-tools to achieve its goal of regional dominance. “It’s a pattern of more bold, aggressive action,” said Robert Hannigan, former head of Britain’s GCHQ intelligence agency.

The hackers used what is known as a “watering hole” attack. They infected a website to which they knew their targets would navigate — in this case, a Ukrainian site that delivered updates for tax and accounting software programs.

It’s a tactic that Russian government hackers also have used to compromise industrial control system networks. The goal here was “the disruption of Ukraine’s financial system,” said Jake Williams, founder of the cybersecurity firm Rendition Infosec.

In a twist, the attackers used malware that appeared to be ransomware — a technique that encrypts victims’ data and decrypts it only if a ransom is paid, to make it appear as though criminal hackers or some group other than a nation state were the culprits.

They deployed NotPetya a month after a different worm, WannaCry, infected computers with ransomware in 150 countries. The U.S. National Security Agency linked that virus to the North Korean government, The Washington Post reported last year.

“For many days, people were classifying NotPetya as an actual ransomware,” said Matt Suiche, founder of Comae Technologies, a cybersecurity firm. “It took a few days for people to understand what it was doing” — that it was permanently wiping data, he said.

The hackers worked for the military spy service’s GTsST, or Main Center for Special Technology, the CIA reported. That unit is highly involved in the GRU’s cyberattack program, including the enabling of influence operations.

15 Comments

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. Follow @nakashimae