**Proprietary Software, Microsoft, and Security Blunders**

By Roy Schestowitz  
Created 15/05/2021 - 7:51pm  
Submitted by Roy Schestowitz on Saturday 15th of May 2021 07:51:29 PM  

- Ireland refuses to pay ransom demand in attack on its national health service [3]

  Micheál Martin, the country's Taoiseach (prime minister), says Ireland will not be paying any ransom.

- Cyber attack 'most significant on Irish state' [4]

  The health service has temporarily shut down its IT system to protect it after the attack.

- 'We will not be paying any ransom' over cyber attack - Taoiseach [5]

  The NCSC said it is also working with the HSE to identify the technical details of the malware used in the incident and will issue an advisory later to share these details.

- Lawmakers roll out legislation to defend pipelines against cyber threats [6] [iophk: Windows TCO]

  The Pipeline Security Act would codify the responsibility of both the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency's (CISA)
responsibility for securing pipelines against threats. The effort is being led by Rep. Emanuel Cleaver (D-Mo.).

It would also require TSA to update pipeline security guidelines and conduct risk assessments, create a personnel strategy for staffing its Pipeline Security Section and improve congressional oversight of TSA's pipeline efforts.

- **Universities need a better menu of defences against cyber-vultures** [7] [iophk: Windows TCO]

- **CIA-backed firm claims DarkSide ransomware site has shut down** [8]

  A CIA-backed threat intelligence firm claims the operator of the DarkSide ransomware gang has lost control of its infrastructure after the malware was used to attack the Colonial Pipeline Company in the US which runs the country's biggest petrol pipeline.

- **Darkside ransomware gang says it lost control of its servers & money a day after Biden threat** [9]

  A day after US President Joe Biden said the US plans to disrupt the hackers behind the Colonial Pipeline cyberattack, the operator of the Darkside ransomware said the group lost control of its web servers and some of the funds it made from ransom payments.

  ?A few hours ago, we lost access to the public part of our infrastructure, namely: Blog, Payment server. CDN servers.? said Darksupp, the operator of the Darkside ransomware, in a post spotted by Recorded Future threat intelligence analyst Dmitry Smilyanets.

  ?Now these servers are unavailable via SSH, and the hosting panels are blocked.? said the Darkside operator while also complaining that the web hosting provider refused to cooperate.

- **FBI Competent to take on Darkside?** [10]

  How many times have we seen the FBI and other US intelligence capabilities portrayed as deftly taking on our enemies. Now finally here is a really hard test for them to succeed in. Can they do it? We pay you for this, lets see it happen. Just publishing a warning is not enough. Soon.

- **Pipeline [Crack] Points to Growing Cybersecurity Risk for Energy System** [11]
The audacious ransomware attack that shut down a major fuel pipeline and sent Americans scrambling for gasoline in the Southeast this week was not the first time [crackers] have disrupted America’s aging, vulnerable energy infrastructure. And it’s unlikely to be the last.

Across the globe, cyberattackers are increasingly taking aim at the energy systems that underpin modern society. A February report from IBM found that the energy industry was the third most targeted sector for such attacks in 2020, behind only finance and manufacturing. That was up from ninth place in 2019.

- Held to Ransom: Colonial Pipeline and the Vulnerabilities of Critical Infrastructure [12]

The consequences are telling. The operator, taken offline to enable an investigation to be conducted by US cybersecurity firm Mandiant; fuel left stranded at refineries in Texas; a spike in fuel prices at the pump – up six cents per gallon on the week to $2.967 per gallon of unleaded gasoline. ?Unless they sort it out by Tuesday,? warned oil market analyst Gaurav Sharma, ?they’re in big trouble.? The impact would be felt first in Atlanta, then Tennessee, perpetuating a domino effect to New York. ?This is the largest impact on the energy system in the United States we’ve seen from a cyberattack, full stop,? opined Rob Lee of the cybersecurity firm Dragos.

The company, in unconvincing tones, issued a statement that it was continuing to work with third-party cybersecurity experts, law enforcement, and other federal agencies to restore pipeline operations quickly and safely. President Joe Biden rushed to calm fears that this had compromised fuel security. ?The agencies across the government have acted quickly to mitigate any impact on our fuel supply. The deputy national security advisor for cyber and emerging technologies Anne Neuberger waffled to the press that the Biden administration was taking a multi-pronged and whole-of-government response to this incident and to ransomware overall.?

- Chinese Government's Hacker Competition Is Being Used To Find Exploits To Wield Against Uighur Citizens [13]

Anything the Chinese government can weaponize against its Uighur Muslim population, it will. And has. Further details about an iPhone exploit discovered by Chinese hackers show the Chinese government got into the bug bounty program solely to find vulnerabilities to wield against the government’s least-liked residents.

Source URL: http://www.tuxmachines.org/node/151218

Links: