Security: Updates, RDS, FBI, Microsoft, Google and Ransom

By *Roy Schestowitz*
Created *16/05/2019 - 5:28pm*
Submitted by Roy Schestowitz on Thursday 16th of May 2019 05:28:01 PM Filed under Security [1]

- **Security updates for Thursday** [2]

- **Severe Linux kernel flaw found in RDS** [3]

- **FBI Tells The Governor Of Florida About Election Hacking, But Says He Can't Tell Anyone Else** [4]

  > I thought this was America, but whatever. Secrecy in all things government, despite the (often misheld) presumption that our public servants will be open and honest about issues that affect us.
  >
  > It's no secret voting systems and databases are not secure. These are problems that date back 15 years, but have shown little improvement since. Election interference is just another tool in the nation-state hacking kit, and the US is far from immune from these attacks.
  >
  > Federal agencies investigating election interference are at least speaking to officials in states affected by these efforts. But those officials are apparently not allowed to pass on this information to those affected the most: voters.

- **Microsoft?s First Windows XP Patch in Years Is a Very Bad Sign** [5]

THIS WEEK, MICROSOFT issued patches for 79 flaws across its platforms and products. One of them merits particular attention: a bug so bad that Microsoft released a fix for it on Windows XP, an operating system it officially abandoned five years ago.

- **Google Says Titan Security Keys Could Be Hacked; Offers Free Replacement [6]**

  Today Google has announced a security flaw in its Bluetooth Titan Security Key that is used for 2-factor authentication. The security flaw could allow hackers in close proximity to bypass the security mechanism and connect their own devices.

- **Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers [7]**

  FROM 2015 TO 2018, a strain of ransomware known as SamSam paralyzed computer networks across North America and the U.K. It caused more than $30 million in damage to at least 200 entities, including the cities of Atlanta and Newark, New Jersey, the Port of San Diego and Hollywood Presbyterian Medical Center in Los Angeles. It knocked out Atlanta?s online water service requests and billing systems, prompted the Colorado Department of Transportation to call in the National Guard, and delayed medical appointments and treatments for patients nationwide whose electronic records couldn?t be retrieved. In return for restoring access to the files, the cyberattackers collected at least $6 million in ransom.

  ?You just have 7 days to send us the BitCoin,? read the ransom demand to Newark. ?After 7 days we will remove your private keys and it?s impossible to recover your files.?
  At a press conference last November, then-Deputy Attorney General Rod Rosenstein announced that the U.S. Department of Justice had indicted two Iranian men on fraud charges for allegedly developing the strain and orchestrating the extortion. Many SamSam targets were ?public agencies with missions that involve saving lives,? and the attackers impaired their ability to ?provide health care to sick and injured people,? Rosenstein said. The hackers ?knew that shutting down those computer systems could cause significant harm to innocent victims.?

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/788680/rss
[3] https://nakedsecurity.sophos.com/2019/05/16/severe-linux-kernel-flaw-found-in-rds/
[4] https://www.techdirt.com/articles/20190515/14210642216/fbi-tells-governor-florida-about-election-hacking-says-he-cant-tell-anyone-else.shtml
[5] https://www.wired.com/story/microsoft-windows-xp-patch-very-bad-sign/
[6] https://fossbytes.com/security-flaw-googles-titan-security-keys/

[7] https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/