Published on *Tux Machines* (http://www.tuxmachines.org)

Security: BSDcan, Ransom and Exploits

By *Roy Schestowitz*
Created *19/05/2019 - 9:33am*
Submitted by Roy Schestowitz on Sunday 19th of May 2019 09:33:00 AM Filed under Security [1]

- **ssh in https [2]**

  > The wifi network at BSDcan, really the UOttawa network, blocks a bunch of ports. This makes it difficult to connect to outside machines using ?exotic? protocols, basically anything except http or https. There are many ways to resolve this, here?s what I did.

- **These firms promise high-tech ransomware solutions?but typically just pay hackers [3] [iophk: ?Windows continues to enable entire cottage industries around grifting?]**

  > Proven Data promised to help ransomware victims by unlocking their data with the ?latest technology,? according to company emails and former clients. Instead, it obtained decryption tools from cyberattackers by paying ransoms, according to Storfer and an FBI affidavit obtained by ProPublica.
  >
  > Another US company, Florida-based MonsterCloud, also professes to use its own data recovery methods but instead pays ransoms, sometimes without informing victims such as local law enforcement agencies, ProPublica has found. The firms are alike in other ways. Both charge victims substantial fees on top of the ransom amounts. They also offer other services, such as sealing breaches to protect against future attacks. Both firms have used aliases for their workers, rather than real names, in communicating with victims.

- **Google Starts Tracking Zero-Days Exploited in the Wild [4]**

  > The new project, named 0Day ?In the Wild?, is basically a spreadsheet that Project Zero uses

to track vulnerabilities exploited before they became known to the public or the vendor.

The spreadsheet currently lists over 100 vulnerabilities exploited in the wild since 2014. The table includes the flaw?s CVE identifier, impacted vendor, impacted product, the type of vulnerability, a brief description, the date of its discovery, the date when a patch was released, a link to the official advisory, a link to a resource analyzing the flaw, and information on attribution.

Security

Source URL: http://www.tuxmachines.org/node/124018

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://flak.tedunangst.com/post/ssh-in-https
[3] https://arstechnica.com/information-technology/2019/05/these-firms-promise-high-tech-ransomware-solutions-but-typically-just-pay-hackers/
[4] https://www.securityweek.com/google-starts-tracking-zero-days-exploited-wild