Security Leftovers

By Roy Schestowitz
Created 28/02/2022 - 1:43pm
Submitted by Roy Schestowitz on Monday 28th of February 2022 01:43:00 PM Filed under Security [1]

- **Ransomware Used as Decoy in Destructive Cyberattacks on Ukraine** [2] [iophk: Windows TCO]
  
  The wiper uses different corruption methods based on the version of Windows running on the machine and partition type (FAT or NTFS). HermeticWiper can damage both MBR and GPT drives and triggers a system reboot to complete the data wiping process, researchers with Cisco?s Talos division note.

  Although executed on February 23, hours before Russia launched an invasion of Ukraine, the attacks appear to have been in preparation for months.


  The ransomware gang known as ?Cuba? is increasingly shifting to exploiting Microsoft Exchange vulnerabilities ? including ProxyShell and ProxyLogon ? as initial infection vectors, researchers have found.

  The group has likely been prying open these chinks in victims? armor as early as last August, Mandiant reported on Wednesday.

- **Cybercrime getting more destructive, remote workers in the crosshairs** [4] [iophk: Windows TCO]

  In addition, the expanding attack surface of hybrid workers and hybrid IT is a focal point that cyber adversaries are attempting to exploit. For a detailed view of the report, as well as some important takeaways, read the blog.
Derek Manky, Chief, Security Insights & Global Threat Alliances, Fortinet: 'Cybersecurity is a fast-moving and dynamic industry, but recent threat events show unparalleled speeds at which cyber adversaries are developing and executing attacks today. New and evolving attack techniques span the entire kill chain but especially in the weaponization phase, showing an evolution to a more advanced persistent cybercrime strategy that is more destructive and unpredictable.

- **Ransomware not slowing: Relentless and more destructive** [5] [iophk: Windows TCO]

  Ransomware is not slowing down and continues to be relentless and more destructive, a new report has revealed.

  Fortinet released announced the latest semiannual FortiGuard Labs Global Threat Landscape Report. Threat intelligence from the second half of 2021 reveals an increase in the automation and speed of attacks demonstrating more advanced persistent cybercrime strategies that are more destructive and unpredictable. In addition, the expanding attack surface of hybrid workers and hybrid IT is a focal point that cyber adversaries are attempting to exploit.

- **Chinese Experts Uncover Details of Equation Group's Bvp47 Covert Hacking Tool** [6] [Ed: No, this is not a back door [7]]

  A team of Chinese researchers has revealed details of a "top-tier" backdoor used by the Equation Group, a APT group linked to the NSA.

**Security**

Source URL: [http://www.tuxmachines.org/node/161944](http://www.tuxmachines.org/node/161944)

Links:
1. [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)
2. [https://www.securityweek.com/ransomware-used-decoy-destructive-cyberattacks-ukraine](https://www.securityweek.com/ransomware-used-decoy-destructive-cyberattacks-ukraine)
4. [https://www.helpnetsecurity.com/2022/02/28/cybercrime-more-destructive/](https://www.helpnetsecurity.com/2022/02/28/cybercrime-more-destructive/)
7. [http://techrights.org/2022/02/26/proprietary-software-better-avoided/](http://techrights.org/2022/02/26/proprietary-software-better-avoided/)