More good news: Medical equipment is still prone to cracker attacks [2] [iophk: Windows TCO]

A new report from Unit 42 says 72% of health care networks mix [Internet] of things (IoT) and information technology assets, allowing malware to spread from users’ computers to vulnerable IoT devices on the same network. The report also offers a lot of data on non-medical IoT attacks.

There is a 41% rate of attacks exploiting device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. And Unit 42 has seen a shift from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data, and monetary profit via ransomware.

Conficker a Twelve Years Old Malware Attack Connected Objects [3] [iophk: Windows TCO]

Twelve years after its creation Conficker malware is now attacking connected objects. The American firm Palo Alto Networks announces that it has detected Conficker on the connected devices of a hospital, activating a resurgence of the twelve-year-old computer worm. It calls on all owners of connected objects to adopt the security measures recommended by specialists.

According to a report released Tuesday, March 10, 2020, by IT expert Palo Alto Networks, a twelve years old computer worm called Conficker has recently made a comeback. The latter, which emerged in 2008 by taking advantage of security vulnerabilities in Microsoft’s Windows XP operating system, has generated a whole network of zombie machines.

In 2009, Conficker reportedly infected up to 15 million machines. Still active, although it is considered a minor phenomenon and without real risk, it still infected some 400,000
computers in 2015. The proliferation of connected objects would have increased this number to 500,000 devices today.

- [Older] Maastricht Univ. paid €250K to ransomware [attackers]: report

  Maastricht University paid between 200 thousand and 300 thousand euros to [attackers] who had blocked access to the university's digital systems with ransomware, various people involved told the Volkskrant. The university board was forced to pay because the university's backups were also hijacked. The backups - stored on the university servers - contain research data and data from students and staff from the past decades.

- [Older] University of Maastricht says it paid [attackers] 200,000-euro ransom

  The University of Maastricht on Wednesday disclosed that it had paid [attackers] a ransom of 30 bitcoin - at the time worth 200,000 euros ($220,000) - to unblock its computer systems, including email and computers, after an attack that unfolded on Dec. 24.

- [Older] Maastricht University Pays 30 Bitcoins as Ransom to TA505 Group

  A management summary of the Fox-IT report and Maastricht University's response found that during the time frame of October 15 to 23 December 2019 (inclusive of both dates), the TA505 gained control over multiple servers. Following is the timeline of the events in the leadup to the final ransomware attack: [...]

- [Older] FBI warns Zoom, teleconference meetings vulnerable to hijacking

  "The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the FBI cautioned. "As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts."

  It's not just private businesses and children whose meetings could be Zoombombed. Privacy and security issues in conferencing software may also pose risks to national security, as world leaders convene Zoom meetings. In some cases, world leaders such as U.K. Prime Minister Boris Johnson have shared screenshots of their teleconferencing publicly only to reveal Zoom meeting IDs, raising concerns that sensitive information could be compromised.
Every once in a while, I'll see spambot-style traffic from the Windows hosts I infect in my lab environment. On Tuesday 2020-03-31, this happened during a Qakbot infection. I've covered examining Qakbot traffic before, but that didn't include examples of spambot emails sent from an infected Windows computer. Today's diary provides a quick review of some email examples from spambot traffic by my Qakbot-infected lab host.

During the analysis, we reversed this strain of Qbot and identified the attacker's active command and control server, allowing us to determine the scale of the attack. Based on direct observation of the C2 server, thousands of victims around the globe are compromised and under active control by the attackers. Additional information uncovered from the C&C server exposed traces of the threat actors behind this campaign.

Qbot (or Qakbot) was first identified in 2009 and has evolved significantly. It is primarily designed for collecting browsing activity and data related to financial websites. Its worm-like capabilities allow it to spread across an organization's network and infect other systems.

/us/bin/ssh in macos 10.15.4 hangs if used with the -p flag to specify an alternate port and used with a hostname. This was not present in macos 10.15.3

Source URL: http://www.tuxmachines.org/node/135900

Links:
[3] https://neoslab.com/2020/03/16/conficker-a-twelve-years-old-malware-attack-connected-objects-RHp6T29XWmxraFowdjBpN2NWZGx2UUt09