THE OUTDATED XP TESTIMONY ON WANNACRY TO CONGRESS

The Oversight Committee had a hearing on WannaCry last week. I won't have time to watch the hearing for a few days, but I did read the testimony with some alarm. That's because two of the four witnesses appear to have misstated one detail about the attack.

First, Symantec CTO Hugh Thompson suggested that the spread of the ransomware was due to Microsoft not releasing a patch for XP when it had released EternalBlue patches for other systems in March.

> WannaCry spread to unpatched computers. Microsoft released a patch for the SMB vulnerability for Windows 7 and newer operating systems in March, but unpatched systems and systems running XP or older operating systems were unprotected. After the WannaCry outbreak began, Microsoft released a patch for XP and earlier platforms. Four days after the initial outbreak these patches were widely applied and new infections slowed to a trickle.

The implication here is that the ransomware primarily affected XP, and only because there hadn't been a patch available.

Retired General Touhill suggested this outdated system was actually Windows 95 — and claimed that Microsoft had released that patch in March, along with the supported system patches.

> Systems using unpatched versions of the Windows 95 operating system have been highlighted as exemplar victims of the Wannacry attack. Microsoft who, after a

> long and very public notification process, discontinued support to the Windows 95 operating system in 2014, about 19 years after its initial release. However, in light of the warnings and their own research, in March of this year Microsoft issued a rare emergency patch to Windows 95, nearly three years after they had discontinued support of the software. Despite these extraordinary actions, many organizations still did not heed the warnings and properly patch and configure their systems. As a result, they fell victim to Wannacry.

In fact, XP (to say nothing of Windows 95) was not the problem. Windows 7 was. Kaspersky Lab (which Congress has spent time of late demonizing as potential Russian spies) first pointed this out on May 19.

> Chief among the revelations: more than 97 percent of infections hit computers running Windows 7, according to attacks seen by antivirus provider Kaspersky Lab. By contrast, infected Windows XP machines were practically non-existent, and those XP PCs that were compromised were likely manually infected by their owners for testing purposes. That's according to Costin Raiu, director of Kaspersky Lab's Global Research and Analysis Team, who spoke to Ars.
>
> While the estimates are based only on computers that run Kaspersky software, as opposed to all computers on the Internet, there's little question Windows 7 was overwhelmingly affected by WCry, which is also known as "WannaCry" and "WannaCrypt." Security ratings firm BitSight found that 67 percent of infections hit Windows 7, Reuters reported.
>
> The figures challenge the widely

> repeated perception that the outbreak was largely the result of end users who continued to deploy Windows XP, a Windows version Microsoft decommissioned three years ago. In fact, researchers now say, XP was largely untouched by last week’s worm because PCs crashed before WCry could take hold. Instead, it now appears, the leading contributor to the virally spreading infection were Windows 7 machines that hadn’t installed a critical security patch Microsoft issued in March

Days later Sophos confirmed that analysis.

> Though the lack of patching and exposure of port 445 were easily identified problems, the reasons why Windows 7 was an easier target than XP remain somewhat clouded.
>
> During testing, SophosLabs found that XP wasn’t the effective conduit for infection via the EternalBlue SMB exploit that many thought it was, while Windows 7 was easily infected. The research showed that WannaCry ransomware can affect XP computers – but not via the SMB worm mechanism, which was the major propagation vector for WannaCry.
>
> [snip]
>
> Various security companies arrived at a similar conclusion, putting the infection rate among Windows 7 computers at between 65% and 95%. SophosLabs puts that number even higher: our analysis of endpoint data for the three days that followed the outbreak shows that Windows 7 accounted for nearly 98% of infected computers.

It’s still a question of whether a victim patched their computer or not, but Microsoft did make a patch available for Windows 7 along with other supported systems. Though, as Sophos notes, unless users were paying extra for support, they might not have noticed the patch was there.

> Microsoft had addressed the issue in its MS17-010 bulletin in March, but companies using older, no-longer-supported versions of the operating system wouldn’t have seen it unless they were signed up for custom support, ie Microsoft’s special extended – and paid-for – support.

That suggests one problem with the patching wasn’t the timeliness, but the secrecy. But, Congress might not learn that detail given the testimony they got last week.

Three days after the attack started, Homeland Security Czar Tom Bossert was still claiming WannaCry was spread via phishing. Now Congress is getting other debunked reporting.

We might respond better to these threats if the government was getting information that was at least as accurate as that information available to lowly hippie bloggers.