THE ETERNALBLUE SOURCE MIGHT HAVE BEEN ABLE TO "FISH DOD WITH DYNAMITE;" WHY DIDN'T IT?

Let's look at some dates the WaPo's sources and Shadow Brokers are giving for the EternalBlue exploit that caused havoc around the world starting on Friday.

Yesterday, WaPo had a story on how concerned people within NSA were about the EternalBlue Windows exploit used in the WannaCry ransomware. It was so powerful, one source described, it was like "fishing with dynamite."

> In the case of EternalBlue, the intelligence haul was "unreal," said one former employee.
>
> "It was like fishing with dynamite," said a second.

But that power came with risks. Among others, when the NSA started using the powerful tool more than five years, the military would have been exposed to its use.

> Since the NSA began using EternalBlue, which targets some versions of Microsoft Windows, the U.S. military and many other institutions have updated software that was especially vulnerable.

Though Cyberscoop notes the US military hasn't been entirely protected from WannaCry. An IP address associated with the Army Research Lab in Fort Huachuca was infected (though that could have been a deliberate attempt to respond to the ransomware).

> WannaCry ransomware infected a machine

> tied to an IP address associated with the Army Research Laboratory, CyberScoop has learned. The information, found on a list of affected IP addresses provided by a security vendor, would mark the first time the ransomware was found on a federal government computer.
>
> The security vendor, who provided the data on condition of anonymity to discuss sensitive material, observed communications from the victim IP address to the attackers' known command and control server on May 12; confirming that the ransomware infection involving the ARL was in fact successful.
>
> The IP address is tied to a server block parked at a host located at Fort Huachuca, Arizona. The type of machine the IP address is attached to is unknown.

In the early days of EternalBlue, the WaPo explains, it would often crash the infected computer, resulting in a bluescreen that might alert victims to its presence. That opened the possibility that the victim might discover the exploit and then turn it back on the US.

> "If one of our targets discovered we were using this particular exploit and turned it against the United States, the entire Department of Defense would be vulnerable," the second employee said. "You just have to have a foothold inside the network and you can compromise everything."

The WaPo puts the date before which DOD was vulnerable to its own weapon at 2014.

> What if the Shadow Brokers had dumped the exploits in 2014, before the government had begun to upgrade software on its computers? What if they had released them and Microsoft had no ready

> patch?

In yesterday's post, Shadow Brokers claimed the Windows exploits released last month – which it had first named in January – came from a 2013 OpsDisk.

> In January theshadowbrokers is deciding to show screenshots of lost theequationgroup 2013 Windows Ops Disk.

I'll have a bit more to say about Shadow Brokers' claims yesterday. But if this description of the source of the exploit is correct – an ops disk dating to 2013 – it opens up the possibility it was discovered around the same time (perhaps in response to the bluescreen effect). If it did, then it would have been able to attack DOD with it.

I keep asking people what the source for Shadow Brokers' files might have been able – might still be able – to steal from the US using the tools in question. This timeline seems to suggest the Ops Disk would have been deployed before DOD was prepared to withstand its own weapons.