SHADOW BROKERS FURTHER INCITES WAR BETWEEN "SCUMBAG MICROSOFT LAWYER" AND NSA

The other day, Microsoft President and Chief Legal Officer Brad Smith wrote a blog post about the WannaCry ransomware exploiting his company's products to disrupt the world. At one level it was one of the first entries in what will surely be an interesting policy discussion once there's an aftermath to the crisis, calling for collective action and a Digital Geneva Convention.

But at another level, Smith's post provided an opportunity to bitch out the CIA and NSA, the leaked and stolen exploits of which have really fucked with Microsoft in the last few months.

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.

> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits.

Joining the many people who object to the analogy between Tomahawks and hacking exploits, the entity that caused this crisis, Shadow Brokers, is none too impressed with Smith's response, either. Along with suggesting NSA was paying Microsoft to sit on vulnerabilities and unleashing a load of expletives (you can click through for both of those), Shadow Brokers lays out the tensions between Microsoft, its enterprise contracts with the government, and the NSA's reticence about the vulnerabilities in Microsoft products it is exploiting.

> Despite what scumbag Microsoft Lawyer is wanting the peoples to be believing Microsoft is being BFF with theequationgroup. Microsoft and theequationgroup is having very very large enterprise contracts millions or billions of USD each year. TheEquationGroup is having spies inside Microsoft and other U.S. technology companies. Unwitting HUMINT.
>
> [snip]
>
> Microsoft is being embarrassed because theequationgroup is lying to Microsoft. TheEquationGroup is not telling Microsoft about SMB vulnerabilities, so Microsoft not preparing with quick fix patch. More important theequationgroup not paying Microsoft for holding vulnerability. Microsoft is thinking it knowing all the vulnerabilities TtheEquationGroup is using and paying for holding patch.

Then Shadow Brokers brings the hammer: threatens to dump (among other offerings in an "exploit of the month club") a Windows 10 vulnerability.

> TheShadowBrokers Monthly Data Dump could be being:
>
> - *web browser, router, handset exploits and tools*
> - *select items from newer Ops Disks, including newer exploits for Windows 10*
> - *compromised network data from more SWIFT providers and Central banks*
> - *compromised network data from Russian, Chinese, Iranian, or North Korean nukes and missile programs*

Heck, at this point, Shadow Brokers doesn't even need to have this exploit (though I'm guessing the NSA and Microsoft both may be erring on the side of caution at this point). Because simply by threatening another leak after leaking two sets of Microsoft exploits, Shadow Brokers will ratchet up the hostility between Microsoft and the government.

It might even force some disclosure about exploits more critical to NSA's current toolkit than the very powerful tools Shadow Brokers already used to create a global ransomware worm.