Facts about the Attack on Anthem

On January 26, 2015

78 Million

patient records were exposed.

The breach is believed to be the work of a well-resourced cyberespionage group, which Symantec calls Black Vine. They appear to have access to a wide variety of resources to let it conduct multiple, simultaneous attacks over a sustained period of time. They used:

- attacker-owned infrastructure
- zero-day exploits
- custom-developed malware

Three variants are named:

1) Hurix, 2) Sakurel, and 3) Mivast

detected as Trojan.Sakurel

Backdoor.Mivast

All variants have the following capabilities:

- Open a back door
- Execute files & commands
- Delete, modify, and create registry keys
- Gather and transmit information about the compromised computer

Top 10 Sub-Sectors Breached by Number of Incidents

Healthcare	120	Wholesale Trade	10
Business	20	Eating and Drinking Places	9
Education	20	Executive, Legislative, & General	9
Insurance	17	Depository Institutions	8
Hotels	14	Social Services	6

Symantec