US companies' experience and attitudes towards security threats

Quantitative survey within Large and Medium companies in the USA

MillwardBrown

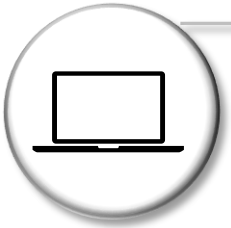
Bitdefender

Released: April, 2015

Methodology

Where?
- United States of America

Who?
- Medium and large companies



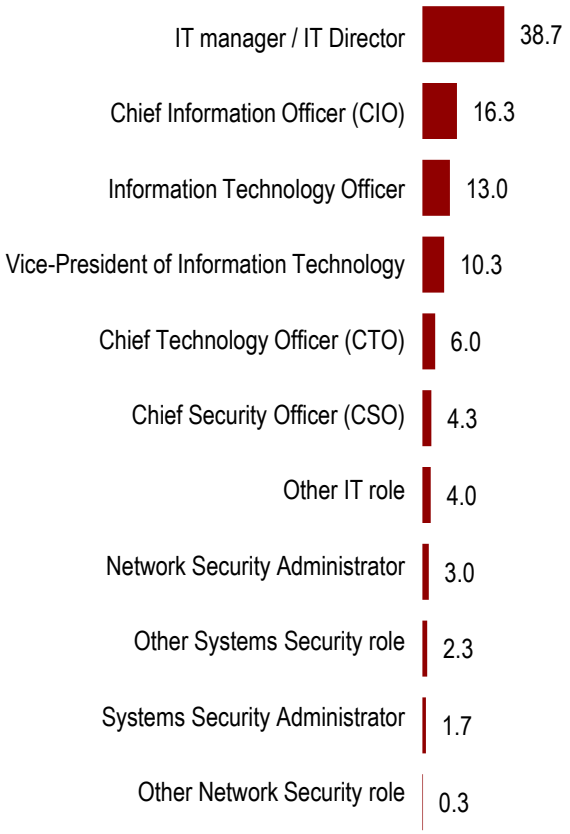
How?
- CAWI (Online self completed interviews)

When?
- 02 – 10 April 2015

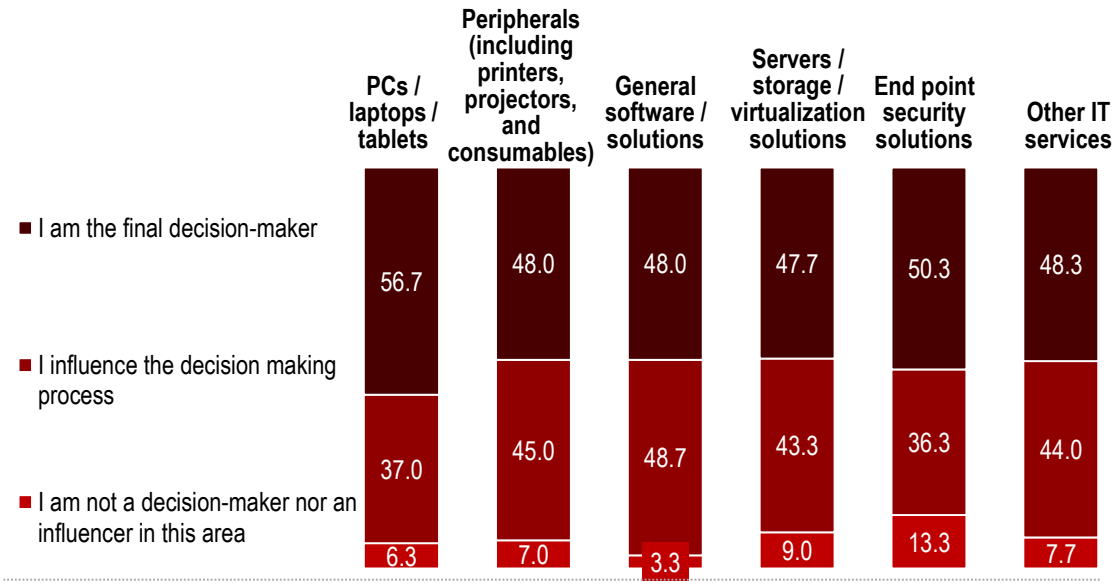
Sample Profile

N=300
%

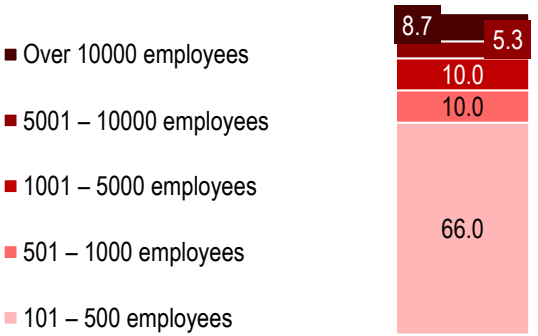
Current position



Role in procuring…



Number of employees



Key findings

- **Firewall and anti-virus/malware** are the features used mostly by the companies that were interviewed. Performance in **prevention is the benefit valued the most**, but also the power of limiting the impact while security solutions are in use.

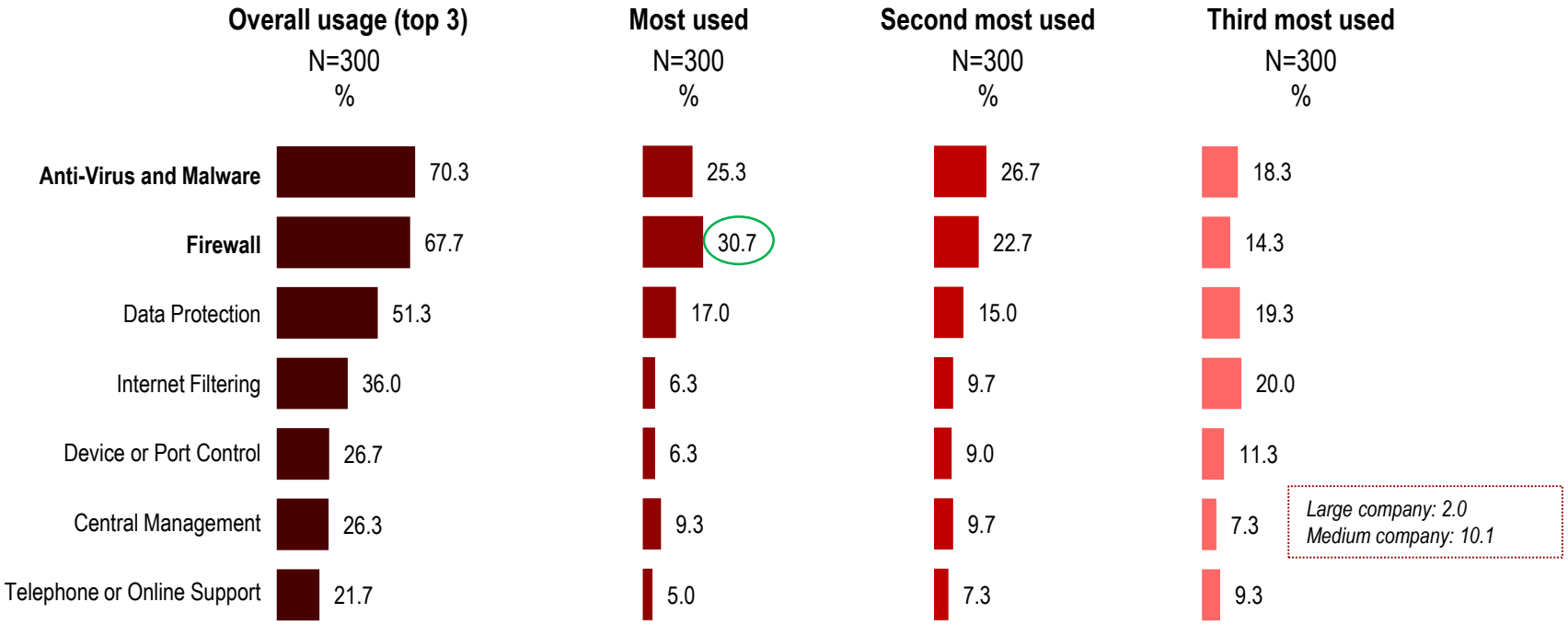
- **All investigated types of attacks** are perceived as **relatively equally hard** to detect and mitigate. Still, **APT types** are **having the edge**, almost 1 in 5 large and medium companies mentioning it.

- **Password cracking** is, out of the tested types of threats, the one **experienced very recent** (last 3 months) **by the most** (25%) of the interviewed companies.

- Overall, the areas with the **highest impact** after attacks occur, are related to **time spent** (either with Help Desk or in-house IT support) and that of **employee productivity**.

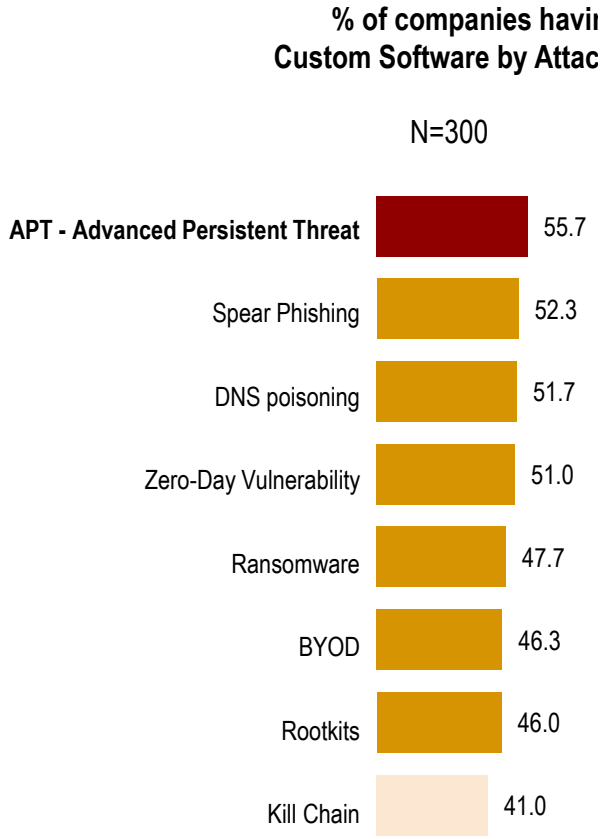
Results

Firewalls are the feature used the most - almost a third of the companies using them the most. Anti-virus/malware are used second most often.



Q13. Please select out of the following endpoint security features the top 3 ones that you leverage most in your organization.

On average, the target audience companies use custom software for 4 types of threats. Most common are those against APTs, while for Kill Chain are least used.

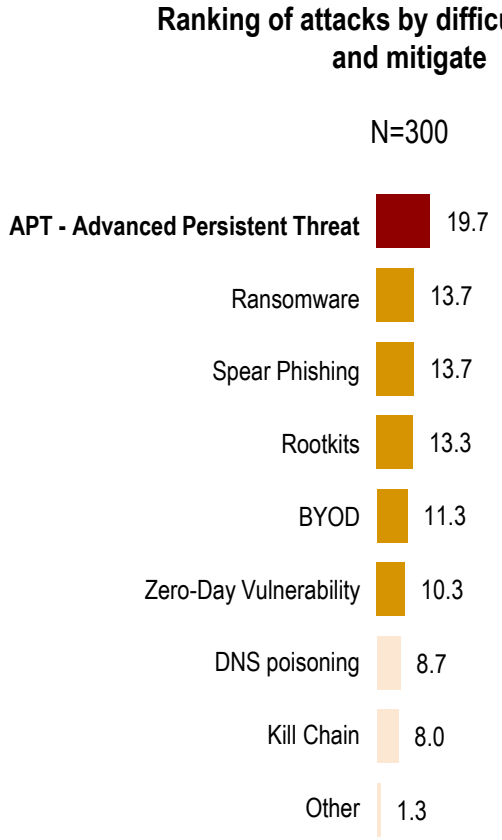


OTHER INFORMATION LAYERS:

- there are no significant differences by company size;
- have significantly more custom software companies with *high virtualization level* and those that had experienced *high impact* of previous attacks;

Q1. Does your organization have custom software to address each of the following attacks?

APTs are the attacks that seem to pose most of difficulties to the companies' security.



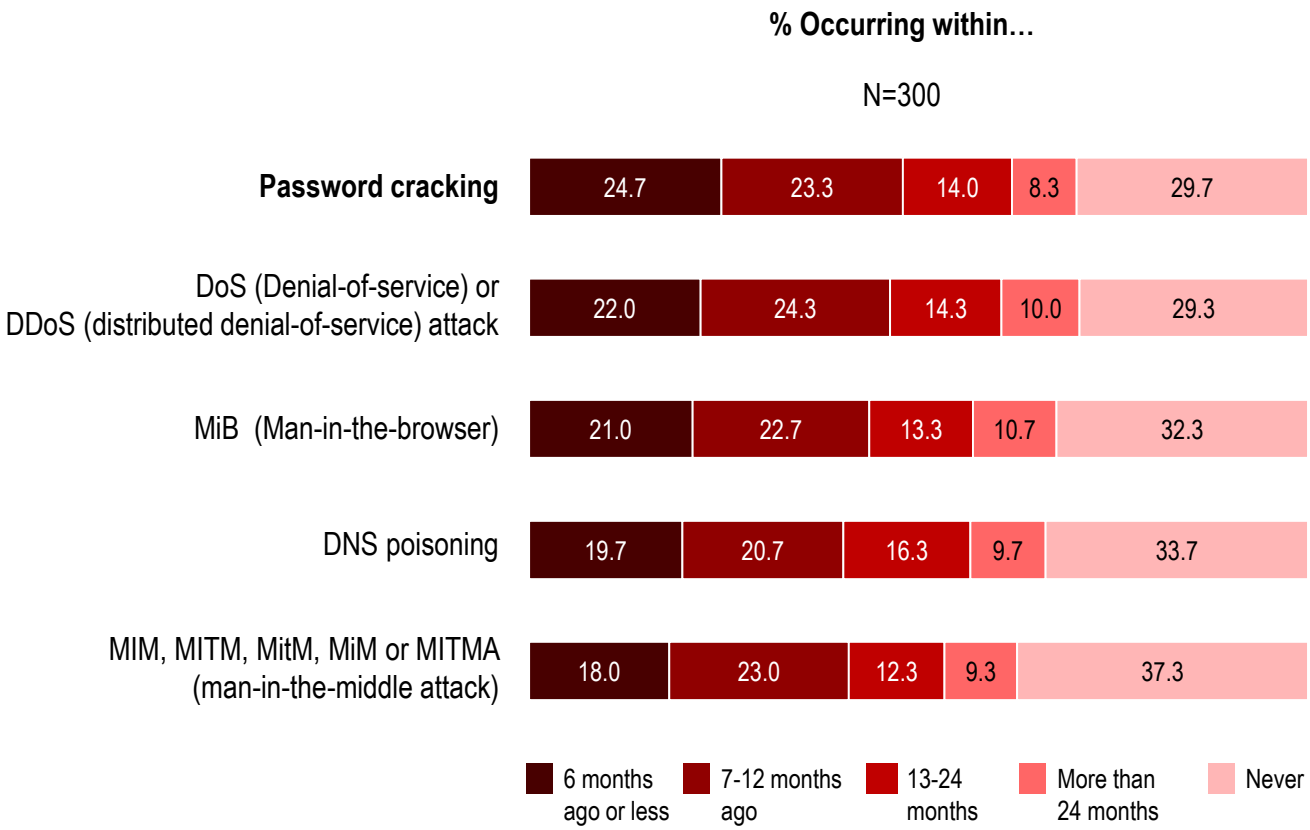
OTHER INFORMATION LAYERS:

- There are some risks towards *Ransomware* and *Rootkits* type of attacks – they rank relatively higher by difficulty compared to their ownership ranking seen previously;
- On the other hand, in the case of *Zero-Day Vulnerability* and *DNS poisoning* companies although feeling more confident, more are using software to protect from them.

- Companies with *limited attach experience* consider *Ransomware* and *Rootkits* as being more difficult to tackle. The latter is perceived as more difficult by companies with not so recent attack experiences.

Q2. In your opinion, what attack type is the hardest to detect and mitigate?

Password cracking is the attack experienced most recently by a quarter of all companies interviewed. *Man in the middle* attack are experienced least from the set analyzed.



Q3. When did your organization last register each of the following online attacks?

Thank you!