January | 2019

#CYBERWEATHER

#cyberweather gives you an update on the key information security incidents and phenomena of the month. We want to give our readers an overview of what has happened in the field of cyber security during the past month. The situation can be:

calm

worrying

serious

TRAFICOM

Cyber weather January 2019

Network performance

- January was quiet in terms of DoS attacks
- Winter storm Aapeli affected communications networks in Åland the most
- Widespread Microsoft Office 365 outage on 24-26 January

Data breaches & leaks

- More than a billion usernames and passwords were posted online. Most credentials are from previous data breaches

Malware & vulnerabilities

- Microsoft Exchange vulnerability allows attackers to gain domain admin privileges
- Attackers breach targets and spread ransomware via Remote Desktop Protocol (RDP) open to the internet

Spying

- Manipulation of domain records enabled spying on web traffic by redirecting user traffic to attacker-controlled infrastructure
- Advanced smartphone spying made the headlines again

Scams and phishing

- Massive password leak collections cause concern but most credentials have been previously included in other leaks
- Rise in CEO fraud using compromised Office 365 email accounts

IoT and automation

- Japanese law will allow the government to hack into people's IoT devices
- Critical vulnerabilities found in WiFi chips firmware

TRAFICOM