TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

August 2024

#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cyber security.

Cyber weather can be:

 calm

 worrying

 serious

Cyber weather, August 2024

Data breaches and leaks

- In the data breaches, the summer continued to be calm, and the usual autumn growth in the number of reports has not been seen.

Scams and phishing

- Tax refunds were the most popular topic of scams in August. Tena of different text message scams attempted to steal online banking credentials.
- Banking credentials were phished under other pretexts, such as electricity companies, telecommunications operators, the Kanta service, the authorities and, of course, the banks.

Malware and vulnerabilities

- SonicWall SSL VPN vulnerability is actively exploited.
- More observations have been made of Quad7 and Mirai botnets than usual.
- Updating devices and renewing old ones are still emphasised in protecting against security threats.

Automation and IoT

- The management of IoT systems is increasingly moving to the cloud. Public attention was drawn to the fact that the cybersecurity of cloud-based remote management systems for embedded generation and storage of electricity is not always good enough.
- For end-users of services, the situation is difficult if no safe alternatives are available.

Network performance

- In August, 10 disruptions were detected in public communications networks.
- Recently, a lot of short-term denial-of-service attacks have been reported on the services of Finnish organisations. However, the impact has been limited.

Spying

- APT29 reportedly accessed some UK government emails as a result of a data breach against Microsoft.
- The same operator used methods used by commercial spyware in Mongolia. A breached government website was used to breach other targets.

NCSC-FI's tips and recommendations for improving cyber security preparedness:

Threat analysis and threat modelling are key tools in managing cybersecurity risks. Threat analysis and the introduction and updating of threat modelling provide a systematic method for identifying and preparing for cybersecurity risks. We published an article on the subject.

Our home network and router security guidelines are still topical.[9] Recently, we have observed more activity of two botnets taking over home routers in Finland. Botnets are used both as part of distributed denial-of-service attacks and as a proxy for harmful network traffic in cyber attacks.

Microsoft will begin phasing in forced multi-step authentication on Azure, Intune, and Entra ID administrator portals. As part of forcing MFA to be used, Microsoft recommends creating so-called Break glass IDs. More information on tenant-specific schedules can be found in the Message Centers of the aforementioned services.

Overview of cyber weather in August

- August was exceptionally calm regarding the security incident reports we received.
- In the cases reported, various campaigns of phishing and scams against citizens were highlighted. Especially suomi.fi themed phishing messages were a nuisance in mid-August. Additionally, the tax refund theme continues too.
- The importance of contingency planning and continuity planning is emphasised especially in ransomware cases in organizations and companies of all sizes.
  - A data breach can have very serious financial consequences. At worst, the effects of a ransomware attack can paralyse an organization for weeks or even forever.
  - It is also possible to get better and more effective help in resolving the issue by reporting these issues quickly. In the best case scenario, the NCSC-FI may be able to provide tools for decrypting ransomware.
  - In August, we published an article on ransomware operations and how to protect yourself against them.

Cyber security trends
in the past 12 months