NHS RANSOMWARE ATTACK

Cyber threats

Hanna Dinser

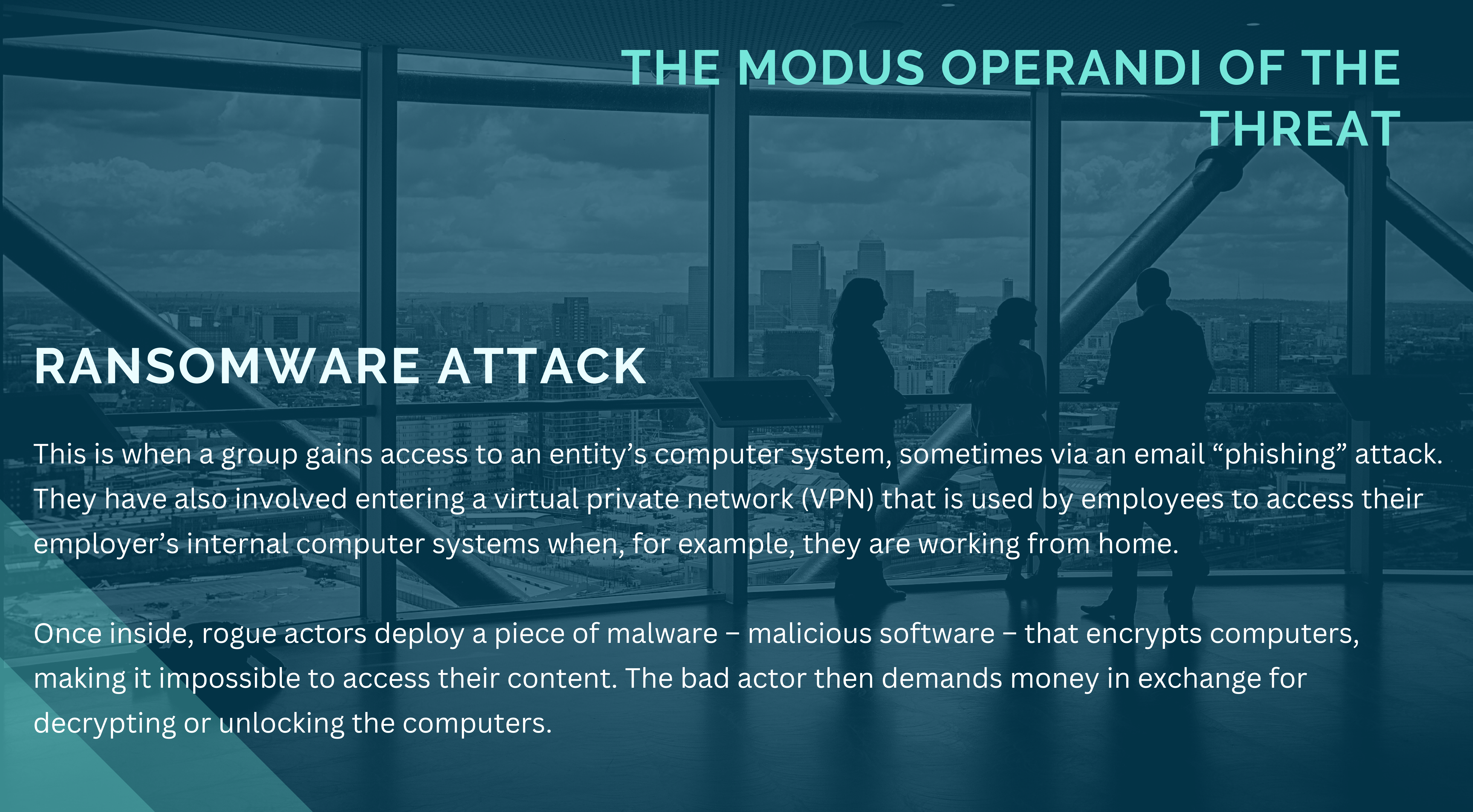
The effected information resource

Advanced, the UK company that provides software for various parts of the health service was hit by the attack 4th of august 2022hen Text hinzufügen

- Caused widespread outages across the NHS
- Affected services including patient referrals
- Ambulance dispatch
- Out-of-hours appointment bookings
- Mental health services
- Emergency prescriptions.

Source: The Guardian, 2022

THE MODUS OPERANDI OF THE THREAT



RANSOMWARE ATTACK

This is when a group gains access to an entity's computer system, sometimes via an email "phishing" attack. They have also involved entering a virtual private network (VPN) that is used by employees to access their employer's internal computer systems when, for example, they are working from home.

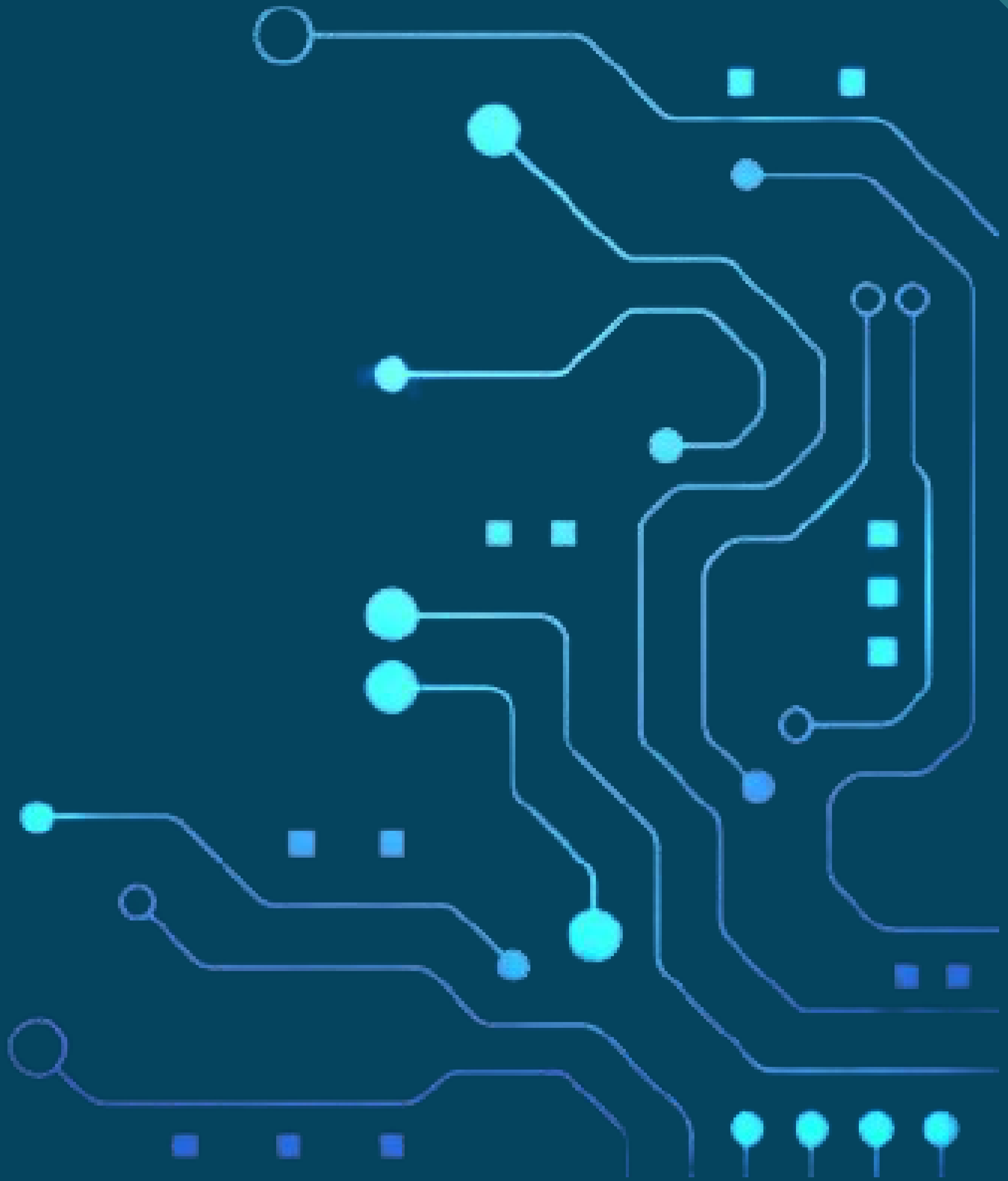
Once inside, rogue actors deploy a piece of malware – malicious software – that encrypts computers, making it impossible to access their content. The bad actor then demands money in exchange for decrypting or unlocking the computers.

THREAT ACTORS

No group has been named as the attacker, but it has been reported that it is likely to be a criminal gang rather than a state organisation.

The most notorious ransomware group in recent times is the one behind attacks using the Conti malware, which hobbled the Irish healthcare system last year and the Costa Rican government earlier this year.

This Russian-linked criminal group appears to have wound down its Conti malware attacks. However, there has been widespread speculation that the same group is behind a new piece of malware called Black Basta.



PROTECTION MEASURES

Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.

Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process.

Keep your operating system and software up-to-date with the latest patches.