NOTICEBORED

Elevator pitch

Malware

Malware (**mal**icious soft**ware**) has come a long way since the simple viruses, crude network worms, jokes and hoaxes of the 1970's and 80's. Very few organizations have escaped malware infections. Modern malware actively evades antivirus software, hiding itself in ways that even skilled forensic specialists struggle to identify, staying undetected for months or years. APT (Advanced Persistent Threat) malware is multifunctional, deeply embedded in systems, remotely-controlled, updated and configured.

Malware is increasingly used for criminal purposes, for instance stealing valuable industrial secrets, intellectual property, passwords and personal information, threatening to disclose it (remember Sony?) or encrypting it for extortion (ransomware). Bank Trojans are targeting Finance Departments and draining corporate bank accounts, diverting and laundering the funds before anyone realizes what has happened, while retail PoS (Point-of-Sale) payment card readers and bank ATMs (Automated Teller Machines) are under assault from malware.

We know malware has been used for military/political purposes at least once already (Stuxnet), and there are indications that malware may be pre-installed in IT systems before they even leave the factory.

The escalating risk suggests that, despite our ongoing investment in preventive controls, we should anticipate and be prepared for more frequent and/or more serious malware incidents. Without solid incident management, business continuity and IT disaster recovery arrangements, it's just a matter of time before a malware infection gets out of hand.

For more information

Please contact the CISO/Information Security, or browse the intranet *Security Zone*.