NOTICEBORED

Executive briefing

Malware (malicious software)

Executive summary

The battle between those developing and deploying malware for nefarious purposes, the IT security companies attempting to detect and prevent infections, and organizations trying to make good use of their IT systems and networks has been raging for years. If anything, it appears to be escalating. Malware is proving such an effective cyberweapon that criminals and other adversaries are actively investing in even more sophisticated, sneaky and capable tools.

Strategic aspects

Ever since the simple viruses, crude network worms, jokes and hoaxes of the 1970's and 80's, malware risks have been steadily increasing. After four decades of evolution, 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, and remotely-controlled, updated and configured. Malware is increasingly used for criminal purposes, 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, while retail PoS (Point-of-Sale) payment card readers and bank ATMs (Automated Teller Machines) are also under assault from malware. It is not idle speculation to suggest that malware is being actively developed and deployed for military and political purposes, raising the grim prospect of advanced cyberweapons and perhaps cyberwar.

Risk and security management aspects

The escalating risk suggests that, despite our ongoing and necessary investment in preventive and detective controls, we should anticipate and be prepared to respond to more frequent and/or more serious malware incidents. Without solid incident management and business continuity arrangements, it's just a matter of time before a malware infection seriously impacts this organization, whether directly or through the supply chain and broader business dependencies.

Governance aspects

- Conventional malware controls such as antivirus software are necessary but not sufficient.
- Malware protection is essential for all IT systems, including Internet of Things (IoT) and Bring Your Own Device (BYOD) equipment, including your home office and mobile systems by the way.
- Anomaly and intrusion detection systems provide an additional level of capability *provided* they are professionally specified, installed, monitored and maintained. Ignored alerts are worthless.
- Malware incident reporting, detection, assessment and response processes need to be well-practiced to improve the speed and effectiveness of the response. Awareness is a starting point.
- Sound business continuity arrangements, including resilience, recovery and contingency aspects and perhaps insurance, may be our last hope in the event of extreme outbreaks or incidents.

For more information

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