McGrathNicol

The life of a Hacked PC

A compromised or "Hacked PC" affects more than just that device

It introduces risk to an entire connected ecosystem and can play a critical role in a much larger web of cybercrime. This not only includes theft of an identity or banking credentials but also presents a multitude of options for the astute cybercriminal.

Modern corporate and home networks are far less perimeter based and rely on trust to operate in a secure and reliable manner. Trust between employers and employees, between family members and between businesses and their customers. We are obliged to protect a raft of sensitive information that is in our control and failure to do so can result in a loss of trust in our brand, not to mention the potential impact on revenue or regulatory sanction.

Be alert, not alarmed

Our connectivity means that we are only as resilient as our weakest link, however it is essential that we look past the fear and work together to build resilience. We need to collaborate on risks and threats, educate and challenge each other and uphold our end of the bargain by ensuring the devices and networks in our control are appropriately maintained on a regular schedule.

You would not keep driving your family around in a car with alarms ringing and the engine light on, so why tolerate vulnerable and poorly maintained digital devices in our connected ecosystems? It is critical that we take the time to educate our employees, friends and family about the shared risk of cybercrime.

Effective detection and building resilience

The difference between effective and ineffective resilience is in the detail and hinges on how quickly you are able to respond when an abnormal incident occurs. The balance between proactive protection measures and detective intel capabilities is difficult and will be a different fit for each business. However, the fact remains, the shorter the window, the more you can deal with the hackers on your own terms. Effective detection capabilities will include technological solutions as well as capable people.

No matter which way you look at it, you need to ensure your equipment is in good shape and basic hygiene is mandatory (refer to the Essential Eight diagram). Once your devices and networks are secure, you should consider prioritising an investment to shorten the gap between detection and response. Not knowing you have been hacked will fast become an unacceptable excuse.

Malicious uses for a Hacked PC

Bot activity
- Spam zombie
- DDoS extortion zombie
- Click fraud zombie
- Anonymisation proxy
- CAPTCHA solving zombie

Account credentials
- eBay/PayPal fake auctions
- Online gaming credentials
- Website FTP credentials
- Skype/VoiP credentials
- Cleint side encryption certificates

Reputation hijacking
- Facebook
- Twitter
- LinkedIn
- Google+

Financial credentials
- Bank account data
- Credit card data
- Stock trading account
- Mutual fund/401k account

Web server
- Phishing site
- Malware download site
- Warez/privacy server
- Child pornography server
- Spam site

E-mail attacks
- Webmail spam
- Stranded abroad advance scams
- Harvesting e-mail contacts
- Harvesting associated accounts
- Access to corporate e-mail

Virtual goods
- Online gaming characters
- Online gaming goods/currency
- PC game lincence keys
- Operating system license key

Hostage attacks
- Fake antivirus
- Ransomware
- Email account ransom
- Webcam image extention

Source: https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

The Essential Eight

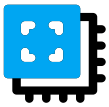
Implementing a regular maintenance schedule does not have to be a challenge. The Australian Government provides some guidance and practical solutions for making your digital devices more secure, allowing you to uphold your end of the bargain.

To prevent malware running

Application whitelisting*

A whitelist only allows selected software applications to run on computers.

Why? All other software applications are stopped, including malware.



Patch applications*

A patch fixes security vulnerabilities in software applications.

Why? Adversaries will use known security vulnerabilities to target computers.

Disable untrusted Microsoft Office macros

Microsoft Office applications can use software known as 'macros' to automate routine tasks.

Why? Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.

User application hardening

Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet.

Why? Flash, Java and web ads have long been popular ways to deliver malware to infect computers.

To limit the extent of incidents and recover data

Restrict administrative privileges*

Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them.

Why? Admin accounts are 'the keys to the kingdom', adversaries use these accounts for full access to information and systems.

Patch operating systems*

A patch fixes security vulnerabilities in operating systems.

Why? Adversaries will use known security vulnerabilities to target computers.

Multi-factor authentication

This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically something you know, like a passphrase, something you have, like a physical token, and/or something you are, like biometric data.

Why? Having multiple levels of authentication makes it a lot harder for adversaries to access your information.

Daily back up of important data

Regularly back up all data and store it securely offline.

Why? That way your organisation can access data again if it suffers a cyber security incident.

* Top 4 mitigation stratgies to protect your Information and Communications Technologies (ICT)

Source: https://www.asd.gov.au/publications/protect/essential-eight-explained.htm