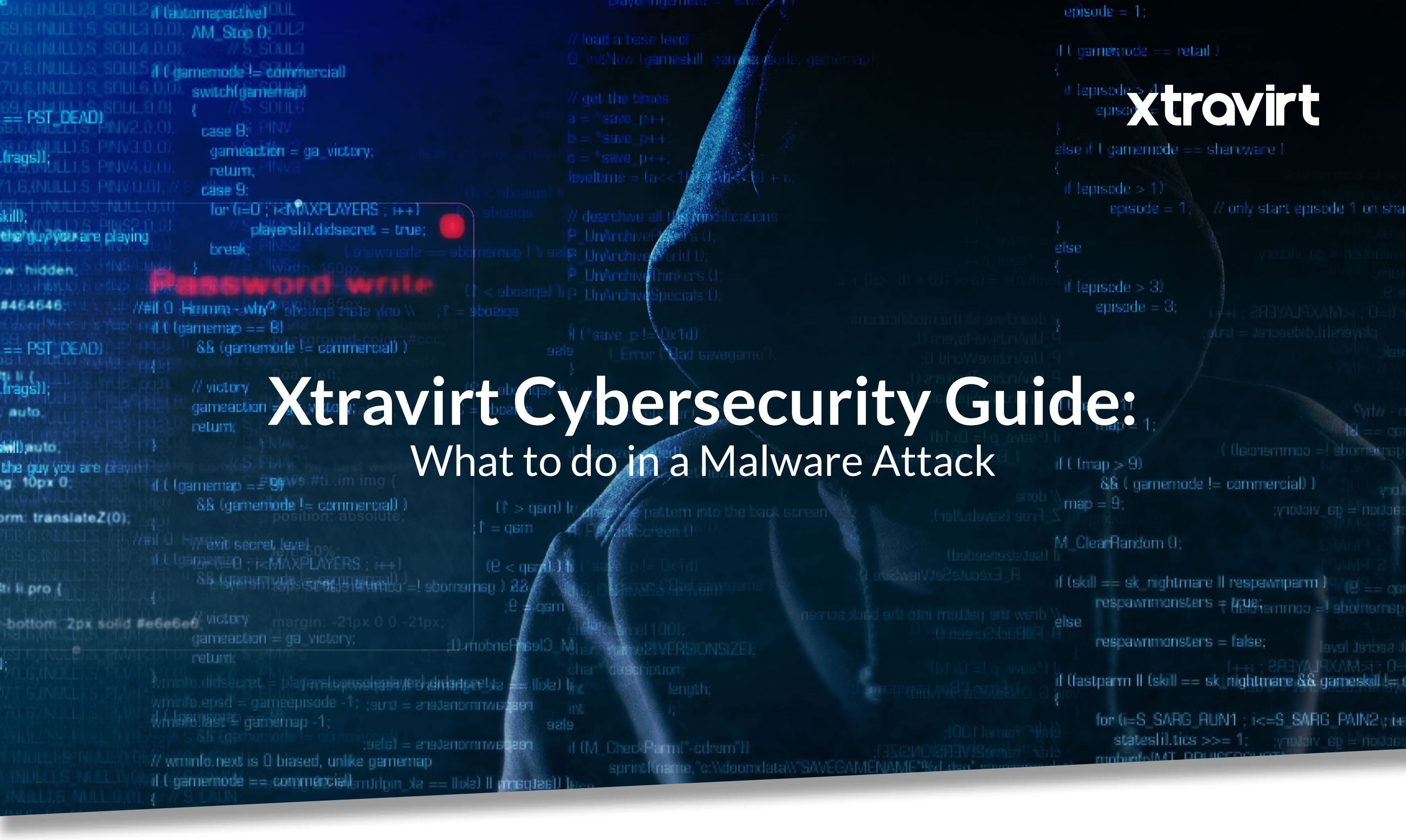

Xtravirt Cybersecurity Guide:

What to do in a Malware Attack

This high-level guide has been put together by Xtravirt to assist customers in undertaking an orderly damage limitation exercise. Some of these points may appear obvious, but in a pressured situation such as an outbreak, these first-principles can often be missed.

1 Protect the Perimeter

- With the WannaCry outbreak, one of the key points of the exploit is an attack on the legacy SMB 1.1 protocol. One of the important first steps is to ensure that access to port TCP 445 is restricted, to both external traffic, and within the environment where intervening firewalls exist. This may mean custom rules to permit certain trusted subnets.
- Client-side firewalls, such as the integrated Windows firewall may also be used to block access, but this should be tested first.
- Disable SMB v1 on Windows Vista and later versions. This is a registry change and will require a reboot. For further details see 'How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server'
- Consider disabling File and Print sharing on all client systems, and where possible, servers.
  - One option is to use Group Policy to do this centrally. This is carried out under Computer Configuration > Administrative Templates> Network > Network Connections > Windows Firewall. On the Domain Profile, set "Windows Firewall: Allow file and printer sharing exception" to disabled.
- Ensure HTTP and HTTPS can reach the address: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - access to this site prevents the WannaCry malware from encrypting devices, so preventing damage.

2 Patching Systems

- Although this will not fix systems already infected, ensure that the systems are fully patched, both with the latest anti-virus identities and with Windows Updates to prevent spread.
- With regard to anti-virus, most corporate solutions include central management consoles – check that all systems are fully patched and operational and remediate as required.
- With supported Microsoft Windows operating systems, ensure that all devices are patched to the current level. Depending on your patch management strategy, carry out a check on Windows System Update Server (or your chosen solution) to confirm that the relevant patch is deployed.

Remediate any missed systems:

  - KB4012598 for Windows Vista/ Server 2008 (Also now available for Windows XP and Server 2003)
  - KB4012212 (Individual patch) or KB4012215 (Monthly rollup) for Windows 7/Server 2008R2.
  - KB4012213 (Individual patch) or KB4012216 (Monthly rollup) for Windows 8.1/Server 2012R2
  - KB4012214 (Individual patch) or KB4012217 (Monthly rollup) for Windows Server 2012.
  - For Windows 10 it depends on the release. In all cases refer to the Microsoft Security Bulletin

- Ensure that all backups are current and verified, ideally carry out a test restore to an isolated recovery server. As stated above, this may seem obvious, but don't assume that all is well with backups – what if the latest backup failed, or worse, is infected?

3 Managing Infected Devices

- Keep in touch with both Microsoft and your Security Solution Vendor – they are actively developing countermeasures and tools to remove the infection from devices.
- For further information
  - Symantec - What you need to know about the WannaCry Ransomware
  - Sophos – Wanna Decrypter 2.0 ransomware attack: what you need to know
- With regard to infected devices:
  - Immediately isolate the machine from the rest of the network. This may mean physically switching it off or disconnecting it from the network.
  - If no data is stored locally on the device, immediately wipe and rebuild the machine.
  - At this stage encrypted data is not yet recoverable, though vendors are working on this. Either wipe the device and recover from backups or await updates from the vendor.
  - Attempt to identify the time of infection – this may be easier said than done, but may help identify the state of backups (whether the contents are infected/encrypted).

Above all, stay calm. Anti-virus and patching strategies are put in place to mitigate such attacks, however, there will always be an opening in even the tightest environment. Be aware of the tools available to assist, and support is available from a wide range of places.