BIZCOMMUNITY

Ransomware: Here today, here tomorrow

By Derek Manky

19 May 2020

With all our energy of the past several weeks focused on adapting to the global crisis, security may have taken a back seat. But cybercriminals haven't forgotten. FortiGuard Labs has been actively monitoring the threat landscape during this time, and we have seen a significant increase in threats targeting individuals through phishing and infected websites.

Derek Manky, Chief Security Insights & Global Threat Alliances at Fortinet

Email attachments contain infected and malicious content, which explains why we recorded a 131% increase in viruses during March of this year. It also explains why we have seen a reduction in traditional attacks as cybercriminals shift focus.

Incidents of ransomware are likely to rise as cybercriminals look to use compromised end-user devices as a conduit back into a core network that may not be being watched as carefully as it once was.

We are at an especially vulnerable moment in our transition to a digital economy. Organisations need to take steps now to protect their networks and networked resources from the growing problem of sophisticated ransomware.

While each network environment is different, here are 20 things any organisation can begin to implement today to reduce their risk from ransomware and other advanced threats.

1. Wherever possible, patch and update operating systems, devices, and software. Make this a priority for your remote workers ¬– especially those using personal devices to connect to the corporate network.
2. For devices that can't be patched, ensure that appropriate proximity controls and alerts are in place.
3. Make sure that all endpoint devices have advanced security installed, such as anti-exploit and EDR solutions.
4. Also make sure that access controls, such as multifactor authentication and even Network Access Control solutions are in place.
5. Use NAC to inspect and block bring-your-own-devices that do not meet security policy.
6. Segment your network into security zones to prevent the spread of infection and tie access controls to dynamic segmentation.
7. Use inventory tools and IOC lists to prioritise which of your assets are at the most risk.
8. Update your network IPS signatures, as well as device antivirus and anti-malware tools.
9. Back-up systems and then store those backups offline – along with any devices and software you may need in the event of a network recovery.
10. Make sure that ransomware recovery is part of your BCDR, Identify your recovery team, run drills, and pre-assign responsibilities so systems can be restored quickly in the event of a
11. successful breach.
12. Update your email and web security gateways to check and filter out email attachments, websites, and files for malware.
13. Make sure that CDR (content disarm and recovery) solutions are in place to deactivate malicious attachments.
14. Use a sandbox to discover, execute, and analyse new or unrecognised files, documents, or programs in a safe environment.
15. Block advertisements and social media sites that have no business relevance.
16. Use zero-trust network access that includes virus assessments so users can't infect business-critical applications, data, or services.
17. Use application whitelisting to prevent unauthorised applications from being downloaded or run.
18. Prevent unauthorised SaaS applications with a CASB solution.
19. Use forensic analysis tools to identify where an infection came from, how long it has been in your environment, ensure you have removed all of it from every device, and ensure it doesn't come back.
20. Plan around the weakest link in your security system – the people who use your devices and applications. Training is essential but limited. Proper tools, such as secure email gateways, for example, can eliminate most if not all phishing emails and malicious attachments.

21. Leverage people, technology, and processes to quickly gather threat intelligence about active attacks on your networks and act on it, using automation where possible. This is crucial to stopping an advanced attack in its tracks.

Even though we are all running as fast as we can to keep our businesses up and running, we are also more exposed than ever to criminals who want to take advantage of this crisis. Ransomware and other advanced threats have not slowed down just because we are busy. In fact, based on our ongoing analysis of the threat landscape, the opposite is true.Most organisations should have their remote worker strategy in place. Now is a perfect time to review the steps outlined above, conduct a thorough review of your security policies, and make necessary adjustments. Prioritise your challenges and work through them one at a time. Every step you take now to tighten down your policies and practices is a threat averted. And we could all use one less thing to worry about right now.

ABOUT THE AUTHOR

Derek Manky, Chief Security Insights & Global Threat Alliances at Fortinet