WHITE PAPER

Preventing Malware Infestations with

Smart Next-Gen IT Asset Management (ITAM) Combined with Certain Configuration Management Database (CMDB) Capabilities

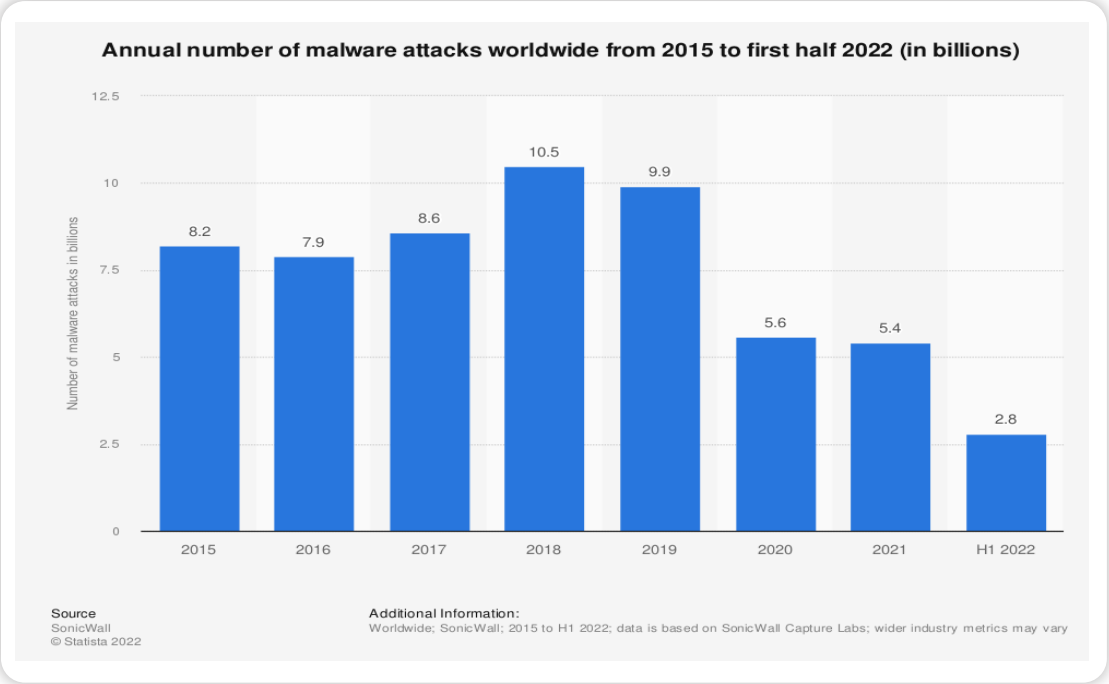
Organizations continue to get attacked by malware. Malware can cause significant damage to organizations and ransomware is proving to be its most lucrative form. Is your company prepared?

CONTENTS

Introduction	1
The Importance of Preventing Malware Attacks	2
How to Use Smart Next-Gen ITAM to Prevent Malware Attacks	3
Conclusion	5
Sources	6
About Apexa iQ	7

INTRODUCTION

Organizations continue to get attacked by malware. Malware is malicious software designed to disrupt or gain access to a system without authorization, that causes significant damage to organizations. According to Statista, data shows that in the first half of 2022 alone, the number of malware attacks was estimated at 2.8 billion, +11% year over year.



Based on data collected by SonicWall Capture Labs threat researchers, the most significant culprits behind the rise in malware have been cryptojacking and IoT malware, which have risen 30% and 77%, respectively, year to date.

Ransomware is proving to be the most lucrative form of malware. The BlackByte gang claimed responsibility for the San Francisco 49er's ransomware attack last year. The White House recently released a new cybersecurity strategy that "... underlines ransomware as a major threat and stresses how the administration "strongly discourages the payment of ransoms" and will continue targeting ransomware gangs operating from safe havens like Russia, North Korea, and Iran.

THE IMPORTANCE OF PREVENTING MALWARE ATTACKS

ITAM/CMDB teams have a shortage of qualified personnel who can identify which patches are high priority and which ones can wait their turn. “Security teams are overwhelmed,” says Piero DePaoli, senior director of product marketing of security operations for ServiceNow in a Workflow report.

The report goes on to state that “62% of surveyed companies say they can’t tell whether software vulnerabilities are being patched in a timely way and 57% say their patching efforts fail because their teams are still using spreadsheets and emails to track and assign patching tasks”. Finding every asset in today’s IT estates can be an enormous task to do with spreadsheets, a static configuration management database, or an IT asset management system.

Smart next-gen IT asset management platforms can streamline your patch management efforts, reducing the time and money needed to perform them. Unpatched systems leave companies vulnerable to malware. Apexa iQ can pinpoint all of the vulnerabilities and give you a roadmap to remediation in order of criticality.

> “
>
> With Apexa, I’m **confident** that all my assets are **configured and patched effectively.**
>
> Brad Kirlin | SVP/CTO, Fidelity Bank

Brad Kirlin, SVP/CTO at Fidelity Bank comments “Apexa iQ sees every IT asset. Using the platform, we discovered a DNS server that we didn’t know existed and left us vulnerable to hackers since it wasn’t configured properly. With Apexa, I’m confident that all my assets are configured and patched effectively.”

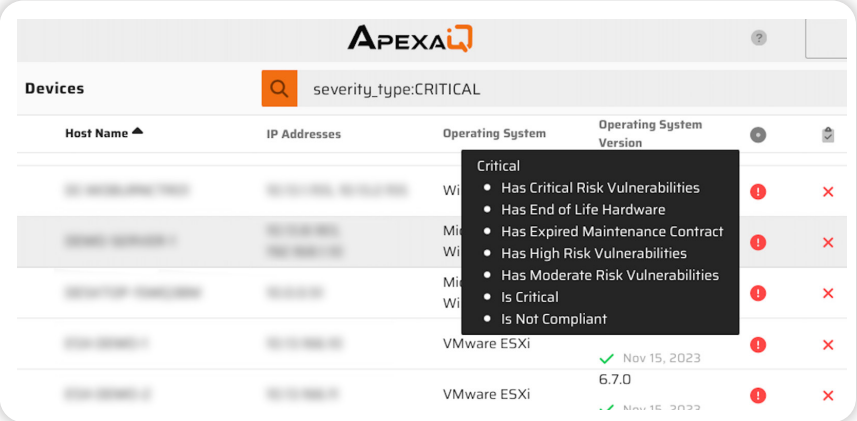
“The Apexa platform allows you to see the end-of-life status and the criticality of all your assets, either hardware or software that protects your crucial business and customers. **Malware infestations are preventable if you keep impeccable IT hygiene.** Apexa is the platform that will enable you to keep this level of hygiene in a way that was never available before” comments Lokesh Aggarwal, President and CEO of Apexa iQ.

HOW TO USE SMART NEXT-GEN ITAM TO PREVENT MALWARE ATTACKS

1. Real-Time Asset Management to Identify Your End-Of-Life, Critical, and Vulnerable Assets

Smart ITAM systems help organizations keep an up-to-date inventory of all hardware and software assets, their end-of-life status and vulnerabilities. They can help identify any unmanaged or unapproved devices or software that may be more vulnerable to malware attacks.

Identify **critical devices** in the Apexa platform



With Apexa iQ, the smart IT asset management system, you can see your entire IT estate in near real-time. Apexa helps IT teams protect against malware by providing an automated and comprehensive view of known vulnerabilities for every asset in order of criticality, making it an efficient and effective way to identify and remediate all vulnerabilities to improve your IT hygiene.

2. Automate and Prioritize Patch Management

Smart ITAM systems can help identify and prioritize software updates and security patches to ensure that all devices and software are running the latest and most secure versions. This can help reduce the risk of known vulnerabilities being exploited by malware.

"My infrastructure inventory at a large bank resembled the junk drawer that I have at home collecting odds and ends for 40 years. **Apexa iQ is the magic wand that organizes the drawer and tells you what products in said drawer need remediation or replacement**" comments Constantine Gavalas, CTO Sterlingshire.

3. Monitor Access Control to Identify Unauthorized Users

By marrying data sources like Identity Providers with other vulnerability analysis, smart ITAM/CMDB systems can help control access to sensitive data and systems, ensuring that only authorized users have access. Ensuring that only authorized users have access is a critical step to prevent malware infections caused by insider threats.

4. Monitoring and Reporting to Detect Unusual Activity

Security information and event management (SIEM) integrated with ITAM/CMDB systems provide continuous vulnerability, end of life, end of support, product decommissioning, false positive reduction, and patch information to security operations centers that monitor and report on the IT environment,

which can help detect any unusual activity or security breaches, including those caused by malware.

CONCLUSION

Overall, statistics support the need to utilize a smart ITAM/CMDB system to find and prioritize vulnerabilities in your IT estate. However, it is important to note that ITAM systems should be used in conjunction with other security measures, such as CMDB-informed anti-virus software and employee training, to provide a layered defense against malware.

WE CAN HELP YOU

Gain Better Visibility

Optimize Security

Simplify Operations

Lower TCO

AI-Driven Decision-Making

SOURCES

Petrosen, A. (Aug 3, 2022.) Annual number of malware attacks worldwide from 2015 to first half 2022. Retrieved March 7, 2023, from https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Kent, C. (Apr 5, 2018.) Annual number of malware attacks worldwide from 2015 to first half 2022. Retrieved March 3, 2023, from https://www.servicenow.com/workflow/it-transformation/ponemon-vulnerability-response-study/

Gatlan, S. (Mar 2, 2023.) White House releases new U.S. national cybersecurity strategy. Retrieved March 3rd, 2023. https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/white-house-releases-new-us-national-cybersecurity-strategy/amp/

SonicWall. (Mid-Year Update: 2022) SonicWall Cyber Threat Report. Retrieved March 4th, 2023. https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf

ABOUT APEXAiQ

ApexaiQ® is a SaaS-based agentless platform that gives IT leaders the confidence they need to mitigate risk within their IT estate. The platform discovers your entire IT estate in near real-time — on-premises, co-located, and in the cloud. It discovers, aggregates, and normalizes the entirety of your asset inventory and vulnerabilities in near real-time. Instantly, organizations gain visibility and clarity into their entire infrastructure, inventory, and health so that they can take the right action at the right time. The platform prioritizes your organization's vulnerabilities and allows you to streamline multiple aspects of your IT Asset Management, Configuration Management, Database, and Security Orchestration and Remediation workflows.

For more information, contact Apexa iQ at contact@apexaiq.com.