USE CASE

Protecting Your Network from Malware

Executive Summary

Businesses continue to evolve as digital technologies reshape industries. The workforce is mobile, and speed and efficiency are imperative, necessitating dynamic, cloud-based infrastructures and connectivity, as well as unhindered, secure application access — from anywhere, on any device, at any time. Leaders must remove hurdles to progress, but new business initiatives and processes increase the attack surface, potentially putting companies at risk.

Many businesses are embracing a zero trust security model to meet these challenges head on. A zero trust architecture assumes that everything on the network is hostile; gone are the days of "inside versus outside" and perimeter security, as too is the mantra of "trust, but verify." In their place, organizations must adopt a "verify and never trust" outlook, authenticating and authorizing every device and user before delivering applications or data, and monitoring application access and network activity through logging and behavioral analytics.

One of the many use cases associated with a zero trust security strategy is protecting your network — and most importantly, your data — from malware.

Protecting Your Network from Malware

The threat landscape is becoming increasingly hostile. Malware and ransomware campaigns, phishing scams, and data exfiltration are growing in volume, sophistication, and prevalence. More than 250,000 new malicious programs are registered every day,[1] and the number of emails containing malware increased from 1 in 220 emails in 2015 to 1 in just 131 emails in 2016.[2] As companies and individuals react to this barrage, attack methods evolve.

Cyber criminals have refined and personalized their techniques, targeting specific companies and probing for vulnerabilities with a distinct purpose. These malicious actors are skilled, patient, and persistent — and highly monetarily incentivized. A 2017 Ponemon Institute report revealed that an alarming 51% of companies had a global data breach in the past five years, and of these, 56% had multiple breaches.[3] Given that 1.9 billion data records were leaked or stolen during just the first half of 2017, well surpassing a total of 1.37 billion in all of 2016, 2018 promises new and daunting challenges.[4] It is clear that business leaders must prioritize security to defend against this onslaught.

As the enterprise threat level is propelled upward and executives attempt to batten down the hatches, their employees, business partners, contractors, supply chains, distribution chains, and visitors demand accessibility, flexibility, and simplicity of the corporate network. Not only does your ecosystem expect the ability to work remotely or while on the go — 79% of global knowledge workers are telecommuters[5] — they assume to do so on any device: mobile, connected IoT (Internet of Things), or BYOD (Bring Your Own Device). Additionally, your users require the adoption of the latest workplace applications, the majority of which are now hosted on the Internet, to facilitate rapid and dynamic global communication and collaboration.

Protecting Your Network from Malware

This drive toward digital transformation and an empowered, enabled workforce inherently means increased exposure for the enterprise. IDC Research reports that 76% of businesses expect remote access to increase in the coming two years.[6] And while 67% of workers use their own devices at work,[7] fewer than 10% of organizations state that they have complete awareness of which devices access their networks.[8] It only takes one compromised device reconnecting to corporate infrastructure to unleash malware that cripples the network or facilitates data exfiltration. Furthermore, traditional access approaches require holes in your firewall and intrusion prevention systems.

Existing security controls are outmatched — at best static and reactive. Current layers likely aren't protecting you against all attack vectors, like the vulnerable back door that is recursive DNS. And security mechanisms that frustrate, impede, or disallow legitimate users, devices, or applications will have low adoption rates and/or will curtail productivity. Benign users may even circumvent these processes, further undermining your corporate security posture and creating more gaps in your defense-in-depth strategy.

Take Action: Implement Zero Trust

The best defense against malware and other advanced, targeted threats is to proactively apply "verify and never trust" broadly, across devices, users, and requests on your network; locality is no longer a sufficient indicator of validity. You must assume that the environment is hostile and audit all activity, remaining vigilant to the variety of threat vectors your network sees every day, such as malicious or homographic domains, phishing emails, malware-laden advertisements, infected files downloaded via the web, typosquatting sites, compromised URLs shared via social media, malevolent plugins, and tainted computer storage media. Adopting a zero trust security model — simply authenticating and authorizing every device and user before delivering applications or data, and monitoring application access and network activity through logging and behavioral analytics — can simply, uniformly, and efficiently protect your network against cyber threats.

Read "**Moving Beyond Perimeter Security**" to learn more about adopting a zero trust security model, or visit **akamai.com/etp** to learn more about Akamai's cloud-based, centrally managed, and easily scalable solution for protecting your network against malware.

SOURCES

1) https://www.av-test.org/en/statistics/malware/
2) Symantec Internet Threat Security Report, https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_
3) Ponemon Institute: Data Protection Risks & Regulations in the Global Economy Study, http://www.experian.com/assets/data-breach/white-papers/2017-experian-global-risks-and-regulations-study.PDF
4) Gemalto Breach Level Impact Report, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf
5) PGi Global Telework Survey, http://go.pgi.com/gen-genspec-15telesur-SC1129
6) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
7) https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices
8) https://www.securedgenetworks.com/blog/topic/strategy

Akamai