Ransomware Attacks: Don’t Let Your Guard Down

A recent report from blockchain data company Chainalysis shows that extortion payments for ransomware declined significantly in 2022. The decrease is attributed to the disruption of major ransomware gangs, a weakening in crypto values, and organizations finally stepping up their cybersecurity practices. According to U.S. Deputy Attorney General Lisa Monaco, the industry has pivoted “to a posture where we’re on our front foot.” Based on her view, companies are more focused on making sure they’re doing everything to prevent attacks in the first place and invest in business continuity and backup software that allow computer systems to restart after they have been infected. Does this mean we can refocus on other attack vectors and tactics?

Not so fast. A quick Google ransomware search under ‘News’ will reveal plenty of recent high-profile attacks on Dole, the City of Oakland, and Regal Medical Group and illustrate that even if ransomware appears to be slowing down, organizations cannot let their guards down.

History has shown that cyber adversaries are often adjusting their tactics and techniques to account for evolutions of their victims’ defense strategies before starting a new wave of attacks. For instance, threat actors have shifted from just infecting systems with ransomware to multi-faceted extortion where they steal data and threaten to release it to the public or even sell it. In those cases, traditional ransomware defense tools are less effective.

And while organizations might try to limit their risk exposure to these extortion schemes by taking out cybersecurity

insurance policies, going forward this approach might no longer prove efficient. As insurers like Lloyds continue to add restrictions on payouts, including excluding losses related to state-backed cyber-attackers, fewer companies will be able to rely on cybersecurity insurance to mitigate catastrophic risk. Instead, companies need to increase their ransomware preparedness. This is especially true for the recovery of endpoints, which represent an essential tool for remote workers to conduct business in today's work-from-anywhere environment. In this context cyber resiliency plays an important role, allowing businesses to improve their ability to prepare and quickly recover endpoints from ransomware attacks.

Increasing Ransomware Cyber Resilience

Unfortunately, while organizations are very concerned about the time to recover from ransomware attacks, they often solely focus on prevention tools, without planning for the worst-case scenario: falling victim to an attack. In turn, it is important to increase an organization's ransomware preparedness and assure that the tools needed for remediation, eradication, and recovery are not just in place but also functioning as expected.

To assist organizations in increasing cyber resilience in their ransomware response, consider the following capabilities:

- ***Check strategic ransomware readiness across endpoints*** by identifying key controls (e.g., anti-virus/anti-malware, endpoint protection, or endpoint detection and response solutions) and device management tools that are required to minimize ransomware exposure and assure expedited recovery efforts.
- ***Enable ransomware cyber hygiene across endpoints*** by establishing application resilience policies to ensure that identified mission-critical security applications

and device management tools are installed and functioning as intended.

- ***Assess device security posture*** bycontinuously detecting and reporting on anti-malware, as well as detection and response software deployed on endpoint assets.
- ***Discover sensitive endpoint data*** by scanning endpoints for financial information, social security numbers, personally identifiable information (PII), protected health information (PHI), and intellectual property to identify at-risk devices and ensure proper back-up via existing tools.
- ***Self-healing for endpoint security and device management software*** by leveraging application resilience to keep essential tools installed, healthy, and effective to ensure their availability for recovery purposes.
- ***Inform users in a timely and coordinated fashion*** about mitigation stepsby displaying messages directly on user devices, preventing unnecessary help desk support calls and fragmented communications.
- ***Expedite recovery tasks*** by gathering precise insights, executing custom workflows, and automating commands for device recovery by leveraging a library of custom scripts to assist with tasks such as identifying machines that have been infected and encrypted, quarantining endpoints (e.g., disable networking or unlock specific device ports), or supporting the re-imaging of devices.

History has shown that when it comes to ransomware, organizations cannot let their guards down. Instead, companies need to increase their ransomware preparedness and response because it’s only a matter of time before cyber criminals reload with new exploits and tactics.

Ransomware Attacks: Don’t Let Your Guard Down