The Harsh Reality of Modern Ransomware

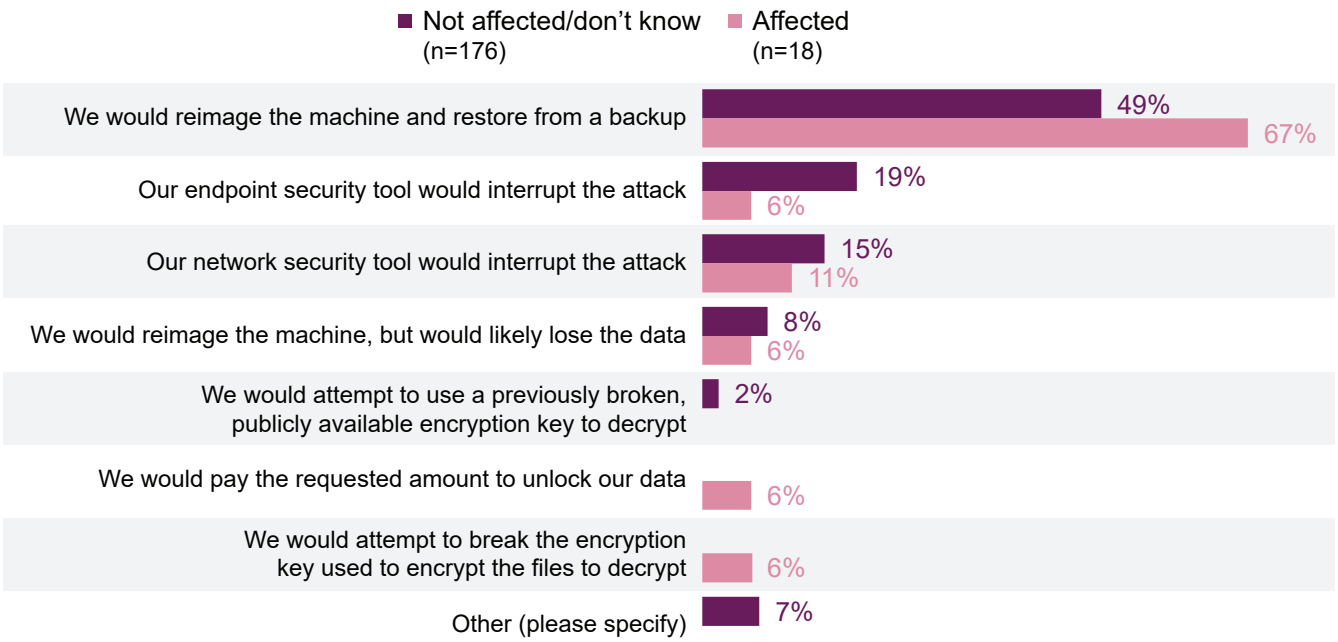
The 451 Take

While the first incidence of 'ransomware' as currently understood dates to 1989, its evolution reached an inflection point around 2014 and, since then, has quickly risen as a key concern for security teams in organizations large and small. One of the more challenging aspects of ransomware is that there has been a shift in how it affects environments. Originally, ransomware was more likely to affect single endpoints or perhaps network shares reachable from that compromised endpoint. Certainly, it was an issue to be addressed, but a relatively minor one in the grand scheme of things.

The attacks have shifted in the past couple of years. Opportunistic ransomware still exists, but criminals, driven by higher payouts from more impactful events, appear to have started deploying ransomware as the final act in more elaborate attack campaigns: silently compromise an initial beachhead, then use that to move laterally across the environment, exfiltrate sensitive corporate data and silently obtain broad administrative access to a large swath of the IT infrastructure. Then, and only then, does the attacker explicitly disrupt operations and demand ransom. Faced with the potential for catastrophic damage, many organizations are more amenable to making exceptionally large payouts.

While not all ransomware behaves this way, many strains do, which puts additional pressure on security teams to find a way to defend the organization against attackers that may move quietly for days or weeks.

Expected and Actual Responses to a Ransomware Attack



Q: If your organization were to become the victim of a ransomware attack, how would it most likely respond first?

Base: Respondents using endpoint security technology who have not or don't know whether they have been a victim of a ransomware attack in the past 12 months

Q: How did you handle the ransomware event?

Base: Respondents currently using endpoint security technology and have been a victim of ransomware in the past 12 months

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020

How are organizations planning to protect themselves against ransomware? How effective are current defense methods? The data above comes from 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020 study. In this survey, participants were asked how they expect to manage a ransomware incident and, for a smaller sample of those who indicated that they had been affected by ransomware (approximately 10% of respondents), how they actually reacted. While the smaller sample size means some results should be considered anecdotal, they're still informative.

Business Impact

Even under the best of circumstances, people expect disruption. Approximately half of respondents indicated that their primary response would be to restore from backup. This likely stems from an expectation that ransomware affects a small set of systems at a time, which is something that can no longer be counted on given the changes in how attackers launch encryption activities – only as a last link in a chain of compromise that can affect a much larger portion of the organization.

Can common security protection controls be counted on? The data points to a disparity between those that expected their tools to be more responsive and those that saw actual results from tooling: both network and endpoint percentages were lower in the affected group. Many factors likely play into this – Was there sufficient coverage from a deployment perspective? Were configurations and updates adequate against the threat? – but the trend points to some level of disappointment with how controls appear to have performed.

Backups are the essential 'lifesaving' response. The data shows that 67% of those affected by ransomware relied on their backups for recovering. This speaks to the need for a well-coordinated practice between teams working the security incident response processes and those in charge of backing up systems. A key point is that attackers know this, too, and likely see backup management systems as high-priority targets, meaning they should be particularly well-defended.

Paying ransom is a bitter pill, but one taken sometimes. While no one said they would plan to pay any ransom, a small proportion (6%) of those surveyed indicated that they did. The relevance of this is that the modern security response playbook to ransomware events should likely include mechanisms to perform a payout. Incidentally, this also highlights the need for incident response to be a well-thought-out process involving adequate legal counsel.

Looking Ahead

The multiple drivers for change – be it the pandemic response or broader digital transformation efforts – are expected to persist moving forward. Security teams are constantly being asked to maintain – even improve – the organization's security posture regardless of how large or varied its technology estate becomes. The increased adoption of cloud-based technologies also introduces disruption in the form of distributed and elastic workloads, often deployed with limited oversight from security.

The survey data points to an outlook where existing security controls and approaches appear to be less effective than expected, particularly against ransomware. It's unlikely that there is a single cause for this: depending on the nuances of each organization, factors could include the level of sophistication of the threat actors, the placement of security controls in relation to the organization's workflows and infrastructure, or the effective level of maturity of the organization's security operations practices.

Moving forward, we expect organizations will need to rethink security approaches to catch attackers as soon as possible after initial compromise, but before they inflict severe damage or establish robust persistence. This will require a combination of protection technologies, properly deployed, detective controls that can provide actionable insights, and adequate response processes that can meet scale/speed demands.