MARSH

Ransomware Stats Every Business Needs to Know

Ransomware attacks are intensifying in frequency, severity, and sophistication — up 148% due to the wider attack surface and rise in remote work associated with the pandemic.

RANSOMWARE, BY THE NUMBERS

- Increase in ransomware attacks, fueled by the pandemic: **148%**
- Anticipated global ransomware recovery costs by the end of 2021: **$20 billion**
- Average ransom demand in Q4 2020: **$154,108** (-34% from Q3 2020)
- Average days of downtime in Q4 2020: **21 days** (+11% from Q3 2020)
- Percentage of ransomware in Q4 that included the threat to leak exfiltrated data: **70%** (+43% from Q3 2020)
- How quickly a new Remote Desktop Protocol (RDP) port — one of the top three ransomware attack vectors — is discovered after first connecting to the Internet: **90 seconds**
- How many misconfigured RDP ports are open to the Internet: **4.7 million**
- Average number of ransomware attacks that have occurred daily since January 1, 2016: **4,000**
- Email messages that contain malware (email phishing is also included in the top three ransomware attack vectors): **1 in 3,000**

What Does It All Mean?

The average ransom demand dropped in Q4 2020. Why? Cyber criminals are increasingly using the threat of data leakage to encourage ransom payments, but not necessarily deleting the exfiltrated data even if the ransom is paid. Ransomware victims are losing trust that their data will be safely deleted, and as such, are refusing to give in to cyber extortion.

While average ransom payment amounts declining is good news for companies, the volume of attacks is still increasing and data exfiltration remains a serious threat. To avoid payment, organizations must be able to effectively restore and recover their data and files — and their networks — from their back-ups or rebuild from scratch!

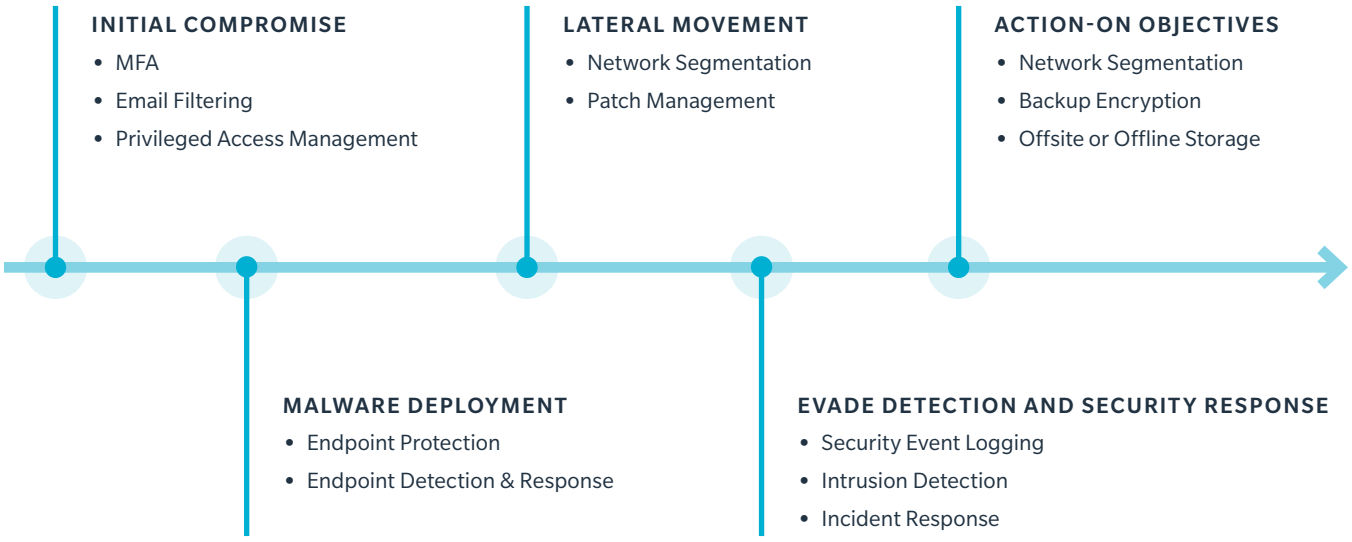
What Can You Do?

Preparation is key. With the continued threat of data exfiltration and prolonged downtime looming large, we recommend you carefully review your **backup strategy**. This includes examining what is backed up, where it's hosted, how often backups occur, and who is responsible and accountable for execution of the back-up strategy. Finally, it is important to exercise and test backup systems regularly.

Cyber insurance should not be overlooked: it can be a valuable tool in the fight against ransomware. Insurance may offer comprehensive coverage for ransom payments, associated costs, and access to vendors and it is also driving organizations to improve their security controls. Certain security controls are starting to be requirements for cyber insurance coverage, namely Multi-Factor Authentication (MFA).

In the fourth quarter, the top three attack vectors for ransomware included email phishing, RDP compromise, and software vulnerabilities. Controls can offer some protection against each attack vector, and at each stage of a ransomware attack. Below is an example of how a ransomware attack may be executed, as well as examples of just a few of the controls that can be helpful at each attack stage.

Timeline of a Ransomware Attack — And Compensating Controls



What Services Can Help Me?

Cyber risk management providers, brokers, and insurers can often provide cost-effective protection and a range of resources and services to help you prepare, respond, recover, and recoup losses from ransomware attacks. This may include:

PREPARATION:

- Cyber incident response planning and updating
- Evaluation of ransomware preparedness
- Cyber security framework and vulnerability assessments
- Employee training and education
- Cybersecurity best practices
- Cryptocurrency ransom payment support
- Analysis of financial impact
- Vendor identification

RESPONSE:

- Secure incident management services
- Vendor identification: including legal counsel, forensic experts, public relations support, and data restoration service providers
- Breach notification services
- Cryptocurrency ransom payment support
- Claims support for insurance recovery

RECOVERY:

- Event partnership and support, including claims support and advocacy
- Cyber insurance to cover lost revenue, extra expenses, and associated ransomware costs
- Proof of loss preparation and support
- Update/re-evaluation of incident response plans

COVERAGE FOR:

- Lost revenue and extra expenses to continue operations
- Restoration or recreation of corrupted or destroyed data and other intangible assets
- Network or hardware restoration or repair
- Regulatory fines and penalties
- Privacy events
- Reputational harm

Marsh Can Help:

Marsh's end-to-end suite of ransomware offerings include cyber risk management and insurance. A few highlights: we can help your organization prepare in advance of a ransomware attack, building and testing a complete cyber incident response plan. We can also design and deliver a cyber insurance policy with ransomware coverage tailored to your unique organization. Learn more about ransomware and how we can help you here.