Devolutions

Ransomware Rising: What's Happening & How to Protect Your Organization

THE TITLE OF THE SCARIEST BEAST ON THE CYBERTHREAT LANDSCAPE NOW BELONGS TO RANSOMWARE

It is not malware. It is not spyware. It is not Trojans. It is not even DDoS. No, according to experts the title of the scariest beast on the cyberthreat landscape now belongs to ransomware.

What is Ransomware?

Ransomware is a type of software that hackers use to prevent victims from accessing their own data. Unless victims comply with financial demands within a specified period, their data will be permanently erased (or at least, that is the chilling threat). In some cases, hackers also threaten to exploit and expose a victim's personal information on the dark web.

The amount of money that hackers demand varies. Interestingly, some hackers appear to have a basic sense of economics, in that they insist on smaller payments from individuals compared to organizations. This is not motivated by empathy. It is driven by practicality. Hackers know that organizations have bigger pockets. As such, an individual victim may be ordered to pay several hundred dollars (via a cryptocurrency such as Bitcoin that cannot be traced), while an organization may be ordered to pay tens or even hundreds of thousands of dollars.

Recent research has revealed that the average ransom paid out has climbed to $170,704 per incident (all figured USD). To make things even worse, only 8% of victims who pay a ransom get 100% of their data back. And so, why should victims comply with hackers' demands? Because the price of remediating a ransomware attack — including investigation, downtime, lost orders, operational costs, and other factors — has skyrocketed from $761,106 in 2020 to $1.85 million in 2021. Basically, most victims "do the math" and determine that it makes financial sense to pay less to hackers and get some or most of their data back vs. pay more in remediation costs and get none of their data back.

How Ransomware Works

While hackers are becoming increasingly sophisticated, the fundamentals of ransomware are fairly straightforward: once the malicious software downloads onto an endpoint or network, it encrypts data and adds an extension to files, which makes them inaccessible. There are various methods that hackers use to deploy ransomware, including:

- Embedded in macros (e.g., Word files)
- Spam email attachments
- Social engineering
- Malvertising
- Removable USB drives
- Chat messages
- Vulnerabilities in browser plug-ins ("drive-by attacks")

Ransomware Statistics

Earlier, we highlighted some alarming ransomware statistics. Unfortunately, there are some more chilling numbers to add to the conversation courtesy of PurpleSec:

- In 2021, an organization falls victim to a ransomware attack once every 11 seconds.
- Global ransomware costs are expected to reach $20 billion by the end of 2021.
- 20% of ransomware victims are SMBs.
- 85% of MSPs see ransomware as a common threat to SMBs.
- 50% of information security professionals who were surveyed do not believe their organization is prepared to deal with a ransomware attack.
- Most common types of ransomware: CryptoLocker (66%), WannaCry (49%), CryptoWall (34%), Locky (24%), Petya (17%), CryptXXX (14%), notPetya (12%)
- Most common operating systems targeted by ransomware: Windows (85%), MacOS (7%), Android (5%), iOS (3%)

Notable Attacks

Below are some of the biggest ransomware attacks in 2020 and 2021:

- ACER (ransom paid: $50 million)
- JBS Foods (ransom paid: $11 million)
- CWT Global (ransom paid: $4.5 million)
- Colonial Pipeline (ransom paid: $4.4 million)
- Brentagg (ransom paid: $4.4 million)
- University of California at San Francisco (ransom paid: $1.14 million)

And very recently on July 2, 2021, hackers attacked Kaseya IT and demanded that the management software firm pays a whopping $70 million — or else their corporate data, plus the data of hundreds of their customers, will be wiped out and/or exposed on the dark web.

How to Protect Your Organization

There is no way to 100% eliminate the risk of a ransomware attack. As long as there is going to be computing, there will be hackers.

However, there are some effective ways that organizations should — or frankly, given the potential consequences, they must — adopt to reduce their exposure and vulnerability. The Center for Internet Security (CIS) advises 15 actions:

1. Develop a comprehensive incident response plan, that clearly identifies what to do — and who should do it — in the event of a ransomware attack.
2. Implement a backup system that supports multiple iterations or archived data in case one copy of the backup has infected or encrypted files. Backups should also be regularly tested for data integrity and to ensure operational readiness.
3. Deploy anti-virus and anti-spam software, and add a warning banner/signature on all emails that reminds users about the dangers of clicking links and opening attachments.
4. If practical, disable script macros and force users to view rather than option files that are transmitted through email. Embedding malware inside Word/Excel macros is a common vector for ransomware attacks.
5. Keep all devices, software, hardware, and applications (including cloud locations) fully updated and patched, preferably through a centralized patch management system.
6. Use application whitelisting and software restriction policies to block the execution of programs in common ransomware locations (e.g., temporary folders).
7. Use a proxy server for Internet access.
8. Use ad blocking software.
9. Restrict access to common ransomware vectors, such as social networking sites and personal email accounts.
10. Implement the Principle of Least Privilege (POLP).
11. Implement network segmentation and zero-trust architecture.
12. Assess and monitor third parties who have access to the network, and ensure that they diligently follow cybersecurity best practices.
13. Participate in cybersecurity information sharing programs and organizations (e.g., MS-ISAC and InfraGard).
14. Provide end users with ongoing cybersecurity training on topics such as social engineering and phishing.
15. Implement a reporting plan that tells end users how and when to report unusual or suspicious activity.

Dealing with an Attack

The CIS also provides some advice on how to respond in the event of a ransomware attack:

- Immediately disconnect the infected system from the network.
- Determine whether affected data may require additional mitigation or reporting requirements (e.g., electronic protected health information).
- See if a decryptor such as No More Ransom! can help.
- Restore files from regularly maintained backups.
- Report the attack to the appropriate authority based on the country and jurisdiction. Organizations in the U.S. should contact the MS-ISAC, the FBI and/or the Internet Crime Complaint Center (IC3).

The Bottom Line

Organizations — including and especially SMBs — cannot afford to take a passive, wait-and-see stance when it comes to protecting themselves against ransomware, as the costs and consequences of an attack can be devastating. They must be proactive and strengthen their cybersecurity profile now rather than later. Adopting all the recommendations listed above will go a long way in helping organizations avoid falling victim to ransomware and other cyberthreats.