ustomer-inspired

enterprise solutions

RANSOMWARE: WHAT IS IT AND HOW TO PREVENT IT

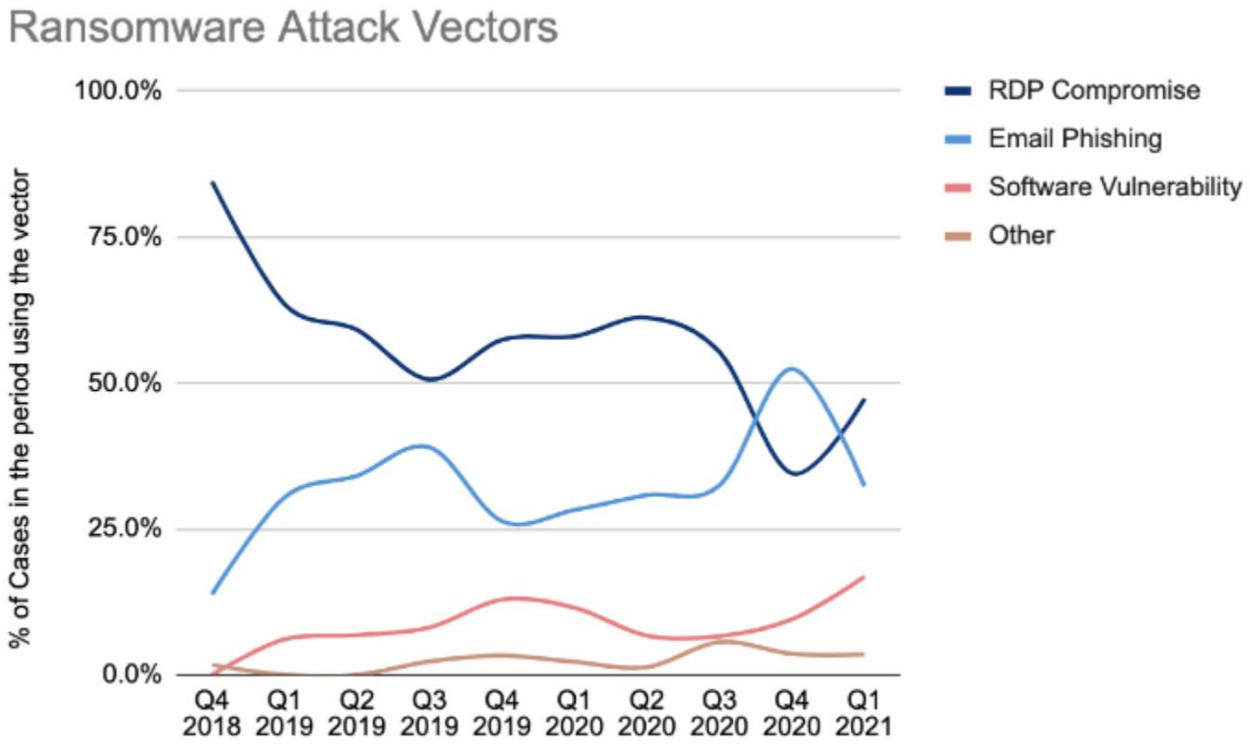
Today we will be covering:

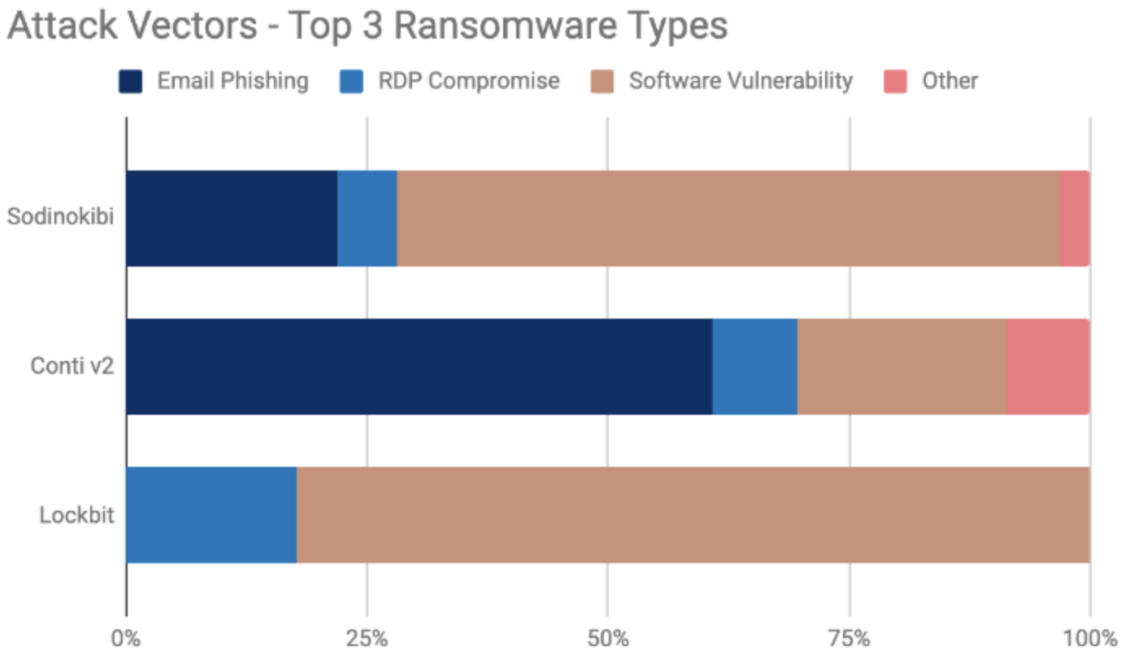
- What is Ransomware?
- Do you have some Ransomware attack examples?
- How much can a Ransomware attack cost?
- How do I prevent Ransomware?

RANSOMWARE – WHAT IS IT?

- Malware that encrypts files, servers and computers
- Ransomware spreads throughout your network via weak passwords, poor security restrictions, unpatched systems and lack of segmentation
- Ransomware attacks are up 119%
- The goal of ransomware is to require you to pay a ransom payment to the hacker typically through Bitcoin
- Once you have paid a ransom hackers will target you again, you must completely rebuild all systems

RANSOMWARE – WHAT IS IT?





RANSOMWARE– WHAT DOES IT COST?

Average Ransom Payment

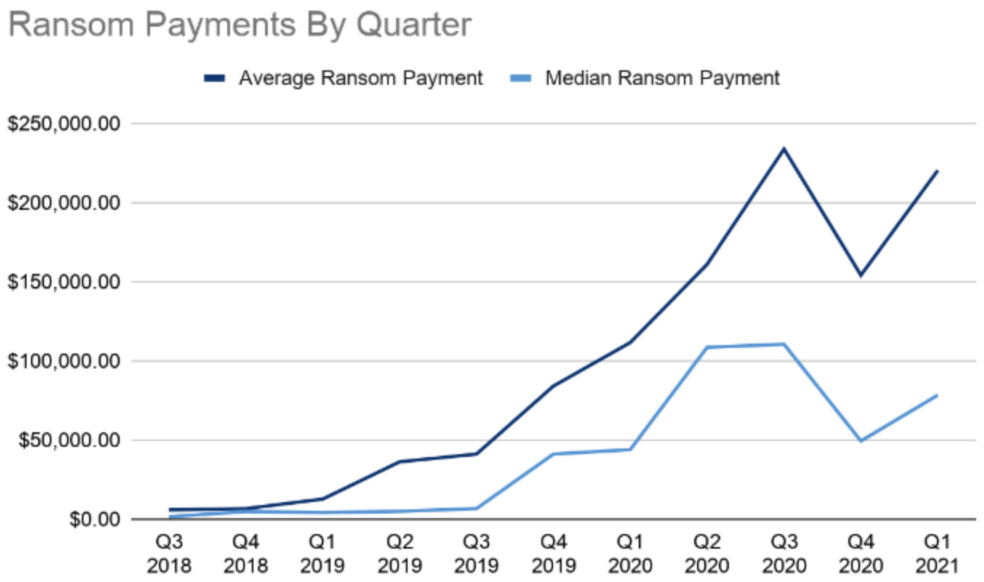
$220,298

+43% from Q4 2020

Median Ransom Payment

$78,398

+59% from Q4 2020



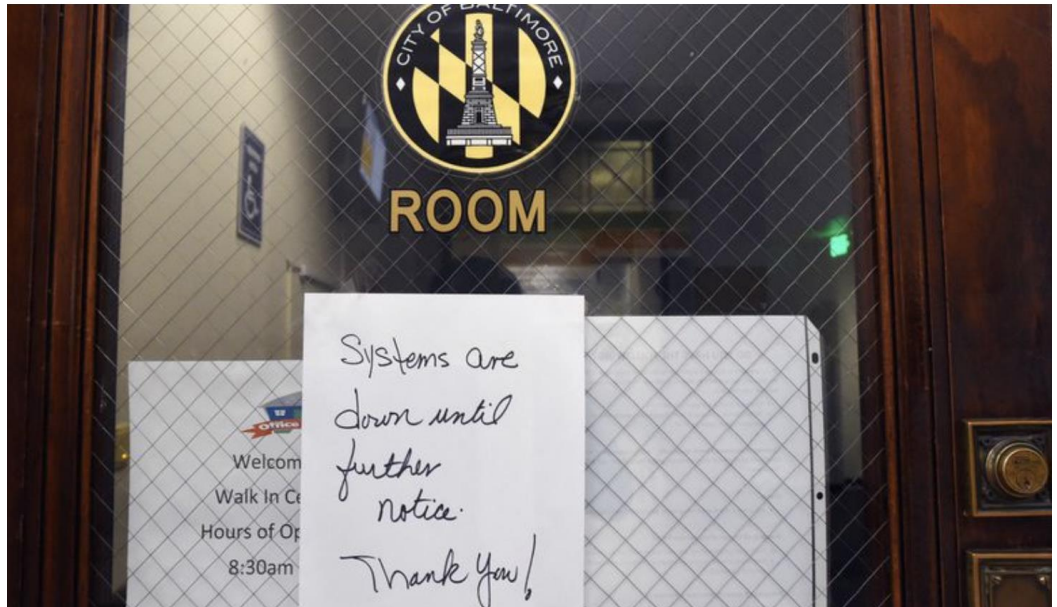
RANSOMWARE– WHAT DOES IT COST?

Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts

Ian Duncan

The Baltimore Sun |

May 29, 2019 | 7:45 PM



Colonial Pipeline paid $5 million ransom to hackers

PUBLISHED THU, MAY 13 2021•2:05 PM EDT | UPDATED THU, MAY 13 2021•6:38 PM EDT


Eamon Javers
@EAMONJAVERS


Amanda Macias
@AMANDA_M_MACIAS

SHARE

KEY POINTS

- Colonial Pipeline paid a ransom to hackers after the company fell victim to a sweeping cyberattack, one source familiar with the situation confirmed to CNBC.
- A U.S. official, who spoke on the condition of anonymity, confirmed to NBC News that Colonial paid nearly $5 million as a ransom to the cybercriminals.

RANSOMWARE– WHAT DOES IT COST?

Average Days of Downtime

23

+10% from Q4 2020

RANSOMWARE PREVENTION – TWO FACTOR AUTHENTICATION

- Two factor authentication requires a user to enter their password and then use an app to enter a code to complete authentication
- Two factor authentication is a must for all VPN connections or other remote access solutions
- Configure for all web email connections
- Consider it for administrative access
- Consider it for core applications

RANSOMWARE PREVENTION – LAYER 7 FIREWALL

- Basic firewalling is not enough to stop ransomware
- Advanced firewalls with properly configured rulesets and features are the first line of defense in preventing ransomware
- Limit your attack surface – Open only required inbound ports (Close RDP!!!)
- URL filtering for known attack sites
- File blocking to prevent known virus files
- Filter on DNS and unknown sites
- Use SSL decryption
- Keep your software up to date

RANSOMWARE PREVENTION – ENDPOINT PROTECTION

- Anti-virus software is not enough
- Software should have AI to detect new patterns
- Software should auto update from cloud
- Management and monitoring are key requirement and must be used by IT staff
- Install on all endpoints, including servers

RANSOMWARE PREVENTION – EMAIL FILTERING

- Verify Email source and destionation
  - Enable Sender Policy Framework (SPF) to detect forged email addresses
  - Enable DomainKeys Identified Mail (DKIM) to verify domains
  - Utilize DMARC with SPF and DKIM
- Configure advanced filtering policies
- Limit Office 365 admin access
- Require encryption for sensitive data
- Enable DLP rules
- Don’t share passwords in email

RANSOMWARE PREVENTION – IMPROVE WINDOWS SECURITY

- Limit administrator groups to only specified accounts
- Use separate accounts for administrative access
- Restrict user accounts to prevent full administrative rights to PCs
- Use the free toola from Microsoft
- Lockdown file servers using the principle of least privilege for file and share permissions
- Consider using OneDrive for user drives
- Use patch management software for all servers and desktops
- Restrict server Internet access
- Limit RDP access

RANSOMWARE PREVENTION – PROTECTED BACKUPS

- Backups should be taken regularly based upon RPOs
- Backup should allow for quick restores to overwrite encrypted data
- Many ransomware programs are now attacking backup servers and encrypting backup data
- Backup systems should not be joined to the domain
- Backups should be replicated to DR site and to the cloud
- Backup appliance should be air gapped from the network

RANSOMWARE PREVENTION – WHAT DID WE NOT COVER?

- Cybersecurity insurance
- Incident response
- Compliance
- Security policy
- Application security
- Post-incident recovery
- Tabletop Exercises
- Penetration Testing
- User Education

ustomer-inspired

enterprise solutions