Fighting Ransomware in Midsize Enterprises

Paul Furtado
Key Issues

• Midsize Enterprise Definition
• The Elephant in the Room — To Pay or Not to Pay
• How Much of a Threat Is Ransomware
• Why They Do It
• What Can You Do to Help Prevent It
• You’ve Been Hit, Now What?
Defining Midsize Enterprises
The Midsize Enterprise Operational Environment

100 Employees
$50 Million

500 Employees
$500 Million

1,000 Employees
$1 Billion

<$20M
IT Budget

<30
IT Staff

57%
No CISO

5.3%
IT Spending as a Percentage of Revenue

4.9%
IT Security Spending as a Percentage of IT Budget

25%
IT Budget Spent on Cloud (IaaS, PaaS, SaaS)
To pay or not to pay ... That is the Question.
To Pay or Not to Pay

It’s a Business Decision!

payment should be a last resort

“The FBI encourages victims to not pay a hacker’s extortion demands. The payment of extortion demands encourages continued criminal activity, leads to other victimizations, and can be used to facilitate additional serious crimes.”
To Pay or Not to Pay

It’s a Business Decision!

But Remember
All Bitcoin transactions are public, traceable and permanently stored in the Bitcoin network.
Payment increases your chances of being targeted again.

Payment Is No Guarantee of Recovery
How Much Do I Have to Pay?

$178,254
average ransomware payment for 1Q20

Does not include downtime costs
5-10x of the actual ransom amount

Source: Coveware Ransomware 2Q20 Report

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.
How Much Do I Have to Pay?

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Ransom</th>
<th>+/- Qtr/Qtr</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Q18</td>
<td>$5,593</td>
<td></td>
</tr>
<tr>
<td>4Q18</td>
<td>$6,733</td>
<td>20.4%</td>
</tr>
<tr>
<td>1Q19</td>
<td>$12,762</td>
<td>89.5%</td>
</tr>
<tr>
<td>2Q19</td>
<td>$36,295</td>
<td>184.4%</td>
</tr>
<tr>
<td>3Q19</td>
<td>$41,198</td>
<td>13.5%</td>
</tr>
<tr>
<td>4Q19</td>
<td>$84,116</td>
<td>104%</td>
</tr>
<tr>
<td>1Q20</td>
<td>$111,605</td>
<td>33%</td>
</tr>
<tr>
<td>2Q20</td>
<td>$178,254</td>
<td>60%</td>
</tr>
</tbody>
</table>

Source: Coveware Ransomware 2Q20 Report
What Happens When You Pay?

96% Recovered

4% Lost

16 days
Average number of days to remediate ransomware incident

Source: Coveware Ransomware 1Q20 Report
How Much of a Threat Is Ransomware?
Ransomware Threat Level

Ransomware Increase in March 2020

148%

Source: Carbon Black, Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks
Primary Payload Delivery Mechanisms

- Spear Phishing
- Remote Desktop Connection Compromise
- Malware Wrappers
Deployment Timelines

Dwell time

In most cases, at least **3 days** passed between the first evidence of malicious activity and the ransomware deployment.

After-Hours Deployment

In **76%** of cases, ransomware was deployed outside working hours.

Source: FireEye
A business will fall victim to a ransomware attack every 14 seconds by 2019, and every 11 seconds by 2021.

Source: CyberSecurity Ventures, 2019 Annual Cybercrime Report
1Q20 Malware Increase vs. 4Q19

- **Mobile**: 71%
- **Linux**: 8%
- **Mac OS**: 51%
- **PowerShell**: 689%

Source: McAfee Labs Threat Report (July 2020)
Ransomware Threat Level

Cognizant expects to lose between $50M and $70M following ransomware attack.

May 2020

Travelex Paid $2.3 Million to Ransomware Gang.
April 2020

Carnival Cruise Lines Gets Hit With Ransomware Attack
August 2020

Carnival detected a ransomware attack on one of its brands that accessed and encrypted its information technology system. The company said it believes personal data of its guests and employees were accessed in the attack.
The Scary Part

Doppelpayner

Your network has been penetrated.

This link and your decryption key will expire in 21 days after your systems were infected. Clicking this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in your network have been encrypted with flawless algorithm. Backups were either encrypted or deleted and backup disks were formatted. There is no working decryption software that may solve this. Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of certain files.

Also, we have gathered all your private sensitive data. If you do not have to pay, we would share it. It may harm your business reputation.

Attention!

What happened?

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have created a list of what files were encrypted. We do not hijack your data. This data will be released. If you want to release the data, we can assist you and use a guest, then you can negotiate.

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers. To contact us and purchase the key you have to visit our website in a hidden Tor network.

Source: Coveware Blog, 2020
Why Do They Do It?
What’s My Data Worth?

Accounts

• Restaurant/Retailer Gift Cards: 15%-50% of value

• Hotel Loyalty Programs: $10-$20

• Login Credentials: $3-$30

• Email Accounts: $1-$15
What’s My Data Worth?

Identities

- Stolen Identity (Name, DOB, SSN): $0.10-$1.50
- ID/Passport Scans: $1-$35
- Scanned Documents (Utility Bill, etc.): $0.50-$45
- Full ID Packages (Name, Address, SSN, Email, Bank Acct., etc.): $30-$100
Hired Guns

Malware

- Cryptocurrency Miner: $10-$200
- Office/O365 Macro Downloader Generator: $5-$10
- Ransomware Toolkit: $0-$250
Hired Guns

Services

- Hacker for Hire: $100+
- Custom Phishing Page: $3-$12
- DDoS Short Duration <1 hour: $5-$20
- DDoS Short Duration >24 hour: $10-$1,000
Hired Guns

Social Media

- 100 Likes on Social Media: $0.13-$3
- 500 Social Media Followers: $2-$6
- 100K Social Media Video Views: $200-$250
What Can You Do?
Good News

The good news:
– It can be defended against in the same way as malware

• The effects are very different:
  – Data is encrypted and decryption key not made available until ransom is paid

• But … fundamentally operates exactly the same as typical malware:
  – It enters the organization the same way as malware
  – It propagates the same way as malware
More Good News

You **don’t** always need to spend more money!

Do The Fundamentals Well!

PEOPLE

PROCESS

TECHNOLOGY
Common Failure Points

Employees and Users

Awareness Training

• Not a “one and done” scenario
• Better to have smaller, repeated increments than one long session
• Use digital signage/TVs
• Trickle marketing
• Same rules for all staff
Common Failure Points

Spam Filter

- Implement URL protection
- Use email/attachment sandboxing
- Actively block bad domains
Common Failure Points

Endpoint Protection

- Disable USB storage access
- Use tools that implement non-signature technologies — heuristics, behavioral monitoring, AI/ML
- Update your EPP in a timely fashion
Common Failure Points

Web Filter/Firewalls

- Enable gateway antivirus
- Block risky file extensions (javascript, vbscript, powershell, etc …)
- Use HTTPS filtering
- Block unnecessary ports
Common Failure Points

57% of organizations that had a breach found the root cause to be a known vulnerability.

Poor Patching

56% of known vulnerabilities are not patched within 90 days of release.

53% of ransomware vulnerabilities had a CVSS v.2 score of <8.0.
Common Failure Points

Insufficient Backups
Common Failure Points

Close Open Doors

• Block unnecessary ports on endpoints
• Implement strong IAM policies including MFA
• Implement PAM solutions or monitoring of administrator and system accounts
I’ve Been Hit!
Now What?
8 Steps for Ransomware Response

1. Isolate the system(s)
2. Identify point of entry and then close it
3. Identify time of entry
4. Prepare a new device from image
5. Scan backups to ensure no infection
6. Restore files to a time prior to infection
7. Investigate all systems in contact with the impacted resource
8. Conduct a post-incident review
Free Decryption Tool

NO MORE RANSOM!

No More Ransom
Third-Party Resources

1. Engage with legal counsel
2. Utilize MSSP/MDR providers as part of your security team
3. Have an incident response retainer with a third-party company
4. Engage with your insurance provider (if applicable)
5. Engage with law enforcement where necessary
Summary
Cost-Effective and High Value Security in an Era of Uncertainty

Low Cost/No Cost Security:

1. Ransomware prevention is doable and manageable
2. Do the fundamentals well
3. Ensure you have adequate backups of all critical data
4. Get outside help if you can’t do it yourself!
**Action Plan**

**Next Week**
- *Validate* you have a comprehensive incident response plan
- *Ensure* you have backups of all critical data

**Next Month**
- *Prepare* a tabletop exercise for ransomware — partial and full scenarios
- *Review* your awareness training and modify accordingly

**Next Quarter**
- *Test* your tabletop exercise with your incident response plan
- *Adjust/correct* IRP as required
“The only thing harder than defending yourself against ransomware is explaining to your CEO and customers why you didn’t protect yourself from an attack”
Recommended Gartner Research

- How to Respond to the 2020 Threat Landscape
  John Watts (G00719273)

- Defend Against and Respond to Ransomware Attacks
  Brad LaPorte and Paul Webber (G00463878)

- How to Prepare for and Respond to Business Disruptions After Aggressive Cyberattacks
  Roberta Witty, Michael Hoeck and David Gregory (G00405082)
Thank You!

Paul Furtado, CISM, CGSK
Sr. Director, Analyst

✉️ p.furtado@gartner.com
LinkedIn: www.linkedin.com/in/paulfurtado
Twitter: @ciofurtado