Last Line of Defense

Hardening Backup Systems Against Ransomware
We enable dynamic, collaborative cross-team intelligence for better engagements.

We believe unique security challenges require creative engagements.

We help you gain the ultimate advantage through our dedicated research team.

We believe in creating effective security progress through empathy and doing right.

Our industry leaders and tool creators do the hands-on work.
Best-In-Class Consultants

Meet Full-Service Security Offerings

- Security Testing & Analysis
  - Penetration Testing
  - Red/Blue/Purple Team
  - Web/Mobile Testing
  - IoT/Hardware Assessment

- Program Assessment & Compliance
  - Business Risk Assessment
  - Security Program Assessment
  - PCI Assessment

- Security Program Management
  - Program Building
  - Policy Development
  - Virtual CISO

- Remediation Assistance & Training
  - Remediation Services
  - Cloud Configuration Review
  - Defensive Backup
  - Infrastructure Assessment
  - Security Training & Education

- Incident Response & Forensics
  - Incident Response
  - Threat Hunting
  - Tabletop Exercises
  - Malware Analysis

---

TrustedSec
Overview
Ransomware groups attempt to destroy backup systems to cripple their victims and force payouts.

In this webinar, Mike Owens and Paul Sems from the TrustedSec Remediation Team will conduct threat modeling for these kinds of attacks on backups, identify common protection gaps, and provide hands-on best practices for hardening backup systems against ransomware.

“Hardened, trustworthy backups are the difference between disaster and disaster recovery.”
Threat Model:

ASSUME BREACH!
Threat Model: Assume Breach

- A ransomware group gained access to the network.
- They elevated to Domain Administrator privileges.
- They infected all systems on the network.
- They attempted to corrupt all identified backups.
- Finally, they detonated the ransomware.

"Pay them," they tell you, "or else..."
## Threat Model: Assume Breach

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Servers</td>
<td>Encrypted</td>
</tr>
<tr>
<td>File Systems</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Critical Applications</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Workstations</td>
<td>Encrypted</td>
</tr>
</tbody>
</table>
The 23 BTC ($1,000,000) Question is...

Did the attacker get to your backups?  
Or do you have a chance to recover?
Disaster... Yes
Recovery... ???
Disaster Recovery

Human-Operated Ransomware is a Different Beast

- **Traditional:** Disaster Recovery designed for system failures and Acts of God.
- **Now:** Human-operated ransomware **actively targeting backups** for destruction.
How Ransomware Works

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

Source: https://www.cert.govt.nz/business/guides/protecting-from-ransomware/
Attack on Irish National Health Service

In May 2021, a Conti ransomware infection shut down the Irish Health Service Executive IT systems across the country.

80% of the HSE’s environment was encrypted, causing a severe and long-lasting disruption to healthcare services.

Irish HSE Recovery Timeline

It took the Irish Health Service Executive four months to recover all systems from the attack.


Without the decryption key ... it is highly likely that the recovery timeframe would have been considerably longer.
The Considerations
... Do you have ‘em?
... Can you use ‘em?
... Are they hardened?
... Are you watching?
The Controls
Got Backups?
Primary, Off-Site, and Off-Network

- Critical information systems identified
- Driven by business requirements and risk tolerance
- Off-Site is limited value against ransomware
- Off-Network is REALLY OFF-NETWORK
  i.e., inaccessible to attackers who control the production network & infrastructure
Can You Recover...

... From primary backup?
... From off-site?
... From off-network?

What if the entire network is encrypted?
Check your hidden dependencies!
Harden Against Crypto-Malware

- Lock down configuration
- Block ports and protocols
- Patch application and firmware
- Network segmentation, isolation

Applies to all three backup locations!
Compromised Administrator Protections

- Limit admins with access
- Strong Authentication
- Isolate the AD group
- Consider separate domain!
- Access to off-network backup should NOT be linked to Active Directory, on-network resources
When the attackers have access to the domain admin account there is little (we) can do to protect our installation.

That’s why (we) usually recommend using a separate domain to run backup software, this could protect (our) instance in case of the primary domain is compromised.
Protect Against Modification or Deletion

- Single user should not be able to modify or delete backups!
- Immutability protections:
  - Time-based retention settings
  - Requiring multiple administrators
- Protect against backup poisoning
Backup Monitoring and Alerting

If a tree falls in the forest...
Monitoring Backup Process Issues

- Health of backup processes
- Administrator logins (and failures!)
- Modified or deleted backup jobs

What constitutes a security event?
When does the security team get involved?
Questions?
The information security industry is constantly evolving — keep up by following TrustedSec's active social media, blogs, podcasts, and webinars.

www.TrustedSec.com/blog
Presenters

Paul Sems
Managing Director of Remediation Services
paul.sems@trustedsec.com

Mike Owens
Security Consultant Remediation Team
mike.owens@trustedsec.com
References and Additional Reading


Thank You!