EXECUTIVE SUMMARY

Critical Cybersecurity Incident Response Report

Ransomware Attack & 8-Month System Compromise

Ishwar Retail - November 2025

CRITICAL ALERT: URGENT EXECUTIVE BRIEFING

Date: November 20, 2025

Classification: CONFIDENTIAL - Public Release

Severity: CRITICAL

Status: INCIDENT CONTAINED - RECOVERY IN PROGRESS

INCIDENT OVERVIEW

What Happened

Your organization experienced a **sophisticated, multi-phase cyberattack** involving:

1. **8-Month Unauthorized Access** (February - October 2025)
2. **Social Engineering Attack** - Fake technical support impersonation
3. **Ransomware Deployment** - Professional-grade encryption malware
4. **Complete System Compromise** - Business-critical files encrypted

Key Facts

Metric	Details
Attack Discovery	**October 27, 2025**
Initial Breach	**February 2025 (estimated)**
Breach Duration	**8 months undetected**
Ransomware Deployed	**October 27, 2025, 20:09 PM IST**
Files Encrypted	**187+ business-critical files**
Systems Affected	**GINESYS ERP, Financial Records, Customer Data**
Threat Actor	**Netekan (LockBit Variant Operator)**
Ransom Demanded	**Contact via Telegram: @Dy_supa**

🎯 HOW THE ATTACK HAPPENED

Phase 1: Social Engineering (February 2025)

The Call:

```
• Attacker called posing as "GINESYS Technical Support"
• Claimed urgent system updates/maintenance required
• Convinced staff to install remote access software
• Gained full administrative access to systems
```

Red Flags Missed:

- ✖ No verification of caller identity
- ✖ Unauthorized software installation (ScreenConnect)
- ✖ Administrative access granted to unknown party
- ✖ No IT security approval process

Phase 2: Silent Infiltration (February - October 2025)

8 Months of Unauthorized Access:

```
• Attacker maintained persistent backdoor access
• Reconnaissance of business systems
• Credential harvesting
• Data exfiltration (likely but unconfirmed)
• Identification of critical assets
• Planning ransomware deployment
```

Evidence Found:

- ✓ 30+ ScreenConnect installations (October 27-28)
- ✓ 3 AnyDesk installations (October 27-28)
- ✓ 2 UltraViewer installations (October 27-28)
- ✓ Browser history analysis confirms suspicious activity
- ✓ Timeline reconstruction shows 8-month access window

Phase 3: Ransomware Deployment (October 27, 2025)

Attack Execution Timeline:

Time	Event	Impact
20:09 PM	**Attacker uploads "WhatsApp Installer.exe"**	**Malware staged**
20:09 PM	**10 identical copies created (redundancy)**	**Backup deployment**
20:15 PM	**Ransomware execution begins**	**Encryption starts**
20:15 PM	**Shadow copies deleted (recovery prevention)**	**Backups destroyed**
20:15-20:19 PM	**Mass file encryption (187+ files)**	**Data loss**
20:19 PM	**Ransom notes deployed**	**Extortion begins**

Technical Details:

- **Malware:** Custom LockBit Black variant "Netekan"
- **Encryption:** ChaCha20 + RSA-4096 (military-grade)
- **File Extension:** .U3QL0GAyM
- **Victim ID:** EFE4C8C2C98D1E57791E6EBEC7BB48A1

💥 BUSINESS IMPACT ASSESSMENT

Critical Systems Affected

1. GINESYS ERP System

- ✗ Business operations halted
- ✗ Inventory management inaccessible
- ✗ Point of sale disrupted
- ✗ Supply chain visibility lost

2. Financial Systems

- ✗ Accounting records encrypted
- ✗ Banking data inaccessible
- ✗ Financial reporting disabled
- ✗ Audit trail compromised

3. Customer Data

- ✗ Customer records encrypted
- ✗ Contact information inaccessible
- ✗ Order history lost
- ✗ Privacy breach potential

4. Business Documents

- ✗ Contracts and agreements
- ✗ Employee records
- ✗ Tax documents
- ✗ Operational procedures

Financial Impact

Direct Costs:

- Forensic investigation and incident response
- IT system recovery and rebuilding
- Data recovery attempts
- Legal and compliance costs
- Potential ransom payment (NOT RECOMMENDED)

Indirect Costs:

- Business downtime and lost revenue
- Employee productivity loss
- Customer trust and reputation damage
- Regulatory fines (if data breach confirmed)
- Increased insurance premiums

Estimated Total Impact: High - Business-critical disruption

🔍 ROOT CAUSE ANALYSIS

Security Failures Identified

1. ✗ NO SECURITY AWARENESS TRAINING

- Staff fell victim to social engineering
- No verification procedures for support calls
- Trusted unknown callers claiming to be technical support

2. ✗ NO ANTIVIRUS / ENDPOINT PROTECTION

- Malware executed without detection
- No real-time threat prevention
- No behavioral analysis or sandboxing

3. ✗ ADMINISTRATOR ACCOUNT MISUSE

- Daily operations with full admin privileges
- Ransomware gained unrestricted system access
- No principle of least privilege

4. ✗ NO BACKUP STRATEGY

- Backups stored on same system (encrypted!)
- No offline or cloud backups
- No 3-2-1 backup rule implementation

5. ✗ NO EMAIL/WEB FILTERING

- Phishing attacks reaching users
- No link/attachment scanning
- No URL reputation checking

6. ✗ NO NETWORK MONITORING

- 8 months of unauthorized access undetected
- No anomaly detection
- No security information and event management (SIEM)

7. ✗ NO INCIDENT RESPONSE PLAN

- No procedures for breach response
- Delayed detection and containment
- No forensic preservation protocols

🛡 THREAT ACTOR PROFILE

Attacker Information

Alias: Netekan

Affiliation: LockBit Ransomware-as-a-Service (RaaS)

Contact Methods:

- Telegram: @Dy_supa
- Email: Netekan@keemail.me
- Email: Sir.silentloki@tutanota.com

Sophistication Level: Medium-High

- Professional ransomware operation
- 8-month reconnaissance period
- Strong encryption implementation (RSA-4096)
- Multiple communication channels
- Anonymous infrastructure

Motive: Financial extortion

- Ransom payment demanded
- No ideological or political agenda
- Part of organized cybercrime network

Tactics:

- Social engineering (technical support impersonation)
- Long-term persistent access (8 months)
- Remote access tool deployment
- Shadow copy/backup deletion
- Professional-grade encryption
- Anonymous communication channels

🔐 ENCRYPTION ANALYSIS & RECOVERY OPTIONS

Decryption Verdict: IMPOSSIBLE WITHOUT ATTACKER'S KEY

Encryption Method:

```
1. File encrypted with ChaCha20 (fast symmetric encryption)
2. ChaCha20 key encrypted with RSA-4096 public key
3. RSA private key held by attacker only
4. Mathematically unbreakable without private key
```

Why Decryption is Impossible:

- RSA-4096 provides 2^4096 possible keys
- Would take thousands of years to crack with current technology
- Quantum computers cannot break RSA-4096 yet
- No known vulnerabilities in this encryption implementation
- Public key is embedded in malware (won't help decrypt!)
- Private key is on attacker's server only

Recovery Options Assessment

Option 1: Pay Ransom ✗ NOT RECOMMENDED

- No guarantee of decryption key
- Funds criminal operations
- May be illegal in your jurisdiction
- You become target for future attacks
- Ethical and legal concerns

Option 2: File Recovery (PhotoRec/TestDisk) ✓ RECOMMENDED

- Success Rate: 30-60% for deleted/lost files
- Free, open-source tools
- Can recover file fragments
- Non-destructive process
- Best realistic option

Option 3: Shadow Copy Recovery ✗ NOT POSSIBLE

- Ransomware deleted all shadow copies
- vssadmin delete executed during attack
- No Windows restore points available
- Confirmed via forensic analysis

Option 4: Backup Restoration ✗ NOT AVAILABLE

- On-system backups were encrypted
- No offline backups found
- No cloud backup configured
- Critical backup failure

Option 5: Law Enforcement Assistance ✓ RECOMMENDED

- Report to FBI IC3 / local cybercrime unit
- Potential key recovery if attacker caught
- Contribute to threat intelligence
- Required for insurance claims

📊 COMPREHENSIVE FORENSIC FINDINGS

Digital Evidence Collected

Malware Sample:

- File: WhatsApp Installer.exe
- MD5: 1e70f04efea4307e62b3c51006c617ce
- Size: 1,096,224 bytes (1.04 MB)
- Type: PE32 .NET Assembly
- Classification: LockBit Black variant "Netekan"

Encrypted Files:

- Extension: .U3QL0GAyM
- Count: 187+ files affected
- Types: .mdf, .ldf, .xlsx, .docx, .pdf, .jpg, etc.
- Locations: C:\backserv\, C:\inetpub\, C:\IMPBACK\

Ransom Note:

- File: U3QL0GAyM.README.txt
- Victim ID: EFE4C8C2C98D1E57791E6EBEC7BB48A1
- Contact: Telegram @Dy_supa
- Language: English with grammar errors (non-native speaker)

Attack Timeline Evidence:

- Browser history (Chrome database analyzed)
- File timestamps (NTFS metadata)
- Download records (30+ remote access tools)
- System event logs
- Recent files and shortcuts

Remote Access Evidence:

- ScreenConnect: 30+ downloads (Oct 27-28)
- AnyDesk: 3 downloads (Oct 27-28)
- UltraViewer: 2 downloads (Oct 27-28)
- Pattern indicates attacker control

Key Investigation Findings

1. Attack Vector Confirmed:

- Social engineering call (fake GINESYS support)
- Remote access tool installation (ScreenConnect)
- 8-month persistent unauthorized access
- Manual ransomware deployment

2. Data Exfiltration Risk:

- 8 months of system access = HIGH risk of data theft
- No direct evidence found (attacker covered tracks)
- Must assume customer/financial data stolen
- Regulatory notification may be required

3. Backup Failure:

- All backups on same system (encrypted)
- No offline/offsite backups
- Critical business continuity failure
- Violates backup best practices

4. Shadow Copy Deletion:

- Ransomware executed: vssadmin delete shadows /all /quiet
- All Windows restore points removed
- Only 12-byte metadata shell remains
- Recovery via shadow copies impossible

5. Security Control Failures:

- No antivirus/EDR detected malware
- No firewall blocked remote access
- No SIEM alerted on suspicious activity
- No user training prevented social engineering
- Multiple layers of defense absent

⚡ IMMEDIATE ACTIONS REQUIRED

Critical Actions (Next 24-48 Hours)

1. CONTAIN THE INCIDENT ✓ COMPLETED

- ✓ Disconnect affected systems from network
- ✓ Disable compromised accounts
- ✓ Block attacker contact methods
- ✓ Preserve forensic evidence

2. START FILE RECOVERY ⚠ URGENT

- Begin PhotoRec recovery on affected drives
- Check for any unencrypted backups
- Scan external drives and USB devices
- Recover deleted files before overwrite
- **TIME-CRITICAL:** Start immediately!

3. REPORT TO AUTHORITIES ⚠ REQUIRED

- File report with FBI IC3 (www.ic3.gov)
- Contact local cybercrime unit
- Report to state/national cybersecurity agency
- Required for insurance claims

4. NOTIFY STAKEHOLDERS

- Inform executive leadership
- Brief IT/security teams
- Prepare customer notification (if data breach)
- Contact cyber insurance provider
- Engage legal counsel

5. CHANGE ALL CREDENTIALS

- Reset all passwords from clean device
- Revoke remote access permissions
- Update admin credentials
- Implement multi-factor authentication
- **Do this from uncompromised system!**

🛡 RECOVERY & REMEDIATION PLAN

Short-Term Recovery (This Week)

Phase 1: File Recovery

```
1. PhotoRec file recovery on all affected drives
2. Manual search for unencrypted copies
3. Check cloud storage for synchronized files
4. Recover from any discovered backups
5. Prioritize business-critical data
```

Phase 2: System Rebuilding

```
1. Format and reinstall Windows on affected systems
2. Apply all security updates and patches
3. Install endpoint protection (EDR/antivirus)
4. Restore recovered files to clean systems
5. Test business application functionality
```

Phase 3: Security Hardening

```
1. Implement principle of least privilege
2. Enable Windows UAC (User Account Control)
3. Deploy email/web filtering
4. Configure firewall rules
5. Disable unnecessary services
```

Long-Term Security Improvements (30-90 Days)

1. BACKUP STRATEGY - CRITICAL

- Implement 3-2-1 backup rule:
- 3 copies of data
- 2 different media types
- 1 copy offsite/offline
- Deploy automated cloud backup
- Test backup restoration monthly
- Store backups offline (air-gapped)

2. ENDPOINT PROTECTION

- Deploy EDR solution (CrowdStrike, SentinelOne, etc.)
- Enable real-time threat detection
- Configure behavioral analysis
- Implement application whitelisting
- Regular malware scanning

3. EMAIL SECURITY

- Deploy email filtering (Mimecast, Proofpoint)
- Enable SPF, DKIM, DMARC
- Scan all attachments
- Implement link protection
- Quarantine suspicious emails

4. NETWORK SECURITY

- Deploy next-gen firewall
- Implement network segmentation
- Monitor network traffic (SIEM)
- Deploy intrusion detection (IDS/IPS)
- VPN for remote access only

5. ACCESS CONTROL

- Implement multi-factor authentication (MFA)
- Principle of least privilege
- Regular access reviews
- Privileged access management (PAM)
- Disable unnecessary admin accounts

6. SECURITY AWARENESS TRAINING

- Mandatory cybersecurity training for all staff
- Phishing simulation exercises
- Social engineering awareness
- Incident reporting procedures
- Quarterly security refreshers

7. INCIDENT RESPONSE PLAN

- Document IR procedures
- Define roles and responsibilities
- Establish communication protocols
- Conduct tabletop exercises
- Maintain forensic readiness

8. MONITORING & DETECTION

- Deploy SIEM solution
- 24/7 security monitoring
- Anomaly detection
- Threat intelligence feeds
- Regular security audits

💰 COST-BENEFIT ANALYSIS

Investment in Security vs. Incident Cost

Current Incident Costs:

- Forensic investigation: $10,000 - $50,000
- System recovery: $20,000 - $100,000
- Business downtime: $50,000 - $500,000+
- Legal/compliance: $10,000 - $100,000
- Reputation damage: Incalculable
- **Total: $90,000 - $750,000+**

Preventive Security Investment:

- Endpoint protection: $50 - $100 per user/year
- Email filtering: $30 - $80 per user/year
- Backup solution: $500 - $5,000/year
- Security training: $100 - $500 per user/year
- SIEM/monitoring: $10,000 - $50,000/year
- **Total: $20,000 - $80,000/year**

ROI: Prevention costs 5-10% of incident response costs

REGULATORY & LEGAL CONSIDERATIONS

Compliance Requirements

Data Breach Notification:

- If customer data was stolen → Notification required
- Timeline: 30-72 hours in most jurisdictions
- Notify: Customers, regulators, credit bureaus
- Document: What data, how many affected, remediation

Regulatory Bodies:

- Data protection authorities (GDPR if applicable)
- Industry regulators (financial, healthcare)
- Law enforcement (FBI, local cybercrime)
- Insurance providers

Legal Considerations:

- Preserve all evidence (chain of custody)
- Attorney-client privilege for communications
- Potential liability for data breach
- Insurance claim filing requirements
- Contractual obligations to customers/partners

KEY RECOMMENDATIONS

Executive Decision Points

1. DO NOT PAY RANSOM

- No guarantee of decryption
- Funds criminal operations
- Ethical and legal concerns
- Makes you future target

2. FOCUS ON RECOVERY

- PhotoRec file recovery (best option)
- Rebuild systems from scratch
- Restore from any available backups
- Prioritize business-critical systems

3. INVEST IN SECURITY

- This attack was 100% preventable
- Basic security controls would have stopped it
- Cost of prevention < Cost of incident
- Protect against future attacks

4. REPORT TO AUTHORITIES

- Legal requirement in most cases
- Helps catch attackers
- Contributes to threat intelligence
- Required for insurance claims

5. IMPLEMENT SECURITY PROGRAM

- 30-day security improvement plan
- 90-day comprehensive security overhaul
- Ongoing monitoring and maintenance
- Regular training and awareness

📞 NEXT STEPS & CONTACTS

Immediate Actions Checklist

- [ ] Review this executive summary with leadership
- [ ] Approve emergency budget for recovery
- [ ] Start PhotoRec file recovery TODAY
- [ ] Report to FBI IC3 and local authorities
- [ ] Engage cybersecurity professionals for remediation
- [ ] Notify customers if data breach confirmed
- [ ] File insurance claim
- [ ] Implement short-term security improvements
- [ ] Schedule security training for all staff
- [ ] Develop 90-day security improvement plan

Contact Information

Incident Response Team:

Aman Rajak

Cyber & Tactical Technology Chief Technology Officer

Tech Sanrakshanam, SHOR Foundation

Law Enforcement:

- FBI IC3: www.ic3.gov
- Local Cybercrime Unit: [Contact Information]

Cybersecurity Resources:

- CISA: www.cisa.gov
- No More Ransom: www.nomoreransom.org
- US-CERT: www.us-cert.gov

📊 APPENDIX: TECHNICAL DETAILS

Threat Intelligence

Indicators of Compromise (IOCs):

- MD5: 1e70f04efea4307e62b3c51006c617ce
- File: WhatsApp Installer.exe
- Extension: .U3QL0GAyM
- Victim ID: EFE4C8C2C98D1E57791E6EBEC7BB48A1

Threat Actor TTPs:

- MITRE ATT&CK: T1566 (Phishing)
- MITRE ATT&CK: T1219 (Remote Access Software)
- MITRE ATT&CK: T1486 (Data Encrypted for Impact)
- MITRE ATT&CK: T1490 (Inhibit System Recovery)

Contact Methods:

- Telegram: @Dy_supa
- Email: Netekan@keemail.me
- Email: Sir.silentloki@tutanota.com

Report Attribution

Prepared and Published By:

Aman Rajak

Cyber & Tactical Technology Chief Technology Officer (CTO)

Tech Sanrakshanam

SHOR Foundation

Date: November 20, 2025

Document Version: 2.0 - Comprehensive Executive Release

Classification: Public Document

This executive summary has been prepared for leadership decision-making and public awareness regarding cybersecurity incidents, incident response, and security best practices.

END OF EXECUTIVE SUMMARY

For complete technical details, forensic analysis, and investigation findings, refer to the Full Incident Report (122 pages).