Ransomware has evolved. It was once automated malware that haphazardly encrypted data. The current generation of ransomware is a strategic campaign of data exfiltration and extortion with ransom as an afterthought. Ransomware campaigns initially use live-off-the-land techniques combined with specialty tools that are highly obfuscated to avoid detection. Dwell times average in the 4-6 week range as attackers curate data exfiltration for maximum impact. Victims who refuse to pay extortion must prepare for public disclosures of exfiltrated data.

The economics of ransomware are evolving as well. Ransomware as a Service (RaaS) can be invoked to encrypt systems and collect the ransom, shortening cycles between campaigns. Similarly, attackers running campaigns can buy access to networks through an open marketplace. Boutique services have evolved among security providers to negotiate and pay ransom on behalf of clients. Government regulators are beginning to pursue Office of Foreign Assets Control (OFAC) controls against payments to banned entities. Navigating these trends requires expert advice with deep understanding of your business context.

<table>
<thead>
<tr>
<th>User re-uses credentials on web sites</th>
<th>Attacker finds credentials or access for sale</th>
<th>Attacker accesses vulnerable systems</th>
<th>Attacker acquires privileged identity</th>
<th>Attacker curates collection of data to steal</th>
<th>Attacker triggers ransomware</th>
<th>Attacker follows with extortion demand</th>
</tr>
</thead>
</table>

Where could we have stopped it?

- Security Awareness Training
- Cyber Threat Intelligence
- Password Policy Controls
- Vulnerability Management
- Multi-Factor Authentication
- Geo-fencing
- Advanced Threat Protection
- Advanced Threat protection
- Privileged Identity/Access Management
- Data Loss Prevention
- Intrusion Detection Systems
- Endpoint Detection and Response
- Endpoint Detection and Response
- Backup Hygiene
- Cyber Insurance
- Incident Response
- Law Enforcement
- Crisis Management

The attacker is evolving and so can you. Combine operational resilience, cyber threat intelligence, and cyber security to confidently adapt to an evolving threat landscape.
## Incident Response

### 1. Identity
**Prepare:** follow a three-tiered identity architecture recommended by Microsoft. Never allow domain administrators to use their domain credentials unless they are absolutely needed for the task at hand.
**React:** change privileged account passwords using the Microsoft script to change the Kerberos ticket granting ticket twice rapidly to lock out possibly compromised domain credentials.

### 2. Backups and Recovery
**Prepare:** store three copies of your critical data on at least two different forms of media with at least one off-site. Test your backups in a full restoration at least yearly and then re-adjust when they fail. Plan your full operational resilience lifecycle.
**React:** pull backups offline and test as soon as possible. Monitor backup integrity.

### 3. Immediate Response
**Prepare:** protect your endpoints (servers and workstations) with Endpoint Detection and Response (EDR) tools that monitor active processes and memory threads.
**React:** deploy EDR with fresh threat intelligence. If you already have an EDR tool, deploy it more broadly, use fresh indicators of attack, and monitor agent health.

### 4. Managed Detection and Response-MDR
**Prepare:** engage with a Managed Security Service Provider (MSSP) throughout the onboarding process. Fully understand the limitations of MSSP visibility and service provision as part of a holistic security approach. Consider full service MDR.
**React:** alert your MDR provider to the indicators you have seen and/or notify your internal Security Operations Center.

### 5. Plan and Organize
**Prepare:** a static plan will not be sufficient for evolving threats. Incident Response (IR) plans should be updated and practiced soon. Include critical components such as crisis communication plans, engagement of counsel, technical support resources, etc.
**React:** establish a trusted channel (mobile phones or a conference bridge service) for use if attackers are already insider your mail system.

### 6. Extortion
**Prepare:** response to a ransomware attack includes more than just technical resources. Investigation and internal context for implicated systems are needed to assess risk of disclosure if extortion attempts are made.
**React:** review this issue with counsel and start an investigation immediately to determine the scope of the compromise. Preserve logs to enable investigation after the event.

---

Schedule a call with our digital forensic and incident response experts today by contacting us at IR@Protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 locations in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of Fortune 100® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

All referenced of trademarks are the property of their respective owners. © 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0120
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.