Mature your Ransomware defense with Open Security

Sridhar Muppidi
IBM Fellow & CTO
### IBM X-Force Threat Intelligence Index

A leading cyber threat intelligence report to help organizations understand geographic and industry risks with data and insights

Cyber threat intelligence can help organizations analyze risks, allocate resources, and understand threats relevant to your industry and geography. The annual IBM X-Force Threat Intelligence Index sheds light on recent trends defining the threat landscape. Based on data collected from real attacks, this report offers recommendations to help you bolster your security strategy for the future. Take a look at some of the key findings.

#### Overview

Cyber threat intelligence can help organizations analyze risks, allocate resources, and understand threats relevant to your industry and geography. The annual IBM X-Force Threat Intelligence Index sheds light on recent trends defining the threat landscape. Based on data collected from real attacks, this report offers recommendations to help you bolster your security strategy for the future. Take a look at some of the key findings.

#### Key Findings

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The #1 threat was ransomware</strong></td>
<td>Ransomware was the top threat type, comprising 29% of attacks. Software-as-a-Service (SaaS) ransomware attacks peaked in 2020. The estimated cost of ransomware was $1.4 billion.</td>
</tr>
<tr>
<td><strong>Manufacturing was the second most-attacked industry</strong></td>
<td>Manufacturing moved up to second place in 2020, up from fifth in 2019.</td>
</tr>
<tr>
<td><strong>35% of attacks leveraged vulnerabilities</strong></td>
<td>Stolen credentials was the initial attack vector in 72% of attacks.</td>
</tr>
<tr>
<td><strong>COVID-19 provided opportunity for threat actors</strong></td>
<td>The global pandemic gave sophisticated attackers fresh targets, including organizations involved in the vaccine supply chain.</td>
</tr>
<tr>
<td><strong>Cybercriminals are moving to the cloud</strong></td>
<td>With pandemic cloud spending up and 30% of cloud workloads currently powering 10% of cloud workloads, attackers are seeing the benefits of open-source frameworks.</td>
</tr>
<tr>
<td><strong>Europe was the biggest geographic target</strong></td>
<td>North America, previously the top target, Asia, Europe, Middle East, and Africa, and Central and South America all shared Europe in number of attacks in 2020.</td>
</tr>
</tbody>
</table>

#### Discover more

<table>
<thead>
<tr>
<th>Discover more</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost of a Data Breach</strong></td>
<td>Explore highlights, including top factors that can help reduce costs.</td>
</tr>
<tr>
<td><strong>Cloud Threat Landscape Report</strong></td>
<td>Read about threats and best practices to secure this cloud.</td>
</tr>
<tr>
<td><strong>X-Force Research Hub</strong></td>
<td>Explore research and insights from IBM Security X-Force.</td>
</tr>
</tbody>
</table>
**Current state of Ransomware attacks**

- **Increase in Double Extortion:** Occurs about 60 percent of the time attackers couple ransomware with stealing data.
- **Shift to Ransomware-as-a-Service:** Affiliate or franchise operations, enables multiple infection vectors using the same ransomware.
- **Ransomware Business is booming:** It is estimated that Sodinokibi/Revil earned $120M.
- **Supply Chain is a new attack surface:** We start seeing ransomware attacks originated from supply chain and living-off-the-land.

**Typical Attack Lifecycle**

**Campaign & Infection**
- Attackers target users with Phishing/spam attacks.
- The phase-one malware is downloaded and executed.

**Staging & Recon**
- Malware scans the machine to analyze the admin rights, make itself run at boot, disable recovery mode and delete shadow copies.
- Attackers will start a phase of reconnaissance of the network.

**Privilege Access**
- Malware enables threat actors to gain access to privileged account credentials to move laterally within the compromised network and identify high value assets.

**Exfiltration & Encryption**
- Threat actors exfiltrate high value data for double extortion.
- Deploy ransomware to encrypt all the valuable files and backups at large scale to disrupt business operations.
- Ransom notification.
Typical Ransomware Attack Lifecycle

1. **Campaign**
   - Initial Access: Phishing email with malicious Microsoft Office attachment
   - Microsoft Office macro execution to download / execute malware
   - Malware sets persistence via scheduled tasks or run key
   - Command and Control

2. **Infection**
   - Interactive attacker establishes access to system
   - Post exploitation toolset is downloaded
   - Second stage malware is downloaded
   - Privilege access

3. **Staging**
   - Install additional backdoor
   - Gather Credentials
   - SMB Lateral Movement
   - Additional command and control
   - Active Directory
   - Reconnaissance
   - Gather list of domain admins and domain controllers

4. **Encryption**
   - SMB Lateral Movement
   - Recon
   - Gather lists of hostnames/subnets to target for ransomware
   - Search for Domain Admin credentials
   - Obtain Domain Admin credentials
   - Stage ransomware on share
   - Deploy ransomware using domain admin credentials via PsExec/SMB/Group Policy
   - Exfiltration
   - Install backdoor
   - Data Theft via winscp/rcp/clone
We need a comprehensive approach to Protect & Detect

We need a comprehensive approach to Protect & Detect

We need a comprehensive approach to Protect & Detect

We need a comprehensive approach to Protect & Detect
... and a battle-tested incident response plan

- Simulate an attack
- Test your processes
- Test your team
- Improve your responses
Traditional security is fragmented
Traditional security is fragmented

- Too much to do
- Too many vendors
- Too much complexity
- Too many alerts
1. Maturity model for addressing Ransomware

**Prepare**
Manage business disruption by identifying high-value assets and enabling recovery
- Discover, classify, record high-value assets and enable MFA for access
- Use a risk-based approach to strengthening security posture and operations
- Define a cyber resiliency (back-up / recovery) plan
- Segment, limit, continuously assess need for access
- Rehearse incident response through adversarial simulation exercises, pen testing, etc.
- Educate personnel on cyber security & IR

**Protect**
Contain business disruption with early detection and accelerated response
- Ensure enterprise-level visibility by monitoring high value assets for suspicious access activity
- Enforce least privilege access and mandatory access control for high value assets
- Reduce attack surface with micro-segmentation, rule optimization and enforcement
- Deploy a threat-intel driven full-fledged EDR solution across endpoint and server systems
- Enable AI-based detection and response (rule/ML, IoC/IoB)

**Prevent**
Minimize business disruption by reducing the attack surface
- Ensure risk-centric protection with Zero-Trust Principles
- Achieve continuous detection and automated response through XDR
- Infuse security and privacy by integrating config & threat management with DevSecOps
- Predict protection breaches through cyber deception technologies
- Enable autonomous healing by using full-stack integrity, provenance and AI-based data recovery

Threat Responders need to be more collaborative.
2. Open approach for modern security

- Multicloud
- Open
- Simple
- Composable

Exemplar Open Technology

- Red Hat Ansible
- OpenStack
- ANIX
- Parquet
- MITRE ATT&CK
- OpenCybersecurity Alliance
- IBM Sysflow
Modern and unified approach across full threat lifecycle

**Detect**

51% increase in ability to detect attacks

**Investigate**

60x improvement in investigation time

**Respond**

8x increase in speed to respond to security incidents

“Providing insight and detecting threats across multiple security systems”
- Large Multinational Bank
Thank you