The Evolving Threat Landscape
Extortion Tactics

**Encryption**
Victims pay to regain access to encrypted data

**Data Theft**
Hackers threaten to release stolen data if ransom is unpaid

**Denial of Service**
DoS attacks shut down victim’s public websites

**Harassment**
Customers, business partners, employees and media contacted
Emerging Trends

- Harassment campaigns up ~20% in 2022
- Data theft in 70% of ransomware cases in 2022
Industries posted on ransomware leak sites

Top 10 industries of organizations posted on dark web leak sites in 2022

- Manufacturing
- Professional & Legal Services
- Wholesale & Retail
- Construction
- High Technology
- Education
- Healthcare
- State & Local Government
- Financial Services
- Transportation & Logistics
Ransomware Groups Targeting Education (Leak Site Data)

- **Vice Society**: 33 Cases
- **Lockbit 2.0**: 16 Cases
- **Lockbit 3.0**: 9 Cases
- **BlackCat (ALPHV)**: 8 Cases
- **BlackLian, Snatch**: 6 Cases
- **Hive**: 5 Cases
- **BlackByte, Quantum, STORMOUS**: 3 Cases
- **Conti, Suncrypt**: 2 Cases
- **54BB47H (Sabbath), CLOP, CUBA, IceFire, Sodinokibi (REvil)**: 1 Case
Industries Targeted by Vice Society (Leak Site Data)

- Education: 40 cases
- Healthcare: 13 cases
- State and Local Government: 12 cases
- Manufacturing: 10 cases
- Professional and Legal Services, Wholesale and Retail: 7 cases
- Financial Services: 4 cases
- Media and Entertainment: 3 cases
- Federal Government, High Technology, Hospitality, Non-profit, Utilities and Energy: 2 cases
- Construction, Insurance, Telecommunications, Transportation and Logistics: 1 case
Know your enemy – Vice Society
Vice Society

- First appeared in Mid-2021
- Has targeted educational organizations in US & Canada
- Adopts other ransomware executables vs. creating their own
- Unit 42 observed ransom demands between $1,020,000 – 3,400,000 (2022 – 2023 data)
- Differences between initial and final ransom demands can be significant due to negotiation with the threat actor
Leak Site – Victim Example

View documents >>
The quantity of stolen data does not directly correlate to the negative impact of its theft.
MAKE AN ACTION PLAN

1. Extend your team with a Unit 42 Retainer

2. Validate your security posture with a Ransomware Readiness Assessment and Business Email Compromise Assessment

3. Under attack? Call in Unit 42 Incident Responders

North America
866.486.4842
(1.866.4.UNIT42)

UK
+44.20.3743.366

EMEA
+31.20.299.3130

APAC
+65.6983.8730

Japan
+81.50.1790.0200
Thank You