paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

The Evolving Threat Landscape

Ben Chase
Director, Unit 42

Unit 42

What can you expect from an attack?

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

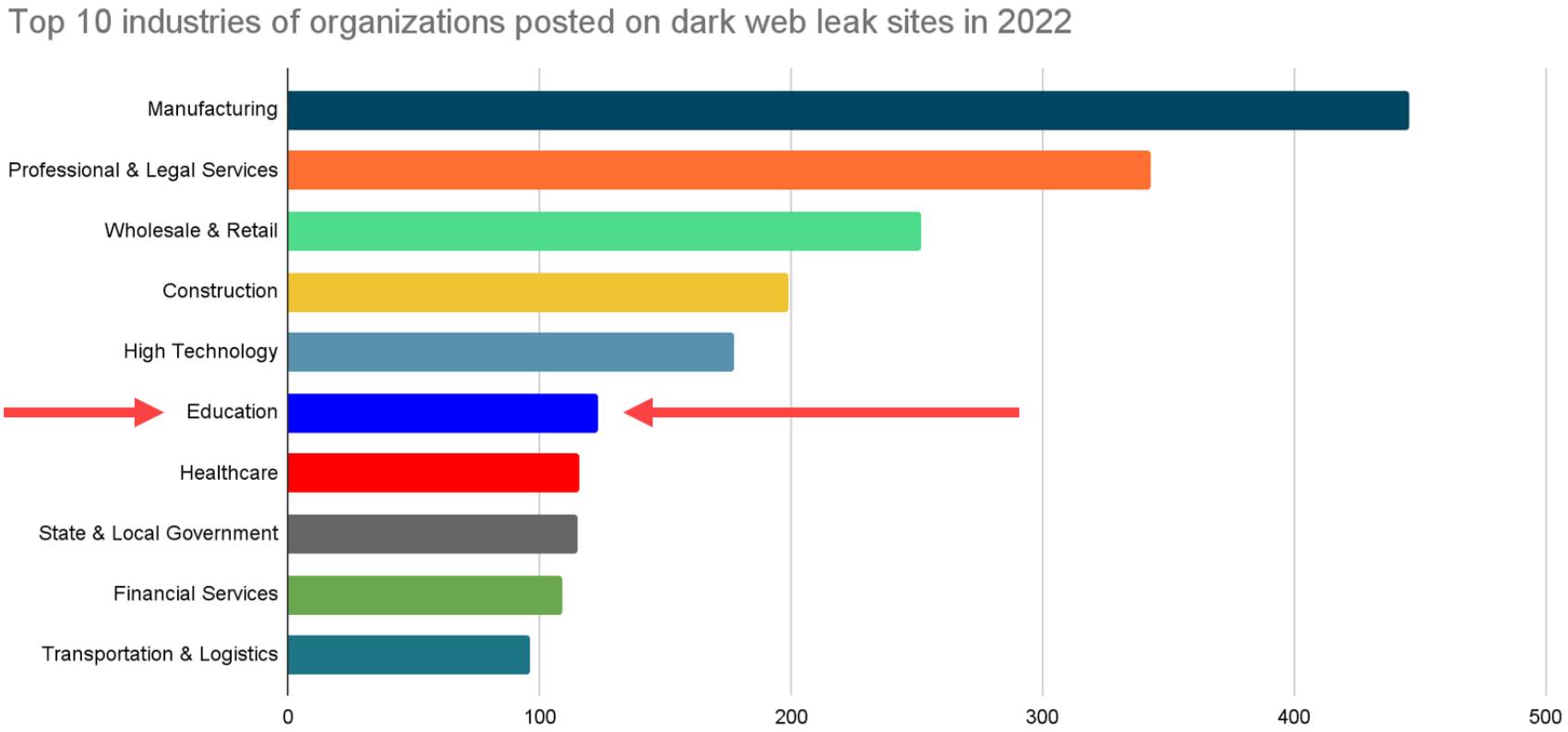
Harassment

Customers, business partners, employees and media contacted

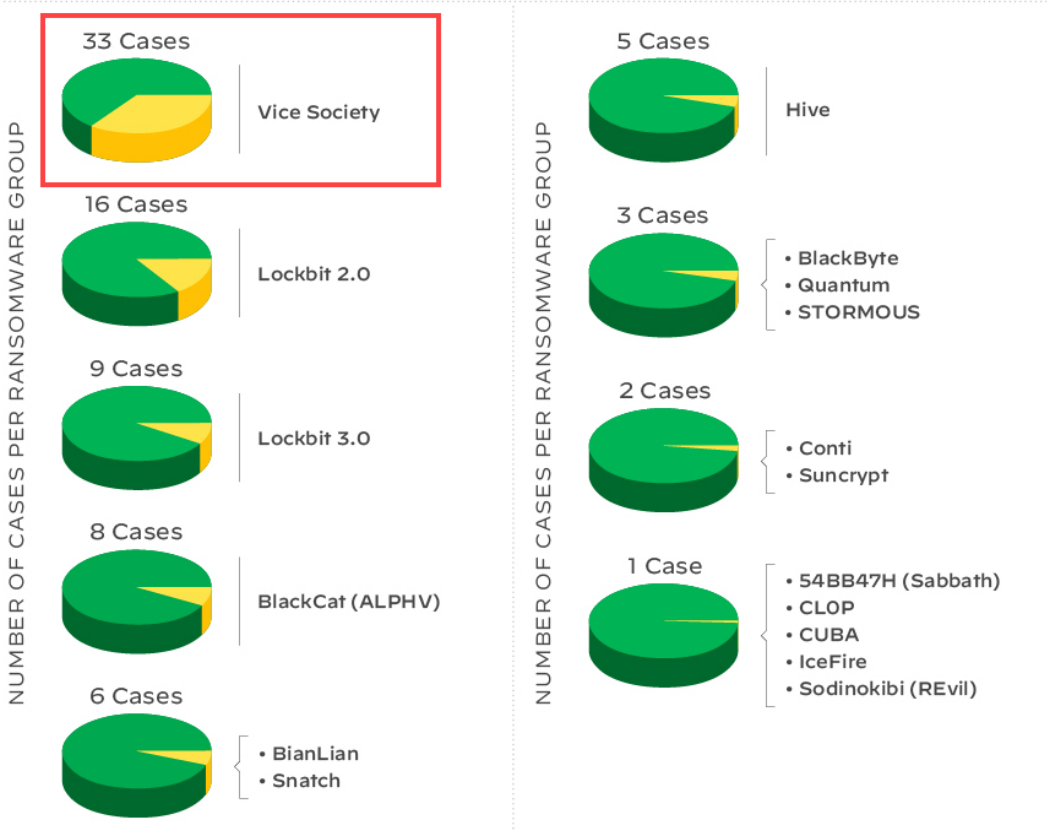
Emerging Trends

- Harassment campaigns up ~20% in 2022
- Data theft in 70% of ransomware cases in 2022

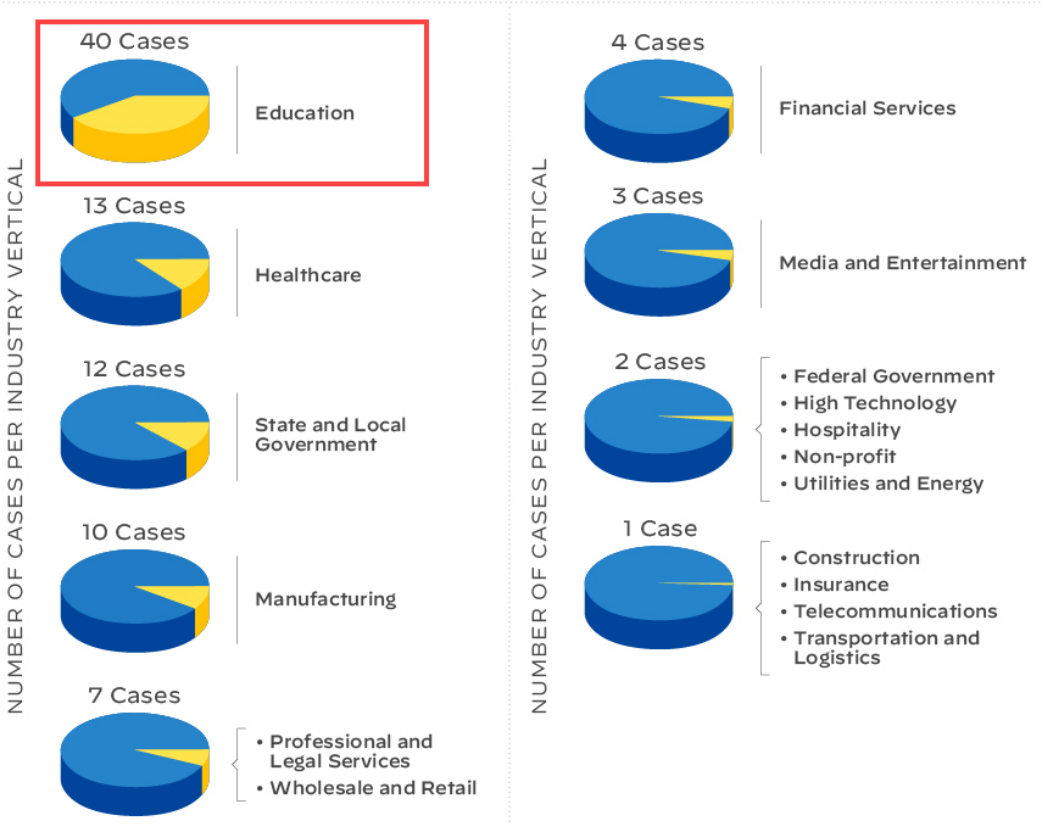
Industries posted on ransomware leak sites



Ransomware Groups Targeting Education (Leak Site Data)



Industries Targeted by Vice Society (Leak Site Data)



Unit 42 Storytime

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

Index of /[redacted]

../
Admissions/
Admissions_Systems/
Admissions_Tuition_Exchange/
Board_of_Trustees/
Business_Office/
Business_Office_VP/
_Assistant_Dean/
_Dean/
_Dean_Contracts/
_Registrar_Office/
Facilities_Planning/
Financial_Auditing/
General_Counsel_Private/
Grad_Common/
Human_Resources/
Mail_Services/
Operational_Budget_-_Dean_of_College/
Payroll_Reports/

[redacted]

[redacted] College
[redacted].edu/
United States

[redacted] is a private institution with a public conscience, a residential campus with global reach. Students and faculty throughout all [redacted] schools - the undergraduate [redacted], the [redacted], and the [redacted] - pursue new ways of knowing by combining classic liberal learning with pioneering collaboration.

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**

UNIT 42
BY PALO ALTO NETWORKS

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


THREAT
VULNERABLE
RANSOMWARE
ATTACK
EXPLOIT
BRIEF
NETWORK
MALWARE
CVE
UNIT
SERVER
TRAFFIC
TREND
CRYPTOJACKING
USE
CLOUD
NEW
MICROSOFT
REPORT
TOOL
DNS
LEAK
GROUP
EXCHANGE
TUTORIAL
FILE
AWS

Thank You