ThreatDown™
Powered by Malwarebytes

Threat Brief: Vice Society

The #1 threat to schools, colleges, and universities

May 2023

In the last 12 months, the Vice Society ransomware gang has conducted more attacks against education targets globally, and in the USA and the UK individually, than any other ransomware group.

Ransomware attacks against education cause misery and disruption, have delayed exams and cancelled school days, destroy data, violate data privacy norms and laws, and require expensive, time-consuming recovery efforts.

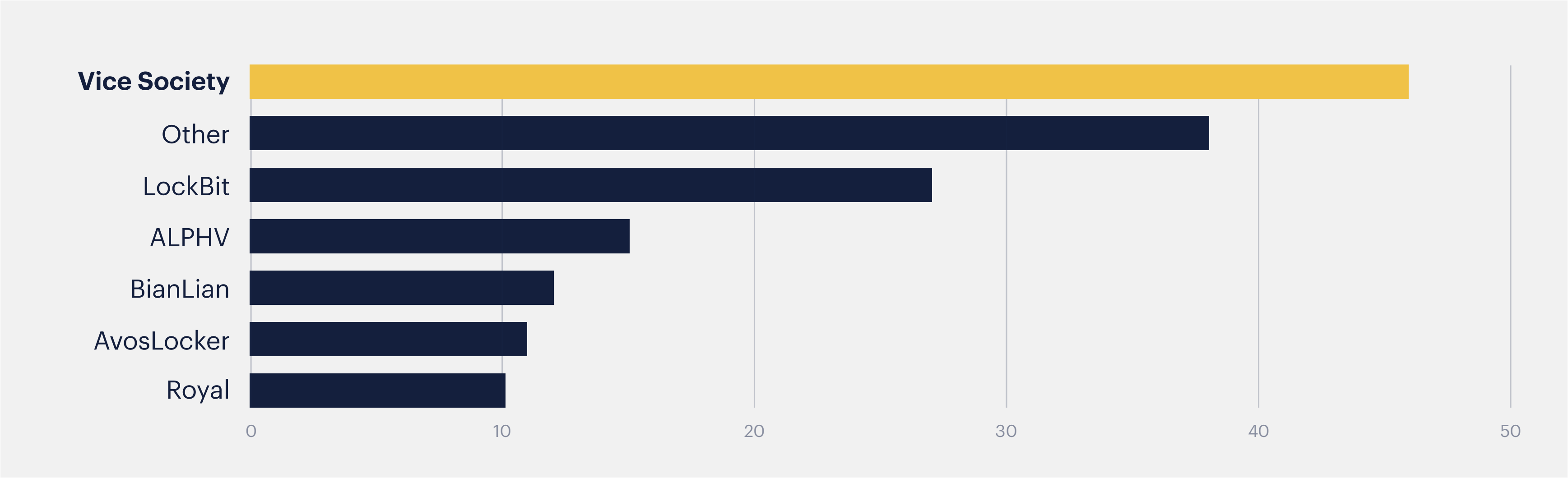
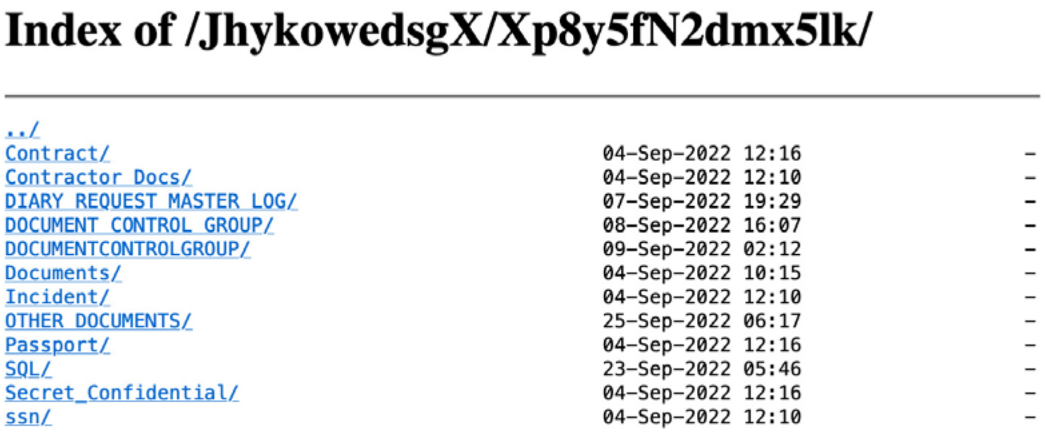


Figure 1: *Known attacks on education targets ordered by ransomware gang, April 2022-March 2023*

In September 2022, Vice Society attacked the Los Angeles Unified School District (LAUSD), the second largest school district in the USA with 640,000 students. After LAUSD refused to pay a ransom, Vice Society leaked a reported 500GB of data, including information marked “Secret” and “Confidential,” on the dark web.

In the same month, it left the Scholar’s Education Trust, a multi-academy trust that operates six UK schools, without access to its computer systems. A few days later a similarly disruptive attack on the UK’s prestigious Pate’s Grammar School led to sensitive and confidential information, including passport scans, being leaked online.



Index of /JhykowedsgX/Xp8y5fN2dmx5lk/

```
../
Contract/                                          04-Sep-2022 12:16                   -
Contractor Docs/                                   04-Sep-2022 12:10                   -
DIARY REQUEST MASTER LOG/                          07-Sep-2022 19:29                   -
DOCUMENT CONTROL GROUP/                            08-Sep-2022 16:07                   -
DOCUMENTCONTROLGROUP/                              09-Sep-2022 02:12                   -
Documents/                                         04-Sep-2022 10:15                   -
Incident/                                          04-Sep-2022 12:10                   -
OTHER DOCUMENTS/                                   25-Sep-2022 06:17                   -
Passport/                                          04-Sep-2022 12:16                   -
SQL/                                               23-Sep-2022 05:46                   -
Secret_Confidential/                               04-Sep-2022 12:16                   -
ssn/                                               04-Sep-2022 12:10                   -
```

Figure 2: *LAUSD data leaked on the dark web*

Between April 2022 and March 2023, 39% of known Vice Society attacks hit education, compared to an average of 4% across all the other ransomware gangs tracked by Malwarebytes.

In the USA, Vice Society has been the most prolific among a number of groups actively attacking education in the last 12 months, while in the UK it accounted for a staggering 70% of all attacks on the sector.

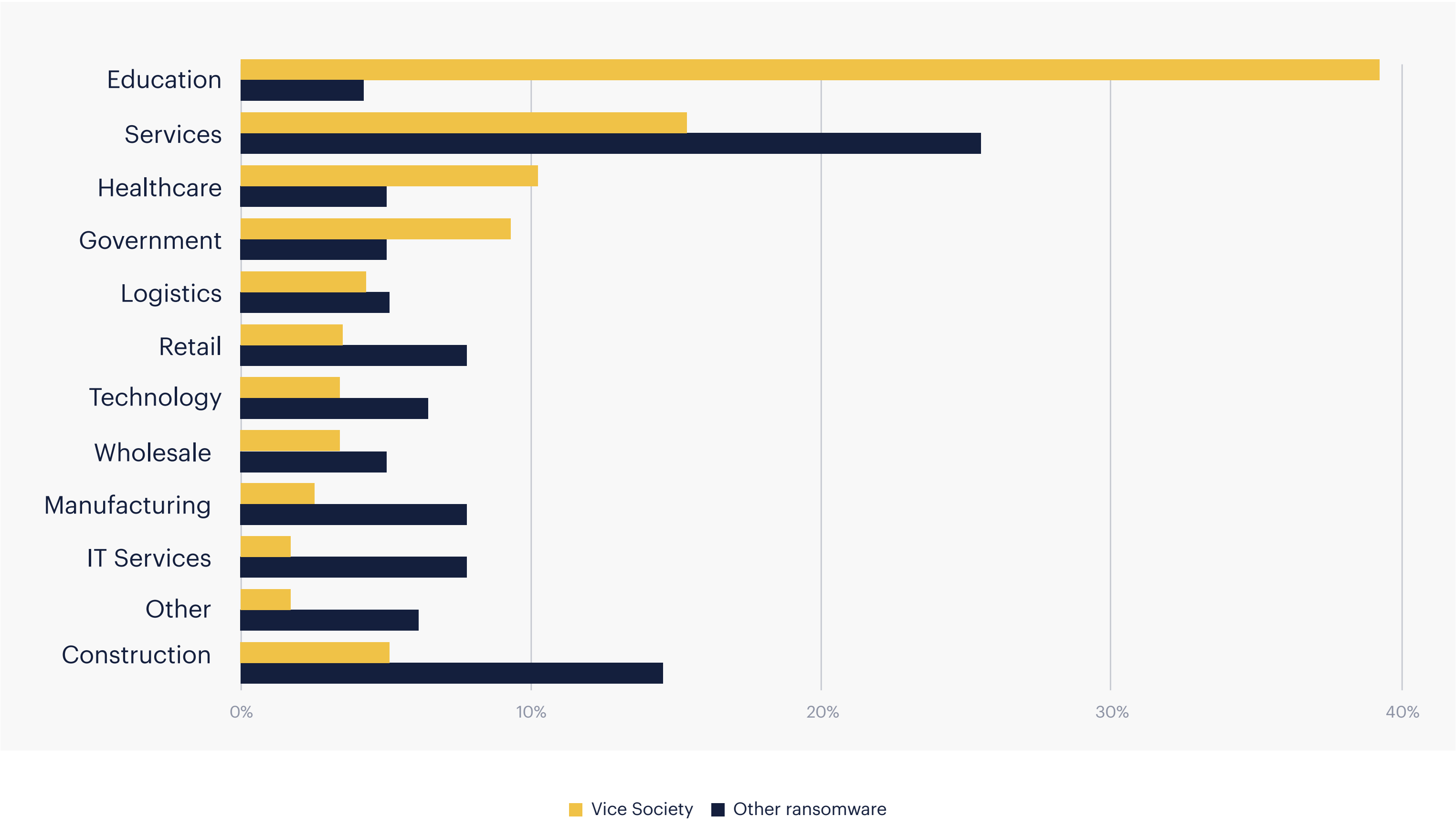


Figure 3: *Distribution of known ransomware attacks by industry sector, April 2022-March 2023*

Vice Society's targeting of education is undoubtedly deliberate and has likely allowed the gang to develop domain-specific techniques and expertise.

According to the [US Cybersecurity and Infrastructure Agency (CISA)](), "School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting … can still put school districts with robust cybersecurity programs at risk."

A Vice Society attack is not directed at an individual computer but uses encryption and data theft to compromise an entire organization. To achieve this, attackers may work for several days, or even weeks, inside a victims' network before running their ransomware.

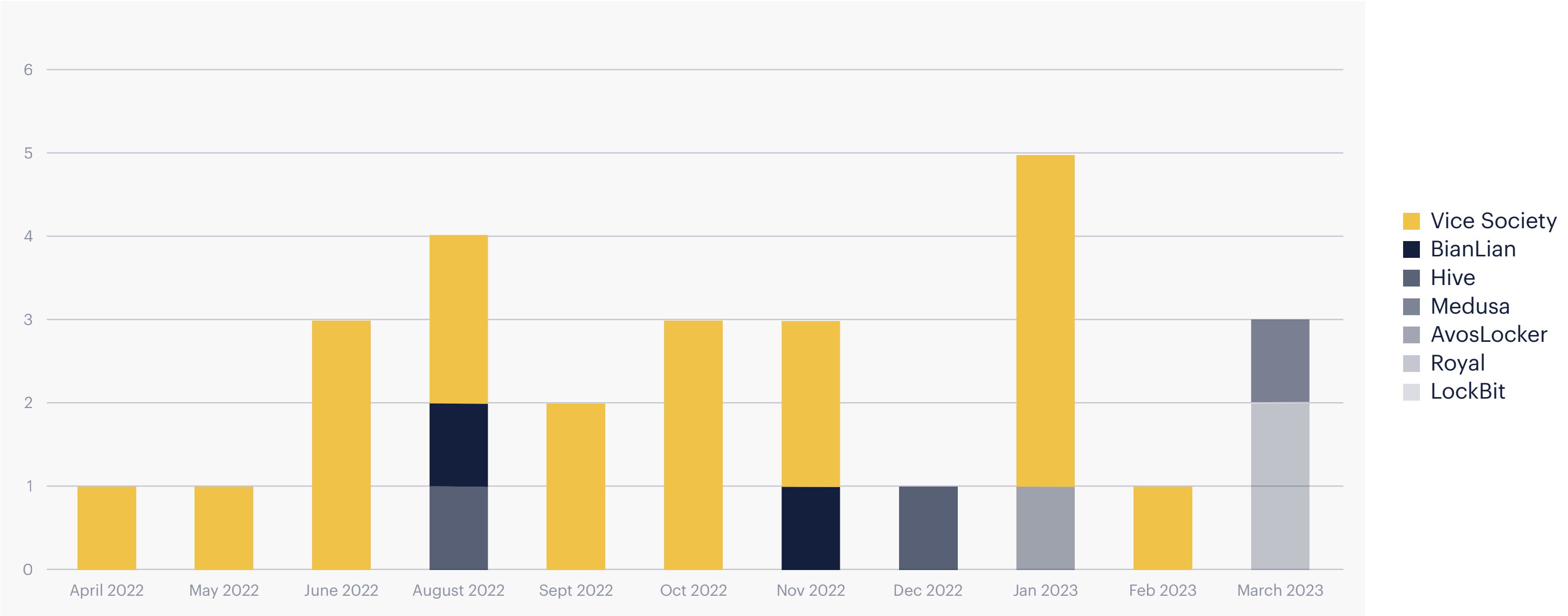


Figure 4: *Known attacks against UK education targets, April 2022-March 2023*

After a successful attack, Vice Society demands a ransom in return for deleting stolen data and providing a decryption tool. Ransom demands are reported to have exceeded $1 million. (The average ransom payment across all ransomware gangs in Q4 2022 was $410,000.)

Victims' details and stolen data are listed on the gang's dark web website, which has adopted branding from the computer game Grand Theft Auto (GTA).

Unlike some of its competitors, Vice Society is not a ransomware-as-a-service (RaaS) vendor. It doesn't produce its own ransomware, nor does it use other criminal gangs—"affiliates"—to carry out attacks.

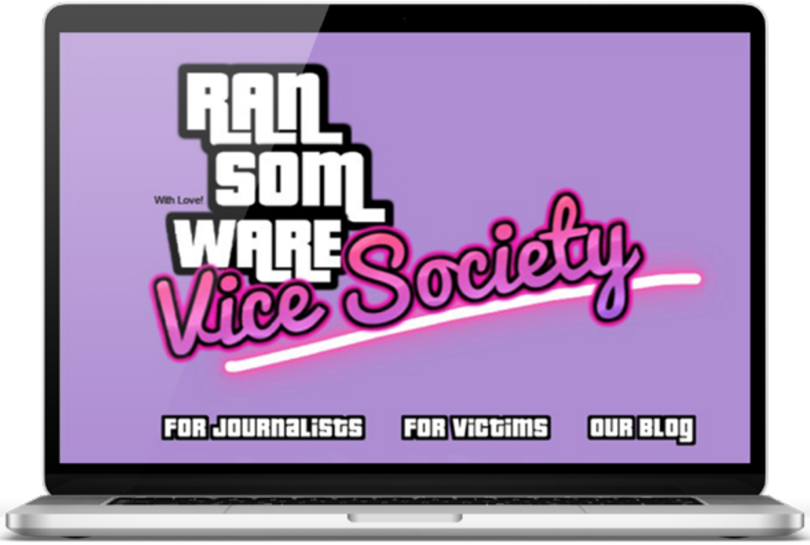


Figure 5: *Vice Society has adopted GTA branding for its website*

PROTECTING AGAINST A VICE SOCIETY ATTACK

Because Vice Society may be active on your network for days before running a ransomware locker, it is not enough to simply stop the locker. By the time it's run, its operators will already have stolen your data, taken steps to cover their tracks, and will have sufficient access to your network to retry their attack.

If Vice Society members gain access to your network they must be discovered and ejected, and their tools, accounts, and backdoors removed.

Vice Society likes to "live off the land," using legitimate tools like PowerShell and the Windows Management Instrumentation (WMI) service to disguise its activity. Detecting this activity is a difficult task for any organization. It requires excellent experienced security professionals with an eye for out-of-place details watching the network's Endpoint Detection and Response (EDR) monitoring 24/7. For resource-constrained schools, the only cost-effective way to access this kind of skillset is through a third-party service like ThreatDown Managed Detection and Response (MDR).

ATTACK PHASES	PROTECTION
Assets	
Software vulnerabilities	Use Vulnerability and Patch Management to identify and prioritize vulnerabilities.
Compromised accounts	Use two-factor authentication on Internet-facing accounts.
Infiltration and theft	
Privilege escalation, may involve print spooler exploits or credential dumping.	Use MDR to identify attackers as they operate inside your network, before they launch ransomware.
Discovery, may involve the use of Advanced Port Scanner and Bloodhound.	
Lateral movement, may utilize PsExec or RDP.	
Data theft, may be accomplished with PsExec or PowerShell.	
Backdoors, may involve SystemBC or proprietary solutions.	
Encryption	
Vice Society has used Hello Kitty and Zeppelin ransomware but may use other types in future.	Use EDR to detect ransomware, identify surreptitious encryption, and roll back affected files to an unencrypted state.
Reinfection	
Even if its ransomware is stopped, Vice Society has not lost access to your network.	Use EDR or MDR to identify initial access, compromised accounts, tools, and backdoors to remove Vice Society operators and prevent another attack.

ThreatDown™
Powered by Malwarebytes

Managed Detection and Response

ThreatDown Managed Detection and Response (MDR) helps schools, businesses, MSPs, and other organizations to stop cyberattacks before they happen, utilizing a team of experienced analysts to detect, investigate, remediate, and hunt for threats. Powering MDR is the company's Endpoint Detection and Response (EDR), which includes Endpoint Protection (EP) and ransomware anomaly detection that stopped 100% of ransomware threats in third-party testing. A 24/7 cybersecurity team is available to help you today.

TRY MDR NOW >

ThreatDown™
Powered by Malwarebytes

www.malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796