SEARCHLIGHT CYBER

RANSOMWARE SPOTLIGHT

VICE SOCIETY'S DARK WEB FOOTPRINT

BACKGROUND ON THE VICE SOCIETY GROUP

Vice Society is a ransomware/data extortion operation. It primarily targets the education sector but also counts healthcare organizations, hospitals, and enterprises among its victims. It is active in the Americas, Europe, Asia, and Oceania but has a particularly high concentration of victims in the USA and UK.

Vice Society has been observed using a custom-branded locker dubbed 'PolyVice', appending encrypted files with a '.ViceSociety' extension. As well as using this, their toolkit includes payloads such as HelloKitty and Zeppelin. Vice Society uses double extortion: as well as encrypting an organization's data, it also exfiltrates and threatens to release it on its dark web leaks site. The group has been observed exploiting popular CVEs for initial access and using both SMB and HTTP to exfiltrate data from a victim network.

TOTAL LISTED VICTIMS

Total number of victims on its leak site: 161

FIRST ACTIVE

First attack listed: August 2021

VICTIM SAMPLE

Dates reflect when the victims were listed on the Vice Society leak site:

- School of Oriental and African Studies (UK, Sep 2022)
- Los Angeles Unified School District (USA, Oct 2022)
- Cincinnati State Technical and Community College (USA, Nov 2022)
- University Institute of Technology of Paris (France, Dec 2022)
- The University of Duisburg-Essen (Germany, Jan 2023)

SUMMARY OF SEARCHLIGHT CYBER FINDINGS

- The ransomware operation Vice Society is prolific. Primarily targeting the education sector (**Figure 1**), it has victims around the world, prompting governments to issue warnings and advisories against the gang's activity.
- Searchlight Cyber analysts conducted an investigation into dark web traffic to and from infrastructure linked to Vice Society's historic victims, identifying a pattern of activity in a window prior to the attacks.
- Combining this data with Open Source Intelligence (OSINT) on Vice Society's attacks, Searchlight Cyber analysts assess with medium confidence that this dark web traffic is related to the attack.
- Further analysis of dark web traffic could uncover a "fingerprint" that could inform incident response, intelligence on the group's TTPs, and help future victims to detect a Vice Society breach.

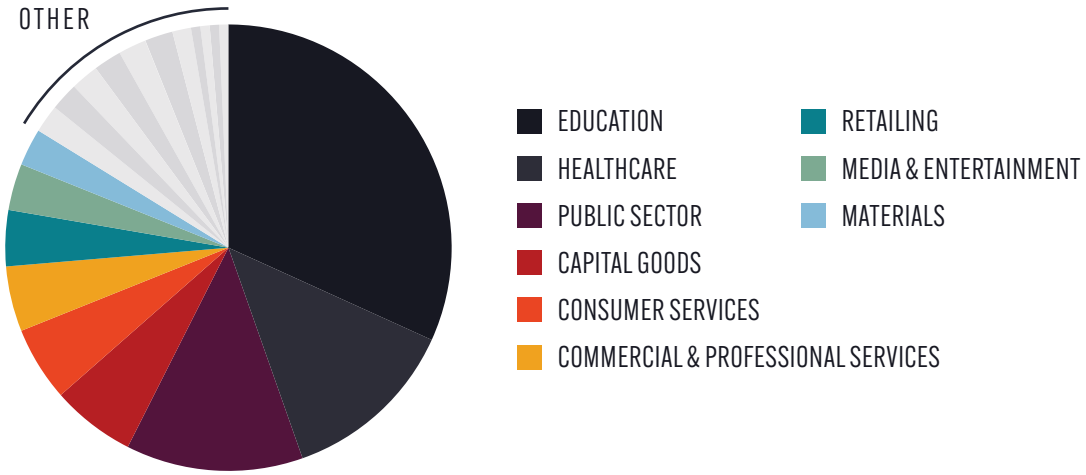

FIGURE 1: VICTIMS LISTED ON THE VICE SOCIETY DARK WEB LEAK SITE, BY INDUSTRY SECTOR.

RESEARCH OVERVIEW

Searchlight Cyber researchers undertook historic dark web traffic analysis on infrastructure related to known Vice Society victims to identify whether indicators of attack could be identified in connections to the dark web network The Onion Router (Tor). While this accounts for only a portion of the network data for each victim, connections to the dark web do indicate anomalous activity that could inform further research alongside the wider threat intelligence community.

This report relates to victims that were listed on Vice Society's leak site and whose attacks have already been reported in the public domain, examining the cases in chronological order of when the attacks occurred:

- Grand Valley State University (USA)
- Pilton Community College (UK)
- Los Angeles Unified School District (USA)

GRAND VALLEY STATE UNIVERSITY

INCIDENT OVERVIEW

Grand Valley State University (GVSU) - a public university in Michigan, USA - was listed on the Vice Society dark web leak site on **June 14, 2022** (Figure 2). The University's data was leaked on **June 18, 2022** when the countdown clock on the leak site ran down. It reportedly contained passports and identity documents for several dozen people.[1] [TA0010][T1486].

According to email communications between the cybersecurity publication DataBreaches and a spokesperson for Vice Society, the group initially gained access to GVSU's system on **May 24, 2022** and negotiated with the university before leaking the documents.[2]

[1] https://www.databreaches.net/grand-valley-state-university-hit-by-ransomware-but-remains-publicly-silent/
[2] https://www.databreaches.net/grand-valley-state-university-hit-by-ransomware-but-remains-publicly-silent/

FIGURE 2: A SCREENSHOT OF GRAND VALLEY STATE UNIVERSITY'S LISTING ON VICE SOCIETY'S DARK WEB LEAK SITE.

DARK WEB NETWORK TRAFFIC

Examining the frequency of connections between infrastructure linked with GVSU and the dark web in 2022, there is a significant spike of dark web activity (4,553,466 percent above the previous maximum observed) between **March 10, 2022** and **July 4, 2022** (**Figure 3**).

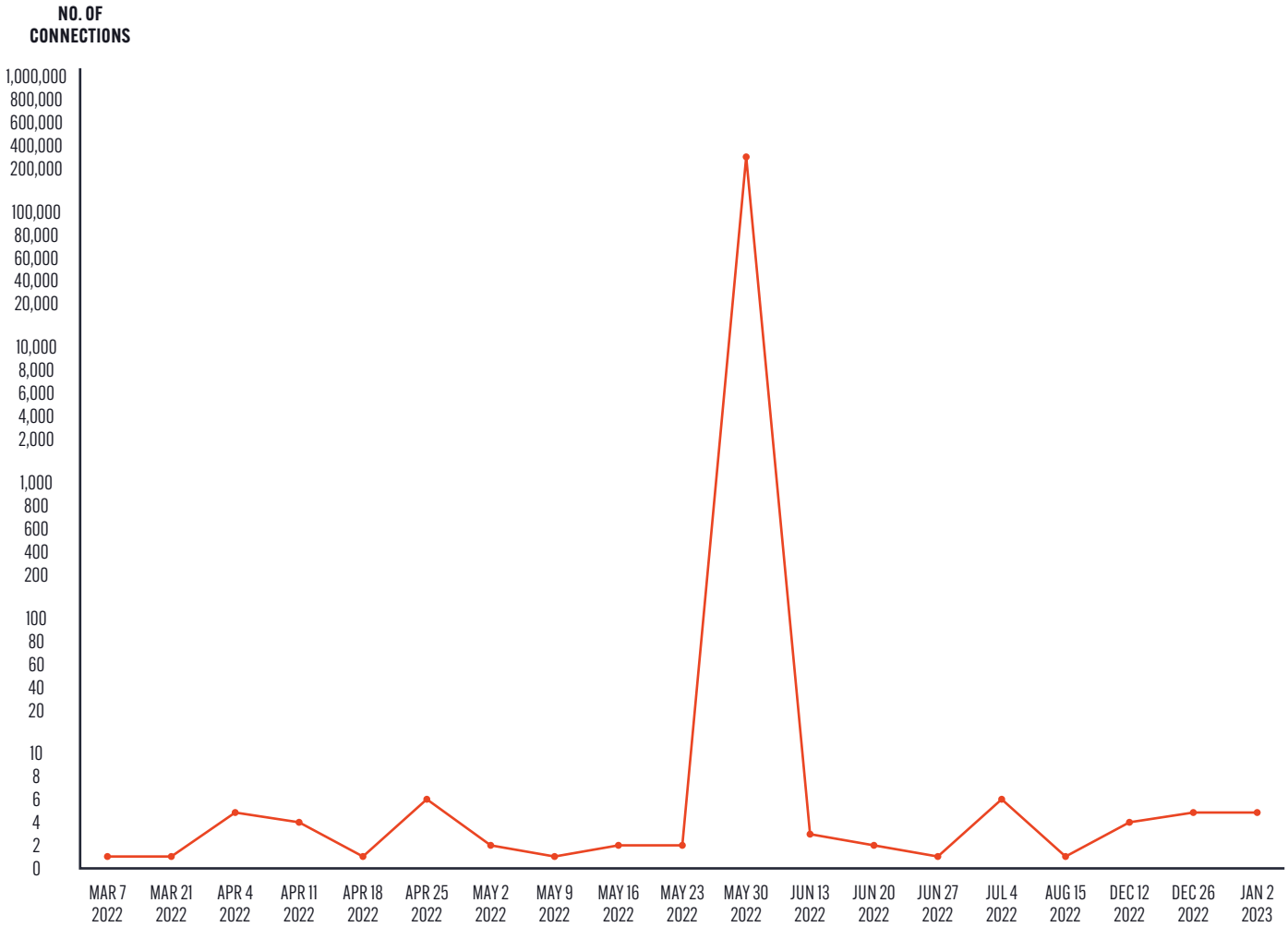

FIGURE 3: OVERALL FOOTPRINT OF DARK WEB ACTIVITY AGAINST GVSU IN 2022 ON A LOGARITHMIC SCALE.

Between **March 10** and **May 4, 2022** via Tor we observed sporadic connections to the following hosts:

- scholarworks[.]gvsu[.]edu
- mybb[.]gvsu[.]edu

Between **May 4** and **May 24, 2022** via Tor we observed the following hosts as having sporadic activity:

- scholarworks[.]gvsu[.]edu
- eis[.]gvsu[.]edu
- www[.]gvsu[.]edu

Then, after a gap in activity, on **May 31, 2022** Searchlight Cyber analysts observed approximately 18 GB transmitted from the university network via Tor connections, and observed approximately 9.2 GB transmitted towards the university network.

Around this date, Searchlight Cyber analysts observed a change of Autonomous System Number (ASN) relating to gvsu[.]edu. According to Silent Push, a Passive DNS tool, the host gvsu[.]edu was using the IP address 148.61.6[.]9 up until around **May 31, 2022** on the ASN 237, when it made the switch to new IP addresses on CloudFlare under the ASN 13335 (CLOUDFLARENET).

The change in ASN at the same time that Vice Society was attacking GVSU's network could be a coincidence. However, it is possible that GVSU changed ASN as a defensive measure to remediate the attack.

We considered three possible hypotheses for the observed data (~18 GB from / ~9.2 GB) towards gvsu[.]edu:

1. The observed network activity via Tor is directly associated with the hostile actions of Vice Society and is supportive of data exfiltration attempts from GVSU, or other actions such as a DOS during the attack.
2. The observed network activity via Tor is indirectly associated with the hostile actions of Vice Society. For example, it may relate to the change of ASN / IP addresses associated with gvsu[.]edu, and in particular any crawlers or bots that may be networked via Tor detecting a change in network configuration, and flooding the host. In this context, it is assumed the change of ASN does relate to the hypothesis of the activity of Vice Society, as the observed network behavior is a consequence of defensive techniques.
3. The observed network activity via Tor is a coincidence. This may include Tor crawlers as outlined above, in the case that the change of ASN at the time of the suspected network breach was coincidental.

On the balance of probability it is more likely that the network activity is either directly or indirectly associated with the actions of Vice Society, given that it coincides with the attack window established through OSINT.

FIGURE 4: A GRAPH TO SHOW ON A LOGARITHMIC SCALE THE DATA TRANSFERRED FROM THE UNIVERSITY NETWORK, DATA TRANSFERRED TOWARDS THE NETWORK, AND CONNECTION COUNTS BETWEEN MARCH 2022 - JANUARY 2023.

INITIAL ACCESS

In this case, dark web network connections may also inform our understanding of how Vice Society gained initial access to the victim. Examining our data from **May 24** - the day Vice Society claims to have gained access - we observe two connections to eis[.]gvsu[.]edu, at 12:51 hours, with 28230 bytes transferred out of the host, and 3472 bytes into the host over port 443. eis[.]gvsu[.]edu is a login portal for the university (**Figure 5**).

Research indicates that the portal uses the WSO2 API Manager, Identity Server & Enterprise Integrator, which was found to have a Remote Code Execution (RCE) [T1505] Flaw on **April 18, 2022** - approximately one month before the attack.[3]

[3] https://nvd.nist.gov/vuln/detail/CVE-2022-29464

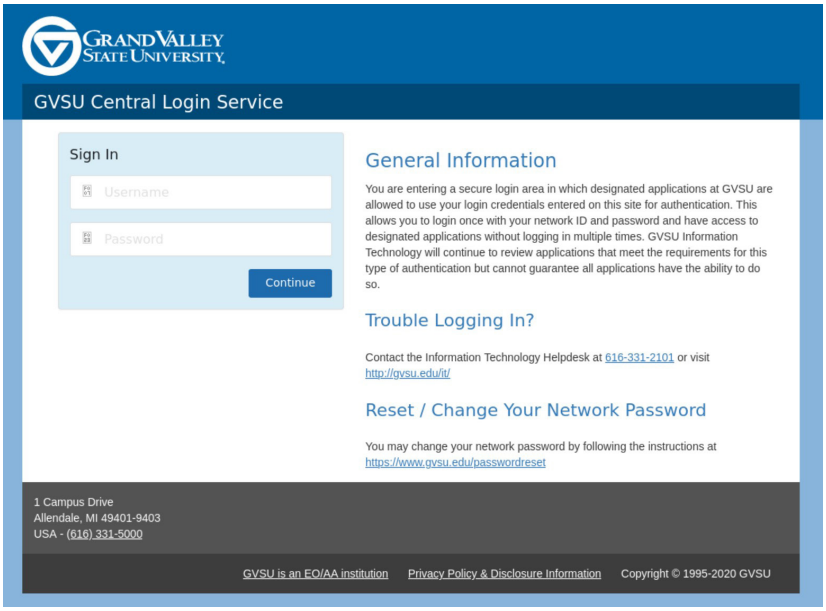

FIGURE 5: SCREENSHOT OF THE LOGIN PAGE FOR THE GVSU PORTAL.

This vulnerability has a CVSSv3 score of 9.8 out of 10, indicating that it is critical. Researchers have demonstrated that by leveraging the vulnerability, an unauthenticated malicious attacker could perform a remote code execution through arbitrary file upload and perform a complete server/system take over.[4]

We cannot say whether Vice Society exploited this vulnerability. However, we know from our own dark web dataset that this RCE flaw was known and discussed on dark web forums (**Figure 6**), marketplaces, and even on YouTube before **May 2022**. Moreover, the use of known CVEs[5] and public-facing websites[6] as an attack vector is consistent with research that has been published on Vice Society's TTPs [T1190].

FIGURE 6: AN EXAMPLE OF A THREAT ACTOR DISCUSSING HOW TO EXPLOIT WSO2 ON A POPULAR DARK WEB FORUM.

[4] https://www.techcert.lk/threat_bulletin/a-critical-unauthenticated-remote-code-execution-rce-flaw-found-in-wso2-api-manager-identity-server-enterprise-integrator/
[5] https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
[6] https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html

PILTON COMMUNITY COLLEGE

INCIDENT OVERVIEW

Pilton Community College is one of more than a dozen UK education institutions to be targeted by Vice Society in 2022. It was announced on Vice Society's dark web leak site on **June 24, 2022** (**Figure 7**). [TA0010][T1486].

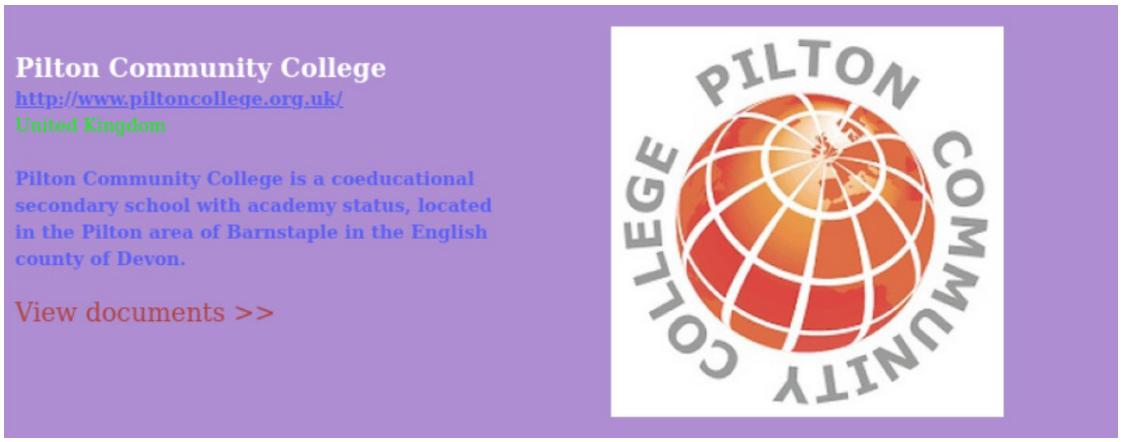

FIGURE 7: A SCREENSHOT OF PILTON COMMUNITY COLLEGE'S LISTING ON VICE SOCIETY'S DARK WEB LEAK SITE.

DARK WEB NETWORK TRAFFIC

Our telemetry indicates a spike of activity on **June 16 and 17 2022**, a week before it was listed on Vice Society's leak site, displayed in **Figure 8**.

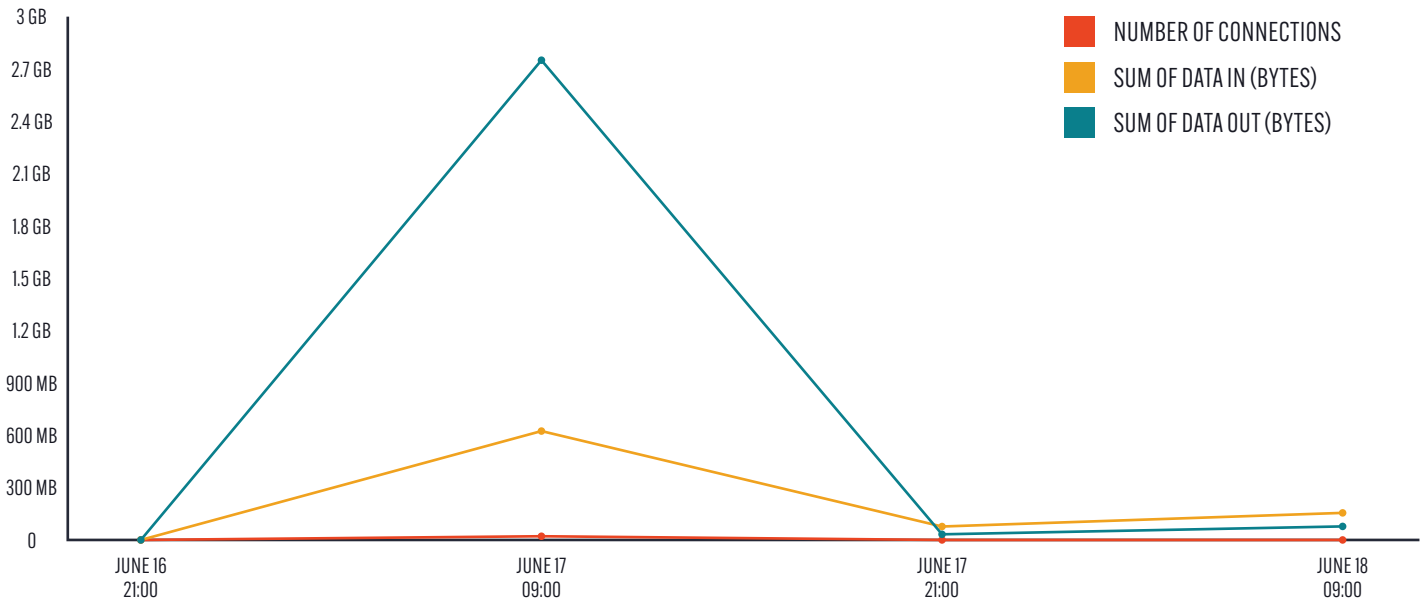

FIGURE 8: A GRAPH OF DARK WEB NETWORK ACTIVITY IN JUNE 2022.

[7] https://www.bbc.com/news/uk-england-gloucestershire-63637883

This graph demonstrates a similar pattern of incoming and outgoing data to that observed in the GVSU case, once again focused at a public website.

The data transferred from Pilton College is not as large as was observed with GVSU, however, the fact remains that a similar behavior is witnessed over Tor with a large spike of data transferred from a targeted host close to the time of attack. Pilton College was not observed changing ASN at or around the time of our data, which supports the hypothesis that the traffic is related directly to the actions of Vice Society.

Once again, this spike could be a coincidence, but given the temporal proximity of both events (GVSU and Pilton College) to their respective attack, it becomes less likely that this is a coincidence, and more likely the spike of Tor traffic does relate to the actions of Vice Society in their attack campaign.

What's more, comparing the ratios of outgoing data : incoming data, there is not much difference between the observations of GVSU and Pilton College, hence, this may be a fingerprint of a Vice Society attack (*assessed with low confidence*).

LOS ANGELES UNIFIED SCHOOL DISTRICT

INCIDENT OVERVIEW

Los Angeles Unified School District (LAUSD), the second largest school district in the USA, was impacted by a ransomware attack on **September 3, 2022**. Days later, a Vice Society representative claimed responsibility for the attack in an interview with the cybersecurity publication BleepingComputer, saying that it had stolen and encrypted "500 GB of data from their network".[8] [TA0010][T1486].

On **September 21**, LAUSD received a ransom demand but did not negotiate, after consulting with the FBI.[9] In **January 2023**, following an investigation, LAUSD confirmed that some of its contractors' sensitive information – including names, addresses, and Social Security numbers – were leaked during the attack and that initial network access was gained by an "unauthorized actor" between **July 31, 2022 and September 3, 2022**.[10] It has been speculated by researchers that Vice Society gained initial access using internal login credentials leaked on the dark web.[11]

FIGURE 9: A SCREENSHOT OF LAUSD'S LISTING ON VICE SOCIETY'S DARK WEB LEAK SITE.

[8] https://www.bleepingcomputer.com/news/security/vice-society-claims-lausd-ransomware-attack-theft-of-500gb-of-data/
[9] https://www.cbsnews.com/losangeles/news/hackers-threaten-to-leak-stolen-information-lausd-does-not-pay-ransom/
[10] https://s3.documentcloud.org/documents/23580634/lausd-notice-of-data-breach-vice-society-ransomware.pdf
[11] https://www.upguard.com/blog/how-did-lausd-get-hacked

DARK WEB NETWORK TRAFFIC

Analyzing dark web traffic to infrastructure related to LAUSD reveals a spike in connections to lms.lausd.net [T1133] between **August 15, and August 22, 2022**. This is in the window of the attack determined by LAUSD's incident response investigation and once again confirms a pattern of dark web activity in the weeks before a victim is listed on the Vice Society dark web leak site.

We observed approximately 500 000 bytes transferred out of the network, and approximately 40 000 bytes sent to the network, split over 16 connections.

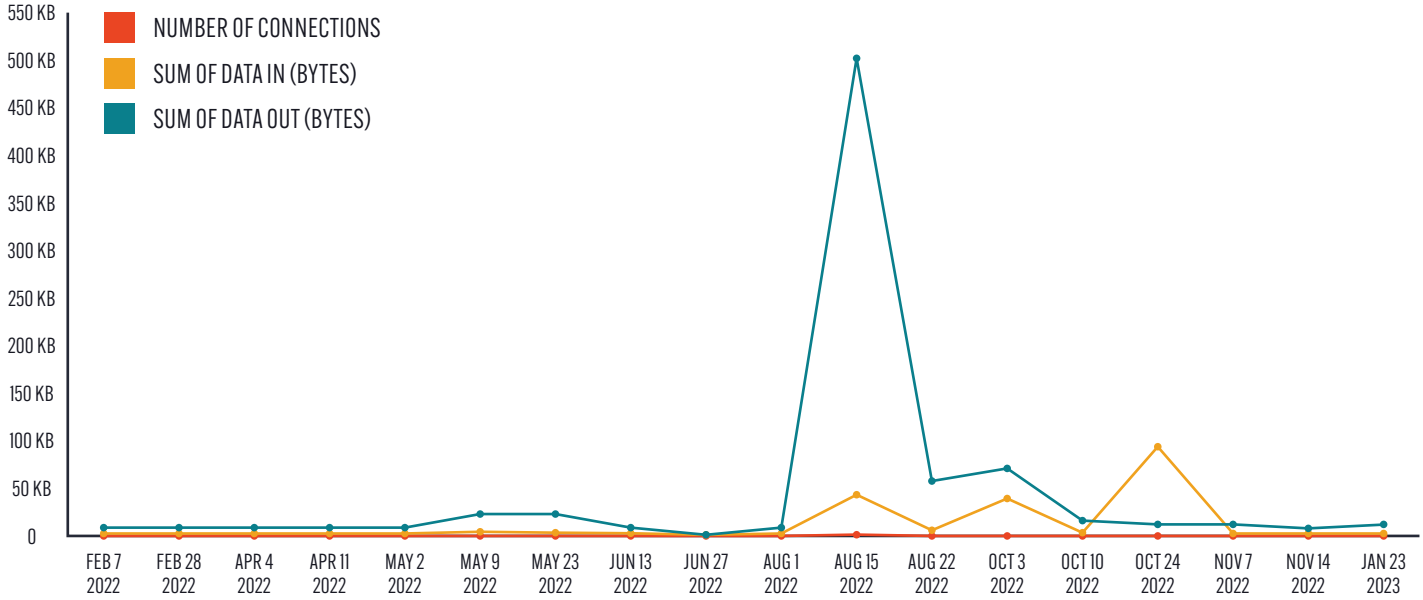

FIGURE 10: CONNECTION OUT AND TOTAL CONNECTIONS TO THE DARK WEB FEBRUARY - DECEMBER 2022.

This activity may be indicative of the threat actor gaining initial access via the web portal, which research indicates is a learning management system. This is consistent with other researchers' hypothesis of how the attack was carried out and - as we have established - is a known tactic of Vice Society.

INITIAL ACCESS

Once again, dark web traffic might provide us with an indication of how Vice Society gained initial access to LAUSD infrastructure. Using our dark web monitoring platform DarkIQ, Searchlight Cyber analysts noted an observable change in behavior in **January 2021** (**Figures 11 & 12**).

FIGURE 11: INCOMING AND OUTGOING DARK WEB TRAFFIC DATA TO LAUSD INFRASTRUCTURE JANUARY 2020 - JUNE 2021. SOURCE: DARKIQ.

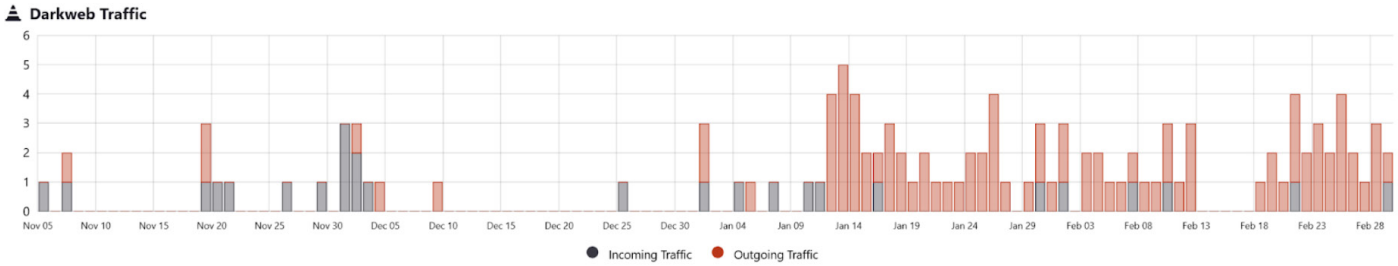

FIGURE 12: INCOMING AND OUTGOING DARK WEB TRAFFIC DATA TO LAUSD INFRASTRUCTURE NOVEMBER 2020 - FEBRUARY 2021. SOURCE: DARKIQ.

This date coincides with research reports from **February 2021** that the school district had been compromised by Trickbot, a malware that is used to infiltrate a network, steal information, and can be used to deploy other malware.

While we cannot say that Vice Society was behind the deployment of Trickbot [TA0011], the pattern of dark web activity does continue up until and beyond the point of attack in **August 2022**.

It is possible that this indicates that Trickbot or a subsequent payload was not successfully cleared from LAUSD's system, allowing Vice Society to gain a foothold to execute the ransomware attack in **August 2022**.

Importantly, we have observed in our data that the IP addresses communicating to the dark web in **August 2022** (the window of the attack) had never connected to the dark web before. This means that, even with the background noise of dark web traffic established since **January 2021**, LAUSD still could have identified new anomalous activity in **August 2022** that would have prompted it to investigate.

KEY TAKEAWAYS

Analysis of dark web traffic could have alerted each of these organizations to anomalous activity in the weeks leading up to the attack by Vice Society, which could be an indicator of compromise. This indicates the value of dark web traffic as a data source for threat intelligence. In summary:

EXAMINING DARK WEB NETWORK TRAFFIC DEMONSTRATES A CONSISTENT PATTERN OF ACTIVITY FOR VICE SOCIETY ATTACKS:

- A spike in dark web network traffic within several weeks prior to the victim being listed on the Vice Society leak site.
- Traffic is directed to organizations' public facing websites or portals, consistent with Vice Society's use of website CVEs to gain initial access.

FURTHER ANALYSIS OF THE DARK WEB TRAFFIC DATA OF VICE SOCIETY VICTIMS COULD HELP INFORM:

- Incident response efforts - by establishing a clear timeline of initial access and reconnaissance.
- Threat intelligence - by contributing supporting data on the group's TTPs, such as the use of CVEs and targeting of public websites.
- Detection - with continuous analysis of dark web networks providing early warning of Vice Society's initial access and reconnaissance. By identifying its unique fingerprint, defenders could not only identify that they are being attacked but also who is attacking them, helping to inform mitigation efforts based on a group's playbook.

THIS ANALYSIS SUPPORTS FURTHER INVESTIGATION OF DARK WEB TRAFFIC AS A THREAT INTELLIGENCE SOURCE:

- To determine whether other ransomware and threat groups have similar "fingerprints" that could help the security community to create profiles that help organizations to detect attacks and identify the perpetrators.
- To be used as a warning sign that organizations could use to trigger early remediative action, which could have a significant impact in mitigating disruption caused by an attack. For example, based on their communications with Tor, the security team could begin a proactive hunt, take steps to isolate infected hosts, and move/backup data before exfiltration is conducted, etc.

While this report demonstrates that dark web traffic provides a unique viewpoint of an attack, we are open that this only provides us with a fraction of the picture. We openly call on the wider cybersecurity and threat intelligence community to collaborate with Searchlight Cyber to help us establish the full picture and determine how dark web intelligence can be used to inform our collective understanding of the TTPs of ransomware operations like Vice Society.