# CASE STUDY

## CITY CREDIT UNION // FINANCIAL SERVICES

### CHALLENGES

➤ DATA LEAKS
➤ PHISHING SITES
➤ SUPPLY CHAIN SECURITY

### SOLUTION

DARK WEB MONITORING

City Credit Union

## PROACTIVELY PROTECTING MEMBERS FROM DATA BREACHES

City Credit Union (City CU) has been serving the Dallas-Fort Worth-Arlington Metropolitan Area since 1942 and today holds $600 million in assets, has more than 35,000 members, and employs 100 staff across five branches. Its IT department is tasked with handling everything from City CU's servers, to maintaining the network, and the cybersecurity protection of its infrastructure and its members.

City CU's team wanted a way to proactively identify if its members had been impacted by third party data breaches. It needed to be able to continuously monitor for the earliest possible sign that member data - including personal information, credit card numbers, social security numbers - had been compromised and was being shared on the dark web.

**Garreth L. Cada, Senior IT Manager at City Credit Union explained:** "Data from our members on the dark web is very concerning to us. Not only is it a risk to their financial security but it could also impact our reputation if that data is taken by cybercriminals and used for fraud. There is nothing we can do to stop other organizations from suffering cyberattacks but we can be proactive in identifying if our members are affected and help them mitigate the impact of their data being leaked. We took it upon ourselves to protect our customers by going out to the dark web and identifying data breaches ourselves."

"

The value that Searchlight's dark web monitoring has contributed to our team is considerable - more than the equivalent of one full time employee. Rather than manually searching the dark web for threats, we are able to take action faster, based on the intelligence that Searchlight surfaces for us.

**GARRETH L. CADA**
Senior IT Manager,
City Credit Union

**SEARCHLIGHT.
CYBER**

# DEPLOYING CONTINUOUS DARK WEB MONITORING

City CU chose Searchlight Cyber for its ability to automatically monitor the dark web, allowing the IT department to detect threats against its members without requiring additional human resource to manually search hidden sites. Searchlight's dark web monitoring solution continuously searches forums, markets, and leak sites on City CU's behalf, automatically generating alerts for the IT department whenever it surfaces a threat related to the credit union or its members.

"Our IT department has a lot of different priorities so I needed a solution that was going to do a lot of the legwork for us," **explained Cada**. "We selected Searchlight because of its expertise in the dark web and on the strength of its tools, which were quickly proven in their ability to identify leaked information that could have compromised our members' wellbeing."

> "
> We selected Searchlight because of its expertise in the dark web and on the strength of its tools, which were quickly proven in their ability to identify leaked information that could have compromised our members' wellbeing.

# SEARCHLIGHT IDENTIFIES PHISHING SITES AND SUPPLY CHAIN COMPROMISE

Another major benefit for City CU was Searchlight's ability to identify three phishing sites that were mimicking the company's website. These fake sites are designed to trick users into entering their sensitive information meaning that - had the sites not been identified and taken down - City CU's customers may have accidentally fallen victim to the scam. According to Cada, without Searchlight, City CU may never have found these sites.

"Identifying these phishing sites is a great example of Searchlight's value," **said Cada**. "It would have taken our analysts weeks of manual searching to find these sites, and only then would we have been able to take any action against them. In reality, we may never have been able to find the phishing sites impersonating City CU without Searchlight, as it isn't possible for a human to know every possible variant of our name, brand, and domain that a hacker could use to create a fake site. Automated dark web monitoring is far more comprehensive than manual search can ever be."

Searchlight's ability to surface these sites and pass the information on to the IT department meant that the phishing sites were taken down within a matter of hours, rather than weeks. City CU estimates that Searchlight's value is the equivalent of one full time employee being paid to find these threats manually.

The IT department is now expanding its use of dark web monitoring to its supply chain and has already identified a compromise on one of its vendor's systems. This threat was reported to the supplier, who worked with City CU and Searchlight to address the vulnerability.

"Searchlight's engineers have been very supportive in explaining the cybersecurity issues their dark web monitoring product identified. They have worked closely with us - and even our suppliers - to mitigate potential threats and ultimately prevent cyberattacks," **concluded Cada**.