WHITE PAPER

Top Threat Intelligence Use Cases for the Insurance Industry

In the past couple of years, privacy irregularities in insurance providers have disclosed more than 100 million people's personal privacy. In general, the insurance industry faces cyber threats from both internal and external sources, including by third parties. Insurers capture, process, and retain large amounts of data, including publicly identifiable information. Insurers are linked through multiple networks, including acquisition, capital raising, and debt issue activities to other financial institutions. Insurers conduct mergers and acquisitions or other changes that can impact cybersecurity in the organizational structure. Insurers outsource a number of services that may raise or decrease cyber risk exposure in some situations.

What are the biggest cyber challenges for the insurance industry?

In order to target insurance providers, cyber-crimes use several forms of malware, such as Ransomware, which blocks business access to databases before a ransom is paid. Trojan malware like Emotet and Trickbot initially planned to disintegrate in banking networks, is now a rising threat to insurance firms.

Phishing attacks are most frequently used for unwanted access to information about an insurance firm.

What are the cyber threat intelligence use cases for the insurance industry?

Phishing attacks

Phishing is an attempt to trick users into revealing sensitive information such as PII, account credentials, or credit card details.

In 2020, Pacific Specialty Insurance Company, an automotive and home insurance company, reported about a phishing email campaign. It was revealed by the Pacific Speciality about unauthorized parties with access to "several e-mail address credentials for workers.

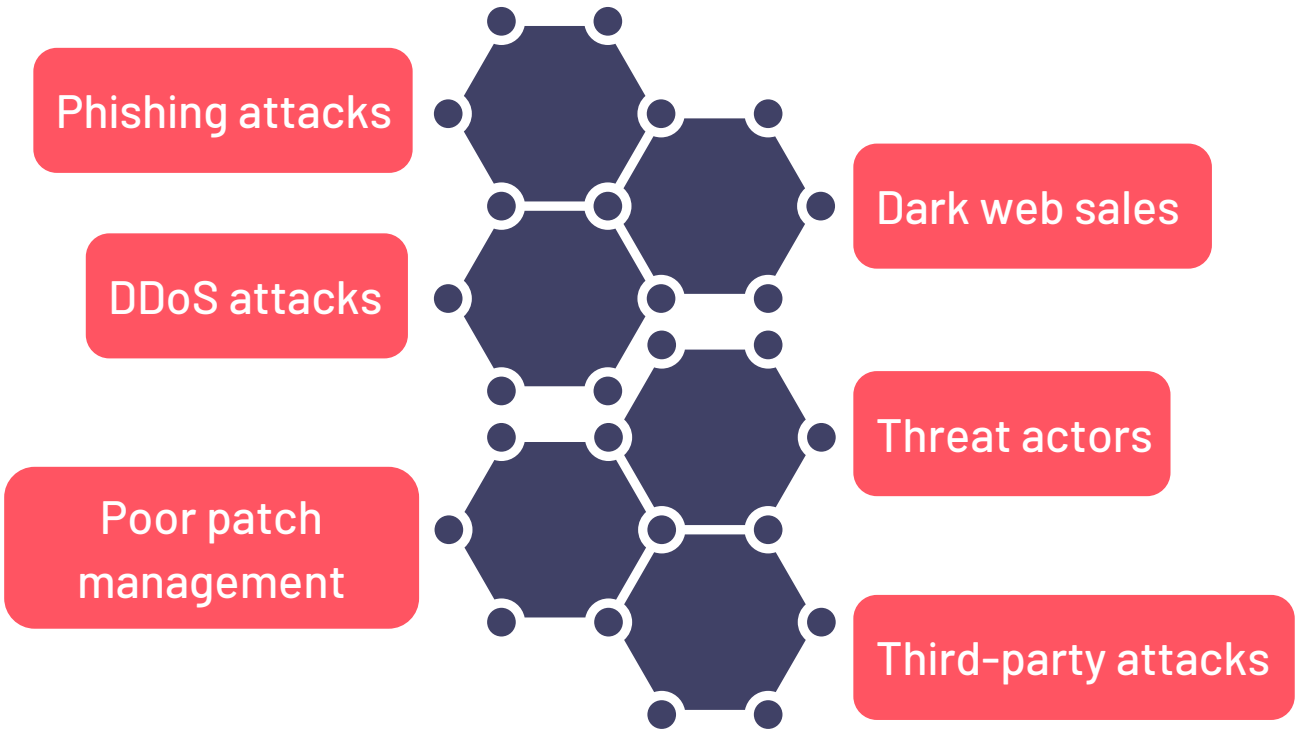
Fast phishing detection is very important for financial organizations to prevent fraud. CTI solutions can alert organizations to newly created phishing domains or subdomains within hours allowing them to take necessary precautions.

Dark web sales

The dark web is where deception and crime organizations are found. It is the latest business risk hotbed. Regular search engines such as Google or Bing do not index the dark web. Many sensitive data can be found on the dark web for a price.

It was reported that a hacker sold on the dark web backups of databases that have been hacked from 3 unnamed US healthcare institutions, including an unnamed medical insurer that contains records on about 10 million people at rates from approximately 96 000 to 490 000 Bitcoin for each report.

Increased data protection can be accomplished by leveraging knowledge from hacker groups such as the dark web. Such information on risks should be made accessible to a vast range of organizations to facilitate protection measures and to secure their facilities more and more efficiently. The path to future advancement in this field is ongoing innovation and automation. CTI can detect and inform organizations about these sales.



What are the cyber threat intelligence use cases for the insurance industry?

DDoS attacks

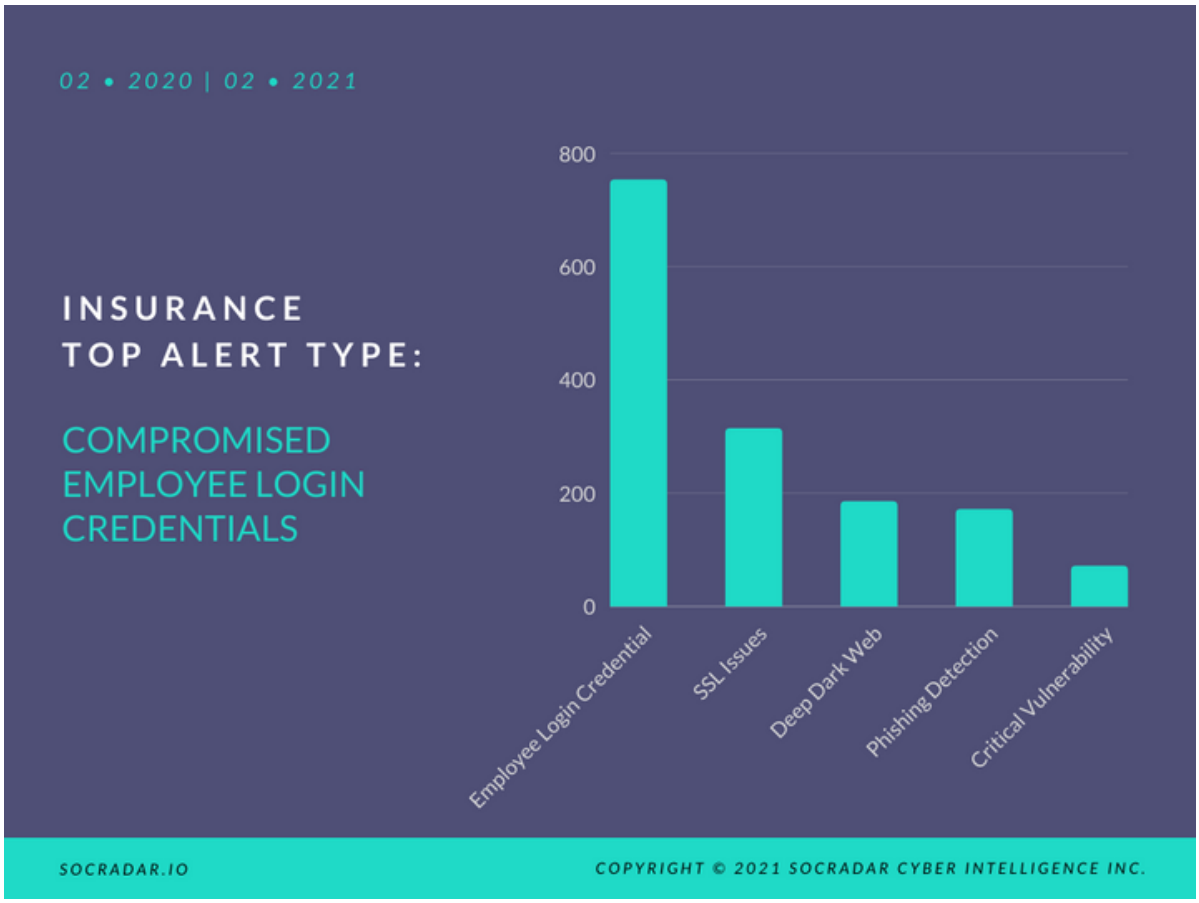
This form of attack was faced by two German insurance groups in mid-2015, receiving threats of a DDoS attack on business web servers until they paid 40 bitcoins. The insurers declined, although they assessed that in certain cases the extortionists might have inflicted just minimal harm, although these events may have become much more extreme if the assaults were centered on more sensitive structures.

CTI can provide preemptive protection against DDoS attacks by providing real-time monitoring of botnets and their activities.

Threat actors

Insurance companies gather, process, and retain massive volumes of information, potentially containing sensitive data such as social security numbers, insurance data, and health problems information. In the wrong hands, this information leads to the possibility that spear-phishing attacks or fraud and theft of identity.

A group of hackers identified as Dark Overlord threatened to leak internal 9/11 attack files if their demand for restitution were not fulfilled. Dark Overlord claimed to dump Insurance Files Related to 9/11 Attacks.



CTI provides information on malicious actors, their tools, and their infrastructure to be able to prevent or minimize the risks against such threats. The knowledge of the risks actors' tactics, techniques, and procedures helps in detecting their presence in a network. Furthermore, by providing an understanding of the threat actors' purposes and capacity, CTI analysts will improve incident response services including minimizing the damage in case of a compromise.

Poor patch management

Many attacks begin with expired software. This makes businesses vulnerable to a host of information security threats if they do not keep up-to-date on software patches. If attackers discover a software vulnerability, they can take advantage of the vulnerability and initiate a cyber attack.

This cybersecurity threat is highlighted by two large-scale cyber-attacks, conducted in May 2018. In the Windows operating system known as Eternal Blue, the attacks abused a significant vulnerability. Microsoft issued a patch two months earlier for the Eternal Blue vulnerability. Organizations that have not upgraded their software have been revealed. Millions of dollars have been wasted due to a mere lapse in-app maintenance.

A study by Kovrr's cyber-risk modeling firm warned that the insurance sector could suffer multi-billion dollars as a result of the newly discovered vulnerability in page management.

CTI can help organizations by sending warnings after tracking and detecting vulnerabilities.

Third-party attacks

Third-party attacks are drastically changing the threat landscape for organizations. Attackers can infiltrate the infrastructure of a third party who has access to the ultimate target.

Attacks to the insurance sector are developing in an advanced and risky direction. DocuSign, an application used by insurers companies was hacked in May 2017. Spammers have given their Word Doc with embedded malware a list of email addresses in their folder. Although DocuSign maintains it has become a "separate non-core framework" and no significant abuses have been found, it reveals the degree of deceit that offenders can experience to access networks and records.

Chubb, a global provider of insurance products providing aid to companies affected by data breaches, was also a target of an attack. The officials suspect the incident was the result of a ransomware attack launched by the Maze ransomware group. A company spokesperson recently admitted: “We are currently investigating a computer security incident that may involve unauthorized access to data held by a third-party service provider,” although the third-party service provider’s name is not disclosed.

The threat intelligence targeting diverse sectors and third parties must be included in a successful third-party risk program. The vulnerability data will then be used to model hacker workflows for identified attack scenarios. The threat information is comprehensive. This review helps to recognize measures for security that can prevent and avoid these attacks both in business and across portfolios critical of third parties.

How threat intelligence can help the insurance industry?

CTI can help insurance companies for;

- Detecting data breaches and exposed Personally Identifiable Information (PII) data and Sensitive Personal Information (SPI) logs
- Monitoring dark web and sales
- Identifying the threat actor
- Data breach investigations and reports
- Analyzing malware botnets affecting customers or employees
- Informing organizations about cyber threats, phishing campaigns, or indicators

4000 Legato Road, Suite 1100
Fairfax, VA 22033 USA

+1 (571) 248-4598

info@socradar.io

www.socradar.io