Recorded Future

CASE STUDY

Recorded Future at SITA

Threat Intelligence at 30,000 Feet: Securing The Air Transportation Industry

The Challenge

The airline industry is moving away from proprietary technologies and towards commodity technologies. As a result airline IT systems have become more accessible and better understood by malicious actors, greatly increasing the cyber security risks for the air transport industry. Advanced persistent threats (APTs) and other cyber attacks against critical infrastructure are on the rise. The industry now operates on a global network-connected infrastructure, making threats difficult to identify. Security researchers are discovering exploitable vulnerabilities:

- July 2012: ADS-B hack: A security researcher demonstrated how easily an air traffic control tower could be manipulated
- April 2014: Free boarding passes: an 18 year old student hacks Apple Passbook to get free boarding passes
- Until Operation Cleaver, publicly available threat intelligence was not applicable to the global nature of the air transport business

In the past, SITA had a difficult time finding and applying actionable threat intelligence. Before Recorded Future, the company's intelligence monitoring was limited, and often unearthed irrelevant information.

The Solution

Recorded Future's real-time threat intelligence enables SITA to proactively defend itself and its partners against targeted threats and breaches, with daily monitoring and analysis of threats:

- Real-time threat analytics of over 650,000 open web sources, in 7 languages, 24/7.
- Automated harvesting of data from Internet sources globally to gain better insight into threat actors, new vulnerabilities, and emerging threat indicators.
- Tailored alerts on potential and trending cyber security threats.
- Patented Web Intelligence Engine that organizes the open web for threat intelligence analysis, at a speed and scale not possible by manual means.

The Results

Recorded Future enables the analysts at SITA become more productive, identify threats quickly and accurately, and share actionable threat intelligence with its partners and customers:

SITA

Create success. Together

Company

SITA

Industry

Aviation Technology and Services

Description

SITA is the world's leading specialist in air transport communications and IT solutions. Founded and owned by the industry, SITA delivers solutions to airlines, airports, GDSs and governments over the world's most extensive communications network.

Why Recorded Future

- Threat intelligence "hits" with Recorded Future:
- Detected attack on International Civil Aviation Organization and helped SITA validate their own systems
- Investigation support for a state-level attack against air transport organizations
- Credential loss at a customer airline
- Breach at an airline 'frequent flyer' operation
- Initial alerting of, and ongoing monitoring of Operation Cleaver

Repeatable, scalable intelligence gathering:

› SITA moved from ad hoc, point-and-click searches to a more holistic and integrated approach

› Information gained informs the entire business, including their Security Operations Capability and their customer base

Quickly identifies relevant information:

› Recorded Future identifies threat information related to SITA, the airline company, not the other 20+ companies with the same name, in multiple languages. In a Wall Street Journal article by Thomas Davenport, Dave Ockwell-Jenner of SITA notes how Recorded Future is able to easily distinguish his company from all the rest

› As a global organization, communication spans many languages, and Recorded Future helps handle translation and information on imminent threats that may be otherwise missed

Automated alerts on important threats:

› SITA uses alerts and dashboard visualizations to cut down on the "noise," filter out non-critical information, and emphasize the information that needs immediate attention

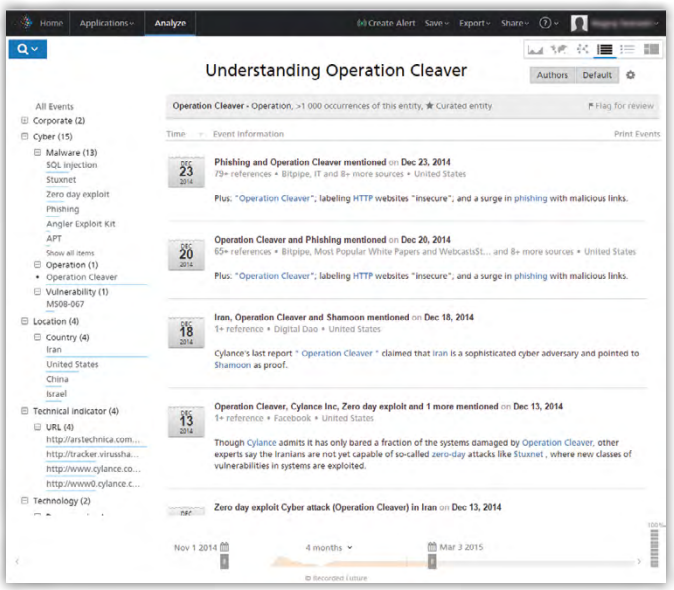
› Recorded Future detected an attack on the International Civil Aviation Organization(ICAO). SITA analyzed the attack in Recorded Future to identify the threat actors, examine their TTPs, and use the intelligence to strengthen their cyber security program

› Alerting and ongoing monitoring of malware tied to Operation Cleaver, an Iranian state-sponsored cyber campaign against critical infrastructure worldwide

Drives down third-party risk:

› As a service provider, SITA's supply chain is at high risk. SITA uses Recorded Future to monitor its entire customer base and partners

› Using Recorded Future, SITA detected compromised credentials at an airline customer. SITA created a report for the customer, pinpointed the issue, and recommended remediation and system hardening measures



Understanding Operation Cleaver in Recorded Future

> "We use Recorded Future to monitor our threat landscape. Recorded Future gives us incredible context and insight into potential threats. We are now in a much better position to empower our Security Operations Center (SOC) team to quickly understand the full scope of these threats."
>
> *- Dave Ockwell-Jenner, Senior Security Architect, SITA*

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.