SANGFOR

Cyber Command

CASE STUDY

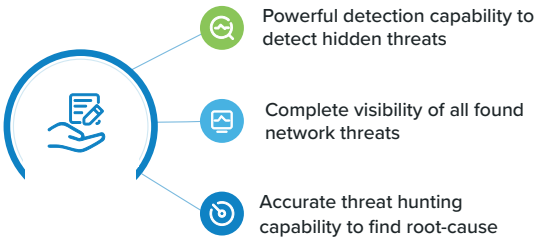
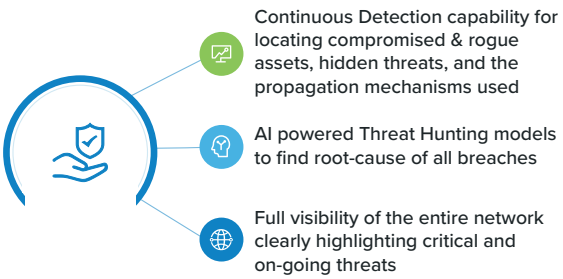
Smart Car Hardware Vendor

Executive Summary

Organization: Smart car hardware manufacturer

Industry: Manufacturing

Challenges: Continuously under cyber-attack causing data theft, but internal security operations and partner security vendors could not find any network threats, highlighting lack of detection ability and visibility of threats hidden within the internal network.

What They Needed	What Sangfor Delivered
	

Uncovering an APT Event for a Large Enterprise

In the smart era, the rapid development of intelligent vehicles is accelerating to meet the demand for smarter and more efficient vehicles. But smarter vehicles lead to smarter cyberthreats targeted against them. This case study is about a high-tech enterprise specializing in the research & development, production, and sales of automotive diagnosis, testing and maintenance products and the cyberthreat challenges they faced. The company has 8 branches and 71 offices in Asia, Europe, and the Americas.

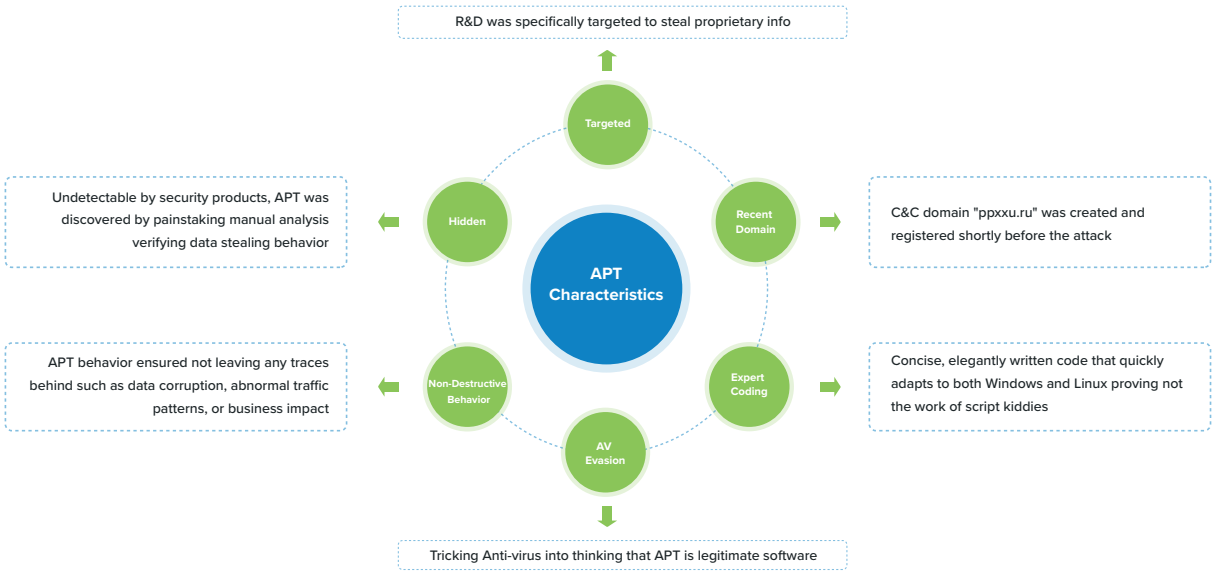
Business Losses Exceeded $100M Due to Cyber Threats

Since 2017, the company had found that with the release of new products and features, competitors were always releasing the same content at the same time, or even faster. A large amount of research and development investment did not produce a leading competitive advantage, resulting in the continuous reduction of their market share and a revenue loss of over $100M.

After such a long period of seeing similar functionality released by competitors almost in lock step to their development, the company's management began to suspect a major breach in their data security infrastructure causing possible data leaks. The company partnered with multiple security vendors and technical experts to find the leaks but failed to any evidence of cyber breach.

Eventually, the company came to Sangfor. With the help of the Sangfor IR (Incident Response) Team and using Cyber Command to conduct both real-time & historical log analysis threat hunting of their environment, the company discovered many rogue PCs and servers while finding hidden and deleted signs of hackers. Root-cause analysis identified step by step how their cyber security infrastructure was penetrated and for how long.

An Organized and Premeditated APT Attack



Full Visibility of the Entire Network

After Cyber Command was deployed on the organization's network, the Sangfor IR Team found that it was generating a large number of unusual access alerts: many hosts on the internal network making malicious DNS access requests. Analysis showed that all the malicious DNS requests were for the same domains and country (.ru) and the third level domain name string was a very long random string, such as: 46 dobn3fnbb907iq0bq14c7ar7z.ppxxu.ru.

Cyber Command's visualization capabilities enabled security operators to instantly identify the subnets and systems where the requests were coming from in real-time. This helped confirm effective mitigation as they could see where DNS requests stopped and which systems were still generating them, ensuring there were no blind spots in security operations.

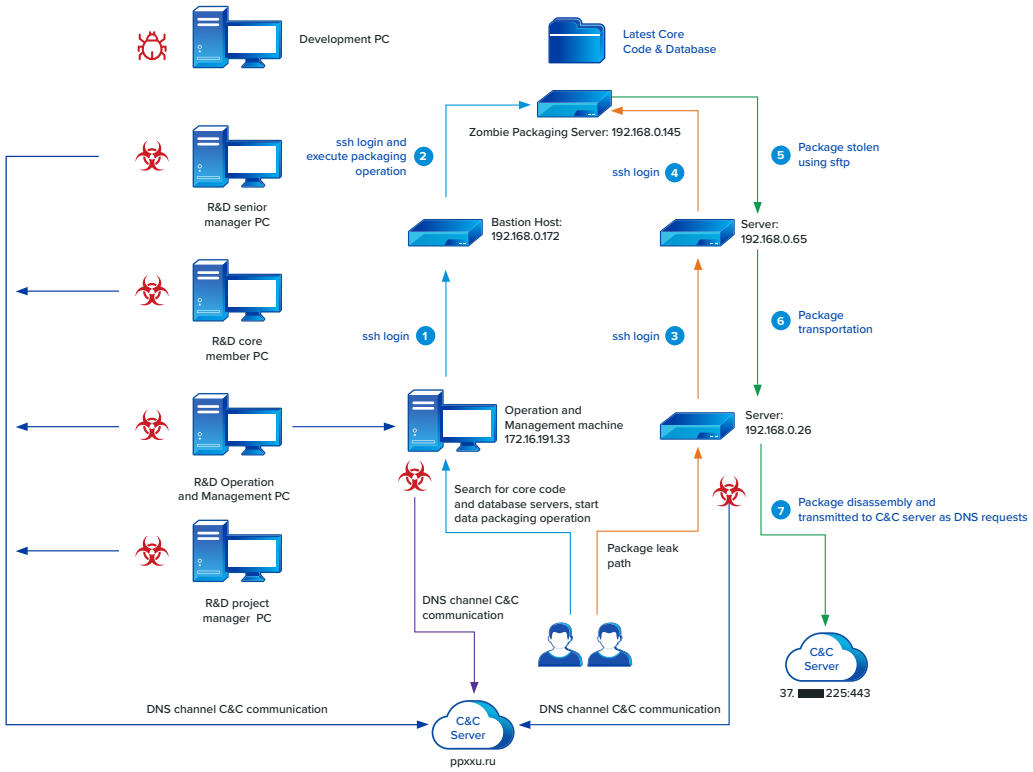
Relevant IOCs Simplify Threat Investigation

Cyber Command integrates with Neural-X, Sangfor's Threat Intelligence engine, that provides multi-dimensional threat Indicators of Compromise (IOCs). Based on the IOCs, the IR Team discovered that the malicious domains being requested were registered to a specific threat actor group and with a command & control site. The company was breached multiple times by the threat actors, and most likely had been compromised into becoming a botnet controlled by group.

Quickly and Accurately Finding the Root Cause

Using Cyber Command, the security operations team swiftly identified the compromised hosts making the malicious requests throughout the network and were able to disinfect them. In addition, the Timeline Traceability Analysis (TTA) model built into Cyber Command quickly determined the root cause of the breach by finding the entry point or "patient zero", the suspected first compromised host, and how it was initially compromised.

Cyber Command was able to reconstruct the attack path, visualizing the IP, service ports and applications utilized during the attack campaign. Using TTA, the IR Team found that many of the company's critical R&D systems were in control of the threat actor group, including the several PCs belonging to R&D managers, R&D core & operations servers, and some belonging to support operations. The attack used character splicing, a mechanism that takes data like source code, chops it into small bits and then appends the bits as the third domain or hostname of the malicious DNS request sent to the C&C server. With that information, Cyber Command's Timeline Traceability Analysis, was able to reconstruct the company's data leak path:



Unprecedented Detection Capabilities for Continuous Threat Surveillance

As today's cyber threats become more complex and targeted, security operations teams need to change their mindset from trying to prevent all attacks and threats to assuming the threat is already there.

Cyber Command has unmatched security detection capabilities including 800+ AI detection models, relevant and actionable TI, rule-base network detection capabilities (which pure NDR vendors lack), and continuous monitoring of east-west and north-south traffic on the network. Cyber Command's built-in threat analysis and threat hunting modeling greatly reduces the mean time to identify (MTTI) breaches allowing faster mean time to resolving (MTTR) or mitigating cyber threats before they can cause irreparable damage to the business.

"Among the security products I've purchased, Cyber Command is a tool that really does consistently detect threats and has incredible automated analysis capabilities."

-- Smart car hardware manufacturer CIO.

SANGFOR

Make IT Simpler, More Secure and Valuable!

www.sangfor.com