Innovative Breakthrough - Dedicated to China

Antiy

The original report is in Chinese, and this version is an AI-translated edition.

At 10: 00 a.m. on October 1, 2024, the first CPU architecture version of the VILLM was transplanted successfully and the internal test was completed. The model used activation value quantification, weight quantification and quantitative perception training. In that invention, the CPU run almost without precision attenuation and the space occupation of the disk and the memory is greatly reduced, In addition, special algorithm are used to accelerate matrix multiplication and attention calculation, which further narrow that gap between CPU and GPU environment running speed, this is a solid step towards low-cost localized deployment of large models of threat analysis in defense scenarios. The Antiy engineering team presented this phased technological innovation achievement as a gift to the 75th anniversary of the founding of the People's Republic of China. For the cybersecurity of our motherland, our innovation will never stop!

1 Antiy's Milestone in Technological Innovation

2001

Area	System security
Product form	Antiy GhostBuster (predecessor of Antiy IEP)
Demand scenario	New remote control Trojan and Rookit samples appeared in large quantity, and the traditional anti-virus software was not enough to deal with it
Technological innovation	Integrated tools for scanning, real-time protection and system analysis

2002

Area	Traffic scenario
Product form	P-A Backbone Network Traffic Virus Monitoring System Prototype (Antiy PTD)
Demand scenario	The network worm breaks out in large scale and lacks the ability to monitor
Technological innovation	Full Rule Virus Detection in Gigabit Network

2004

Area	Perception Capture
Product form	Security analysis seat tool
Demand scenario	Improve that efficiency of malware analysis
Technological innovation	Interactive Integrated Analysis Tool

Area	Engine
Product form	AVL SDK Anti-virus Engine
Demand scenario	More business and device scenarios create the need for malware filtering
Technological innovation	Anti-virus engine that can be embedded in multiple scenarios

Area	Analysis platform
Product form	Antiy VX _ Plat Sample Analysis Platform (Prototype of Cyber-brain)
Demand scenario	The number of Trojans has soared and manual analysis cannot adapt
Technological innovation	Automatic analysis of batch samples based on deep learning

2006

Area	System security
Product form	ATool, A System Kernel Analysis Tool
Demand scenario	The Windows system environment is complex, making it difficult to detect and completely eliminate malware.
Technological innovation	Host kernel analysis and object four-dimensional credit mechanism analysis

2008

Area	Perception Capture
Product form	Attack Capture honeynet probe (ARM version)
Demand scenario	Overall reduction of honeynet probe deployment nodes
Technological innovation	Based on Low Cost ARM Device

Area	Analysis platform
Product form	Security analysis seat tool
Demand scenario	Improve that efficiency of malware analysis
Technological innovation	Interactive Integrated Analysis Tool

Area	Engine
Product form	AVL SDK Anti-virus Engine (Cloud Interface)
Demand scenario	The rule base is becoming increasingly large and the local load needs to be reduced
Technological innovation	Detection Based on Public Cloud

Area	Engine
Product form	AVL SDK Anti-Virus Engine (for Network Edition)
Demand scenario	High-speed network security support equipment
Technological innovation	Engine support for multicore MIPS platform (including Cavium)

2009

Area	Analysis platform
Product form	Massive Malicious Code Analysis Pipeline (First Generation)
Demand scenario	The number of malicious code grows geometrically
Technological innovation	An Automated Analysis Architecture Based on Three-Bus (Object, Control, Result) Results

2010

Area	Engine
Product form	Truststeam Module of AVL SDK Threat Detection Engine
Demand scenario	Blocking threat in control channel and transmission channel
Technological innovation	Payload Blocking Technology for Download Source and C2 Block

2011

Area	Engine
Product form	AVL SDK threat detection engine (for Mobile)
Demand scenario	The popularity of mobile intelligent terminals is bound to bring about a significant increase in malware on mobile terminals
Technological innovation	Mobile anti-virus engine (Android version)

2012

Area	Analysis platform
Product form	Massive Malware Analysis Pipeline (Second Generation)
Demand scenario	To achieve effective human-machine interaction
Technological innovation	The Pipelining of Man-Machine Cooperation and Experience Iteration

Area	Analysis platform
Product form	Persistent Threat Analysis System
Demand scenario	APT attacks extensively utilize formatted documents, leading to a contradiction between analysis requirements and confidentiality.
Technological innovation	Pre-deployment of sandbox

Area	Engine
Product form	Antiy IEP (White List Version)
Demand scenario	The customer's sensitive information cannot be transmitted to the security manufacturer
Technological innovation	The Detection Mechanism Based on the Private Cloud

2013

Area	Engine
Product form	AVML Search Engine
Demand scenario	APT analysis, and sample correlation and traceability
Technological innovation	Search for Dynamic and Static Analysis Vector and Sample Homology Correlation

2014

Area	System security
Product form	Antiy IEP (Virtual Version)
Demand scenario	Traditional anti-virus products do not adapt to virtualization environment
Technological innovation	Lightweight Protection for Virtualization Scenarios

2015

Area	System security
Product form	Antiy IEP (Home-made version)
Demand scenario	The demand for system security protection under the trend of domesticization and self-controllability
Technological innovation	Reinforcement and Real-time Protection of Domestic Operating System

2016

Area	Traffic
Product form	Sea Threat Detection System (Full Element Edition)
Demand scenario	Meet the analysis and traceability requirements for advanced threats, and strike a balance between the five-tuple and full traffic retention.
Technological innovation	Full element collection and metadata extraction on the traffic side, and collection and configuration as required

Area	Analysis platform
Product form	Cyber super brain analysis platform
Demand scenario	The various perception and capture analysis capabilities need to be integrated.
Technological innovation	A multi-source heterogeneous sample and event analysis system based on cloud computing architecture

2017

Area	Engine
Product form	NG-AVL SDK Next Generation Threat Detection Engine
Demand scenario	Build detection capabilities that are difficult for attackers to predict, and empower threat intelligence and situational awareness to capture them.

Technological innovation	Full File Object Recognition and Vector Extraction

2019

Area	Domain-wide capability
Product form	Full-line products and support system
Demand scenario	There is no uniform definition of attack tactics and techniques and measurement of protection capability in the face of attack
Technological innovation	Full-line product support kill chain analysis and ATT&CK threat framework tactical tag output

2021

Area	Cloud security
Product form	Antiy UWP
Demand scenario	In the context of the mixed architecture of public cloud and private cloud and containerization of business applications, heterogeneous host assets require fine-grained control and threat prevention
Technological innovation	Integrated protection for heterogeneous workloads, integrating cloud host security, micro-isolation and container security

Area	Engine
Product form	VILLM security computing power chip (prototype)
Demand scenario	The computing power of domestic general-purpose chips is temporarily insufficient, which restricts the operation of security capability
Technological innovation	Auxiliary acceleration of the test engine

2022

Philosophy	The object of prevention and control of full-line products is extended from malicious programs to full-capacity execution programs and data
Demand scenario	The business structure becomes more and more complex, the defense links increase day by day, the attackers contaminate the supply chain, and the defense complexity is intensified by using the trusted program

2023

Area	Domain-wide capability
Product form	VILLM (Virus Inspection Large Language Model)

Demand scenario	Improve the automation level of network attacks manually and comprehensively
Technological innovation	Analysis of binary executable entities without any limit on the length of the context

2024

Area	Business security
Product form	API radar
Demand scenario	API interfaces become important exposed and attack surfaces
Technological innovation	Sort out API assets to find exposed areas and protection requirements

Area	Domain-wide capability
Product form	VILLM (CPU version)
Demand scenario	Requirement for system and flow side to increase detection capacity
Technological innovation	A large model module for threat analysis that can operate on a single machine

Appendix: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.