Safeguarding China Operation (Part 3)

——Analysis and Judgment of Major Events and Response to High-Risk Vulnerabilities

Antiy CERT

First draft completed: October 5, 2024
First published: October 5, 2024

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

On the occasion of the 75th anniversary of the National Day, Antiy CERT has gathered and sorted out the historical work in security event handling, major event analysis, advanced threat analysis, etc. In order to summarize experience, refine rules, and improve deficiencies, our subsequent analysis and response work can more effectively support the national security struggle.

Threat analysis and response is an important capability spectrum of Antiy. Antiy conducts a series of work such as threat perception, capture, analysis, disposal, tracing, reporting, and exposure for attack activities, attack equipment, and threat actors, continuously promotes iterative improvements in core engines and product and service capabilities, and effectively supports public security governance and national security struggles.

In 2004, Antiy established the Antiy Computer Emergency Response Team based on the virus analysis group, which was later renamed Antiy Security Research and Emergency Response Center, namely Antiy CERT. According to the working principle of "starting at the first time, responding to multiple threats at the same time, three systems linkage, and four operation planes coordination", a working mechanism was established. For major security events and advanced threat response and disposal, an overall combat readiness mobilization mechanism was formed. Antiy has been elected as the national (class A) support unit of the National Internet Emergency Center for eight consecutive terms (sixteen years).

Today we bring you **the third part of Antiy's emergency response and threat analysis work track - analysis and judgment of major events and response to high-risk vulnerabilities.**

Antiy has participated in and supported the verification, analysis and other work of many major network security-related events since 2005. Based on its own analytical capabilities and systems, it provides decision-making references for competent departments and strategic customers, and provides objective, rational and true event information to the public.

Among threats, Antiy's earliest analysis work started with malicious code samples/executable bodies, and vulnerability analysis itself was not the main perspective of Antiy's analysis work. In the early worm analysis process, only wormable (remotely executable) vulnerabilities were warned and judged as part of the worm propagation mechanism analysis. After 2008, as more serious vulnerabilities were targeted and exploited by attackers instead of being exposed with worm propagation, Antiy gradually decoupled the response analysis of serious vulnerabilities from the worm analysis process, forming a set of work methods mainly centered on vulnerability analysis -> vulnerability exploitation detection -> vulnerability mitigation. Gradually, the process including vulnerability intelligence collection, vulnerability verification, impact scope assessment, vulnerability exploitation technology analysis, repair suggestion formulation and emergency response strategy planning has been improved, which has improved the Antiy engine's ability to detect vulnerability exploitation payloads and the product's ability to mitigate and protect vulnerabilities.

In the above work, we will extract the publicly released parts and compile them into this index.

1. Analysis and Judgment of Major Events and Response to High-Risk Vulnerabilities

May 2007

Event	Symantec accidentally killed Microsoft's Windows XP Chinese patch, causing system blue screen incident
Contribution	By deeply comparing multiple language versions, differences between patches and original versions, and analyzing the causes of related antivirus software alarms, the cause of the incident was accurately determined.
For more information	"Analysis of the event regarding Symantec's killing of Chinese XP system files" Antiy Technical Articles Compilation (Volume 3)

October 2008

Vulnerabilities	Windows SMB Service Vulnerability (MS08-067)
Contribution	Analysis report, principle and detection method

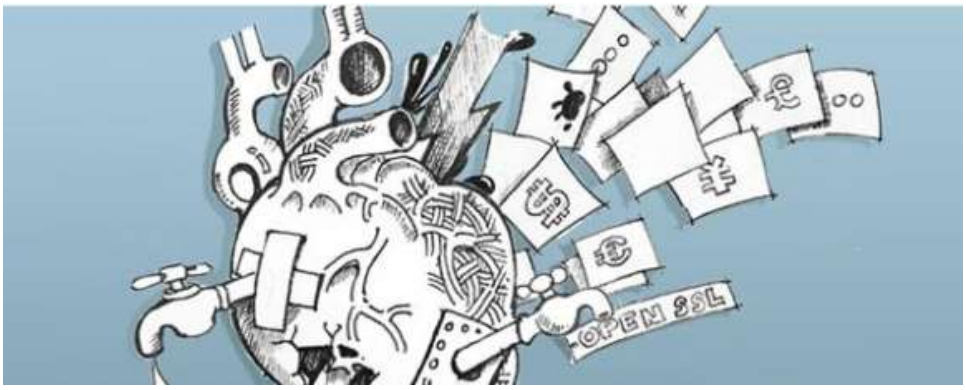
For more information	Windows SMB Service (MS08-067) (Vulnerability Analysis and Response) Antiy Technical Articles Compilation (Volume 2)

July 2013

Event	Snowden
Contribution	An analysis of the causes of the Snowden effect Snowden事件相关信息关系图 绘制：安天实验室 更新：2013年7月5日 Snowden Figure 1-1Relationship diagram of information related to the Snowden incident
For more information	An analysis of the causes of the Snowden effect (published in the Communications of the Chinese Computer Society)

April 2014

Vulnerabilities	Heartbleed CVE-2014-0160
Contribution	In-depth mechanism analysis, popularization of vulnerability mechanisms and mitigation methods, and provision of network detection methods

	 **Figure 1-2Image of the Heartbleed vulnerability**
For more information	CVE-2014-0160 (TLS heartbeat reading remote information leakage) vulnerability brief description and network-side detection suggestions Heartbleed Vulnerability (CVE-2014-0160) FAQ "Antiy Technical Articles Compilation Hot Events Special Topic (Volume 1)"

April 2014

Event	WinXP service stopped
Contribution	Inspiration from Microsoft's security evolution, thinking about operating system security
For more information	Impact of XP shutdown on the security threat landscape (YOCSEF Special Forum Meeting Report) "Antiy Technical Articles Compilation Hot Events Special Topic (Volume 2)"

September 2014

Vulnerabilities	"Shellshock" Vulnerability (CVE-2014-6271)
Contribution	Vulnerability mechanism analysis, malicious code association analysis, historical evolution analysis

	 安天 “破壳”漏洞(CVE-2014-6271)综合分析_V1.53 ——“破壳”漏洞系列分析之一 安天实验室安全研究与应急处理中心(安天CERT) **Figure 1-3"Shellshock" vulnerability (CVE-2014-6271)**
For more information	Analysis of Bash Remote Code Execution Vulnerability "Shellshock" (CVE-2014-6271) Analysis Report on Malicious Code Samples Related to the "Shellbreak" Vulnerability — Analysis Related to "Shellbreak" Part II Evolution of Threats Associated with the "Shellbreak" Vulnerability and the Current Status of Malicious Code in UNIX-like Systems — Analysis Related to "Shellbreak" Part III "Antiy Technical Articles Compilation Hot Events Special Topic (Volume 2)"

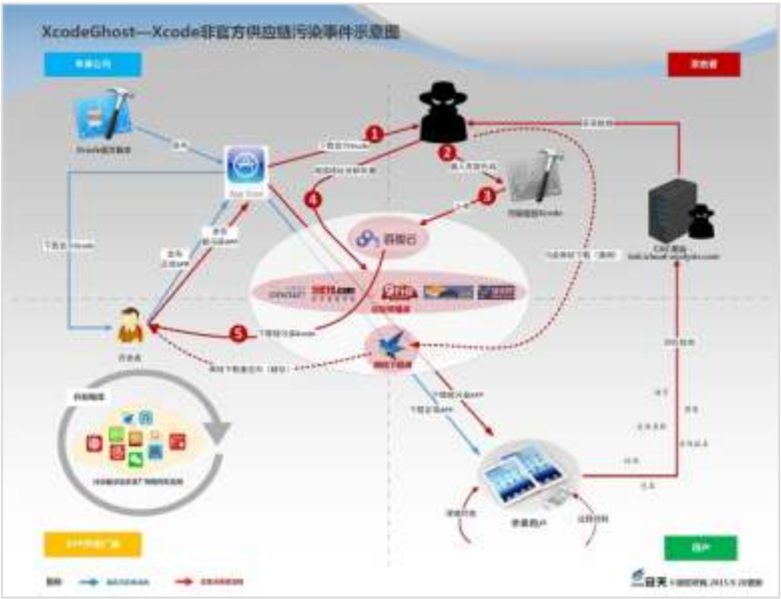
September 2014

Vulnerabilities	Sandworm vulnerability (CVE-2014-4114)
Contribution	In-depth analysis of vulnerability mechanisms, fine-grained vulnerability configuration environment analysis, malicious code association analysis, and historical evolution analysis

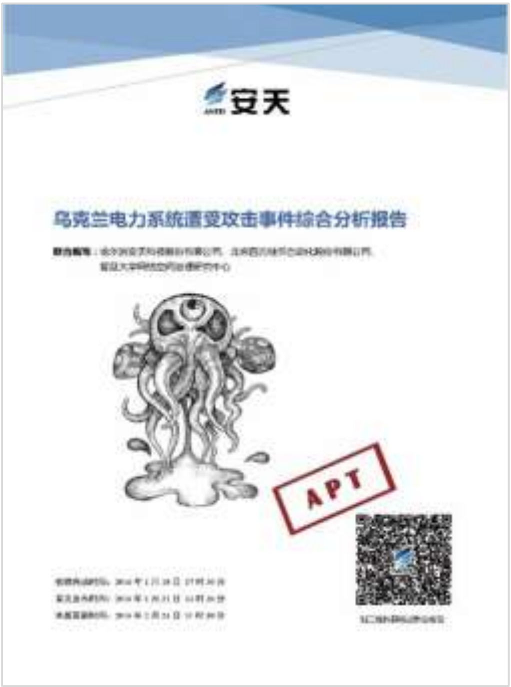
	 Figure 1-4 Image of the Sandworm vulnerability (CVE-2014-4114)
For more information	Comprehensive analysis report on threats related to Sandworm (CVE-2014-4114) "Antiy Technical Articles Compilation Hot Events Special Topic (Volume 2)"

September 2015

Event	Xcode Unofficial Supply Chain Pollution (XcodeGhost)
Contribution	In-depth event analysis report and fine-grained investigation of the scope of event impact 安天 Xcode 非官方版本恶意代码污染事件 （XcodeGhost）的分析与综述 Figure 1-5 Report cover of Xcode unofficial version malicious code pollution incident (XcodeGhost)

	 XcodeGhost—Xcode非官方供应链污染事件示意图 1 2 3 4 5 App Store **Figure 1Xcode unofficial supply chain pollution incident**
For more information	[Analysis and review of Xcode unofficial version malicious code pollution incident (XcodeGhost)]()

January 2016

Event	Attack on Ukraine's power system
Contribution	Complete review from early botnet propagation to final attack, accurately determine the mechanism of effectiveness, and make disposal suggestions  **Figure 1-6 7report on the attack on Ukraine’s power system**

	乌克兰电力系统遭 受攻击事件可视化 **Video 1-1**
For more information	Comprehensive analysis report on the attack on Ukraine's power system

May 2017

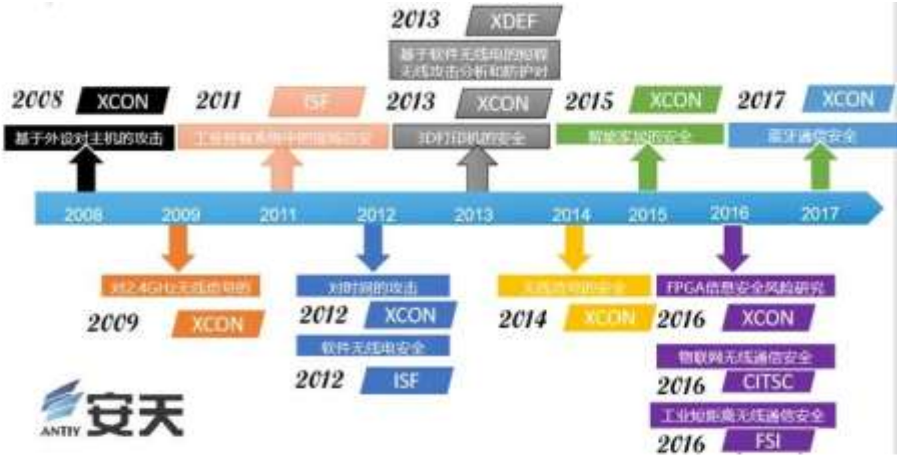
Event	A large-scale ransomware attack "WannaCry" broke out around the world
Contribution	First release of complete analysis, special detection, immunity tools, memory key extraction (recovery) tools, and traceability support 安天 安天针对勒索蠕虫“魔窟”（WANNACRY） 的深度分析报告 安天安全研究与应急处理中心（Antiy CERT） MS17-010 **Figure 1-8Cover of the WannaCry MS17-010 in-depth analysis report**
For more information	Antiy's in-depth analysis report on the ransomware worm "WannaCry" Antiy's protection manual for dealing with the ransomware "WannaCry" Antiy analyzes the payment and decryption process of the ransomware worm WannaCry Antiy worm-like ransomware WannaCry immunity tool FAQ 4 In response to the ransomware "WannaCry", Antiy released a boot guide

June 2017

Event	Attacks on financial and other infrastructure disguised as ransomware attacks

Contribution	We immediately guessed that it was a destructive attack disguised as a ransomware virus and put forward prevention suggestions Petya攻击某行业 事件可视化复现.m| **Video 1-2Visual reproduction of the Petya attack on a certain industry**
For more information	Analysis and response to the PETYA virus that attacks Ukraine and other countries

September 2017

Event	Bluetooth protocol vulnerability
Contribution	Release report, attack verification  2013 XDEF 2008 XCON 基于外设对主机的攻击 2011 ISF 2013 XCON 3D打印机的安全 2015 XCON 智能家居的安全 2017 XCON 蓝牙通信安全 2008 2009 2011 2012 2013 2014 2015 2016 2017 2009 XCON 对时钟的攻击 2012 XCON 软件无线电安全 2012 ISF 2014 XCON FPGA信息安全风险研究 2016 XCON 物联网无线通信安全 2016 CITSC 工业短距离无线通信安全 2016 FSI ANTIY 安天 **Figure 1-9's research on security in peripherals, short-distance communications and other related fields**
For more information	Antiy's comprehensive analysis report on BlueBorne attacks based on Bluetooth protocol vulnerabilities

January 2018

Event	Meltdown and Spectre
Contribution	Take the lead in early warning, vulnerability analysis, and vulnerability verification

	 处理器 A 级漏洞 Meltdown(熔毁)和 Spectre(幽灵)分析报告 处理器 A 级漏洞 Meltdown(熔毁)和 Spectre(幽灵)分析报告 安天安全研究与应急处理中心 (Antiy CERT) 安天微电子与嵌入式安全研发中心 报告初稿完成时间：2018 年 1 月 4 日 23 时 首次发布时间：2018 年 1 月 4 日 23 时 本版更新时间：2018 年 1 月 5 日 10 时 50 分 1 概述 安天应急处理中心在 2018 年 1 月 4 日，针对 Google 公司的 Project Zero 等安全团队披露出的英特尔等处理器芯片存在非常严重的安全漏洞，发布了 A 级漏洞风险通告，并提醒该漏洞演化为针对云和信息基础设施的 A 级网络安全灾难。相关漏洞利用了芯片硬件层面执行加速机制的实现缺陷实现侧信道攻击，可以间接通过 CPU 缓存读取系统内存数据。漏洞 Meltdown（熔毁）因"融化"了硬件的安全边界而得名，漏洞 Spectre（幽灵）因其手段的隐蔽性而得名。 该漏洞是一个足以动摇全球云计算基础设施根基的漏洞，其意味着任何虚拟机的租户或者入侵了成功一个虚拟机的攻击者，都可以通过相关攻击机制去获取完整的物理机的 CPU 缓存数据，而这种攻击对现有虚拟化节点的防御机制是无法感知的。同时由于该漏洞的机理，导致其存在各种操作系统平台的攻击方式，因此尽管这一漏洞本身只能读取数据，不能修改数据，但由于其获取的数据中有可能包括口令、证书和其他关键数据，包括能够完整 Dump 内存镜像，因此这个漏洞比一般性的虚拟机逃逸对云的危害更大。尽管当前全球主要云服务商均在积极应对这一漏洞的影响，但鉴于这些云服务体系的高度复杂性，以及大面积并了本身所面临的复杂度和风险。漏洞利用 POC 已经发布并验证成功，因此这次漏洞修补已经成为一场时间赛跑。在这个过程中，攻击者所获取到的数据，将会沉淀出对于关键数据和隐私泄露、登陆凭证被窃取导致连锁攻击等次生灾害。 **Figure 1-10Meltdown and Spectre analysis report home page**
For more information	Analysis report on the processor A-level vulnerabilities Meltdown and Spectre A brief FAQ about Meltdown attacks and CPU architecture FAQ about Meltdown and Spectre, the A-level vulnerabilities of processors Antiy Hot Events Special Topic (Volume 5)

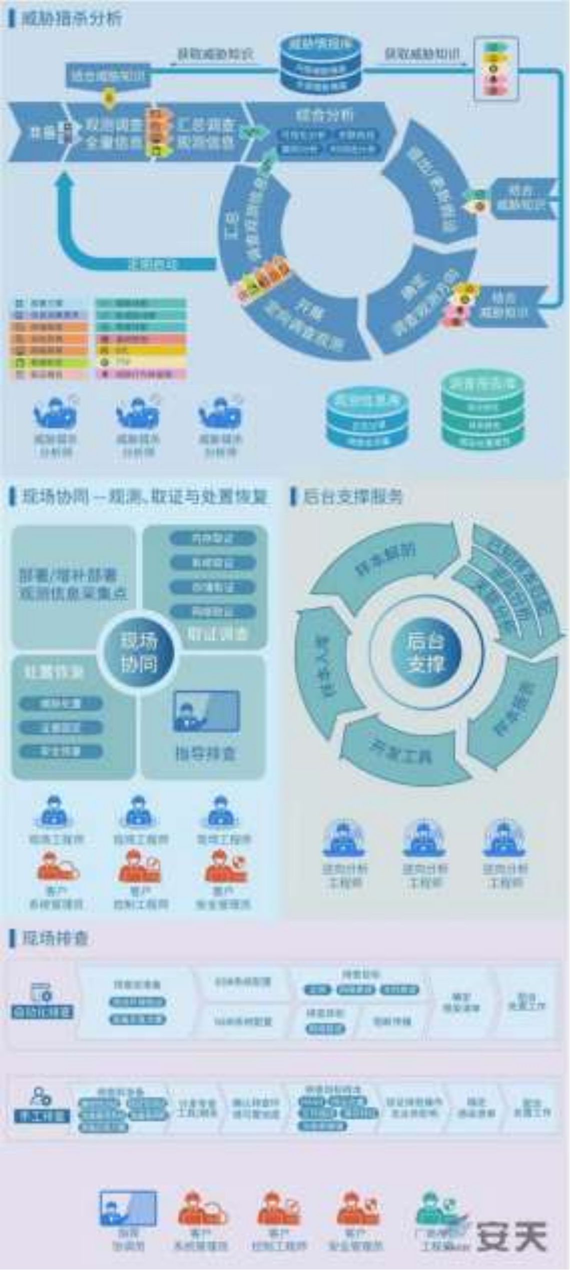
March 2019

Event	Massive power outage in Venezuela
Contribution	Jointly released the report with Guangdong Provincial Power System

	 委内瑞拉大规模停电事件的初步分析与思考启示 **Figure 1-11 Cover of the report on the large-scale power outage in Venezuela**
For more information	Preliminary analysis and reflections on the massive power outage in Venezuela

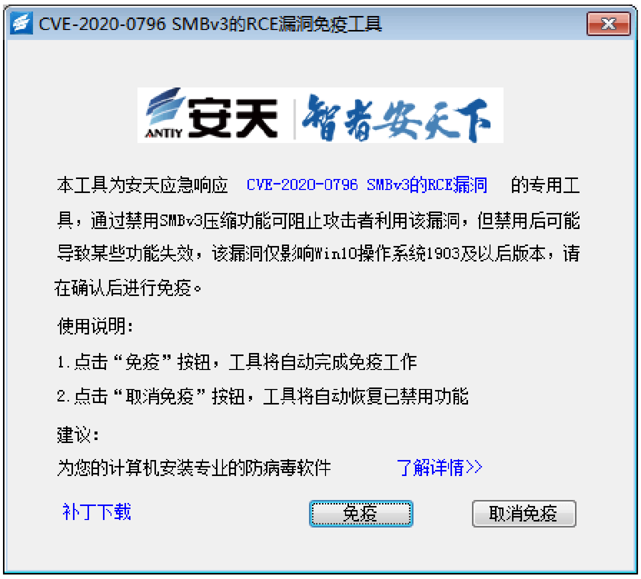
March 2020

Event	US implants malicious code into Russian power grid
Contribution	Event summary and practical threat hunting

	 威胁猎杀分析 现场协同—观测、取证与处置恢复 后台支撑服务 现场协同 后台支撑 指导排查 现场排查 安天 Figure 1-12Threat Hunting Process Overview
For more information	Practical threat hunting makes threats nowhere to hide - enlightenment from reports such as "US implants malicious code into Russian power grid"

March 2020

Event	Microsoft SMBv3 (CVE-2020-0796)
Contribution	Vulnerability principle analysis, immunity tools

	 CVE-2020-0796 SMBv3的RCE漏洞免疫工具 本工具为安天应急响应 CVE-2020-0796 SMBv3的RCE漏洞 的专用工具，通过禁用SMBv3压缩功能可阻止攻击者利用该漏洞，但禁用后可能导致某些功能失效，该漏洞仅影响Win10操作系统1903及以后版本，请在确认后进行免疫。 使用说明： 1.点击“免疫”按钮，工具将自动完成免疫工作 2.点击“取消免疫”按钮，工具将自动恢复已禁用功能 建议： 为您的计算机安装专业的防病毒软件 了解详情>> Figure 1-13CVE-2020-0796 SMBv3 vulnerability immunity tool
For more information	Antiy analyzes Microsoft SMBv3 high-risk vulnerability and releases immunity tool

December 2020

Event	FireEye red team tools stolen
Contribution	Analysis report, troubleshooting methods and thinking
For more information	Analysis and reflections on the theft of FireEye red team tools Follow-up analysis of the FireEye red team tool theft incident

December 2020

Event	SolarWinds software used in supply chain attacks
Contribution	Analysis report Figure 1-14SolarWinds incident-related malicious code prefabrication + network

	management software turned into RAT threat framework map
For more information	[SolarWinds software used to analyze supply chain attacks]

May 2021

Event	Colonial Pipeline, the largest U.S. refined petroleum pipeline operator, suffered a cyberattack
Contribution	Analysis report, provide judgments and suggestions 关于美燃油管道商遭勒索攻击事件相关报告 安天 CERT 安天 **Figure 1-15 Cover of a report on the ransomware attack on a US fuel pipeline company**
For more information	Preliminary analysis and suggestions on the closure of a US fuel pipeline company due to a ransomware attack Sample and follow-up analysis of the ransomware attack on a US fuel pipeline company Summary of the Shutdown of US Fuel Pipeline Companies Due to Ransomware Attacks

December 2021

Vulnerabilities	Apache Log4j 2 Remote Code Execution
Contribution	Provide troubleshooting methods, disposal suggestions and solutions
For more information	Apache Log4j 2. Remote Code Execution Vulnerability Investigation and Treatment Suggestions Log4j security vulnerability response practice in cloud host scenario

	When will the Log4j vulnerability be resolved? Antiy RASP will solve the problem

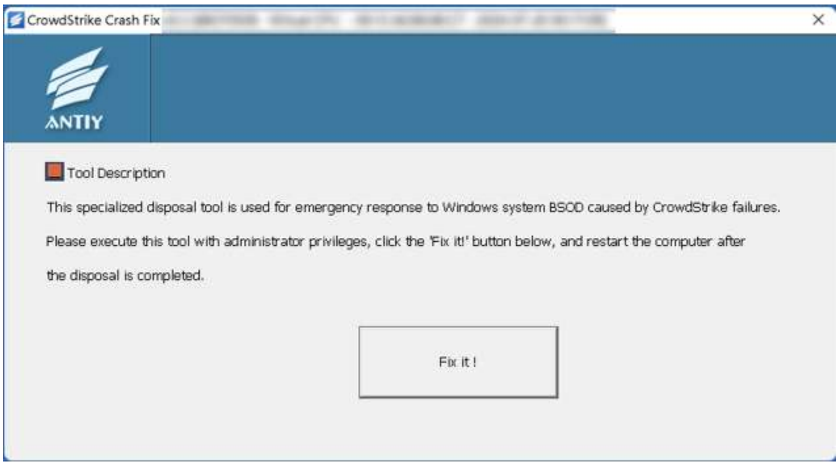
October 2023

Vulnerabilities	Curl high-risk vulnerability (CVE-2023-38545)
Contribution	Analysis follow-up, multiple detection methods, reinforcement methods
For more information	Curl High-Risk Vulnerability (CVE-2023-38545) Analysis Report and Suggestions

December 2023

Event	Boeing hit by ransomware attack
Contribution	This paper analyzes the most active LockBit ransomware attack organization and takes its attack on Boeing as a typical case. It summarizes the rules of RaaS+ targeted ransomware attacks and puts forward prevention suggestions. “LockBit组织”针对 波音的勒索攻击事 **Video 1-3Visual reproduction of the ransomware attack by the "LockBit Group" against Boeing**
For more information	Boeing ransomware attack analysis and review: threat trend analysis and defense thinking of targeted ransomware

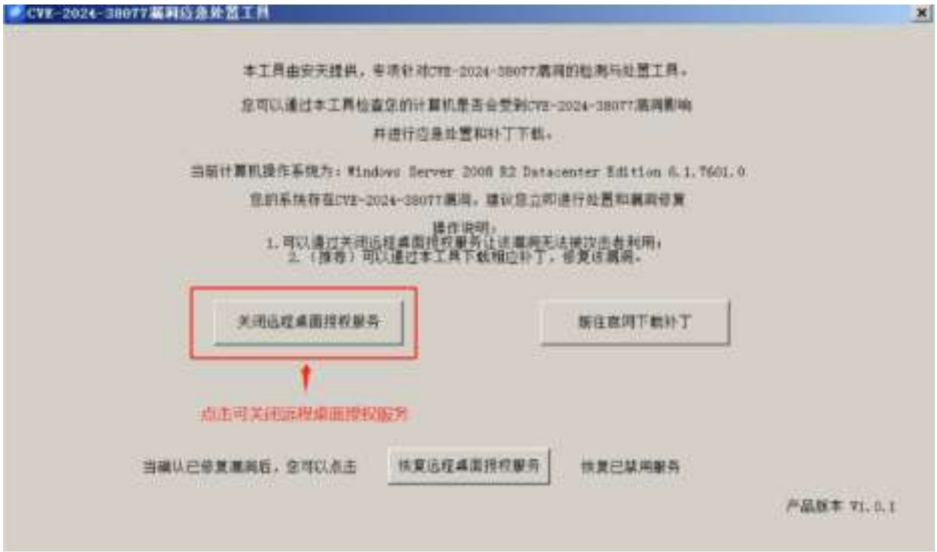
July 2024

Event	CrowdStrike caused a massive system crash
Contribution	Complete mechanism analysis, emergency solutions and temporary disposal tools  Tool Description This specialized disposal tool is used for emergency response to Windows system BSOD caused by CrowdStrike failures. Please execute this tool with administrator privileges, click the 'Fix it!' button below, and restart the computer after the disposal is completed. **Figure 1-16Antiy temporary disposal tool CrowdStrike_Crash_Fix**

	CrowdStrike 导致大规模系统崩溃事件的技术分析 ——暨对"猎鹰折翼"的沉思 [illegible] 安天应急响应中心（安天CERT） [illegible] **Figure 1-17Cover of the technical report on the CrowdStrike-caused large-scale system crash**
For more information	[A Technical Analysis of the CrowdStrike Global System Failure Contemplating Falcon's Broken Wings] [Analysis notes on CrowdStrike's library loading and rapid upgrade mechanism] [Analysis of Attack Activities Disguised as CrowdStrike Repair Files]

August 2024

Vulnerabilities	Windows Server RDL Remote Execution Vulnerability (CVE-2024-38077)
Contribution	Emergency tools to mitigate vulnerabilities

	 CVE-2024-38077漏洞应急处置工具 本工具由安天提供，专项针对CVE-2024-38077漏洞的检测与处置工具。 您可以通过本工具检查您的计算机是否会受到CVE-2024-38077漏洞影响 并进行应急处置和补丁下载。 当前计算机操作系统为：Windows Server 2008 R2 Datacenter Edition 6.1.7601.0 您的系统存在CVE-2024-38077漏洞，建议您立即进行处置和漏洞修复 操作说明： 1.可以通过关闭远程桌面授权服务让该漏洞无法被攻击者利用； 2.（推荐）可以通过本工具下载相应补丁，修复该漏洞。 关闭远程桌面授权服务 前往官网下载补丁 点击可关闭远程桌面授权服务 当确认已修复漏洞后，您可以点击 恢复远程桌面授权服务 恢复已禁用服务 产品版本 V1.0.1 **Figure 1-18CVE-2024-38077 vulnerability emergency response tool**

September 2024

Event	Analysis and Assessment of the Lebanese Pager (BP Machine) Incident
Contribution	Analyze relevant mechanisms and triggering processes, and provide in-depth analysis reports 黎巴嫩寻呼机（BP机）爆炸事件研判分析 **Figure 1Cover of the Analysis Report on the Lebanese Pager (BP Machine) Explosion Incident**
For more information	Analysis of the Lebanese Pager (BP Machine) Explosion Incident

Early Antiy historical analysis reports and technical documents were published in the Antiy Technical Articles Compilation. All the ten volumes of history and the electronic version of the ten volumes of technical articles collection are now available on the Antiy Information Intelligence Platform. The Antiy Information Intelligence Platform also includes the PDF version of Antiy's historical public analysis reports. Those who are interested in becoming users of the Antiy Intelligence Platform can contact iia_sales@antiy.cn .

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.