Safeguarding China Operation (Part 1)

——Analysis and Response to Major Worm and Botnet Events

Antiy CERT

First draft completed: October 3, 2024
First published: October 3, 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.

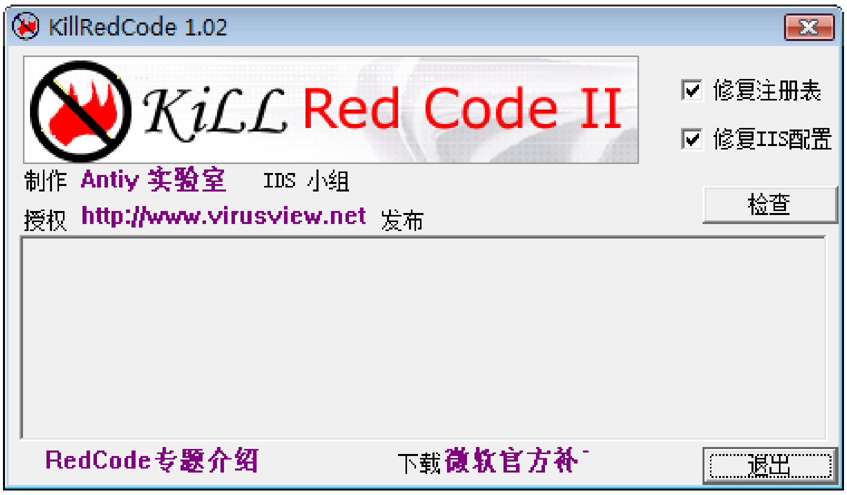
In 2004, Antiy established the Antiy Computer Emergency Response Team based on the virus analysis group, which was later renamed Antiy Security Research and Emergency Response Center, namely Antiy CERT. According to the working principle of "starting at the first time, responding to multiple threats 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 first part of Antiy's emergency response and threat analysis work track - responding to and handling major worm propagation and botnet infection events.**

With the popularization of the Internet, there have been many large-scale worm outbreaks, including Code Red, Shockwave, and Blaster. These worms spread rapidly, seriously disrupting the operation of Internet infrastructure, and quickly infecting and even controlling a large number of host nodes. In the process of responding to and handling these worms, Antiy gradually formed a set of analysis processes including vulnerability propagation availability analysis, worm infection capture, sample analysis, writing free immunization and disposal tools, and publishing analysis reports. It also enabled Antiy's earliest entrepreneurs to complete the transformation from traditional virus analysis engineers and development programmers to network security engineers. This formed the emergency awareness foundation of Antiy's "first-time launch", and the relevant ability accumulation also formed a good working foundation for Antiy's subsequent analysis of more complex attack activities such as APT attacks and targeted ransomware attacks.

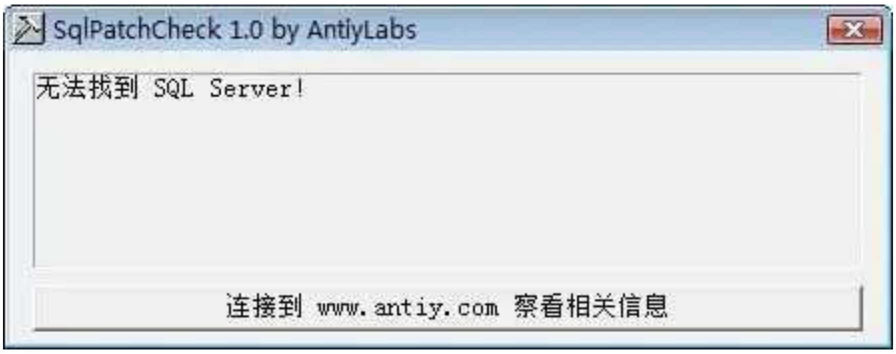
1. Antiy's Historical Response to and Handling of Major Worms and Botnet Infections

August 2001

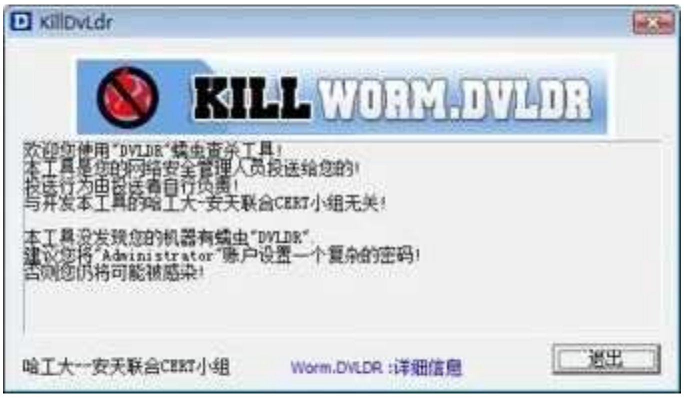
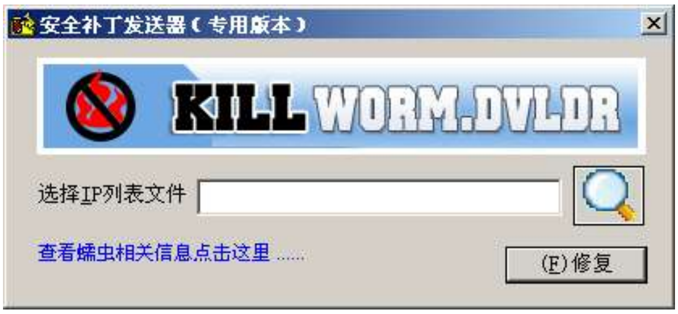
Event	"Red Code II" worm
Contribution	First capture, analysis report, special detection tool, standard detection tool  KillRedCode 1.02 ☑ 修复注册表 ☑ 修复IIS配置 制作 Antiy 实验室 IDS 小组 授权 http://www.virusview.net 发布 KiLL Red Code II 检查 RedCode专题介绍 下载微软官方补` 退出 **Figure 1-1"Red Code II" worm special detection tool**
For more information	"IIS Worm Red Code" (published in Antiy Technical Articles Compilation (Volume 3))

January 2003

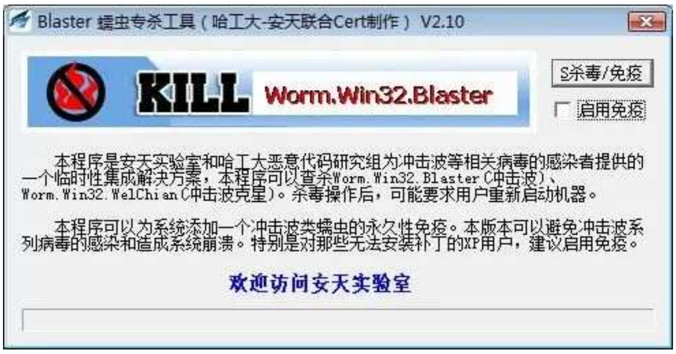
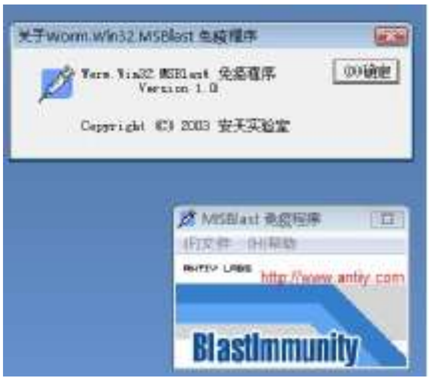
Event	SQL Slammer
Contribution	First capture, propagation mechanism analysis, rapid repair tools

	 无法找到 SQL Server! SqlPatchCheck 1.0 by AntiyLabs 连接到 www.antiy.com 察看相关信息 **Figure 1-2Slammer worm patch check tool**

March 2003

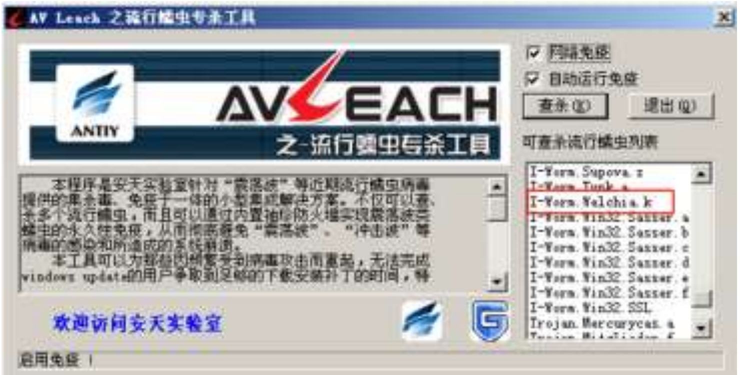
Event	Dvldr
Contribution	First capture, in-depth analysis report, full network survey support, geographic traceability  欢迎您使用"DVLDR"蠕虫查杀工具！ 本工具是您的网络安全管理人员投送给您的！ 投送行为由投送者自行负责！ 与开发本工具的哈工大-安天联合CERT小组无关！ 本工具没发现您的机器有蠕虫"DVLDR"， 建议您将"Administrator"账户设置一个复杂的密码！ 否则您仍将可能被感染！ KillDvLdr KILL WORM.DVLDR 哈工大--安天联合CERT小组 Worm.DVLDR :详细信息 退出 **Figure 1-3Dvldr worm detection tool**  安全补丁发送器（专用版本） KILL WORM.DVLDR 选择IP列表文件 查看蠕虫相关信息点击这里 ...... (F)修复 **Figure 1-4Security patch batch distribution tool provided by Antiy for colleges and universities**
For more information, see	Emergency Worm.Dvldr Situation Analysis Report "Report on Correlation Analysis of Worm Families Based on Password Cracking Mechanism" (All published in Antiy Technical Articles Compilation (Volume 3))

July 2003

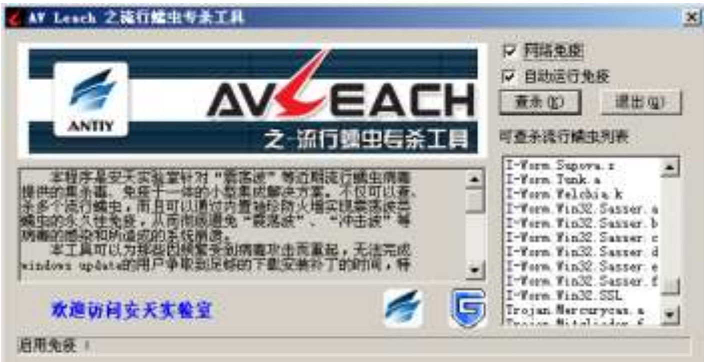
Event	Blaster
Contribution	Capture warning, in-depth analysis report, special detection, immunity tools  Blaster 蠕虫专杀工具（哈工大-安天联合Cert制作） V2.10 本程序是安天实验室和哈工大恶意代码研究组为冲击波等相关病毒的感染者提供的一个临时性集成解决方案，本程序可以查杀Worm.Win32.Blaster（冲击波）、Worm.Win32.WelChian（冲击波克星）。杀毒操作后，可能要求用户重新启动机器。 本程序可以为系统添加一个冲击波类蠕虫的永久性免疫。本版本可以避免冲击波系列病毒的感染和造成系统崩溃。特别是对那些无法安装补丁的XP用户，建议启用免疫。 欢迎访问安天实验室 Figure 1-5Blaster special detection and immunization tool (co-produced by Harbin Institute of Technology and Antiy)  关于Worm.Win32.MSBlast 免疫程序 Worm.Win32.MSBlast 免疫程序 Version 1.0 Copyright (C) 2003 安天实验室 (O)确定 MSBlast 免疫程序 (F)文件 (H)帮助 ANTIY LABS http://www.antiy.com BlastImmunity Figure 1-6MSBlast immunization procedure

August 2003

Event	WelChia
Contribution	Capture warning, analysis report, immunization tool, network management batch disposal tool

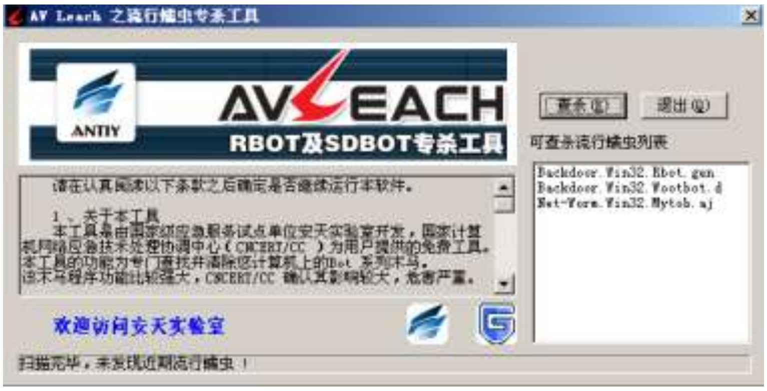
	 AV Leach 之流行蠕虫专杀工具 ☑ 网络免疫 ☑ 自动运行免疫 可查杀流行蠕虫列表 I-Worm.Supova.z I-Worm.Tunk.a I-Worm.Welchia.k I-Worm.Win32.Sasser.a I-Worm.Win32.Sasser.b I-Worm.Win32.Sasser.c I-Worm.Win32.Sasser.d I-Worm.Win32.Sasser.e I-Worm.Win32.Sasser.f I-Worm.Win32.SSL Trojan.Mercurycas.a 本程序是安天实验室针对“震荡波”等近期流行蠕虫病毒提供的集查杀、免疫于一体的小型集成解决方案。不仅可以查杀多个流行蠕虫，而且可以通过内置的防火墙实现震荡波等蠕虫的永久性免疫，从而彻底避免“震荡波”、“冲击波”等病毒的感染和所造成的系统崩溃。 本工具可以为那些因频繁受到病毒攻击而重启，无法完成windows update的用户争取到足够的下载安装补丁的时间，特 欢迎访问安天实验室 启用免疫！ **Figure 1-7AV Lecah's popular worm special detection tool adds protection against WelChia worms**

May 2004

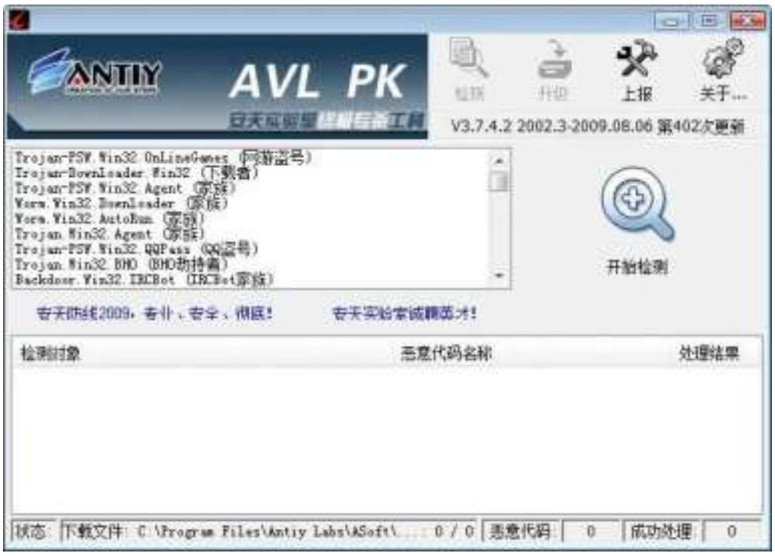
Event	Sasser
Contribution	Capture warning, analysis report, special detection tool, network sky homology analysis and source location determination  AV Leach 之流行蠕虫专杀工具 ☑ 网络免疫 ☑ 自动运行免疫 可查杀流行蠕虫列表 I-Worm.Supova.z I-Worm.Tunk.a I-Worm.Welchia.k I-Worm.Win32.Sasser.a I-Worm.Win32.Sasser.b I-Worm.Win32.Sasser.c I-Worm.Win32.Sasser.d I-Worm.Win32.Sasser.e I-Worm.Win32.Sasser.f I-Worm.Win32.SSL Trojan.Mercurycas.a 本程序是安天实验室针对“震荡波”等近期流行蠕虫病毒提供的集查杀、免疫于一体的小型集成解决方案。不仅可以查杀多个流行蠕虫，而且可以通过内置的防火墙实现震荡波等蠕虫的永久性免疫，从而彻底避免“震荡波”、“冲击波”等病毒的感染和所造成的系统崩溃。 本工具可以为那些因频繁受到病毒攻击而重启，无法完成windows update的用户争取到足够的下载安装补丁的时间，特 欢迎访问安天实验室 启用免疫！ **Figure 1-8AV Lecah’s popular worm special detection tool adds protection against Sasser worms**
For more information, see	"Virus Homology Analysis Based on Typical Development Methods and Coding Psychology" (published in Antiy Technical Articles Compilation (I))

January 2005

Event	RBOT and SDBOT botnets
Contribution	Capture warning, analysis report, special detection tool, provide clues to capture the author

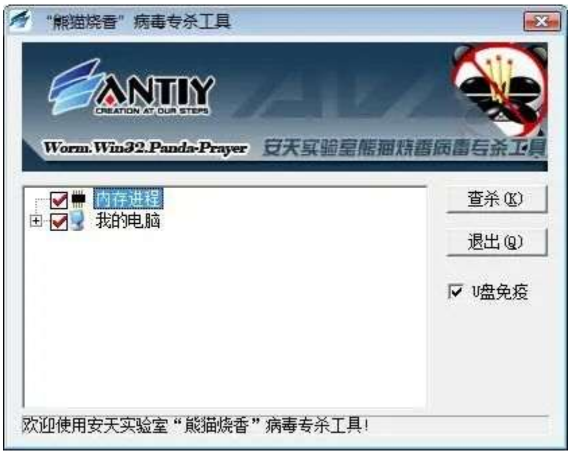
	 AV Leach 之流行蠕虫专杀工具 ANTIY AVLEACH RBOT及SDBOT专杀工具 查杀(C) 退出(Q) 可查杀流行蠕虫列表 欢迎访问安天实验室 Backdoor.Win32.Rbot.gen Backdoor.Win32.Sdbot.d Net-Worm.Win32.Mytob.aj 请在认真阅读以下条款之后确定是否继续运行本软件。 1、关于本工具 本工具是由国家级应急服务试点单位安天实验室开发，国家计算机网络应急技术处理协调中心（CNCERT/CC ）为用户提供的免费工具。本工具的功能为专门查找并清除您计算机上的Bot 系列木马。该木马程序功能比较强大，CNCERT/CC 确认其影响较大，危害严重。 扫描完毕，未发现近期流行蠕虫！ **Figure 1-9AV Lecah's popular worm special detection tool adds protection against RBOT and SDBOT botnets**

August 2006

Event	Mocbot
Contribution	Special detection tools, monitoring and analysis, large-scale containment solutions  ANTIY AVL PK 安天实验室检测专杀工具 检测 升级 上报 关于... 开始检测 检测对象 恶意代码名称 处理结果 V3.7.4.2 2002.3-2009.08.06 第402次更新 Trojan-PSW.Win32.OnLineGames (网游盗号) Trojan-Downloader.Win32 (下载者) Trojan-PSW.Win32.Agent (家族) Worm.Win32.Downloader (家族) Worm.Win32.AutoRun (家族) Trojan.Win32.Agent (家族) Trojan-PSW.Win32.QQPass (QQ盗号) Trojan.Win32.BHO (BHO劫持者) Backdoor.Win32.IRCBot (IRCBot家族) 安天防线2009，专业、安全、彻底！ 安天实验室诚聘英才！ 状态: 下载文件: C:\Program Files\Antiy Labs\ASoft\... 0 / 0 恶意代码: 0 成功处理: 0 **Figure 1-10AVL PK Ultimate Special Detection Tool detects and kills popular worms and Trojans at the time**

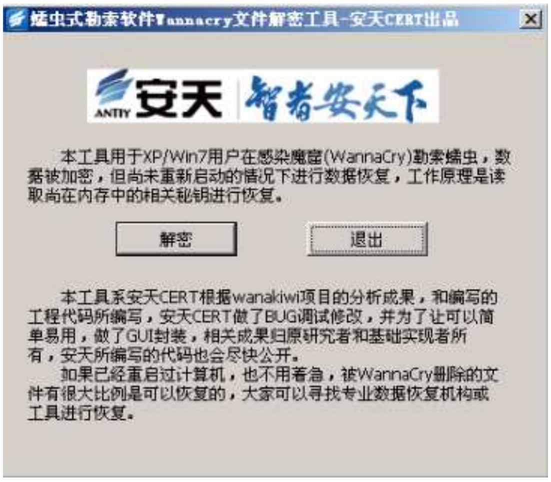
December 2006

Event	Fujacks
Contribution	Capture warning, analysis report, special detection tool

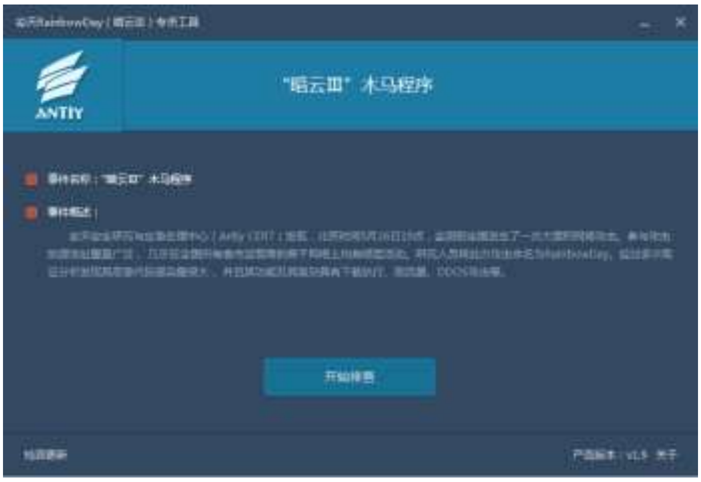
	 "熊猫烧香" 病毒专杀工具 ANTIY CREATION AT OUR STEPS Worm.Win32.Panda-Prayer 安天实验室熊猫烧香病毒专杀工具 ☑ 内存进程 ☑ 我的电脑 查杀(K) 退出(Q) ☑ U盘免疫 欢迎使用安天实验室"熊猫烧香"病毒专杀工具! **Figure 1-11"Fujacks" virus special detection tool**

May 2017

Event	WannaCry
Contribution	First release of complete analysis, special detection, immunity tools, memory key extraction (recovery) tools, and traceability support **Figure 1-12WannaCry special detection tools** **Figure 1-13WannaCry immunity tool**

	 蠕虫式勒索软件Wannacry文件解密工具-安天CERT出品 本工具用于XP/Win7用户在感染魔窟(WannaCry)勒索蠕虫，数据被加密，但尚未重新启动的情况下进行数据恢复，工作原理是读取尚在内存中的相关秘钥进行恢复。 解密 退出 本工具系安天CERT根据wanakiwi项目的分析成果，和编写的工程代码所编写，安天CERT做了BUG调试修改，并为了让可以简单易用，做了GUI封装，相关成果归原研究者和基础实现者所有，安天所编写的代码也会尽快公开。 如果已经重启过计算机，也不用着急，被WannaCry删除的文件有很大比例是可以恢复的，大家可以寻找专业数据恢复机构或工具进行恢复。 **Figure 1-14WannaCry file decryption tool**
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	Dark Cloud III
Contribution	Analysis report, special detection tool  “暗云Ⅲ” 木马程序 事件名称：“暗云Ⅲ” 木马程序 事件概述： [illegible] 开始排查 检查更新 产品版本：v1.5 关于 **Figure 1-15Dark Cloud III special detection tool**
For more information	Antiy's sample analysis and solutions for "Dark Cloud III"

January 2018

Event	Gafgyt

Contribution	Jointly released with Telecom Cloud, infection status
For more information	Uncovering the story behind the IoT botnet Gafgyt family and the NetCore 53413 backdoor

August 2019

eEvent	Mykings
Contribution	Release analysis reports and infection status
For more information	Analysis report on the recent activities of Mykings botnet

April 2020

Event	Tsunami
contribute	Release analysis report and global infection situation
For more information	Analysis of the precise deployment of Tsunami botnet and "Magic Shovel" mining trojan

September 2022

Event	Lilith
Contribution	Publish analysis reports and traceability background
For more information	Follow-up analysis of Lilith botnet and the Jester hacker group behind it

November 2022 - March 2023

Event	Mining
Contribution	Release analysis reports and mining topics
For more information	Analysis of Typical Mining Families Part 4: LemonDuck Mining Botnet Analysis of Typical Mining Families Part 3: Sysrv-hello Mining Worm Analysis of Typical Mining Families Part 2: TeamTNT Mining Organization Analysis of Typical Mining Families Part 1: Outlaw Mining Botnet

December 2023

Event	Mirai
Contribution	Analysis reports, new variants
For more information	Analysis of Mirai botnet variant "Aquabot" and Yayaya Miner mining trojan

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.