Safeguarding China Operation (Part 2)

——Analysis, Response and Disposal of Black Market Activities Such as Ransomware Attacks

Antiy CERT

First draft completed: October 4, 2024
First published: October 4, 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 second part of Antiy's emergency response and threat analysis work track - analysis, response and disposal of black market activities such as ransomware attacks.**

Economic profit has always been one of the main driving forces of cyber attacks, and a network of black and gray industry crimes has been formed around the infringement of information systems, information assets and users.

This has led to a variety of threats such as ransomware attacks, commercial theft, the construction of botnets for DDoS attacks, and mining.

Among them, ransomware attacks are the most harmful form of cybercrime. In the early days, ransomware attacks were spread or distributed through ransomware viruses or software with built-in ransomware codes. After the attack, user data was encrypted or the system was paralyzed, and the ransom was paid. However, today, the main form of ransomware attacks is RaaS (Ransomware as a Service) + targeted attacks. Attackers carry out targeted intrusions, data theft, data encryption, and system destruction on victims, and then threaten users to pay a large ransom by making their system data unusable, selling data, making data public, or reporting related information.

Black market activities such as ransomware attacks has always been an important spectrum of Antiy's engine and government and enterprise product and service capabilities. Following up and analyzing related major security incidents, providing public safety knowledge, and improving user awareness and protection levels are also important supporting capabilities of Antiy in emergency response and disposal. By conducting attack activity perception, sample capture and analysis, vulnerability mechanism and mitigation research, threat intelligence production, release of special detection and disposal tools, and publication of analysis reports, we provide security empowerment for customers and the public.

1. Analysis, Response and Disposal of Black Market Activities Such as Ransomware Attacks

2006

Event	Redplus
Contribution	The first to capture the first ransomware attack sample in China

2013

Event	CryptoLocker
Contribution	Analysis report

August 2015

Event	CTB-Locker

Contribution	Analysis report Figure 1-1CTB-Locker image
For more information	["Attack WPS Sample" is actually a blackmailer]()

August 2015

Work	Analyzing the history of ransomware attacks
Contribution	Ransomware attack classification, evolution history, threat trends, and family analysis
For more information	[Uncovering the true face of ransomware]()

February 20, 2016

Event	The first ransomware attack with Chinese prompts
Contribution	First to capture, first Chinese-language ransomware warning

August 2015

Event	WannaCry
Contribution	First release of complete analysis, special detection, immunity tools, memory key extraction (recovery) tools, and traceability support

	 Figure 1-2WannaCry virus image
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

February 2018

Event	GandCrab
Contribution	In-depth analysis report, encryption principle analysis
For more information	GANDCRAB ransomware targets Dash, Antiy IEP provides effective protection

February 2018

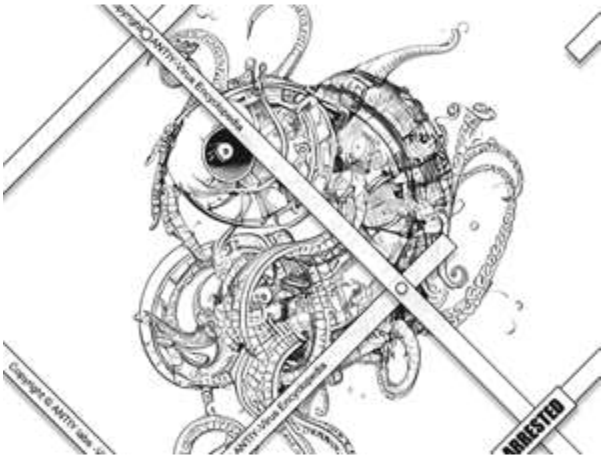
Event	GlobeImposter
Contribution	Analysis of dynamic decryption principles

	 Figure 1-3 GlobeImposter ransomware image
For more information	Beware of GlobeImposter ransomware, Antiy IEP provides effective protection

March 2019

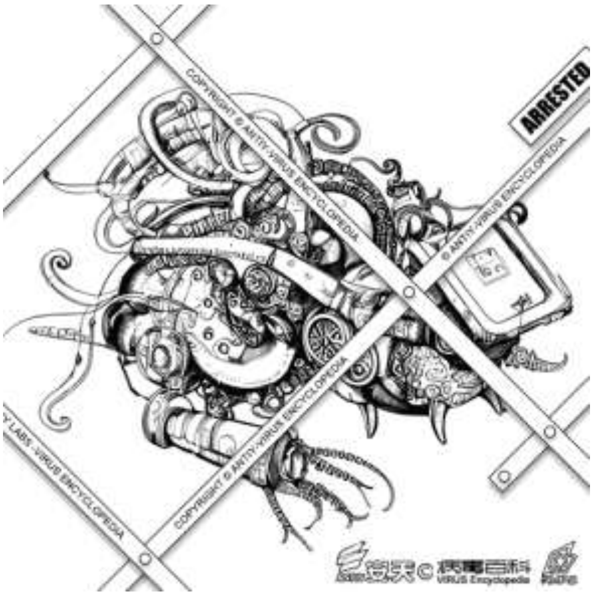
Event	International black industry organizations target financial practitioners in some East Asian countries
Contribution	Event analysis, sample analysis, organizational association and profiling
For more information	International black industry organizations against financial practitioners in some East Asian countries

June 2019

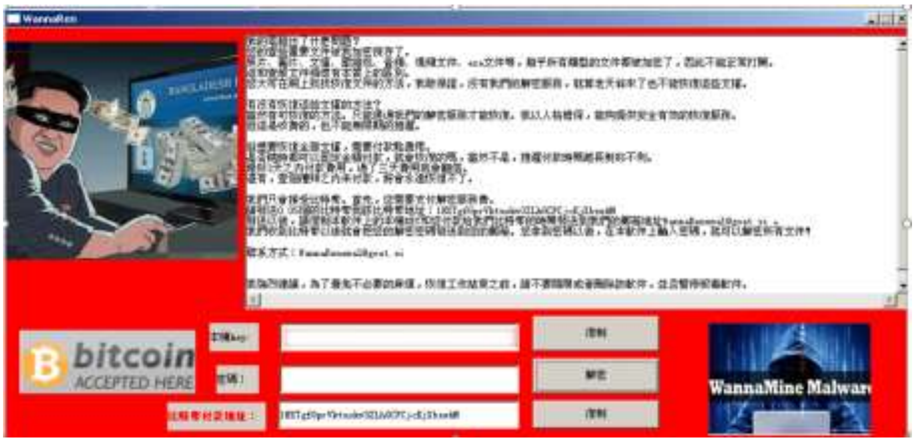
Event	Links to Sodinokibi ransomware group
Contribution	Tissue attribution, association analysis  Figure 1-4 Sodinokibi image

For more information	Analysis of the association between the ransomware Sodinokibi operating organization

October 2019

Event	Phobos ransomware variant
Contribution	Sample attribution, family history  ARRESTED COPYRIGHT © ANTIY-VIRUS ENCYCLOPEDIA ANTIY-VIRUS ENCYCLOPEDIA COPYRIGHT © ANTIY-VIRUS ENCYCLOPEDIA Y LABS - VIRUS ENCYCLOPEDIA 安天 © 病毒百科 VIRUS Encyclopedia **Figure 1-5Phobos ransomware variants**
For more information	Phobos ransomware variant analysis report

April 2020

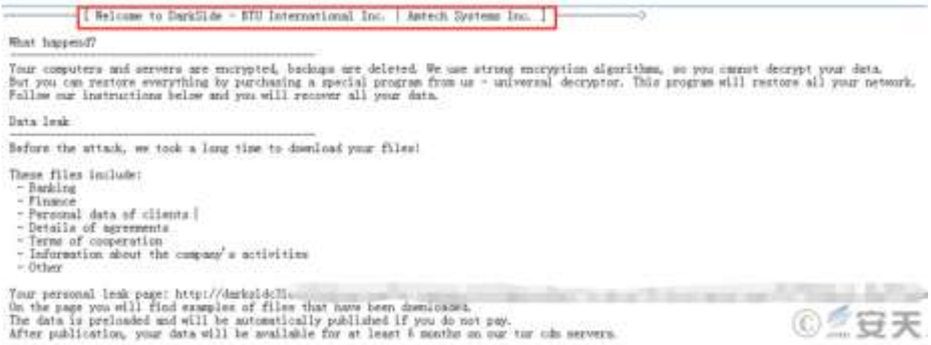
Event	WannaRen ransomware attack
Contribution	Capture warnings, analyze reports, and track and trace  **Figure 1-6 WannaRen ransomware attack pop-up window displayed**

For more information	Review and analysis of WannaRen ransomware

February 2021

Event	"Cloud Shovel" mining trojan
Contribution	Joint release, sample analysis, and disposal plan
For more information	Analysis of the "Cloud Shovel" Mining Trojan Event Targeting a Cloud Platform Server

May-July 2021

Event	US fuel pipeline operator shut down due to ransomware attack
Contribution	Protection suggestions, sample analysis, event sorting and summary  [Welcome to DarkSide - BTU International Inc. | Amtech Systems Inc.] What happend? Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. Follow our instructions below and you will recover all your data. Data leak Before the attack, we took a long time to download your files! These files include: - Banking - Finance - Personal data of clients - Details of agreements - Terms of cooperation - Information about the company's activities - Other Your personal leak page: http://darksidc3l[redacted] On the page you will find examples of files that have been downloaded. The data is preloaded and will be automatically published if you do not pay. After publication, your data will be available for at least 6 months on our tor cdn servers. **Figure 1-7 DarkSide ransomware attack ransom note**
For more information	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 U.S. fuel pipeline company Summary of the Shutdown of US Fuel Pipeline Companies Due to Ransomware Attacks

July 2021

Event	"Phantom Rat" organization steals secrets and attacks
Contribution	Global monitoring, process analysis, sample analysis

	 Figure 1-8Image of the "Phantom Rat" organization
For more information	Analysis of the "Phantom Rat" organization’s espionage and attack activities against my country

August 2021

Event	Agent Tesla new variant
Contribution	Capture and warnings, analysis reports
For more information	Analysis of a new variant of the commercial stealing Trojan Agent Tesla

September 2021

Public Support	China Academy of Information and Communications Technology "Ransomware Security Protection Manual"
Contribution	Telecom, China Mobile, China Unicom, Antiy, DBAPP, Qi An Xin, NSFOCUS, etc.

	CAICT 中国信通院 勒索病毒安全防护手册 中国信息通信研究院 2021 年 8 月 Figure 1-9Ransomware Security Protection Manual

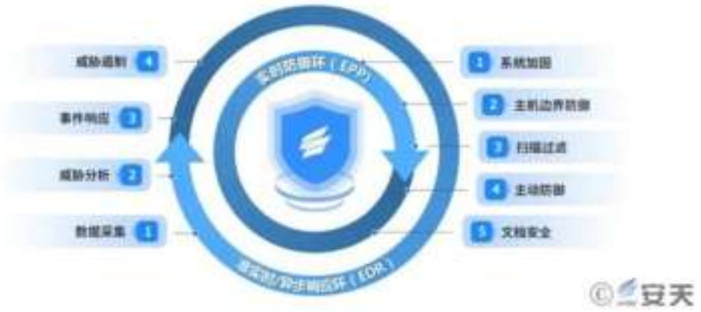
October 20-21

Event	FormBook stealing trojan attack
Contribution	Capture warnings and analysis reports
For more information	Analysis report on a unit that was attacked by the FormBook stealing Trojan

November 2021

Event	RedLine steals secrets
Contribution	Communication channels, analysis reports
For more information	Analysis of the RedLine Stealing Trojan Spreading Through Video Websites Follow-up analysis of the RedLine stealing Trojan spread through video websites

November 2021

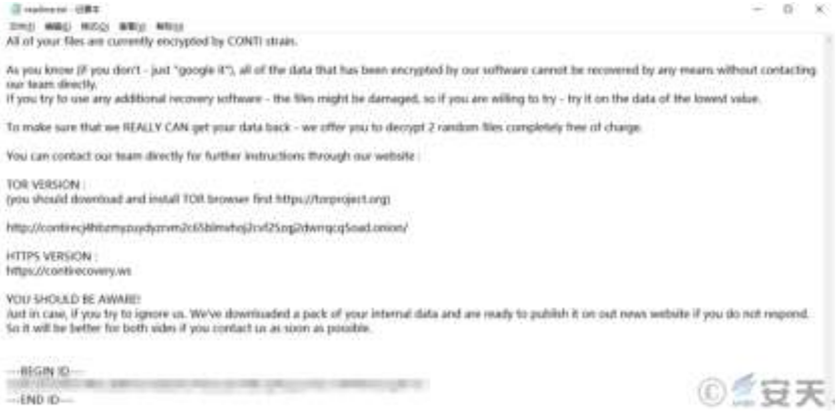
Work	Ransomware attacks and hazards
Contribution	Ransomware attacks  威胁遏制 4 事件响应 3 威胁分析 2 数据采集 1 实时防御环（EPP） （EDR） 1 系统加固 2 主机边界防御 3 扫描过滤 4 主动防御 5 文档安全 ©安天 Figure 1Schematic diagram of the principle of IEP's defense against ransomware

For more information	"Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 1: Four Divisions of Labor in Ransomware Attacks "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 2: Two Typical Modes of Ransomware Attacks "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 3: Common Spreading Methods and Intrusion Paths "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 4: Analysis of the "Ransomware Attack Kill Chain" "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 5: Four Main Types of Ransomware "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 6: Important Attack Characteristics "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 7: Ten Typical Families "Understanding Ransomware Attacks and Dangers from Eight Aspects" Part 8: The Development Trend of Ransomware Attacks

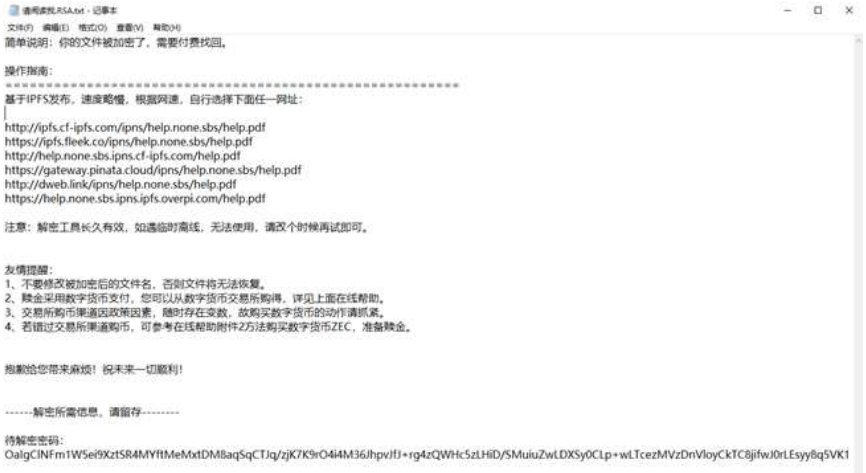
November 2021

Event	H2Miner organizes mining
Contribution	Sample analysis and troubleshooting suggestions
For more information	Dual-platform communication: analysis of active H2Miner mining organization

December 2021

Event	Conti ransomware
Contribution	Organization introduction, victim information sorting, sample analysis  All of your files are currently encrypted by CONTI strain. As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value. To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge. You can contact our team directly for further instructions through our website : TOR VERSION : (you should download and install TOR browser first https://torproject.org) http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/ HTTPS VERSION : https://contirecovery.ws YOU SHOULD BE AWARE! Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible. ---BEGIN ID--- [redacted] ---END ID--- **Figure 1-10Conti ransomware attack ransom letter**
For more information,	Conti Ransomware Analysis Report

February 2022

Event	Coffee ransomware attack
Contribution	Sample analysis, global infection situation, decryption tools  请阅读我.RSA.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 简单说明：你的文件被加密了，需要付费找回。 操作指南： == 基于IPFS发布，速度略慢，根据网速，自行选择下面任一网址： http://ipfs.cf-ipfs.com/ipns/help.none.sbs/help.pdf https://ipfs.fleek.co/ipns/help.none.sbs/help.pdf http://help.none.sbs.ipns.cf-ipfs.com/help.pdf https://gateway.pinata.cloud/ipns/help.none.sbs/help.pdf http://dweb.link/ipns/help.none.sbs/help.pdf https://help.none.sbs.ipns.ipfs.overpi.com/help.pdf 注意：解密工具长久有效，如遇临时离线，无法使用，请改个时候再试即可。 友情提醒： 1、不要修改被加密后的文件名，否则文件将无法恢复。 2、赎金采用数字货币支付，您可以从数字货币交易所购得，详见上面在线帮助。 3、交易所购币渠道因政策因素，随时存在变数，故购买数字货币的动作请抓紧。 4、若错过交易所渠道购币，可参考在线帮助附件2方法购买数字货币ZEC，准备赎金。 抱歉给您带来麻烦！祝未来一切顺利！ ------解密所需信息，请留存-------- 待解密密码： OalgCINFm1W5ei9XztSR4MYftMeMxtDM8aqSqCTJq/zjK7K9rO4i4M36JhpvJfJ+rg4zQWHc5zLHiD/SMuiuZwLDXSy0CLp+wLTcezMVzDnVloyCkTC8jifwJ0rLEsyy8q5VK1 **Figure 1-11Coffee ransomware attack ransom letter**
For more information	Coffee ransomware continues to be active, Antiy releases decryption tool

March 2022

Work	Special Topic: Business Stealing Trojans
Contribution	Special research
For more information	Comprehensive analysis report on commercial stealing Trojans

September 2022

Event	"Magic Thief" secret-stealing Trojan horse spreads on a large scale
Contribution	Joint release, risk warning, infection scale, sample analysis
For more information	Risk warning about the large-scale spread of the "Magic Thief" secret-stealing Trojan

November 2022

Work	Mining family research
Contribution	Mining special
For more information, see	Analysis of Typical Mining Families Part 1 | Outlaw Mining Botnet Analysis of Typical Mining Families Part 2 | TeamTNT Mining Organization Analysis of Typical Mining Families Part 3 | Sysrv-hello Mining Worm

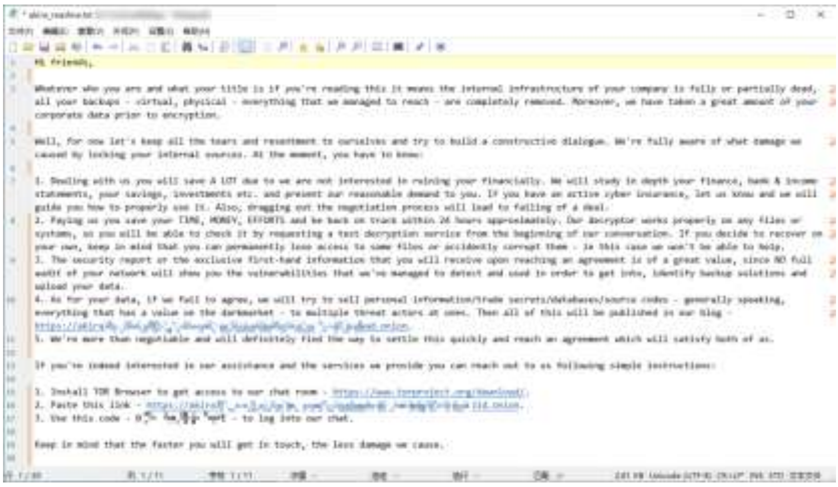
	Analysis of Typical Mining Families Part 4 | LemonDuck Mining Botnet

March 2023 to Present

Event	"SwimSnake" black industry gang
Contribution	First capture, analysis report, special detection tool, census tool Figure 1-12Image of the "SwimSnake" black market gang
For more information	Analysis of a black market group that uses cloud note platforms to deliver remote control Trojans Analysis of the large-scale attack activities launched by the "SwimSnake" black industry gang against domestic users Analysis of recent phishing attacks by the "SwimSnake" black industry gang "SwimSnake" black industry group using WeChat to spread malicious code Special analysis report on the "SwimSnake" black industry gang Analysis of the new round of attacks by the "SwimSnake" black industry gang against financial personnel and e-commerce customer service Recent attack activities of the "SwimSnake" black industry Analysis of phishing attacks carried out by "SwimSnake" black market gangs using malicious documents

May 2023

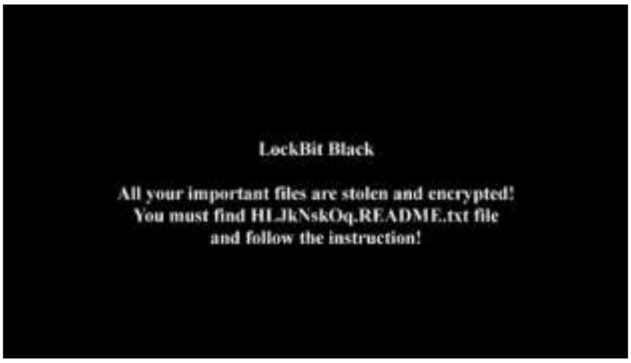
Event	Akira ransomware attack
Contribution	Ransomware attack overview and technical review

	 Hi friends, Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption. Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know: 1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal. 2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help. 3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data. 4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akira[redacted].onion. 5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us. If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions: 1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/. 2. Paste this link - https://akira[redacted].onion. 3. Use this code - [redacted] - to log into our chat. Keep in mind that the faster you will get in touch, the less damage we cause. **Figure 1-13Akira ransomware attack ransom letter**
For more information	Analysis of Akira ransomware suspected of using targeted attack mode

June 2023

Event	Recent attacks by Diicot mining group
Contribution	Monitoring, early warning, joint release
For more information	Analysis of recent attack activities of Diicot mining organization

November 2023

Event	LockBit ransomware attack
Contribution	Sample analysis and targeted ransomware defense thinking  LockBit Black All your important files are stolen and encrypted! You must find HLJkNskOq.README.txt file and follow the instruction! **Figure 1-14 LockBit ransomware attacks modify desktop backgrounds**
For more information	Analysis of LockBit ransomware samples and defense against targeted ransomware

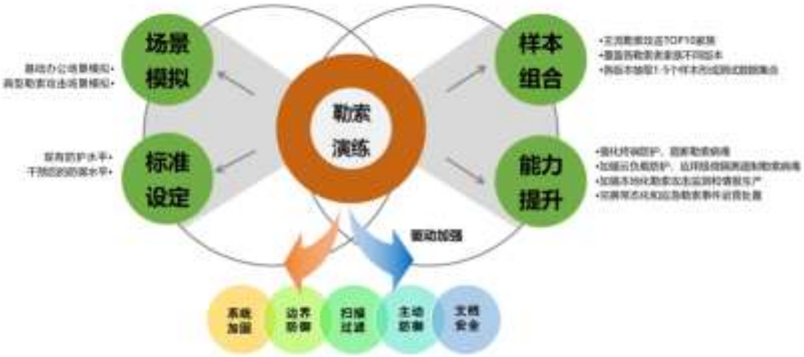
December 2023

Event	Boeing hit by ransomware attack
Contribution	Threat trend analysis, analysis review, defense thinking, sample analysis Figure 1-15 Analysis and Review of the Boeing Ransomware Attack Incident
For more information	Boeing ransomware attack analysis and review: threat trend analysis and defense thinking of targeted ransomware

January 2024

Event	"Dark Mosquito" black production gang
Contribution	Global monitoring, activity timeline, attack process, sample analysis
For more information	"Anmosquito" black market gang spreading Mac remote control Trojan attack activities through domestic download sites

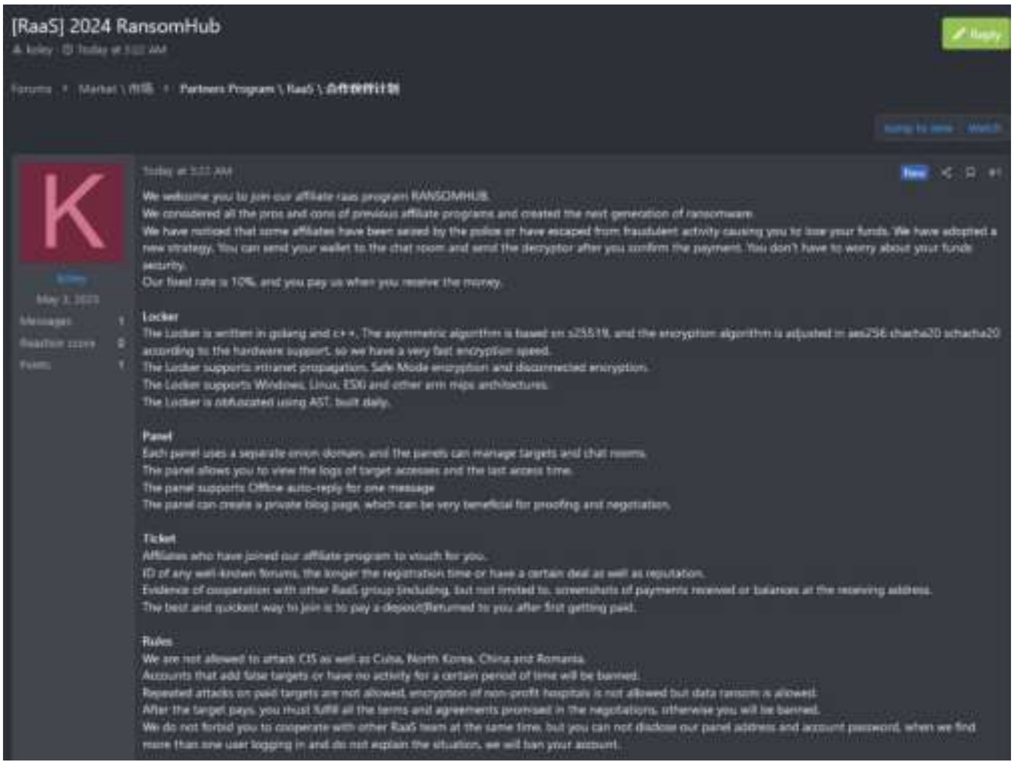
May 2024

Event	Antiy ransomware prevention drill
Contribution	Ransomware protection topics, ransomware prevention and control drill services  场景模拟 标准设定 勒索演练 样本组合 能力提升 驱动加强 系统加固 边界防御 扫描过滤 主动防御 文档安全 Figure 1-16ransomware prevention and control drill service overview
For more information	New anti-ransomware tool | Antiy ransomware prevention and control drill service

May 2024

Event	"Nichan" mining trojan
Contribution	Sample analysis, troubleshooting and removal solutions
For more information	Analysis of the "Nichan" mining trojan activity

September 2024

Event	RansomHub ransomware attack
Contribution	Organizational background, organizational attribution  [RaaS] 2024 RansomHub Reply Forums › Market \ 市场 › Partners Program \ RaaS \ 合作伙伴计划 Jump to new · Watch K New We welcome you to join our affiliate raas program RANSOMHUB. We considered all the pros and cons of previous affiliate programs and created the next generation of ransomware. We have noticed that some affiliates have been seized by the police or have escaped from fraudulent activity causing you to lose your funds. We have adopted a new strategy. You can send your wallet to the chat room and send the decryptor after you confirm the payment. You don't have to worry about your funds security. Our fixed rate is 10%, and you pay us when you receive the money. **Locker** The Locker is written in golang and c++. The asymmetric algorithm is based on x25519, and the encryption algorithm is adjusted in aes256 chacha20 xchacha20 according to the hardware support, so we have a very fast encryption speed. The Locker supports intranet propagation, Safe Mode encryption and disconnected encryption. The Locker supports Windows, Linux, ESXi and other arm mips architectures. The Locker is obfuscated using AST, built daily. **Panel** Each panel uses a separate onion domain, and the panels can manage targets and chat rooms. The panel allows you to view the logs of target accesses and the last access time. The panel supports Offline auto-reply for one message The panel can create a private blog page, which can be very beneficial for proofing and negotiation. **Ticket** Affiliates who have joined our affiliate program to vouch for you. ID of any well-known forums, the longer the registration time or have a certain deal as well as reputation. Evidence of cooperation with other RaaS group (including, but not limited to, screenshots of payments received or balances at the receiving address. The best and quickest way to join is to pay a deposit(Returned to you after first getting paid. **Rules** We are not allowed to attack CIS as well as Cuba, North Korea, China and Romania. Accounts that add false targets or have no activity for a certain period of time will be banned. Repeated attacks on paid targets are not allowed, encryption of non-profit hospitals is not allowed but data ransom is allowed. After the target pays, you must fulfill all the terms and agreements promised in the negotiations, otherwise you will be banned. We do not forbid you to cooperate with other RaaS team at the same time, but you can not disclose our panel address and account password, when we find more than one user logging in and do not explain the situation, we will ban your account. **Figure 1-17 RansomHub organizes RaaS program**
For more information	Analysis of the active RansomHub ransomware attack organization

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.