Safeguarding China Operation (Part 5)

——APT Capture, Analysis and Traceability

Antiy CERT

First draft completed: October 7, 2024
First published: October 7, 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 fifth part of Antiy's emergency response and threat analysis work track - APT capture, analysis and traceability.**

With the exposure of the Stuxnet incident in 2010, Antiy realized in follow-up analysis that the threat of black and gray industry crimes driven by economic interests is not the most serious security threat, but the APT attacks launched by cyber threat actors in countries/regions are more deadly. Antiy analyzed the focus of resources and manpower investment and began to conduct comprehensive special APT tracking and tracing analysis. Antiy gave full play to its strengths in sample reverse analysis, and at the same time superimposed the analysis of threat activities on the background of international situation and geopolitical security competition, and carried out analysis around the dimensions of threat actors (organizations), attack motives and purposes (intentions), attack tactics, attack equipment and payloads (executors). Antiy CERT continuously monitors and tracks more than 500 cyber threat actors related to more than 40 countries and regions, including APT attack organizations with government backgrounds and cybercrime gangs. It also focuses on APT attack activities, submits more than 200 analysis reports to various competent departments, and publicly releases dozens of analysis reports, conference technical reports and other research documents. Among them, the APT-TOCS report is the first time that China has actively captured and publicly named the attack activities of foreign APT organizations against me; the "Equation" series of reports is the world's exclusive exposure of the US samples targeting the three system platforms of Solaris , Linux, and iOS; the "White Elephant" report is the first time that a Chinese security vendor has traced and located the natural person of an APT organization. The Equation Organization's attack on EASTNET is the first sample of a Chinese security vendor that has completely traced and reviewed the entire process of the attack by the US intelligence agency. Our analysis results have been reported or cited by Xinhua News Agency, CCTV News Network, Focus Interview, Global Times, etc., and the China Cyber Security Industry Alliance's "A Historical Review of Cyber Attacks by US Intelligence Agencies" cited many of Antiy's analysis results.

For more information on our related work, please refer to Li Baisong's articles, "Fighting Threats from Across the Ocean: The Heartfelt Words of a 23-Year Cybersecurity Professional" and "Fight Against the Bald Eagle in the Fog."

1. APT Analysis and Traceability

Attack Organization/Action: Stuxnet Worm (US, Israel)

Work Results	Analyze the truth and details of the "Stuxnet" attack, build a simulation environment, and fully analyze the USB ferry mechanism
Publication date of results	September 2010
Publicly available technical reports	Comprehensive Analysis Report on Stuxnet Worm Attack on Industrial Control Systems Subsequent Analysis Report on Stuxnet Worm What happened after WinCC? The paper version of the report is published in "Antiy Technical Articles Compilation (V)

	Industrial Control System Security Volume"

对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告

安天安全研究与应急处理中心(Antiy CERT)

Figure 1-1 Cover of the Stuxnet Worm Attack Analysis Report

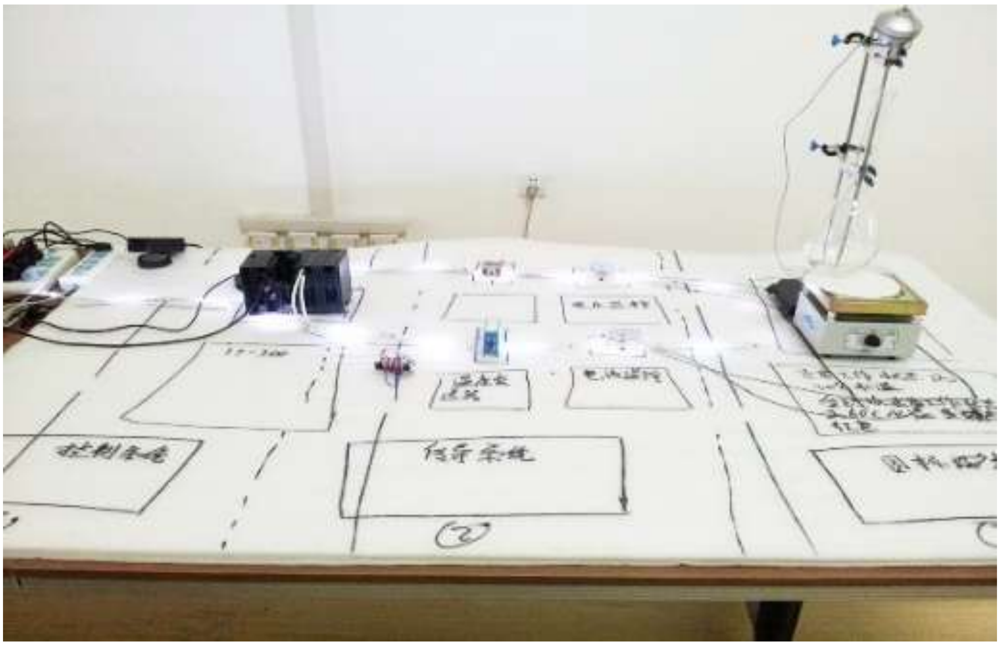


Figure 1-2The simple industrial control system built by Antiy for analyzing the Stuxnet virus (initial prototype)

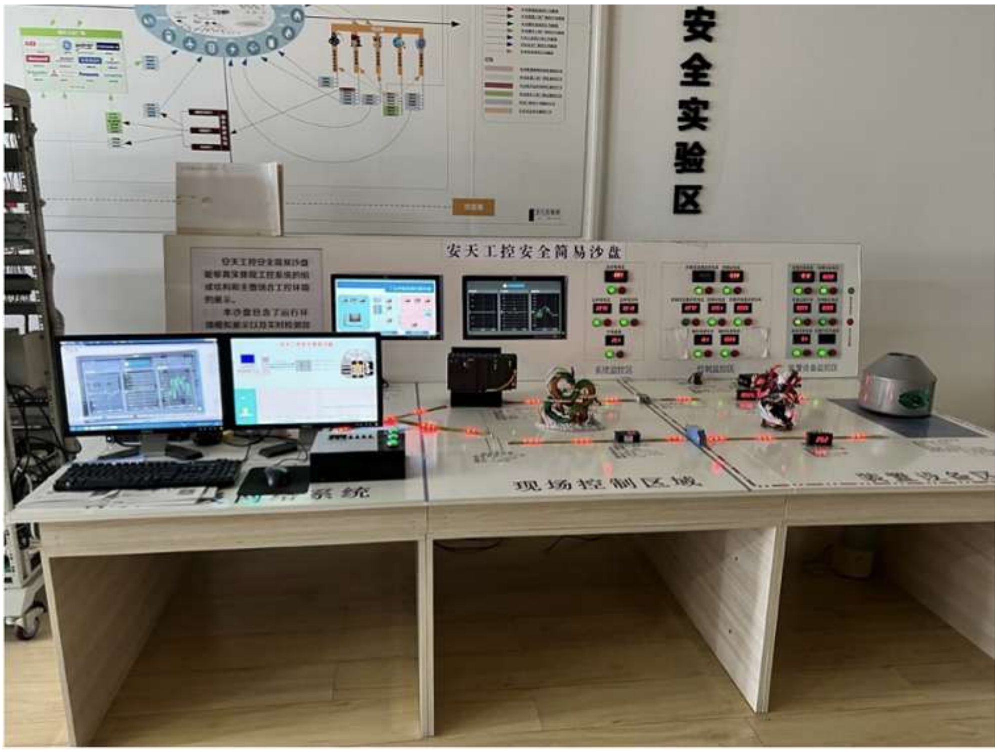


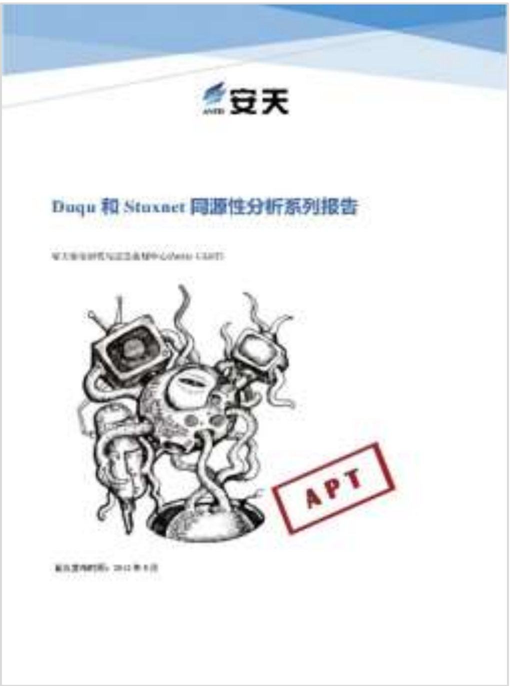
Figure 1-3Antiy's analysis of the simulated sandbox built by Stuxnet

震网攻击活动可视化复现.mp4

Video 1-1Visual reproduction of Stuxnet attack activity

Attack Organization/Action: Duqu Trojan (US)

Work Results	Confirmed the homology between the poisonous song and Stuxnet, and put forward multiple exclusive evidence points
Publication date of results	May 2012
Publicly available technical reports	The paper version was published in the May 2012 issue of Programmer, "Exploring the Mystery of the Duqu Trojan's Origin" "Looking at the security of industrial control systems from the homology between Duqu virus and Stuxnet worm"



安天

Duqu 和 Stuxnet 同源性分析系列报告

[illegible]

[illegible]

Figure 1-4Cover of Duqu and Stuxnet Homology Analysis Report

Table 1-1Comparison of key code genes of Duqu and Stuxnet

<table>
<tr><th>Compare Projects</th><th>Duqu</th><th>Stuxnet</th></tr>
<tr><td>Functional modularity</td><td colspan="2">Yes</td></tr>
<tr><td>Ring0 injection method</td><td colspan="2">PsSetLoadImageNotifyRoutine</td></tr>
<tr><td>Ring3 injection method</td><td colspan="2">Hook ntdll.dll</td></tr>
<tr><td>Injecting into system processes</td><td colspan="2">Yes</td></tr>
<tr><td>Resource embedded DLL module</td><td>One</td><td>Multiple</td></tr>
<tr><td>Exploiting Microsoft vulnerabilities</td><td colspan="2">Yes</td></tr>
<tr><td>Using digital signatures</td><td colspan="2">Yes</td></tr>
<tr><td>Including RPC communication module</td><td colspan="2">Yes</td></tr>
<tr><td>Configuration file decryption key</td><td>0xae240682</td><td>0x01ae0000</td></tr>
<tr><td>Registry decryption key</td><td colspan="2">0xae240682</td></tr>
<tr><td>Magic number</td><td colspan="2">0x90,0x05,0x79,0xae</td></tr>
<tr><td>There is a bug in the running mode judgment code</td><td colspan="2">Yes</td></tr>
<tr><td>There is a bug in the registry operation code</td><td colspan="2">Yes</td></tr>
<tr><td>Attacking industrial control systems</td><td>No</td><td>Yes</td></tr>
</table>

Driver compilation environment	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

Attack Organization/Action: Flame Worm (US)

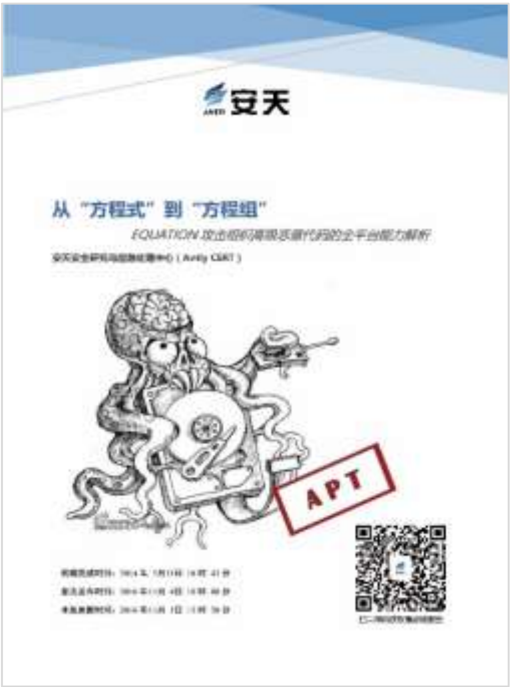
Work Results	Homologous to Stuxnet, over 90% of modules analyzed, the highest share in the industry
Publication date of results	May 2012
Publicly available technical reports	Analysis Report of Flame Worm Sample Set The paper version of the report is published in "Antiy Technical Articles Compilation (V) Industrial Control System Security Volume"

Figure 1-5Cover of Flame Worm Sample Set Analysis Report

Attack Organization/Action: EQUATION (US)

Work Results	Analyze the persistence mechanism of hard disk firmware, command control structure, crack communication encryption method, reveal complete operation capabilities, and exclusively expose Solaris and Linux platform samples worldwide
Publication date of results	March 2015 - January 2017
Publicly available technical reports	"Trojans that modify hard drive firmware - Exploring the attack components of the EQUATION organization" 《Analysis of encryption techniques in some components of EQUATION》 From "Equation" to "Equation Group": Analysis of the Full-Platform Capabilities of the Advanced Malicious Code of the EQUATION Attack Organization

	Analysis of the Equation Organization's EQUATION DRUG Platform The paper version of the report is published in "Antiy Technical Articles Compilation (Twelve) Advanced Persistent Threat (APT) Special Topic" The paper version of the report is published in "Antiy Technical Articles Compilation (Thirteen) Advanced Persistent Threat (APT) Special Topic"


从“方程式”到“方程组”

EQUATION攻击组织高级恶意代码的全平台能力解析

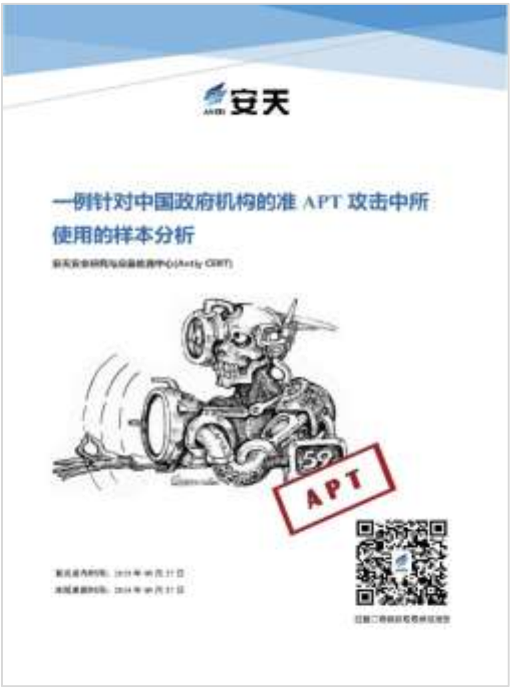
安天安全研究与应急处理中心（Antiy CERT）

Figure 1-6Cover of from "Equation" To "Equation Group" Equation Attack Organization’s Advanced Malicious Code Full Platform Capability Analysis Report

Figure 1-7Equation organization host operation module building block diagram

Attacker Organization/Action: APT-TOCS (OceanLotus) (Vietnam)

Work Results	Actively capture attack activities, the first analysis report naming a specific foreign country, and raise the issue of cyber arms proliferation
Publication date of results	May 27, 2015
Publicly available technical reports	Analysis of samples used in a quasi-APT attack against Chinese institutions The paper version of the report is published in "Antiy Technical Articles Compilation (Twelve) Advanced Persistent Threat (APT) Special Topic"



安天

一例针对中国政府机构的准 APT 攻击中所使用的样本分析

安天安全研究与应急处理中心(Antiy CERT)

Figure1-8 Cover of Analysis of Samples Used in a Quasi-APT Attack Against Chinese Institutions

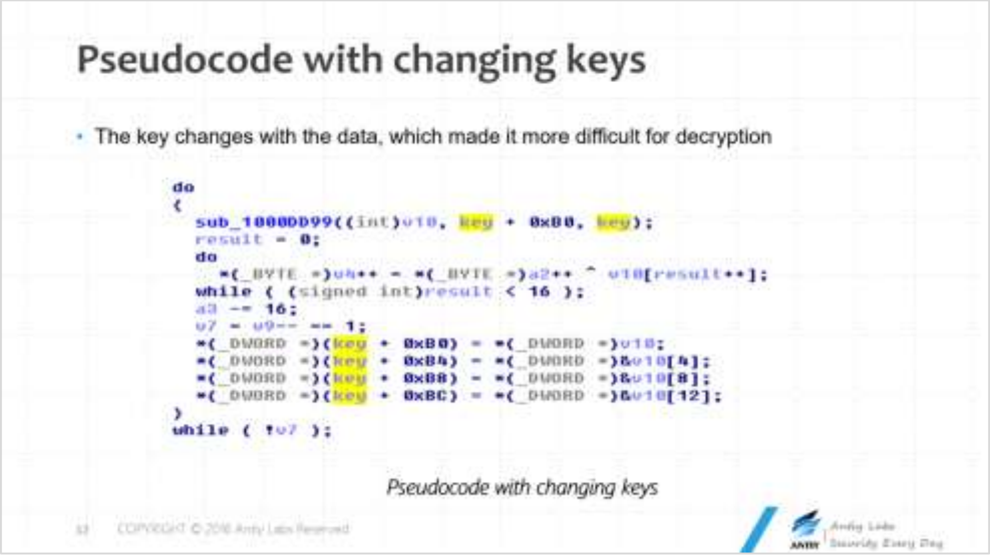
海莲花（APT-TOCS）攻击事件复现.

Video 1-2OceanLotus (APT-TOCS) attack event reappeared

Conference: China-Russia Forum on Cyberspace Development and Security (Moscow)

Report Title	"The Panda’s Scar——The APT Attacks against China"
Work Results	The first technical report on foreign APT attacks on my country was revealed in an international forum
Publication date of results	April 29, 2016
Publicly available technical reports	Panda's Scars: APT in China The paper version of the report is published in "Antiy Technical Articles Compilation

	(Thirteen) Advanced Persistent Threat (APT) Special Topic"



Pseudocode with changing keys

- The key changes with the data, which made it more difficult for decryption

```
do
{
  sub_1000DD99((int)v10, key + 0x80, key);
  result = 0;
  do
    *(_BYTE *)v4++ = *(_BYTE *)a2++ ^ v10[result++];
  while ( (signed int)result < 16 );
  a3 -= 16;
  v7 = v9-- == 1;
  *(_DWORD *)(key + 0xB0) = *(_DWORD *)v10;
  *(_DWORD *)(key + 0xB4) = *(_DWORD *)&v10[4];
  *(_DWORD *)(key + 0xB8) = *(_DWORD *)&v10[8];
  *(_DWORD *)(key + 0xBC) = *(_DWORD *)&v10[12];
}
while ( !v7 );
```

Pseudocode with changing keys

13 COPYRIGHT © 2016 Antiy Labs Reserved

Antiy Labs Security Every Day

Figure 1-9 10Attack organization/operation: White Elephant (India)

Work Results	The first time in China to target a foreign APT organization
Publication date of results	July 2016
Publicly available technical reports	Dance of the White Elephant: Cyber Attacks from the South Asian Subcontinent The paper version of the report is published in "Antiy Technical Articles Compilation (Thirteen) Advanced Persistent Threat (APT) Special Topic" References to early public content of the analysis work: "The Current Status, Challenges and Improvements of Anti-Virus (Part 1)" (Published in the April 2014 issue of the China Computer Society Bulletin 10 roll No. 4 Expect) " APT clues, associations and sample set measurement" (Antiy speech at the China Internet Security Conference in September 2014)

白象的舞步——来自南亚次大陆的网络攻击

安天安全研究与应急处理中心(Antiy CERT)

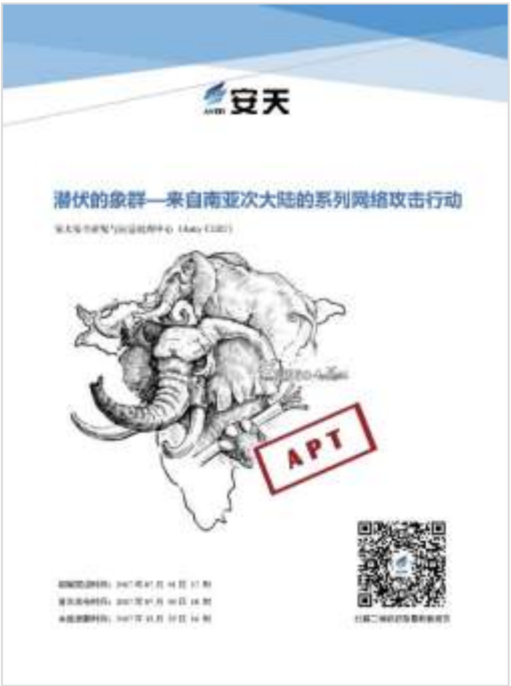
Figure 1-11Cover of Dance of the White Elephant: Cyber Attacks from the South Asian Subcontinent

白象组织对我国的
攻击活动复现.mp4

Video 1-3White Elephant group's attack on China reappears

Attacking Organization/Action: Elephant Group (India)

Work Results	Comprehensive analysis of multiple attack organizations in the South Asian geopolitical context
Publication date of results	December 2017
Publicly available technical reports	"Hidden Elephants: A Series of Cyber Attacks from the South Asian Subcontinent"



安天

潜伏的象群—来自南亚次大陆的系列网络攻击行动

安天安全研究与应急处理中心（Antiy CERT）

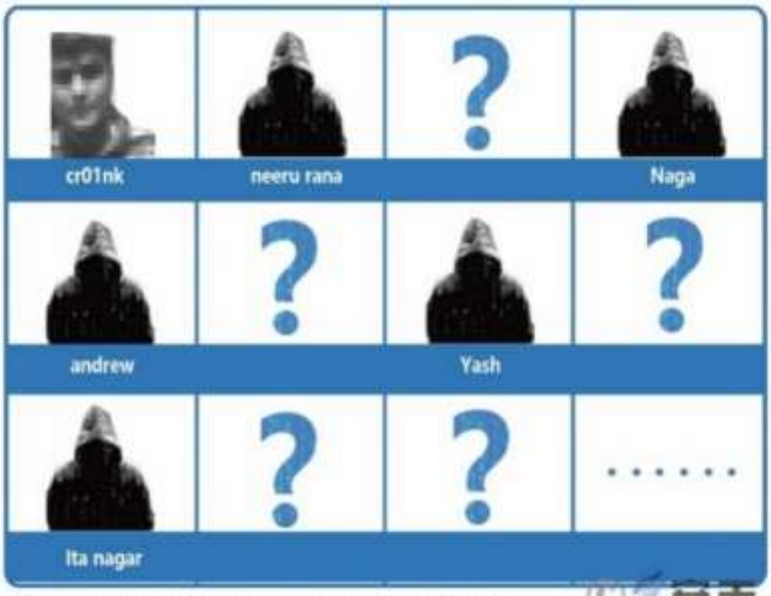
[illegible]

[illegible]

[illegible]

扫描二维码获取最新版报告

Figure 1-12Cover of Hidden Elephants: A Series of Cyber Attacks from the South Asian Subcontinent



本图为安天工程师基于线索分析及互联网公开信息推测绘制的"白象一代"攻击组织成员画像

Figure 1-13Portrait of members of the "White Elephant Generation" attack group drawn by Antiy engineers

Attack Organization/Action: GreenSpot

Work Results	Comprehensive analysis and disclosure of GreenSpot's decade-long attack activities
Publication date of results	September 2018
Publicly available technical reports	GreenSpot's Operation: The Year-Long Attack The paper version was published in "Antiy Technical Articles Compilation (Fourteen)

	Special Topic on Advanced Persistent Threats (APT)" Related media reports: October 7, 2018: Focus Interview "Information Security: Preventing Insiders and Hackers" September 15, 2019: Focus Interview "Cybersecurity: For the People and by the People"

安天

"绿斑"行动——持续多年的攻击

APT

Figure 1-14Cover of GreenSpot's Operation: The Year-Long Attack

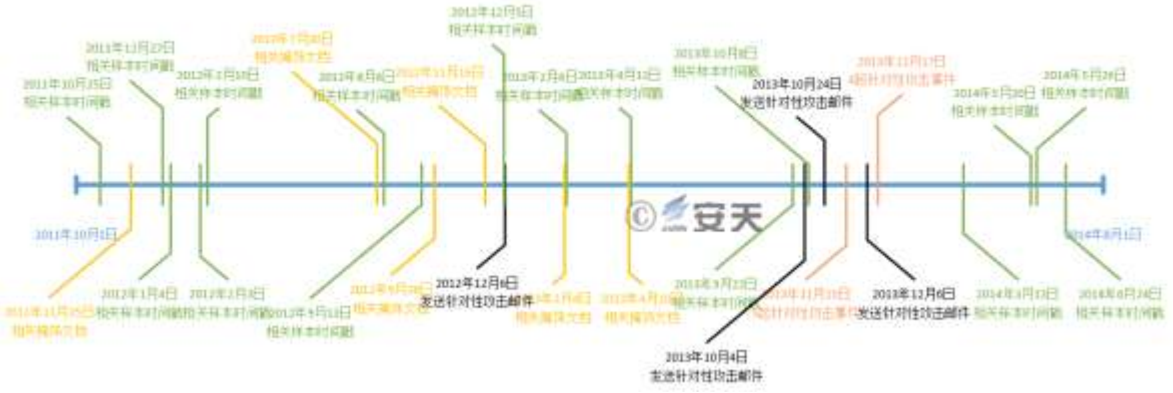


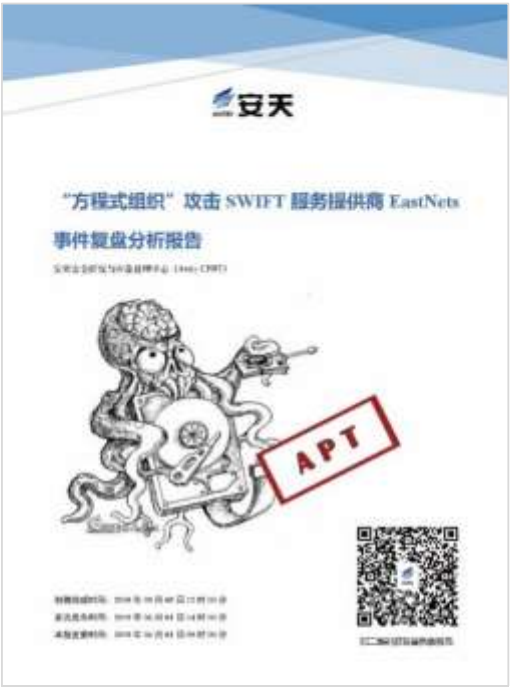
Figure 1-15Timeline of GreenSpot’s attack activities from 2011 to 2014

绿斑事件-可视化
复现.mp4

Video 1-4GreenSpot event - visual reproduction

Attack Organization/Action: EQUATION (US)

Work Results	Complete restoration of the complete operation process of the US attacking other countries' financial infrastructure
Publication date of results	June 2019
Publicly available technical reports	"Review and Analysis Report on the Equation Group's Attack on SWIFT Service Provider EastNets" The paper version was published in "Antiy Technical Articles Compilation (Fourteen) Special Topic on Advanced Persistent Threats (APT)" June 3, 2019: Xinhua News Agency signed article "Hidden Concerns about the Generalization of US Cyber Attack Targets" June 2, 2019: China Internet News Center: "This report slaps the US government in the face! It turns out that these cyber attacks and thefts were all done by them! The US is crying thief" July 21, 2021: Global Times: "The United States is the biggest destroyer of the international cyberspace order" April 15, 2022: Focus Interview: "Jointly Protecting National Security"



安天

“方程式组织”攻击 SWIFT 服务提供商 EastNets

事件复盘分析报告

安天安全研究与应急处理中心（Antiy CERT）

[illegible]

Figure 1-16Cover of Review and Analysis Report on the Equation Group's Attack on SWIFT Service Provider EastNets

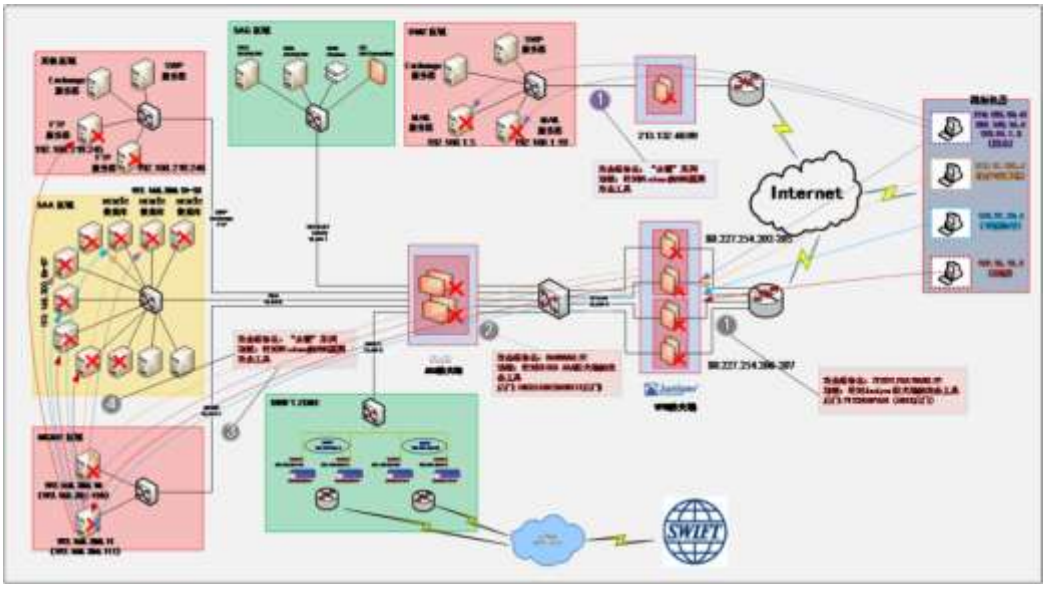


Figure 1-17Review of the overall attack process of the "Equation Group" on the EastNets network

“方程式组织”攻击S
WIFT服务提供商Ea

Video 1-5Visual reproduction of the Equation Group attack on SWIFT service provider EastNets

Attack Organization/Action: Stuxnet (US)

Work Results	Draw a multi-generational engineering map of malicious samples from the United States, and unravel a large number of historical problems left over from Stuxnet
Publication date of results	September 2019
Publicly available technical reports	"Review and Reflection on the Stuxnet Incident Nine Years Ago" The paper version was published in "Antiy Technical Articles Compilation (Fourteen) Special Topic on Advanced Persistent Threats (APT)"

Figure 1of Review and Reflection on the Stuxnet Incident Nine Years Ago

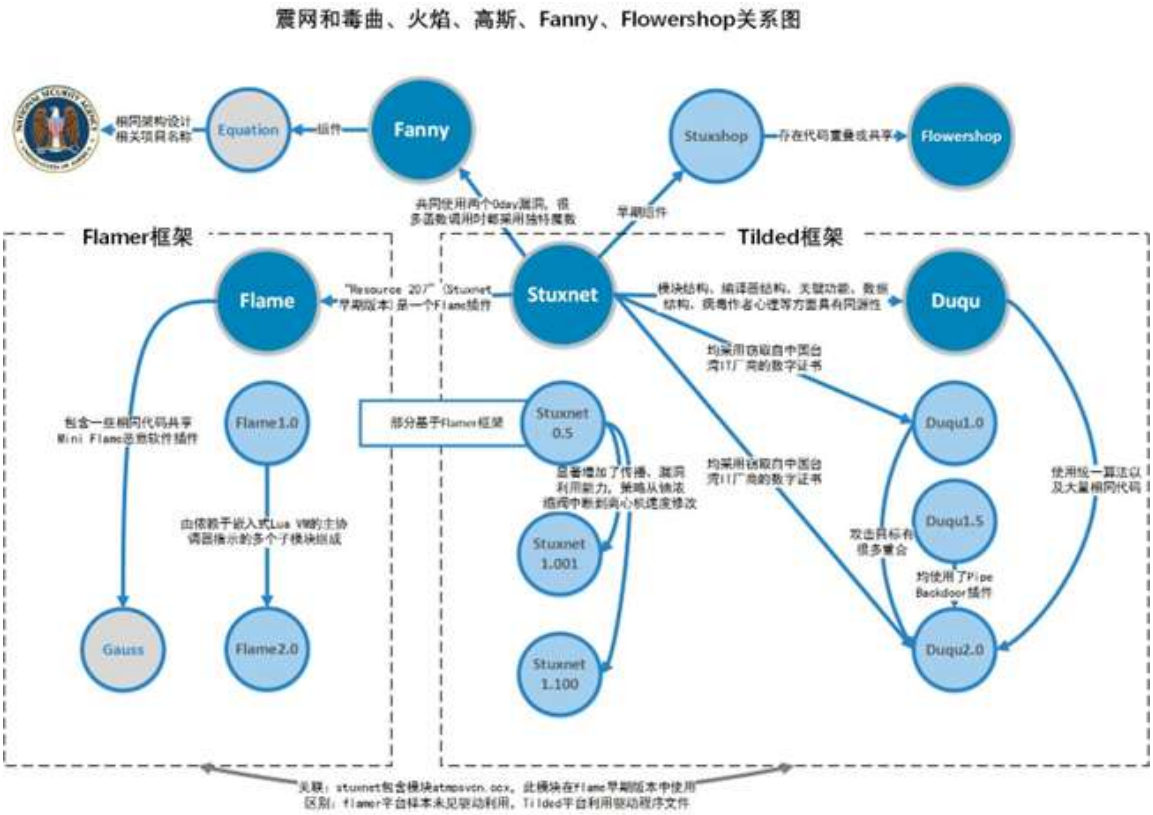


Figure 118and Duqu, Huoyan, Gauss, Fanny, and Flowershop

Attacker Organization/Action: BabyElephant (India)

Work Results	The first new APT organization exposed

Publication date of results	January 2020
Publicly available technical reports	Analysis of Cyber Attack Activities of the "Baby Elephant" Organization in South Asia The paper version was published in "Antiy Technical Articles Compilation (Fourteen) Special Topic on Advanced Persistent Threats (APT)" November 20, 2021: Global Times: "The Indian hacker group "Baby Elephant", which has long invaded many countries in South Asia, has turned its attacks to China"

Figure 1-19Cover of Analysis Report on Cyber Attack Activities by the "Baby Elephant" Organization in South Asia

Attack Organization/Action: Darkhotel

Work Results	Analysis of the technical means of black shop penetration isolation network
Publication date of results	May 2020
Publicly available technical reports	Analysis of Ramsay components used by Darkhotel to penetrate isolated networks The paper version was published in "Antiy Technical Articles Compilation (Fourteen) Special Topic on Advanced Persistent Threats (APT)"

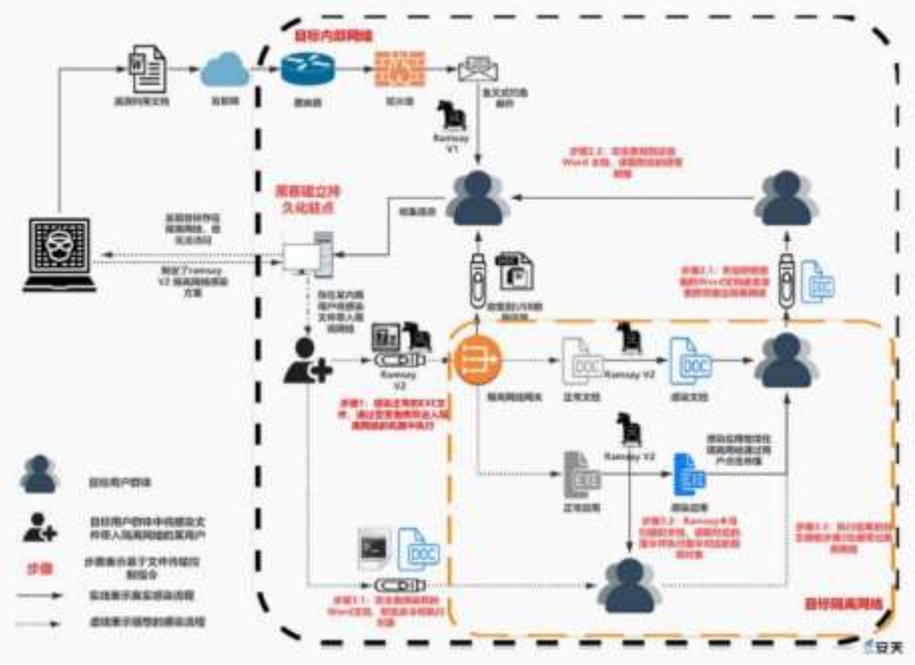


Figure 1-20Ramsay breaks through isolation network conjecture flowchart

Ramsay渗透隔离网窃密流程可视化

Video 1-6Ramsay penetration isolation network espionage process visualization reproduction

Attack Organization/Action: DarkElephant (India)

Work Results	Disclosing India's new APT organization and tracing the organization's natural persons
Publication date of results	June 2022
Publicly available technical reports	"DarkElephant" Attack Organization/Operation: A Decade of Hidden Cyber Attacks The paper version was published in "Antiy Technical Articles Compilation (Fourteen) Special Topic on Advanced Persistent Threats (APT)" June 17, 2022: Global Times: "Another exposure! "Attack on China for ten years"" July 26, 2022: Phoenix TV News: Dark Elephant Group: A Decade of Cyber Attacks

“暗象”组织：潜藏十年的网络攻击

安天应急响应中心（Antiy CERT）

Figure 1-21Cover of "DarkElephant" Attack Organization/Operation: A Decade of Hidden Cyber Attacks

Attack Organization/Action: OceanLotus (APT-TOCS) (Vietnam)

Work Results	The first disclosure of an operating model that uses IoT devices as a springboard and traffic forwarding
Publication date of results	December 2022
Publicly available technical reports	Analysis of Torii Remote Control Network Attack Activities of OceanLotus Organization

安天

海莲花组织 Torii 远控的网络攻击活动分析

Figure 1Analysis of Torii Remote Control Network Attack Activities of OceanLotus Organization

Attack Organization/Action: EQUATION (US)

Work Results	The world's first exposure of the iOS platform sample of DoubleFantasy
Publication date of results	June 2023
Publicly available technical reports	"Quantum" System Breaks Through Apple Mobile Phones: Historical Sample Analysis of Equation Group's Attacks on iOS Systems June 9, 2023: Global Times: "The latest report from Chinese cybersecurity companies shows that the US cyberattack on iPhones began in 2013"

"量子"（QUANTUM）系统击穿苹果手机

——方程式组织攻击iOS系统的历史样本分析

Figure 1-22Cover of "Quantum" System Breaks Through Apple Mobile Phones: Historical Sample Analysis of Equation Group's Attacks on iOS Systems

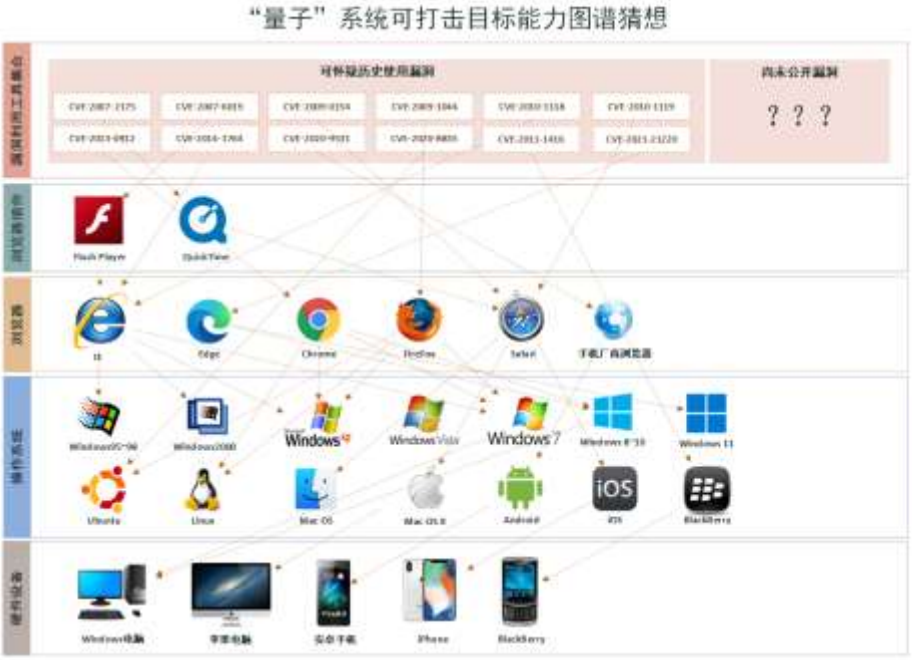


Figure 1-23Graphical analysis of attack scenarios of "quantum" systems

Early Antiy historical analysis reports and technical documents were published in the Antiy Technical Articles Compilation. All eleven volumes of history and the electronic version of the twenty-one 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.