

Analysis of a Group of Phishing Attacks by Taiwan's "Green Spot" Attack Organization Using Open-source Remote Control Trojan

Antiy CERT

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



Completion time of first draft: 09: 00, 13 September 2024 First published: 17 March 2025 15: 58 This edition was updated at 15: 58 on March 17, 2025



Scan QR code for the latest version of the report

1 Overview

In the second half of 2024, Antiy Emergency Response Center tracked APT attacks by Green Spots against specific industry targets in our country. The attacker sends a spear-phishing email to the official account of the target unit, guides the target to visit a malicious website disguised as a certain unit by clicking a link, and the website takes the initiative to jump and download. The victim is induced to save and execute a downloader program disguised as a PDF icon, which retrieves and decrypts a malicious payload disguised as a video suffix running in memory. Up to now, the main malicious loads observed are open source command and control frameworks such as Sliver remote control Trojan [2], in which attackers carry out long-term host control, network lateral movement and theft activities on targets. According to the technical characteristics of the target area and phishing process of the attack, and based on historical analysis data and information and open source intelligence, Antiy CERT comprehensively judges that the source of the attack activity is the "Green Spots" attack organization of Taiwan Province of China. In September 2018, Antiy had once released the group's cyberattack activity report, "Operation'Green Spots' - Attacks That Continue for Years," exposing the group's campaign, which began in 2007.^{[1][2]}

Based on the fact that Antiy has assisted relevant industry management departments in effectively notifying and handling relevant incidents, Antiy decided to publish the analysis results of the attack incident. Based on the fact that Antiy has assisted relevant industry management departments in effectively notifying and disposing of relevant events in the second half of last year, Antiy CERT has decided to officially publish this report. The characteristics of relevant attack activities are as follows:

Attack time	March 2024 (start of attack preparation)
Attack the target	Specific industries and fields in China
Intent to attack	Constant control, stealthiness
Bait type	An EXE executable disguised as a PDF
Method of	Spear phishing mail, document icon camouflage, open source
attack	remote control
Development language	C # language, Go language

Table 1-1 Characteristics of Green Spot Attack Activity 11



Open source remote control Sliver

equipment

Analysis of attack activities 2

2.1 Analysis of malicious websites

The attacker induces the target to visit the malicious website by email, which is disguised as the government information disclosure webpage of a certain authority:



Figure 2-1 Case of malicious webpage 21

When the web page is loaded, it will automatically jump to start downloading the bait loader file:

algument lagest. 1990-14	they' state 'select has d latte		et" claimmeters_test (ii)	for front-family missesoft f	abet, Artal, Beleviles, source	est" /virgan
<pre>cdiv data-sole="ept. ca how1="http:// ca how1="http:// ca how1="http:// ca how1="http:// ca how1="http://</pre>		(株式管理局で、tarpet=* blank**** (株式管理局で、tarpet=* blank****) (株式管理局で、tarpet=* blank****) (株式管理局)	data-Jole-"option_them">	东正地区智理局caperan 中本地区管理局caperan		
<pre>in host="http:/// in host="http:// in host="http://</pre>	att.th* hitle************************************	imis 管理は一 Gargeter blankter 開き 管理は一 Gargeter blankter 管理者は一 Gargeter blankter	data-puls-"option_ites";	西南東区首席局	安天	
eligias.	Contrast and a		* A 1 5 .			



2.2 **Decoy Downloader Analysis**

The decoy downloader is a C # program whose icon is disguised as a PDF document, some examples are used to tamper with the time stamp, and the file name is used to guide the target to click and execute by leading speeches on Party discipline events, personal identity document information and other topics. Take the extension line sample as an example:





Figure 2-3 Case of Decoy Downloader 2-3

Table 2-1 Sample Labels of Decoy Downloader 2-1

Virus name	Trojan / Win64.MSIL.Wagex
Original file name	* * * ID card scan.exe
Md5	* * * * 5B16A9595D20C0E185AB1FAE738F
Processor architecture	Intel 386 or later processors
File size	116.50 KB (119,296 bytes)
File format	Binexecute / Microsoft.EXE [: X86]}
Time stamp	2024: 03: 12 02: 20: 07 [UTC + 8]
Compiled Language	Microsoft Visual C #
Shell type	None

The code content of the downloader is obfuscated, and the sample Main function pair before and after

unobfuscating is as shown in the following figure:







Figure 2-4 Main function codes before and after aliasing 2-4

The main function first calls the method smethod _ 2 to download the encrypted payload data disguised as a video file from the link "https: // 128.199. * * *. * * / mp4 / mov.mp4."



Figure 2-5 Download an encrypted payload disguised as a video file 2-5

The method _ 0 function is then called to decrypt the downloaded mov. mp4 byte array using AES algorithm. Key used for decryption: "Lgumemnmuprrccra," IV: "Nstxrw4o6tnhckbm." The key must be identical with the key used in the encryption to decrypt the data correctly. Iv is a random or pseudo-random value that ensures that the same plaintext produces a different ciphertext each time it is encrypted.



 A Tribert Out2000013 HTD: 20 A Disternal Class Claust 								
	ut UVAL GAUGGATTE FILE OFFICE: GAUGUISESS add/Systell brie_0, arring string_3, string string_4)							
by the set of the set	1777, Gethyres(string_3); g. H771, Gethyres(string_4); site())							
H Ases. Gry = bytes; B ases. If = bytes; B ases. Tabling = Padds T Uppedimentions B using Obscorpfirment	ngRode, Nove. anafare = aen Crantellerryptoriaen (ny. aen 17). aeneryStream = new HennyStream(byre_0))							
aryptoStrea	rnam cryptoStream = name CryptoStream(memoryStream, transform, Cr m.WriteChyte_0, 0, hyte_0.longth); moryStream.Tokrray();	yytoStreaddode.9						
O Contant result.								
100 % -	045							
用冠全華	0-0							
岩際	10		20					
Þ 🛩 byte_0	Right=[0x00054E60]		byteg					
🖉 string_3	LgUmeMnmUpRrCCRA							
string_4	*rStaRW4obTNHckilm*							
⊅ 🛩 bytes	bytes byteg							
b bytes2	bytes2 byte[0x0000010] byte]							
Fiel ars	System Security, Cryptography, AesCryptoServiceProvider System Security, Cryptography.							
🕩 😅 transform	Transform System Security Cryptography Capity Ca							
memoryStream	memoryStream System JO MemoryStream System JO MemoryStream							
▶ 🛹 cryptoStream	System Security Cryptography CryptoStream		System Security Cryptography					
Pier result	byte-toxocch54Esot		(bytel)					

Figure 26 decrypts payload data 2-6

Call smethod _ 1 method, and use GZipStream to extract the AES algorithm to decrypt the resulting byte array.

public static typed small	s myk, badonomic file officer: badooniko: Lidoyte[] byte_0)							
byrell result. suine Ormryftream men	nyftrean = nee Mennyftrean())							
toning GennyStrein	nenoryStrennd = new YeneryGtrenn(byte_0))	11.0						
100 %								
用砂火量								
名牌	1	東盟						
> w byte_0	byte:0 byte() byte()							
> memoryStream	memoryStream System 10.MemoryStream System 30.MemoryStream							
memoryStream2	memoryStream2 System.IO.MemoryStream System.IO.MemoryStream							
System ID.Compression.C2pStream System ID.Compression.C2pStream System ID.Compress								
🖻 🤗 result	sevit superior supere							

Figure 2-7 Decompressing payload data 2-7

Call the method smethod _ 3, and use multiple delegates and unmanaged code to process the byte array extracted by the method smethod _ 1, in order to finally decrypt the payload and execute it.



10 // Teken: 0x000000000 FILD: 111 RVA public static wold sectord_00yte	ordonolilli File Officer deddddafd] byte_0						
Ti Dilandi, (Delegate) gdelegate Ti Infra InfPir - adelegate Con Daritel Concibyre 0, U. InfPi		al Chelegatet)) as 971aus0.0Delegatet.					
Classed, Cheirgann, adelegate2 billion in Standie = gdelegate20 ptr = Classi, method (Classic	2) sectord (Carring) (219651662), (Bodala), sectord (Carring = Terring), Gerthelegen al or American Santa Santa (Santa), (Santa (Carring)) (Santa Santa (Santa)) (-10641 (Santa), (Santa (Santa)), (Santa (Santa)), (Santa)) (Santa (Santa), Santa (Santa) (-10641 (Santa), (Santa)) (Santa (Santa), Santa (Santa) (Santa),	no. (Delegate7)) an OClarath (Delegate7; nac)(1776(12071), dalue).					
100 %							
同節交量	0 2 -	天					
名称	ũ.	227					
Þ ₩ byte_0	byte (0x0100033E)	byteg					
Þ ● ptr	0x000000077295980 System.intil a						
₽ ₽ gdelegate	GClass0.GDelegate0 GClass1.GDelegate6 GClass1.GDelegate6						
Þ 🛩 intPu	Dx00000001E4A0000 System.0000						
gdelegate2	null GClaud.GDb/logate?						
D 🥥 Mtandle	0x200000000000000	System.http://					
🐸 gdelegate3	- iiuli i	GClass0.GDelegate8					

Figure 2-8 processes the decompressed payload data 2-8

2.3 Open source remote control load analysis

The payload data content disguised as the suffix of the MP4 video file is completely encrypted, and the payload obtained after the above decryption and decompression process has the anti-debugging function. Based on the comparison of multiple code positions such as initial entry and main functions, and the JA3 fingerprint of Client Hello packet in C2 control online communication traffic (19e29534fd49dd27d09234e639c4057e), It can be found that the payload is generated by the well-known Open Source Red Team Command and Control Framework project Sliver.

> Extension: key_share (len=38) x25519
[JA4: t13i190800_9dc949149365_97f8aa674fd9]
[JA4_r: t13i190800_000a,002f,0035,009c,009d,1301,1302,1303,c009,c00a,c012,c013,c014,c02b,c02c,
[JA3 Fullstring: 771,49195-49199-49196-49200-52393-52392-49161-49171-49162-49172-156-157-47-53
[JA3: 19e29534fd49dd27d09234e639c4057d[])

Figure 29 The JA3 fingerprint of the Client Hello packet is consistent with the Sliver remote control feature 2-9

According to the open source project introduction [2], Sliver is an open source Red Team command and control simulation framework similar to CobaltStrike that can span Windows, Linux and MAC system platforms. It supports multiple network protocol communication modes such as Mutual TLS (mTLS), WireGuard, HTTP (S) and DNS, and has most post-penetration functions similar to tools such as CobaltStrike and Metasploit.^[2]

Characteristics	Description
Cross-platform support	Support for MacOS, Windows and Linux systems.
C2 Communications	Support command and control communication via Mutual TLS (mTLS), WireGuard,

Table 2-2 Sliver remote control frame characteristics 2-2



	HTTP (S), DNS.
Dynamic code generation	Code obfuscation at compile time to enhance security.
Multiple Payloads	Phased and phaseless loads are supported.
Scripted	Full scripting can be done using JavaScript / TypeScript or Python.
Memory execution	Supports executing .NET assemblies and COFF / BOF loaders in memory.
Other functions	Including process migration, file theft, process injection, user token operation and other post-penetration functions.

3 Attack Mapping from the Perspective of Threat Framework

This series of attacks involves 25 technical points in 10 phases of ATT & CK framework, and the specific behaviors are described in the following table:

Att & CK phase	Specific behavior	Notes					
	Gathering information on the identities of the victims	Collect the identity information of the target					
Reconnaissance	Gathering information about the victims' networks	Collect the target's office email account					
	Gathering information on the victims' organizations	Collect the information of the target office					
	Access to infrastructure	Register domain names and servers					
Resource development	Capacity development	Develop malicious websites, decoy programs, remote control platforms and payloads					
	Create an account	Sign up for an originating account to send phishing mail					
Initial access	Phishing	Attack via spear-phishing email					
Execution	Inducing the user to execute	By inducing the user to click on the bait program starts the Trojan execution flow					
Defensive evasion	Circumventing the debugger	Remote control memory payload with anti - debug capability					
Defensive evasion	Counterfeit	Malicious websites and decoy programs are phishin evasions					
	Discover remote systems	Sliver remote-control internal network remote-detecting system					
Findings	Scan web services	The Sliver remote control can scan the network services of the remote system					

Table 3-1 Technical behavior description of this green spot group attack activity 3-1

「空天 Analysis of a Group of Phishing Attacks by Taiwan's "Green Spot" Attack Organization Using Open-source Remote Control Trojan

	Discovery of system information	Sliver remote control can inquire system version information					
	Discovery system network configuration	Sliver remote control can inquire system network configuration information					
	Discovery of account	Sliver remote control can search system account information					
	Find files and directories	Sliver remote controls access file and directory information					
	Discover the system owner / user	The Sliver remote control can inquire the information of the system's user and authority group					
	Discovery Process	The Sliver remote control can query the current process information of the system					
	Collect local system data	Sliver remote control can collect local system version, account and other data					
Collection	Input capture	Sliver remote control enables input capture					
	Screen capture	Sliver remote control allows screen capture					
Command and	The application layer protocol is used	The Sliver remote control payload uses an application layer protocol to implement command control					
control	Encoded data	The Sliver remote control load command controls the flow to encrypt the encoded data					
Data seeps out	The C2 channel is used for backtransmission	The Sliver remote control payload uses the fixed C2 channel to return the data					
Impact	Manipulation of data Attackers can manipulate victim host data based on Slive remote control						

Mapping the technical points involved in the threatening behavior to the ATT & CK framework is shown in the

following figure:

Million (-	Amontonio	WITCHER	MARINE	BREAKEN.		CONTRACTOR: NOT		HUMPER +++		1991	MANUAL DATE:	MB1121	0.010001111	REPAIRS	
SHEEK .	BRIDER.	AREA.	PURCHARGER D. P.	9824	STATISTICS.	SALHERS .	WERA.		AND DESCRIPTION OF	101	-	STATES AND INCOME.	ADDRESS AND	-	8-1998#	100-00
CATHORNE.	month	4.088	NACO TRAVER	ADDITION A		ancess	RHORA	-		and sectors	******	ACCOUNTS OF	Numbers .	Actours	MOTORAL	-
CETHEN!	Ame -	ACCENTIANE NO.	AUGUATION A	TATE AS ANY	HART	-	-	PARTY, ATTAC	CONTRACT.	annana .	******	MORNINAT	-	NURA	Personal Party of the Person o	ALLIBRO HAR
Contract of	Address of	NURA MORE	WENE .	August States	INGRO-	LEX-LETNE	BR-121		Annianian	*NIMMEN	aune .	-	sises	-	SHORTHR.	-
anter a	-	01.01	PORTAGE MAL	"sandarus	Manual States		NAL PRIMA	1 8	mug	UNTITAR.	amontal a	SHOWN .	NEWSONA BE	SARK .	PERSONAL PROPERTY.	8.8+1.118
Atternals	BOAN	ane .	MARGINE	ARRING	"sillions	ALLANCE#	INDIANOS	1 8	Barrowitz	**LINE	HADRONNE	ACTINUM		manes	einiettiin	max
ATURAUST	anith .	Pagements a	BARRARE .	our-	*****		tentine.	1	BARRY.	ancenia.	aucourt -	AUGUATENS ATTA	REAL PROPERTY.	searce	ennang	Assault .
ALTINTER.	uses	3.000000	Narith S.I.	None of Contraction	1082320	Basta	HERRICH		union pole	TRABUTS		TRIPNE	RREEATRE	minut	10000	inter
RACTING.		HANDAR	RRNWT	-	-	NISHEN	-		PARADIAL OF	NUMBER OF	*ELWINE	CREADOUR IN	-	BRATEARN	CODMINENT N	0.029
*******		HETER	HARPPRAT	Internations.	-	BROMER PE		11 8	*ANBINESS	TRABANT	ANDREA	1	ABORDER .	messes	-	without a
			TIN STREET	Northeast .	BIVEBUR	aen+	WWT-serve	1	n annu	10,475	ABARTH		ARAMITAR AND	TWO ALENG		Sussaires.
			BOARDER.	-	BHILA	BITHERE	BUILD BH		ananture.		BARDWAR		ANTINGUES .	manuat		2344
			BURNESS.	-	Non-BRAT	RETRAKEN	Parrisona.		CRIMINAL PARTY	22,084				exiter		2590
			BREN Anivel	an market	icensor*	-	aouann	1. 8	SH Foreshables	uttie			ess.ien	mona		interati
				10.01		HABITAR	MBDA.		ALLA CORNA	CORPORATE A			-	NUMBER		
. 18				nanimapi		amon		1 8	Colorena Trill				-	PERMIT		
·				PARIMET.		10	HERMAN NYT		coore	-				"mattheast		
				COLUMNS .		RABING OF	ACR FROM		*4+MTH	annun .	1			namous		
-				ARRACT		*******	State Date of the last	1		anaphis in	8	F				
-				Korne-		CONTRACTOR IN	werma.	1		*1218.0						

Figure 3-1 Map of ATT & CK corresponding to this green spot attack activity 3-1

4 Summary

Based on the above analysis, Antiy CERT judges and judges that this is from the background of the Taiwan Province of China's "Green Spots" APT organization's attack activities. The organization was formally named and exposed by Antiy in 2018, and was covered by CCTV Focus [3]. The attacker constructs strong fraudulent materials of social workers for specific industry targets, conducts spear-phishing attacks, and finally implements Trojan implantation and attack methods of open source remote control framework after multiple disguises and encryption of the payload. Have obvious pertinence.^[3]

In order to cope with relevant attacks, it is necessary to build the cornerstone of terminal security and strengthen protection, and the defense level can be composed of email security, network traffic monitoring, terminal protection, XDR linkage analysis and gateway blocking. In particular to terminal security protection software with effective antivirus and main prevention capability and strong anti-phishing function. Based on the characteristics of social workers and the attack stickiness of "spitting chewing gum everywhere," improving safety awareness is also an important part of prevention.

Appendix I: Reference Materials

[1]. Antiy.operation "Green Spots" - an attack that lasts for years [R / OL]. (2018-09-19)

Https://www.antiy.cn/research/notice & report/research_report/20180919.html

[2]. Bishopfox / sliver [R / OL]. (2019-06)

Https: //github.com/BishopFox/sliver

 [3]. Interview in Focus 20181007 Information Security: Prevention of Insider and Anti-Hacker [R / OL]. (2018-10-07)

Http://tv.cctv.com/2018/10/07/VIDEHBYLGmnR5LoYZawu3dZc181007.shtml

 [4]. Critical Infrastructure Security Emergency Response Center. analysis Report on Recent APT Attacks by Green Spot Group [R / OL]. (2020-08-12)

Https://mp.weixin.qq.com/s/275EYNAjOGLn19ng56-czA

Appendix II: IoCs

locs
* * * * 2751F6BB4EFAFEC524BE23055FBA
* * * BA2DB8C3FDD717D83BB693B3ADE9
* * * 0E267C5EBF2DE55D086D0B2393A6
* * * * 5B16A9595D20C0E185AB1FAE738F
* * * * 6B1EBCB43172B5188AD61946D2D0
Ca * * * n [.] com / auto-download.zip
158.247. * *. * * / mp4 / ads.mp4
128.199. * *. * * / mp4 / mov.mp4
Caa * * * n.com
Caa * * * n.org
Ba * * * cingcloud.com
165.22. * * *. * *
158.247. * * *. * *
128.199. * *. * *

Appendix II: About Antiy

Anty 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.

「安天 Analysis of a Group of Phishing Attacks by Taiwan's "Green Spot" Attack Organization Using Open-source Remote Control Trojan

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.