Scanbox Watering Hole Targets Pakistani and Tibetan Government Website Visitors

By Insikt Group
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.

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.
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.

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:

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

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]).

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.
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**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>185.236.76[.]35</td>
<td>tracking.dgip.gov[.]pk</td>
</tr>
<tr>
<td>23.225.161[.]105</td>
<td>tibct[.]net</td>
</tr>
<tr>
<td>103.255.179[.]142</td>
<td>oppo[.]ml</td>
</tr>
<tr>
<td>139.59.90[.]169</td>
<td>tibct[.]org</td>
</tr>
<tr>
<td>183.237.106[.]140</td>
<td>monlamlt[.]com</td>
</tr>
<tr>
<td>104.18.36[.]192</td>
<td>mailshield[.]ga</td>
</tr>
<tr>
<td>104.18.37[.]192</td>
<td>photogram[.]ga</td>
</tr>
<tr>
<td>2606:4700:30::6812[::24c0]</td>
<td>Mail.mailshield[.]ga</td>
</tr>
</tbody>
</table>

**Observable indicators**

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>104.18.36[.]192</td>
</tr>
<tr>
<td>104.18.37[.]192</td>
</tr>
<tr>
<td>2606:4700:30::6812[::24c0]</td>
</tr>
</tbody>
</table>
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.

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();”.

Obfuscated 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.”

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.

```yara
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:

```plaintext
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;)


```

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.