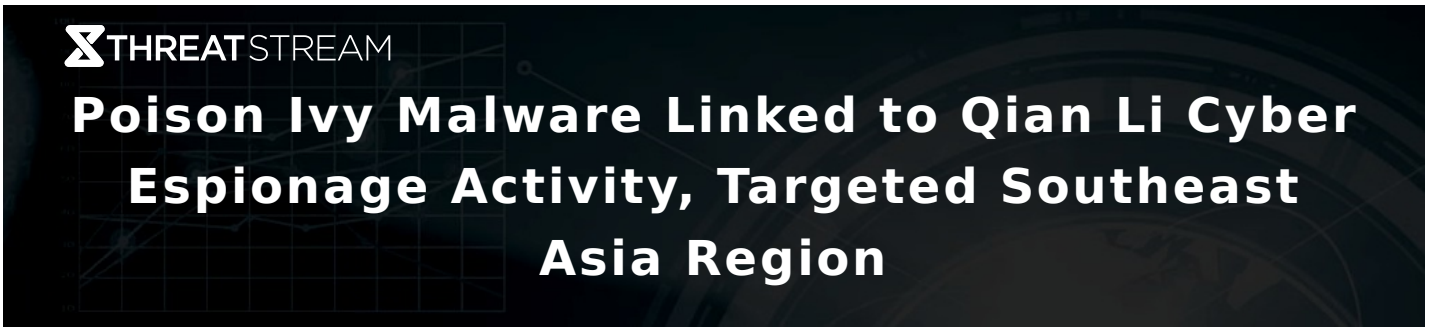

Posted on 2015-09-27 03:52:30 +0000 by **iSIGHT Partners (iSIGHT Partners)**
Last modified on 2015-09-27 03:52:30 +0000

Stage **New**

Traffic-Light Protocol **TLP:Red**

Source **ISIGHT Partners**

Tags 15-00010250 ThreatScape Cyber Espionage

This report is classified **Trusted Circle**
Shared with Trusted Circle iSIGHT

Originally published on September 26, 2015 06:55:00 PM

Overview:

A Poison Ivy malware sample linked to Qian Li cyber espionage activity confirms continued operations against Southeast Asian naval security. Allies from outside the region, including the US, Australia and India, were most likely also affected. We consider the abuse of a regular weekly report an effective social engineering lure because it is less likely to provoke suspicion.

Key Points:

- Analysis of a Poison Ivy malware sample distributed with a maritime security lure document indicates ongoing campaigns targeting Southeast Asian navies and their allies.

Threat Detail:

Cyber Espionage Campaign Probably Intended to Target Regional Navies
iSIGHT Partners analyzed a Poison Ivy sample distributed with a lure document made to look like a report from the Singapore-based Information Fusion Centre (IFC), a regional information sharing body focused on maritime security. Based on technical indicators, the detected Poison Ivy malware is most likely linked to Qian Li cyber espionage activity (also reported as "KeyBoy" or "Pirate Panda" by open sources) and is indicative of continued Chinese interest in targeting assets in Southeast Asia, especially those with naval capabilities that may challenge the People's Liberation Army (PLA) Navy's expanding presence. The use of an IFC-themed lure probably reflects an effort to compromise organizations linked to naval issues in the region, including those in defense and trade.

- The analyzed Poison Ivy sample shares significant similarities with activity that leveraged the Qian Li malware family, including:
    - A DLL export name shared with PHKing malware samples (the primary tool associated with the Qian Li malware suite).
    - A Mutex linked with other Poison Ivy malware that overlapped with PHKing activity.

    - A unique string (MDDEFGEGETGI) that is just one character short of a unique string leveraged by PHKing (MDDEFGEGETGIZ).
- Historic targeting by Qian Li activity includes victims in the US, Australia, Malaysia, the Philippines, Vietnam and India – all members of the IFC.
- These states have opposed Chinese expansion in the region (including the South China Sea and littoral waters throughout Southeast Asia) and are regular targets of China-based actors aligned with state interests.
- For more information on earlier Qian Li malware operations, see Intel-996860, Jan. 21, 2014.

Figure 1: Logo for the Information Fusion Center hosted by the Republic of Singapore Navy (twitter.com)

The identified lure document (MD5: 5b799d953439757db499b960e0061f31, titled "IFCWeeklyReport4Mar-11Mar15.doc") was most likely either made to look like a legitimate weekly report or was compromised from a genuine document. The use of such a decoy most likely indicates the detected malware sample was distributed via a spear-phishing e-mail. We surmise that weekly report lures make effective spear-phishing lures because their regular delivery would not attract suspicion.

- It should be noted that the identified lure document was corrupted at the time of analysis.
- The malicious document exploited the old vulnerability CVE-2012-0158. Additional technical data is available in the Technical Annex.

Outlook and Implications

The analyzed lure document confirms persistent campaigns against stakeholders in the Southeast Asian maritime region. Actors leveraging Qian Li-associated malware have historically targeted organizations in Southeast Asian countries and global allies such as the US, Australia and India and continue to collect information on naval security postures. Furthermore, the continued exploitation of CVE-2012-0158 highlights the importance of ensuring systems are patched and the fact that significant numbers of unpatched systems are almost certainly victimized.

Technical Annex

Execution

Configuration Details for the Poison Ivy sample are as follows:

ID: "WLQS"

Group: "150311"

Password: "admin"

Startup: No

Melt File: Yes

Process Mutex: "(V!hex67)"

Key Logger: No

Files Dropped

After successful execution of the malware (MD5: ed13d1a61535c481306e262556f91f80), it drops the following files to victims' systems:

- %APPDATA%\Roaming\Microsoft\SystemCertificates\SystemCertificates.ocx (MD5: af797d920fda253b27f48941a30664bb)
    - Poison Ivy Binary
- %TEMP%\IFCWeeklyReport4Mar-11Mar15.doc (MD5: 5b799d953439757db499b960e0061f31)
    - Decoy Document (Corrupted)
- %APPDATA%\Roaming\Microsoft\SystemCertificates\HOSTUPDATE.dat (MD5: afebcc31b482a5821c3d7a80b29c7cfb)
    - Binary Data Blob

The malware maintains persistence on victims' systems using the Registry Key:

- Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemCertificates
- Value: rundll32.exe "%APPDATA%\Roaming\Microsoft\SystemCertificates\SystemCertificates.ocx,"SSSS

Network Communications

After successful installation / initialization, the malware attempts to callback to the command and control (C&C) server "babyolo.my03.com" via port TCP/53. However, the C&C is not actively responding, which prevents the sample from attempting the Poison Ivy authentication.

The sample is also configured to reach out on TCP/7433.

Network Intelligence

Passive DNS

Passive DNS was queried for the domain (babyolo.my03.com):

Host/Domain Name	IP	First Seen
babyolo.my03.com	199.71.213.14	2014-01-06
babyolo.my03.com	23.89.192.96	2014-06-02
babyolo.my03.com	103.224.81.58	2014-07-25
babyolo.my03.com	118.193.151.4	2015-06-15
babyolo.my03.com	118.193.133.96	2015-08-17
babyolo.my03.com	103.238.224.209	2015-08-27

Passive DNS was queried for the IP address (118.193.133.96):

IP Address	Host/Domain	First Seen
118.193.133.96	www.babyolo.my03.com	2015-09-15
118.193.133.96	babyolo.my03.com	2015-08-17

IP Information

IP Location: Shihu China

ASN: AS588798

IP Address: 118.193.133.96

Reverse IP: N/A

NetRange:118.193.128.0 – 118.193.255.255

OrgName: Shanghai Anchnet Network Technology Stock Co.,Ltd

Domain Information

The C&C domain in use is a dynamic DNS Domain.

Related Samples

- b33761b1127d912580b7e240f820b0fd (PHKing)
  - www.bannered.4dq.com – C&C
  - www.metacu.ygto.com – C&C
  - www.amberisic611.4dq.com – C&C
  - SSSS – DLL Export
  - credentials.ocx - Filename
- 1f71d381a319e201faa0416f7465d1c3 (Poison Ivy)
  - www.babyolo.my03.com - C&C
  - Y123YYY – Mutex
  - BNGw14+ - ID
- 69b670b8c92da772bf7be866fac35b43 (Poison Ivy)
  - (V!hex67) – Mutex
  - 23.27.112.216 – C&C
  - 50.117.38.164 – C&C

    - !@#edc - Password
- d2d12ccced9814b571216218bf25281a (PHKing)
    - credentials.ocx – Filename
    - SSSS – DLL Export
    - www.myzinfo.myz.info – C&C
- 02d6bf372f688227f86f89b0d5a051e8 (Poison Ivy)
    - poison – Group
    - config0826 – Password
    - www.bannered.4dq.com – C&C
    - (V!hex67) – Mutex

Information Cut-Off Date: Sept. 16, 2015

Comments

This TIP does not have any comments yet.

History

iSIGHT Partners (iSIGHT Partners)	Created Report	2015-09-27 03:52:30 +0000