RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: TTA-R02

Nation State & Hacktivist Attacks: Targeted Hits on Asian Organizations

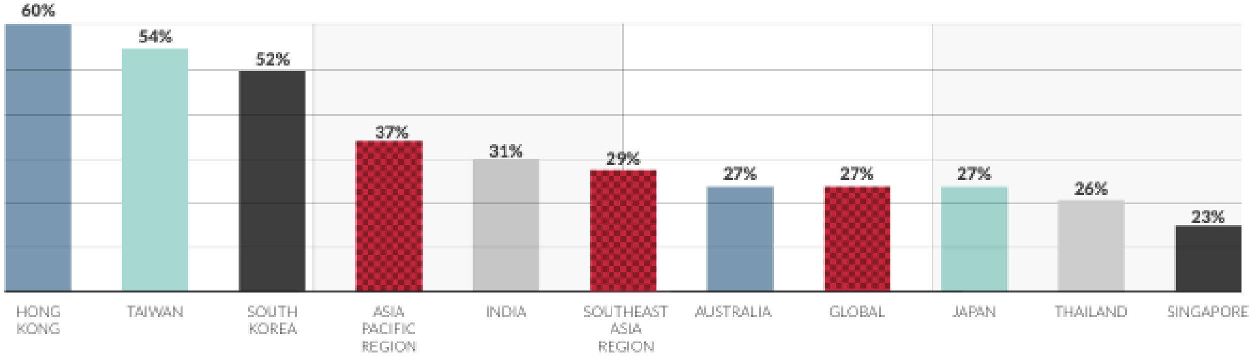
Grady Summers

Senior VP
FireEye / Mandiant
@GradyS

Agenda

- An overview of the threat landscape in Asia
- APT30
- New threat actor activity in Asia
- What should you do?

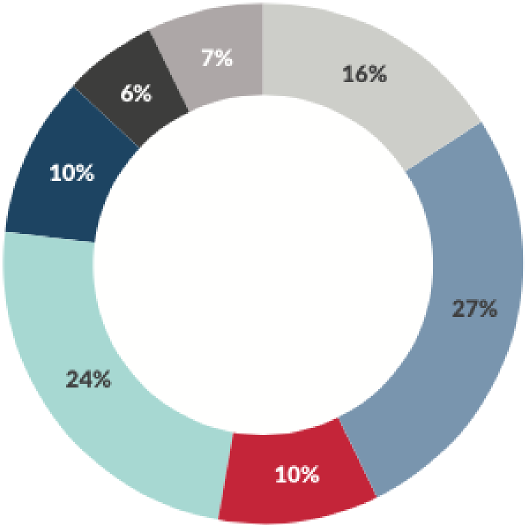
Frequency of Targeted Attacks



Percent of customers detecting targeted attacks, July-December 2014

Industries Targeted

APT AND TARGETED MALWARE DETECTIONS BY INDUSTRY IN SOUTHEAST ASIA



Government	27%	🟦
Telecom	24%	🟩
Financial services	16%	⬜
High-tech	10%	🟥
Transportation	10%	🟦
Energy/utilities	7%	⬜
Education	6%	⬛

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

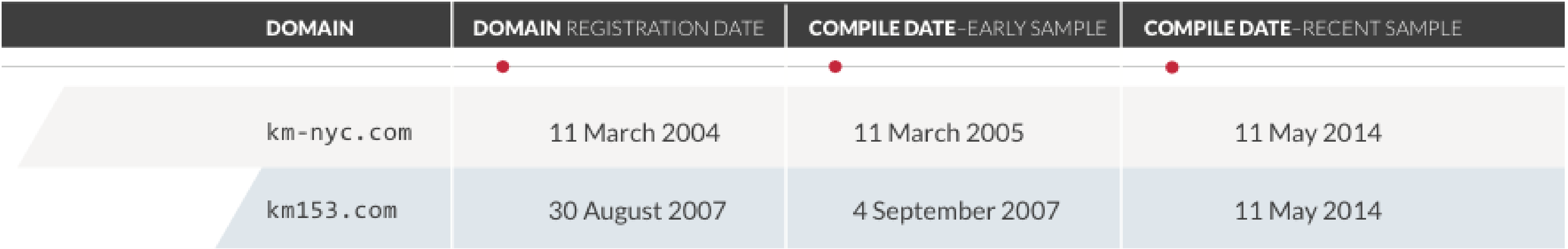
#RSAC

APT30

APT30

- Active for over 10 years
- Highly coordinated and organized
- Majority of victims in Southeast Asia
- Ten industry verticals targeted, including Government, Defense, Financial Services, and Media

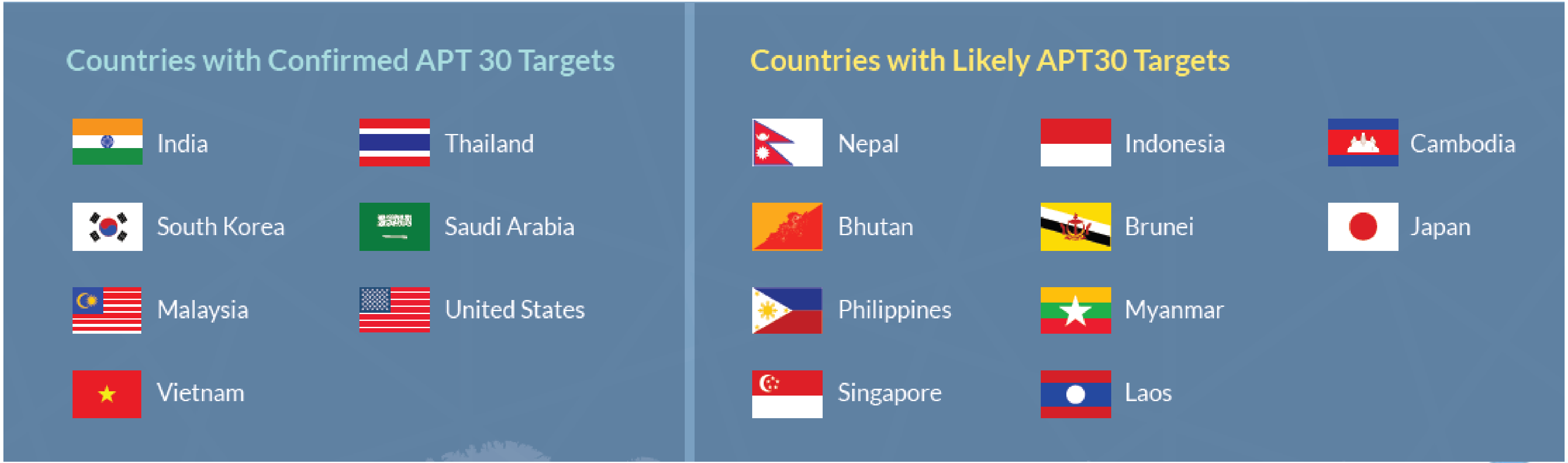
APT30



DOMAIN	DOMAIN REGISTRATION DATE	COMPILE DATE-EARLY SAMPLE	COMPILE DATE-RECENT SAMPLE
km-nyc.com	11 March 2004	11 March 2005	11 May 2014
km153.com	30 August 2007	4 September 2007	11 May 2014

APT30 Targets

- 96% of victim organizations identified by FireEye located in SE Asia



Countries with Confirmed APT 30 Targets

- India
- South Korea
- Malaysia
- Vietnam
- Thailand
- Saudi Arabia
- United States

Countries with Likely APT30 Targets

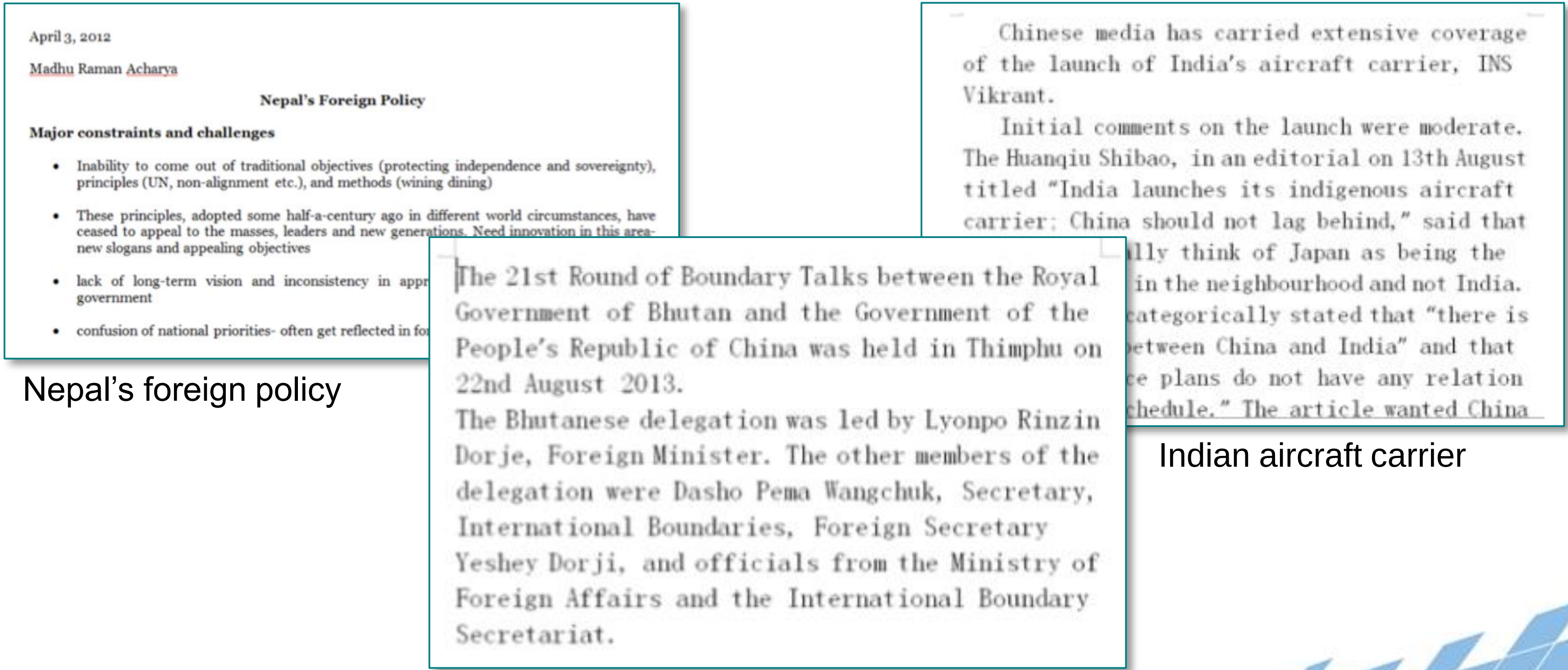
- Nepal
- Bhutan
- Philippines
- Singapore
- Indonesia
- Brunei
- Myanmar
- Laos
- Cambodia
- Japan

APT30 Targeting ASEAN members

Malware samples using aseanm.com domain

Event	Date
899f512f0451a0ba4398b41ed1ae5a6d compiled	5 May 2011 6:35
e6035ec09025c1e349a7a0b3f41e90b1 compiled	5 May 2011 6:35
18th ASEAN Summit, Jakarta, Indonesia	7–8 May 2011
36a6a33cb4a13739c789778d9dd137ac compiled	9 May 2011 3:34
Seventh ASEAN Plus Three Labour Ministers Meeting (7th ALMM+3), Phnom Penh, Cambodia	11 May 2012
572c9cd4388699347c0b2edb7c6f5e25 compiled	11 May 2012 0:06
f3c29a67a7b47e644e9d1a2a0516974e compiled	11 May 2012 0:06
Senior Officials from ASEAN and China meet on implementation of the Declaration on the Conduct of Parties on the East Sea (DOC)	24–25 June 2012
afe8447990ecb9e1cd4086955b7db104 compiled	26 June 2012 1:43
b5546842e08950bc17a438d785b5a019 compiled	26 June 2012 1:43
ASEAN-India Commemorative Summit, New Delhi, India	12–20 December 2012
310a4a62ba3765cbf8e8bbb9f324c503 compiled	20 December 2012 3:53

APT30 – Phishing topics



April 3, 2012

Madhu Raman Acharya

Nepal's Foreign Policy

Major constraints and challenges

- Inability to come out of traditional objectives (protecting independence and sovereignty), principles (UN, non-alignment etc.), and methods (wining dining)
- These principles, adopted some half-a-century ago in different world circumstances, have ceased to appeal to the masses, leaders and new generations. Need innovation in this area- new slogans and appealing objectives
- lack of long-term vision and inconsistency in appr government
- confusion of national priorities- often get reflected in fo

Nepal's foreign policy

Chinese media has carried extensive coverage of the launch of India's aircraft carrier, INS Vikrant.

Initial comments on the launch were moderate. The Huanqiu Shibao, in an editorial on 13th August titled "India launches its indigenous aircraft carrier: China should not lag behind," said that

lly think of Japan as being the in the neighbourhood and not India. ategorically stated that "there is etween China and India" and that e plans do not have any relation hedule." The article wanted China

Indian aircraft carrier

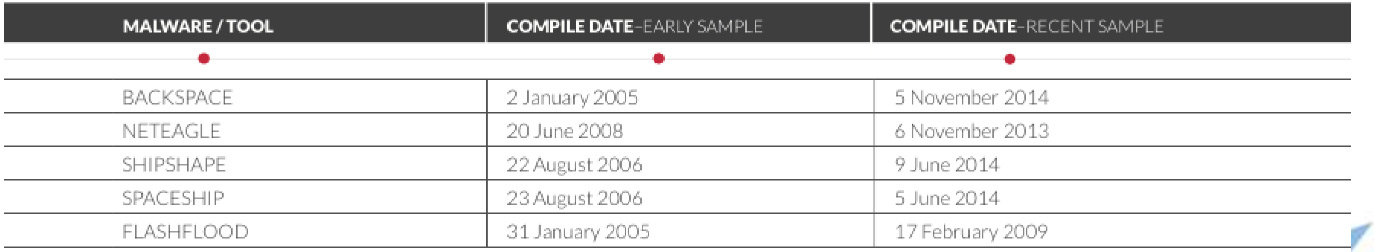
The 21st Round of Boundary Talks between the Royal Government of Bhutan and the Government of the People's Republic of China was held in Thimphu on 22nd August 2013.

The Bhutanese delegation was led by Lyonpo Rinzin Dorje, Foreign Minister. The other members of the delegation were Dasho Pema Wangchuk, Secretary, International Boundaries, Foreign Secretary Yeshey Dorji, and officials from the Ministry of Foreign Affairs and the International Boundary Secretariat.

Bhutan's foreign policy

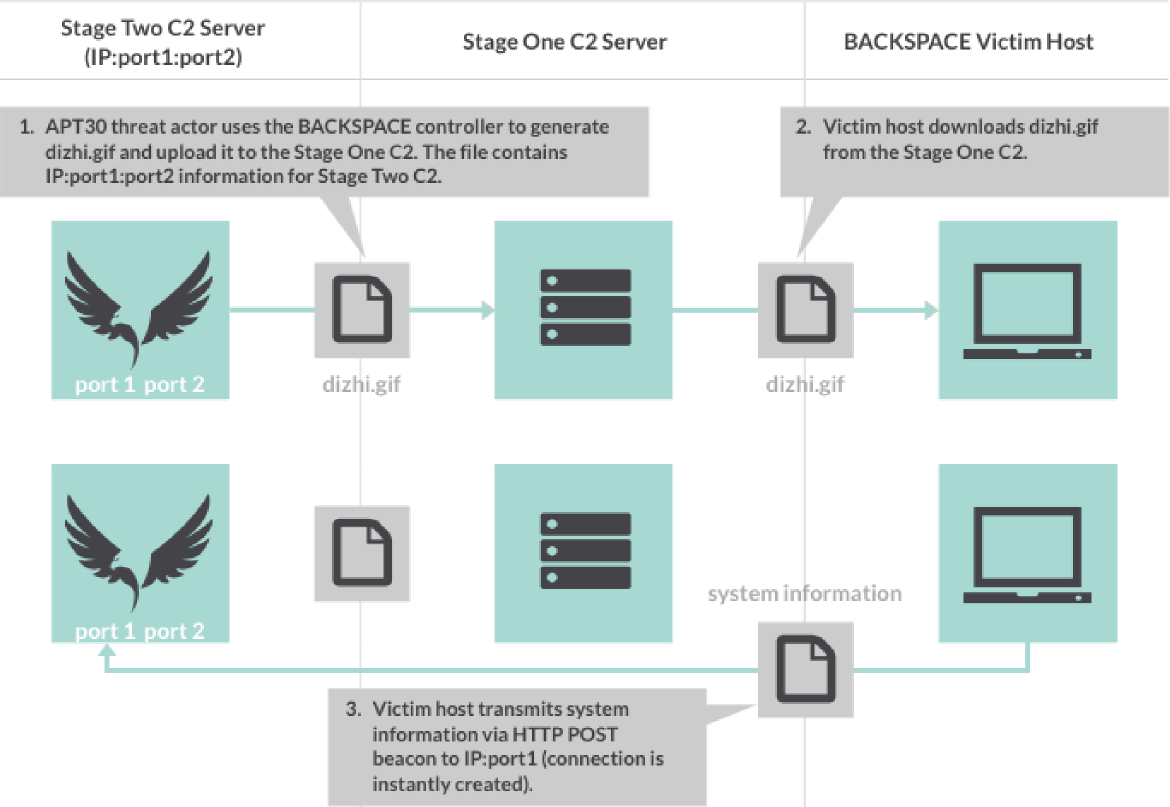
APT30 Tools

- Tool set has remained very consistent over time, with constant improvements
  - Backdoors BACKSPACE and NETEAGLE
    - Earliest variants of BACKSPACE were compiled in 2005
    - Earliest variants of NETEAGLE were compiled in 2008
  - SHIPSHAPE, SPACESHIP, and FLASHFLOOD, designed to infect air-gapped networks via infected removable drives



MALWARE / TOOL	COMPILE DATE-EARLY SAMPLE	COMPILE DATE-RECENT SAMPLE
BACKSPACE	2 January 2005	5 November 2014
NETEAGLE	20 June 2008	6 November 2013
SHIPSHAPE	22 August 2006	9 June 2014
SPACESHIP	23 August 2006	5 June 2014
FLASHFLOOD	31 January 2005	17 February 2009

APT30 Command and Control



Stage Two C2 Server (IP:port1:port2)

Stage One C2 Server

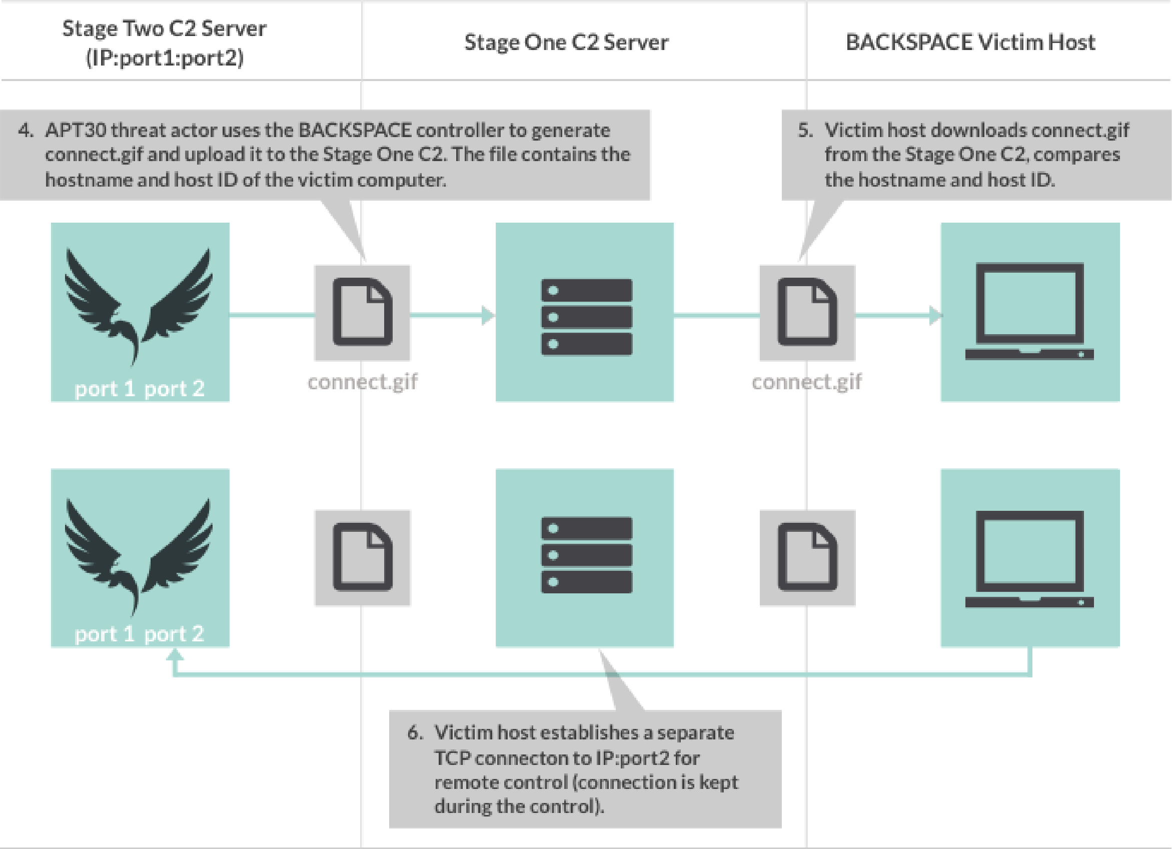
BACKSPACE Victim Host

1. APT30 threat actor uses the BACKSPACE controller to generate dizhi.gif and upload it to the Stage One C2. The file contains IP:port1:port2 information for Stage Two C2.

2. Victim host downloads dizhi.gif from the Stage One C2.

3. Victim host transmits system information via HTTP POST beacon to IP:port1 (connection is instantly created).

APT30 Command and Control



Stage Two C2 Server (IP:port1:port2)

Stage One C2 Server

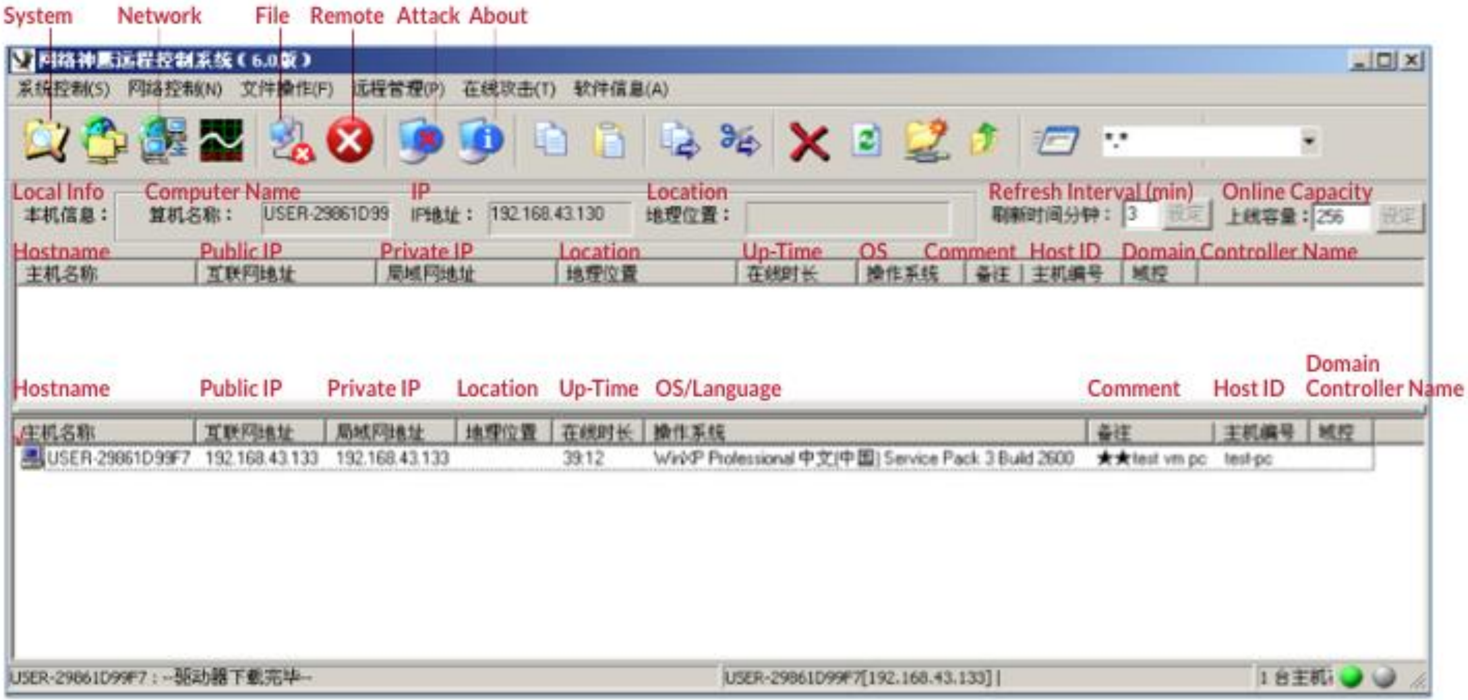
BACKSPACE Victim Host

4. APT30 threat actor uses the BACKSPACE controller to generate connect.gif and upload it to the Stage One C2. The file contains the hostname and host ID of the victim computer.

5. Victim host downloads connect.gif from the Stage One C2, compares the hostname and host ID.

6. Victim host establishes a separate TCP connecton to IP:port2 for remote control (connection is kept during the control).

APT30 – Backspace controller



网络神鹰远程控制系统（6.0版）

系统控制(S) 网络控制(N) 文件操作(F) 远程管理(P) 在线攻击(T) 软件信息(A)

Local Info 本机信息：

Computer Name 算机名称：USER-29861D99

IP IP地址：192.168.43.130

Location 地理位置：

Refresh Interval (min) 刷新时间分钟：3 设定

Online Capacity 上线容量：256 设定

Hostname 主机名称	Public IP 互联网地址	Private IP 局域网地址	Location 地理位置	Up-Time 在线时长	OS 操作系统	Comment 备注	Host ID 主机编号	Domain Controller Name 域控

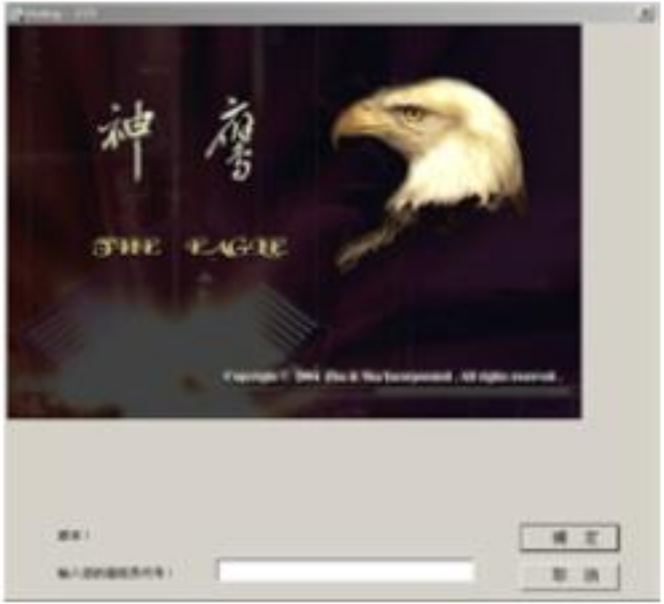
Hostname 主机名称	Public IP 互联网地址	Private IP 局域网地址	Location 地理位置	Up-Time 在线时长	OS/Language 操作系统	Comment 备注	Host ID 主机编号	Domain Controller Name 域控
USER-29861D99F7	192.168.43.133	192.168.43.133		39:12	WinXP Professional 中文(中国) Service Pack 3 Build 2600	★★test vm pc	test-pc	

USER-29861D99F7：--驱动器下载完毕--

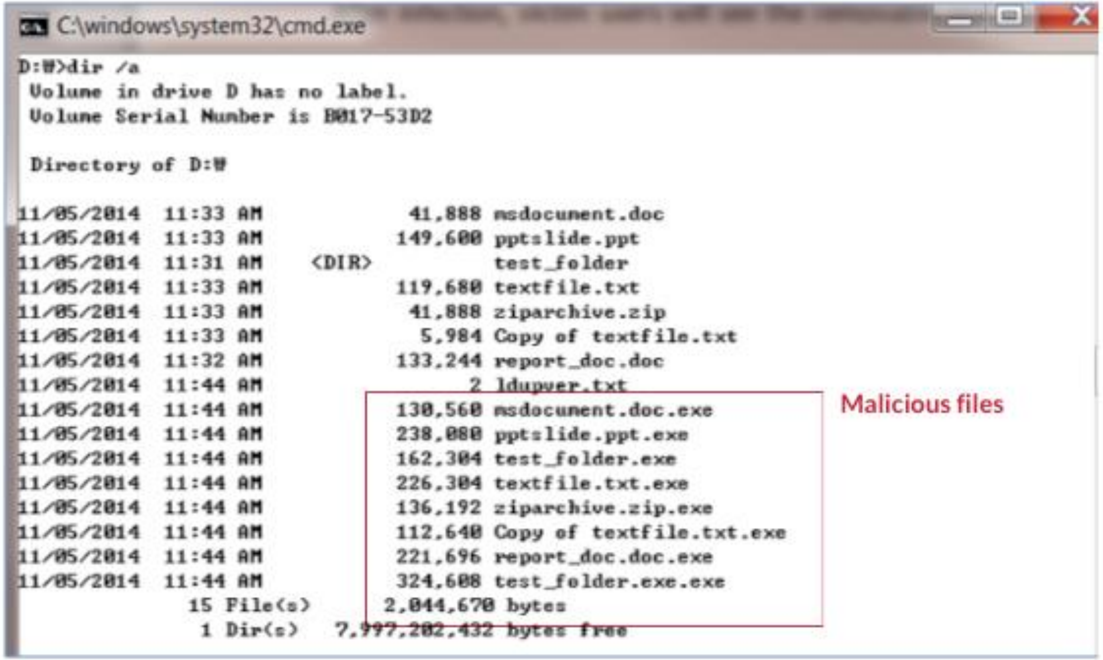
USER-29861D99F7[192.168.43.133] |

1 台主机

APT30 – Backspace controller



APT30 – Penetrating air-gapped networks

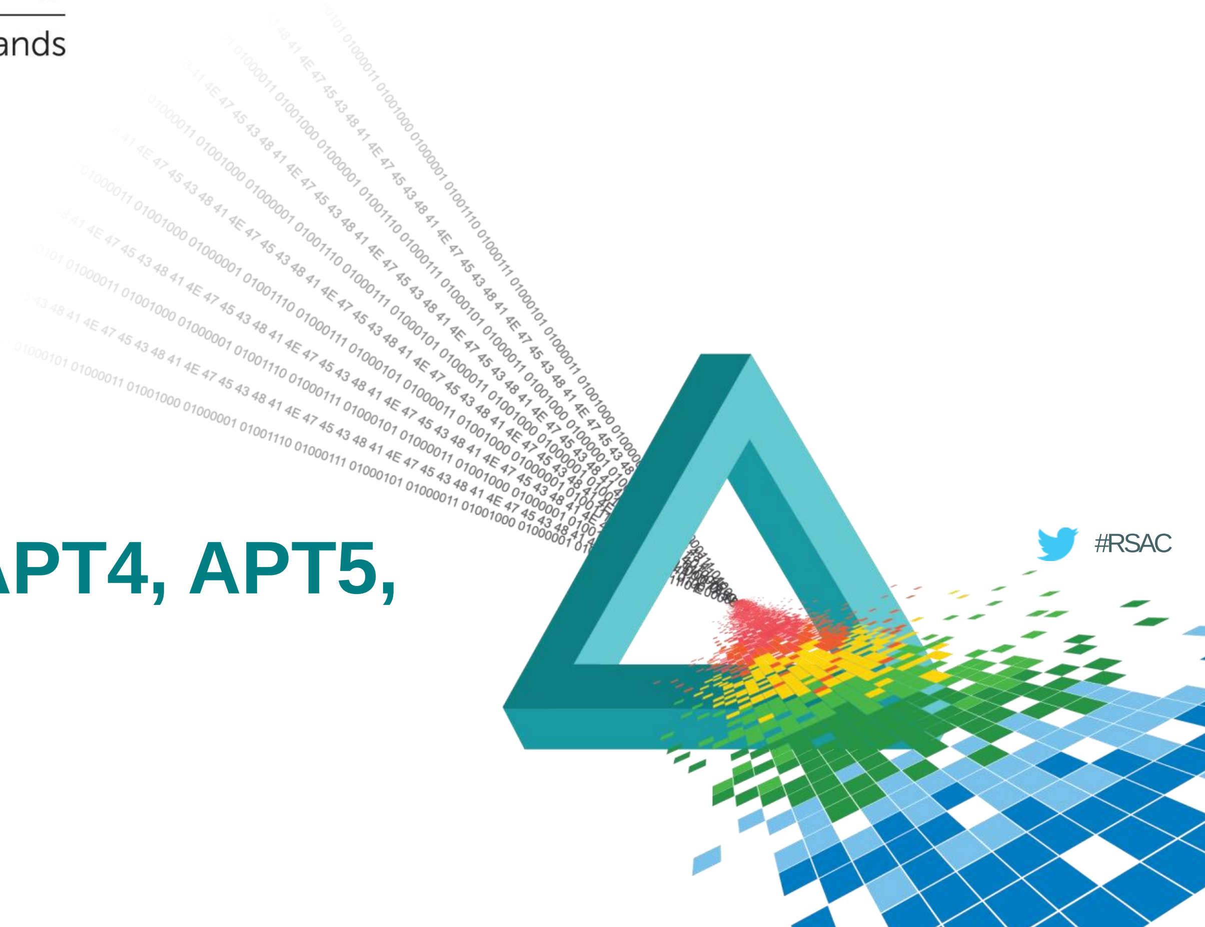


```
D:₩>dir /a
 Volume in drive D has no label.
 Volume Serial Number is B017-53D2

 Directory of D:₩

11/05/2014  11:33 AM            41,888 msdocument.doc
11/05/2014  11:33 AM           149,600 pptslide.ppt
11/05/2014  11:31 AM    <DIR>          test_folder
11/05/2014  11:33 AM           119,680 textfile.txt
11/05/2014  11:33 AM            41,888 ziparchive.zip
11/05/2014  11:33 AM             5,984 Copy of textfile.txt
11/05/2014  11:32 AM           133,244 report_doc.doc
11/05/2014  11:44 AM                 2 ldupver.txt
11/05/2014  11:44 AM           130,560 msdocument.doc.exe
11/05/2014  11:44 AM           238,080 pptslide.ppt.exe
11/05/2014  11:44 AM           162,304 test_folder.exe
11/05/2014  11:44 AM           226,304 textfile.txt.exe
11/05/2014  11:44 AM           136,192 ziparchive.zip.exe
11/05/2014  11:44 AM           112,640 Copy of textfile.txt.exe
11/05/2014  11:44 AM           221,696 report_doc.doc.exe
11/05/2014  11:44 AM           324,608 test_folder.exe.exe
              15 File(s)      2,044,670 bytes
               1 Dir(s)   7,997,202,432 bytes free
```

Malicious files

APT30 Conclusions

- APT30 is a well-organized group with a long-term mission that represents a regional threat.
- Targeted activity and state-sponsored data theft is not simply a US problem.
- The following key points suggest likely sponsorship of APT30 by the Chinese government:
  - Geopolitical issues reflected in APT30s targeting (intended victims, decoy content)
  - Chinese language indicators in their malware
  - Level of organization, implied extent of operations, and long-term activity.



#RSAC

Recent Activity: APT4, APT5, APT10, APT17

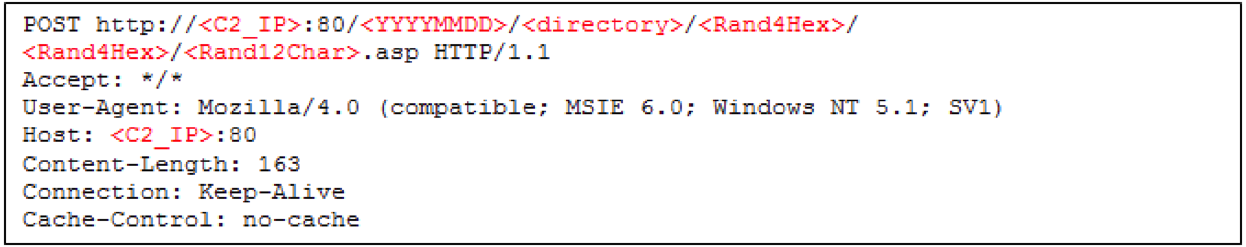
APT4 at Asian Airline Company

- Airline discovered breach in Q2 2015
- Actor is suspected to be APT4
  - Well-written and researched spearphishes with industry themes
  - CCHIP and Sykipot backdoors
  - Heavy use of SSL for C2, usually with the same certificate and a .asp destination
  - Heavy use of compromised PKI credentials

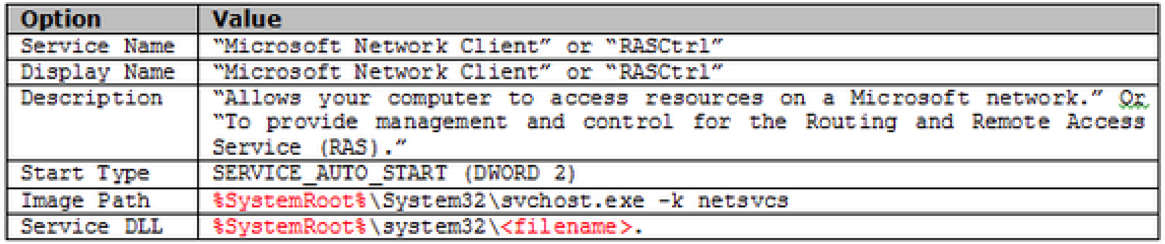
APT10

- Activity in last several months, compromising an east Asian manufacturer and two Japanese public policy organizations
- Have used video game themed phishing emails, which install an actual (trojanized) video game; primarily Angry Birds and Block
  - Other phishing emails are poorly worded and minimally researched
- Uses KABOB backdoor to maintain persistence
- Other APT10 malware is commonly self-signed and suffers from high detection rates by commercial AV

KABOB



```
POST http://<C2_IP>:80/<YYYYMMDD>/<directory>/<Rand4Hex>/
<Rand4Hex>/<Rand12Char>.asp HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: <C2_IP>:80
Content-Length: 163
Connection: Keep-Alive
Cache-Control: no-cache
```



Option	Value
Service Name	“Microsoft Network Client” or “RASCtrl”
Display Name	“Microsoft Network Client” or “RASCtrl”
Description	“Allows your computer to access resources on a Microsoft network.” Or “To provide management and control for the Routing and Remote Access Service (RAS).”
Start Type	SERVICE_AUTO_START (DWORD 2)
Image Path	%SystemRoot%\System32\svchost.exe -k netsvcs
Service DLL	%SystemRoot%\system32\<filename>.

Case Study: APT5 at Defense Contractor

- April 2015 attack against south Asian defense contractor
- APT5 is highly capable, and has been focusing on “SIGINT” technologies by targeting telecommunications, information technology, and defense
- Initially gathered reconnaissance information from compromised hosts
- Stole e-mails, procurement bids and proposals, documents on UAVs, and proprietary product specifications
- Group uses BIRDWORLD and ENCORE backdoors

APT17

- Targeted Japanese software company in March 2015
- Stole code signing certificate for popular Japanese software product
- Compromised company's web server and posted signed malware for customers to download
- APT17 configured BLACKCOFFEE malware to use Microsoft Technet for C2 communications
- BLACKCOFFEE supports ~15 commands, including creating a reverse shell, uploading and downloading files, and enumerating files and processes.

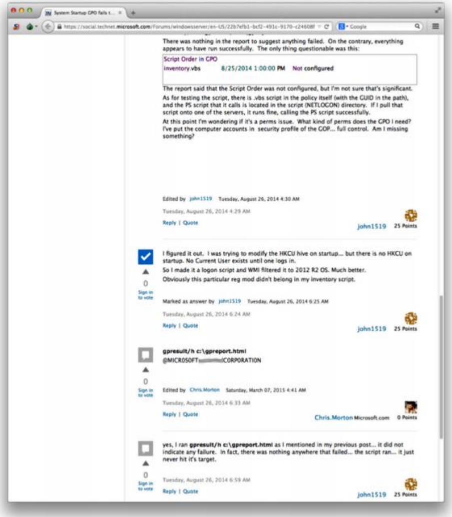
BLACKCOFFEE use by APT17

APT17's Malicious Use of Technet

APT17 encodes an IP address on a newly created TechNet profile or encodes the IP address on a forum thread using one of their profiles

Microsoft TechNet

A TechNet forum thread modified by BLACKCOFFEE:



System Startup GPO fails t...

https://social.technet.microsoft.com/Forums/windowsserver/en-US/22b7efb1-bcf2-491c-9170-c24608f

There was nothing in the report to suggest anything failed. On the contrary, everything appears to have run successfully. The only thing questionable was this:

Script Order in GPO		
inventory.vbs	8/25/2014 1:00:00 PM	Not configured

The report said that the Script Order was not configured, but I'm not sure that's significant.

As for testing the script, there is .vbs script in the policy itself (with the GUID in the path), and the PS script that it calls is located in the script (NETLOGON) directory. If I pull that script onto one of the servers, it runs fine, calling the PS script successfully.

At this point I'm wondering if it's a perms issue. What kind of perms does the GPO I need? I've put the computer accounts in security profile of the GOP... full control. Am I missing something?

Edited by john1519 Tuesday, August 26, 2014 4:30 AM

Tuesday, August 26, 2014 4:29 AM

Reply | Quote

john1519 25 Points

☑

I figured it out. I was trying to modify the HKCU hive on startup... but there is no HKCU on startup. No Current User exists until one logs in.

So I made it a logon script and WMI filtered it to 2012 R2 OS. Much better.

Obviously this particular reg mod didn't belong in my inventory script.

0 Sign in to vote

Marked as answer by john1519 Tuesday, August 26, 2014 6:25 AM

Tuesday, August 26, 2014 6:24 AM

Reply | Quote

john1519 25 Points

gpresult/h c:\gpreport.html

@MICROSOFT[redacted]CORPORATION

0 Sign in to vote

Edited by Chris.Morton Saturday, March 07, 2015 4:41 AM

Tuesday, August 26, 2014 6:33 AM

Reply | Quote

Chris.Morton Microsoft.com 0 Points

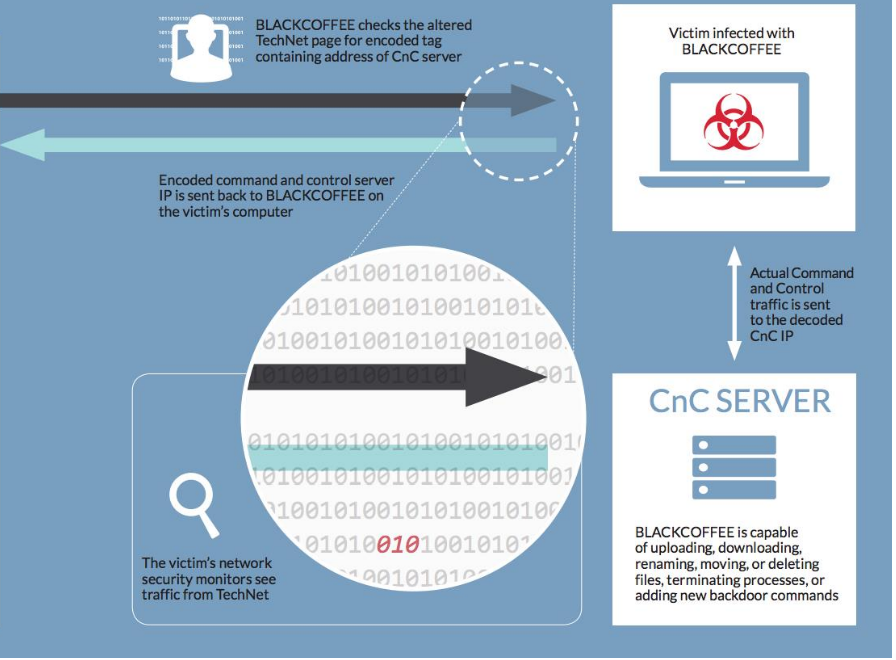
yes, I ran **gpresult/h c:\gpreport.html** as I mentioned in my previous post... it did not indicate any failure. In fact, there was nothing anywhere that failed... the script ran... it just never hit it's target.

0 Sign in to vote

Tuesday, August 26, 2014 6:59 AM

Reply | Quote

john1519 25 Points



BLACKCOFFEE checks the altered TechNet page for encoded tag containing address of CnC server

Victim infected with BLACKCOFFEE

Encoded command and control server IP is sent back to BLACKCOFFEE on the victim's computer

Actual Command and Control traffic is sent to the decoded CnC IP

The victim's network security monitors see traffic from TechNet

CnC SERVER

BLACKCOFFEE is capable of uploading, downloading, renaming, moving, or deleting files, terminating processes, or adding new backdoor commands

APT Interest in India

- In April 2015, FireEye observed a campaign against government and university targets in Pakistan, Nepal, and Bangladesh
- Spear-phishes used MS Word attachment with names like “Pakistan-iran.doc”, which exploit CVE-2012-0158 to deliver a WMI script we call WATERMAIN
- Script has a variable for victim name; we have observed hundreds of string values here
- We suspect Chinese actors were targeting these Indian border countries for information about ongoing and border and diplomatic disputes with India

Common Weaknesses

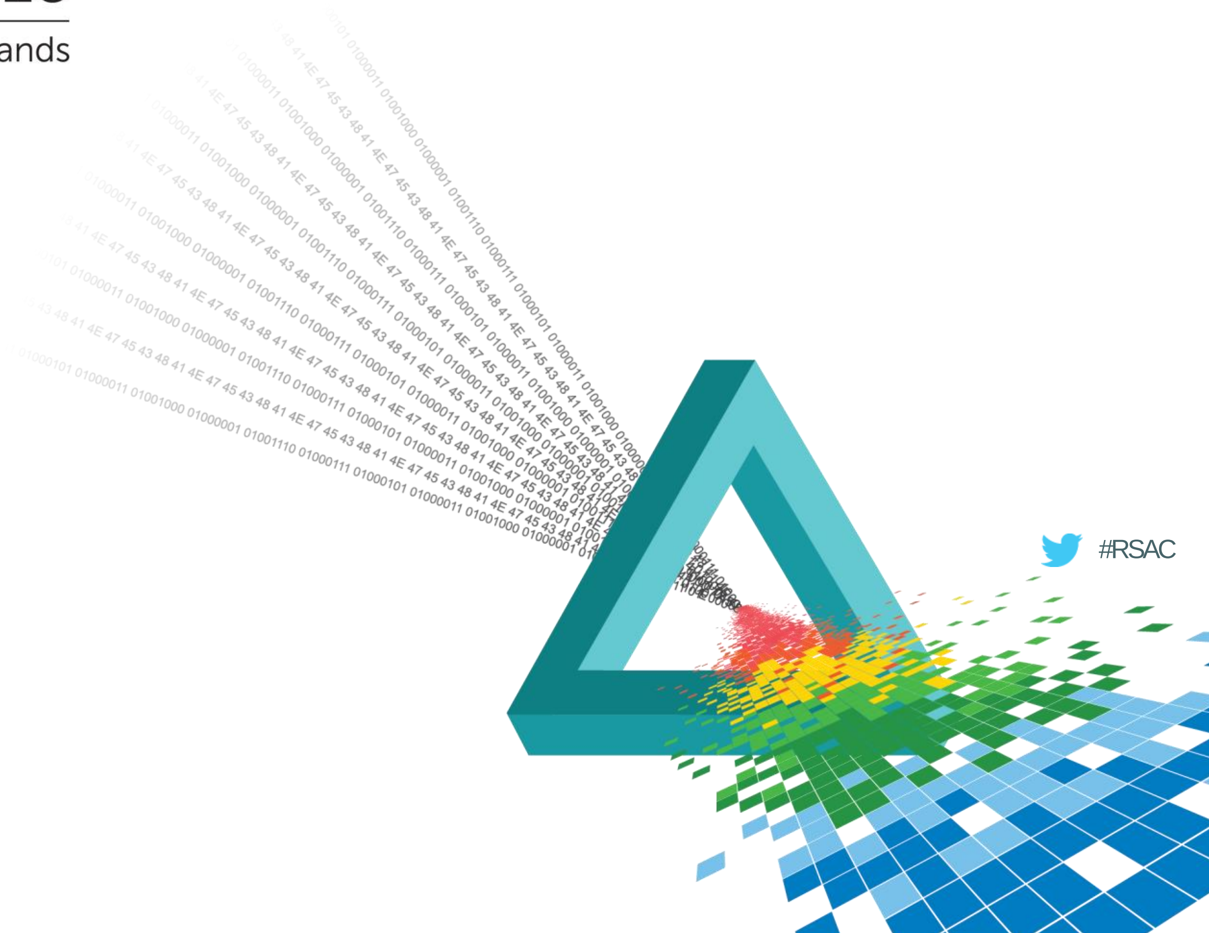
- Lack of instrumentation and collection
  - Attackers always leave footprints, but we’re often not watching
- Lack of network segmentation
- Single-factor authentication for VPN and Outlook Web Access
- Poor credential management
- Inability to detect or prevent spearphishing

Apply What You Have Learned Today

- Next week you should:
  - Use the APT30 indicators to assess your organization
- In the first month following this presentation you should:
  - Establish a repeatable process to apply threat intelligence to your data
  - Evaluate whether you are prepared to detect and respond to a breach like the ones we have discussed
    - Instrumentation and detection, spearphishing detection, communication plan
- Within three months you should:
  - Be planning for the key preventative measures we have discussed: two-factor, credential management, network segmentation

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Questions?