# Leverage OSINT to Trace APT Group

Bowen Pan
360 Enterprise Security Group

# About us.

## 360 Threat Intelligence Center

- A team of 360 Enterprise Security Group
- Focus on threat intelligence and advanced targeted attacks tracing.
- APT threat monitoring and tracing, uncovered several APT Groups.

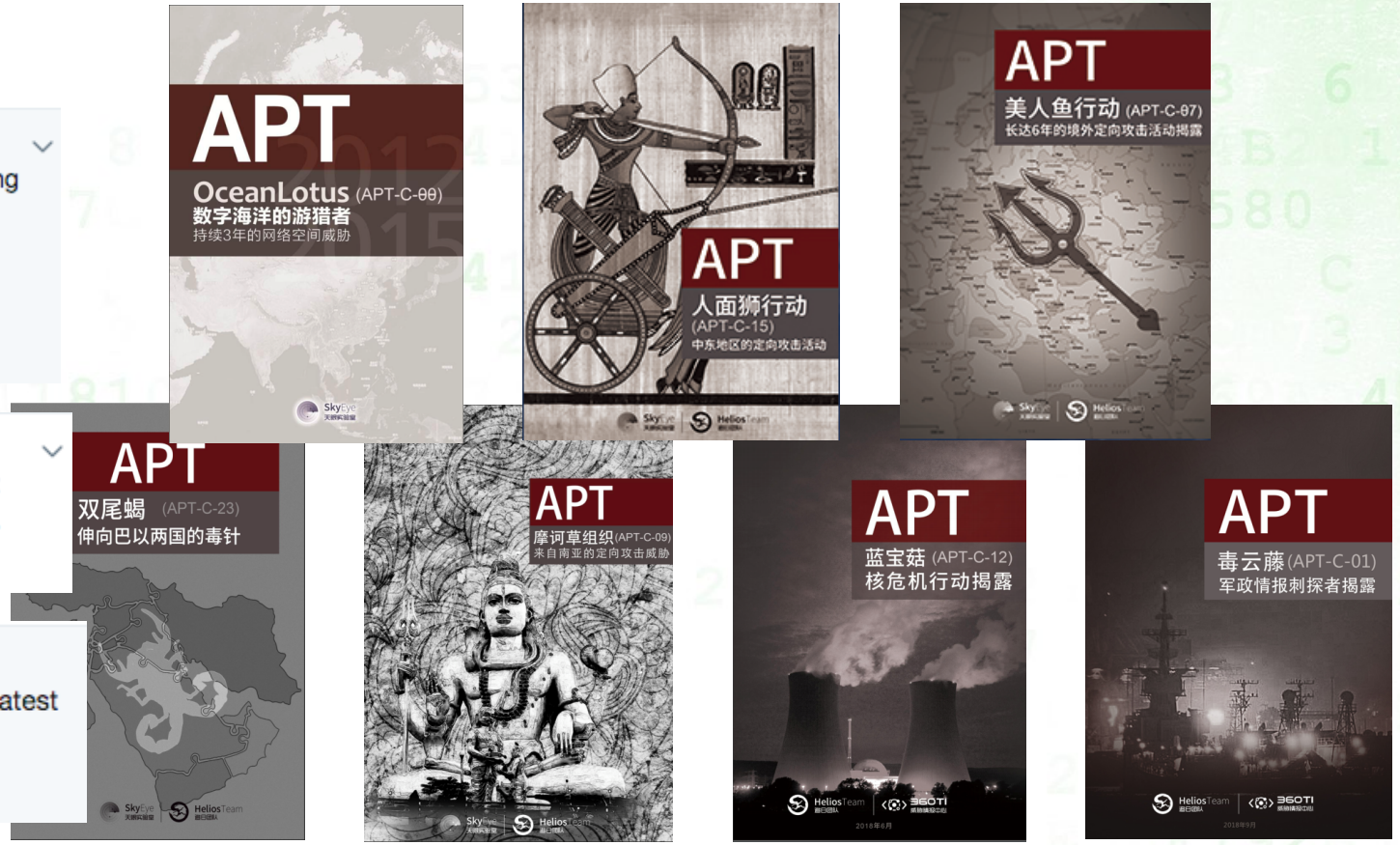
# About us.

**360 Threat Intelligence Center** @360TIC · 9月21日
Full disclosure of #PoisonVine(#APT-C-01) #APT group .
mp.weixin.qq.com/s/-H02Bm08qbOW…

**360 Threat Intelligence Center** @360TIC · 9月12日
Possible #OceanLotus #APT group recent targeted attack cases by exploiting #CVE-2017-11882 and #EternalBlue.
ti.360.net/blog/articles/…
翻译推文
34 45

**360 Threat Intelligence Center** @360TIC · 7月6日
Disclosure of a new #APT group #BlueMushroom (APT-C-12) and its recent campaign Operation NuclearCrisis, report here ti.360.net/uploads/2018/0…
翻译推文

**360 Threat Intelligence Center** @360TIC · 7月26日
Details of APT-C-35 (Donot Team, Arbor's name) #APT group and its latest activities ti.360.net/blog/articles/… .
翻译推文



# Motivation

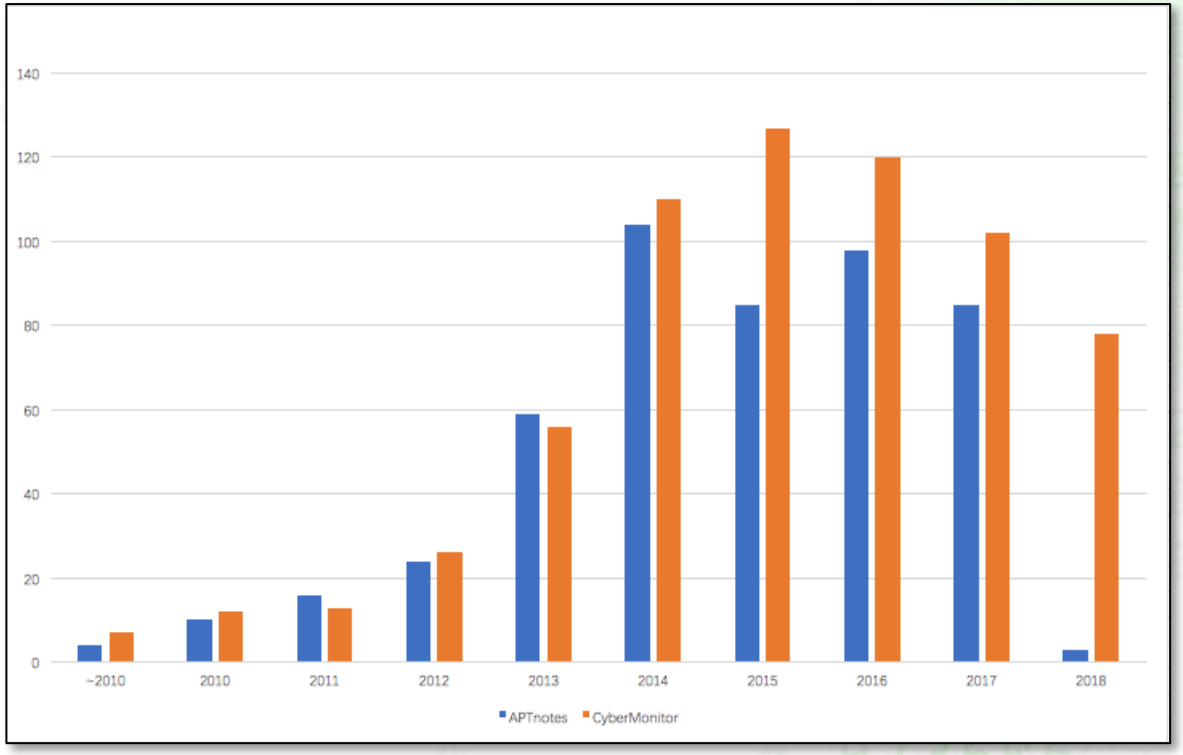
- **Why we need OSINT?**
- Tracing of APT Groups is just like a jigsaw game.
- We need more comprehensive threat intelligence about APT Groups.
- External intelligence will be helpful.

# Motivation

Thanks to the collections of APT reports by researchers.

- https://github.com/aptnotes/data
- https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections

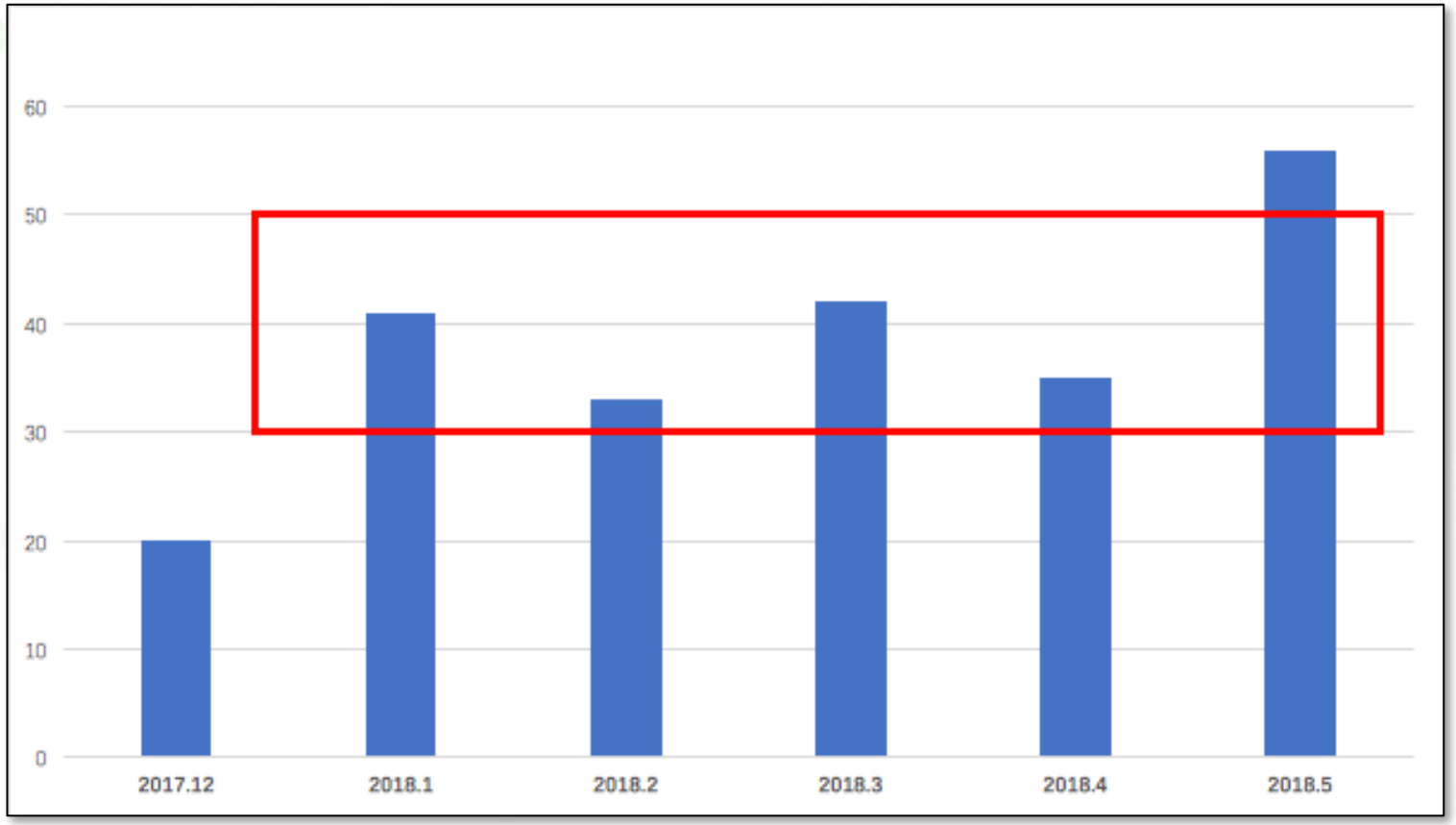
- Update is not timely.
- Report is unstructured, cannot use it directly.
- Report is not INTELLIGENCE.




statistic of between 2010 to 2018.5

# Motivation

Our collections of APT reports from Security Vendors in 2018 1H, average 1-1.6 article per day.



# Motivation

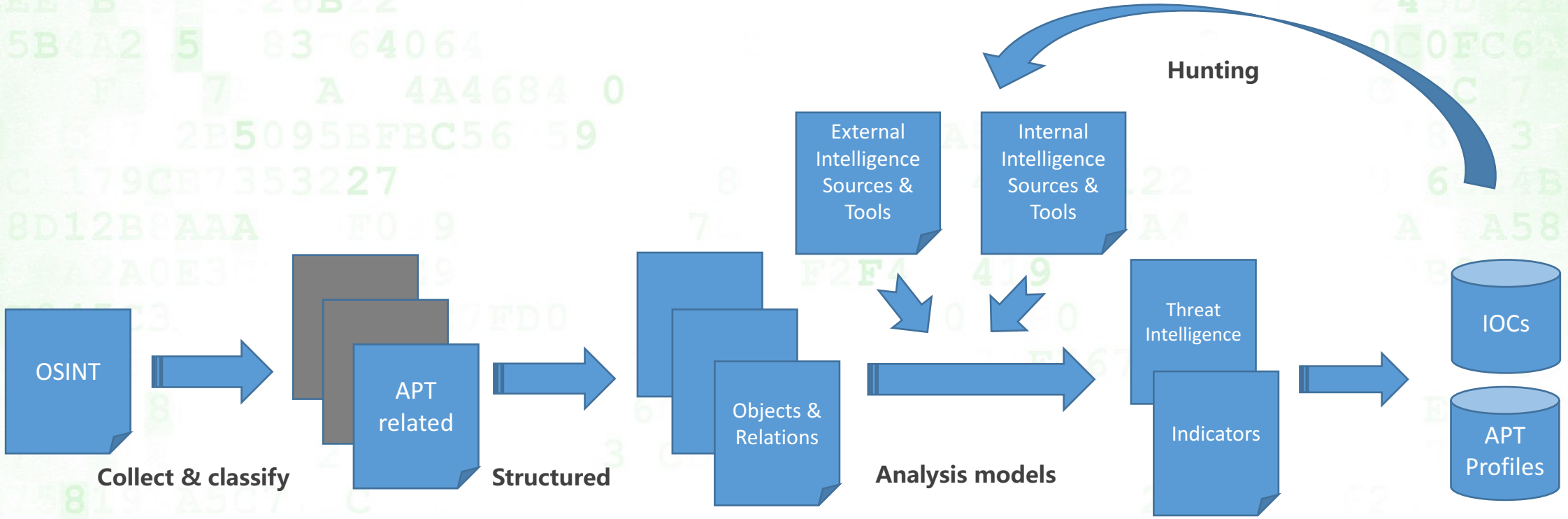
Nearly 100+ APT actors are reported publicly, and dozens of them still conduct threat activities frequently nowadays.

- Construction of APT actors TTP & Profiles.
- Leverage OSINT to trace them.

# Methodology


**Threat Intelligence Lifecycle**

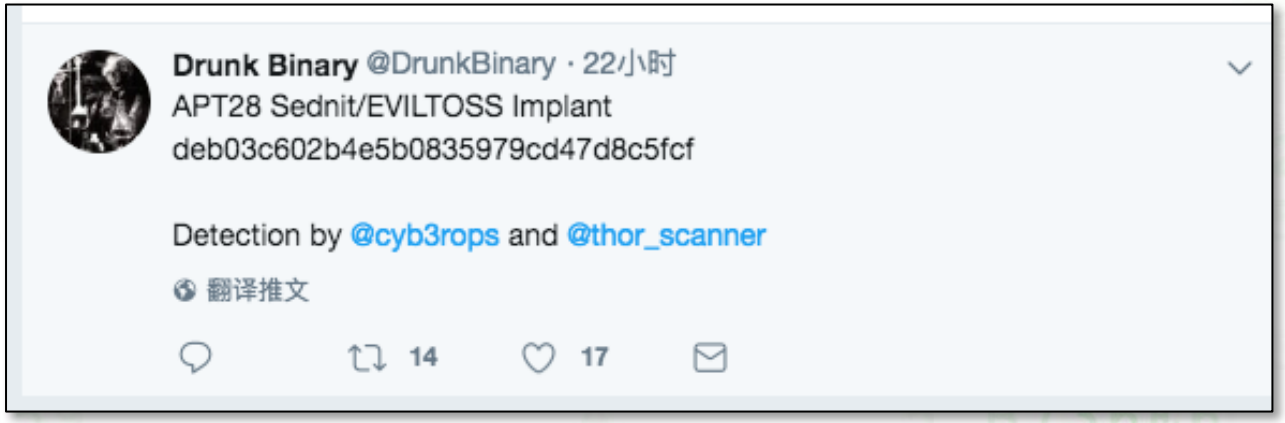
# Methodology



# Methodology - Collect

Sources of OSINT related to APT:

- Security vendors: websites, vendor research blog.
- Security media and news.
- Social media: Twitter, Blogger.
- Public threat feed.

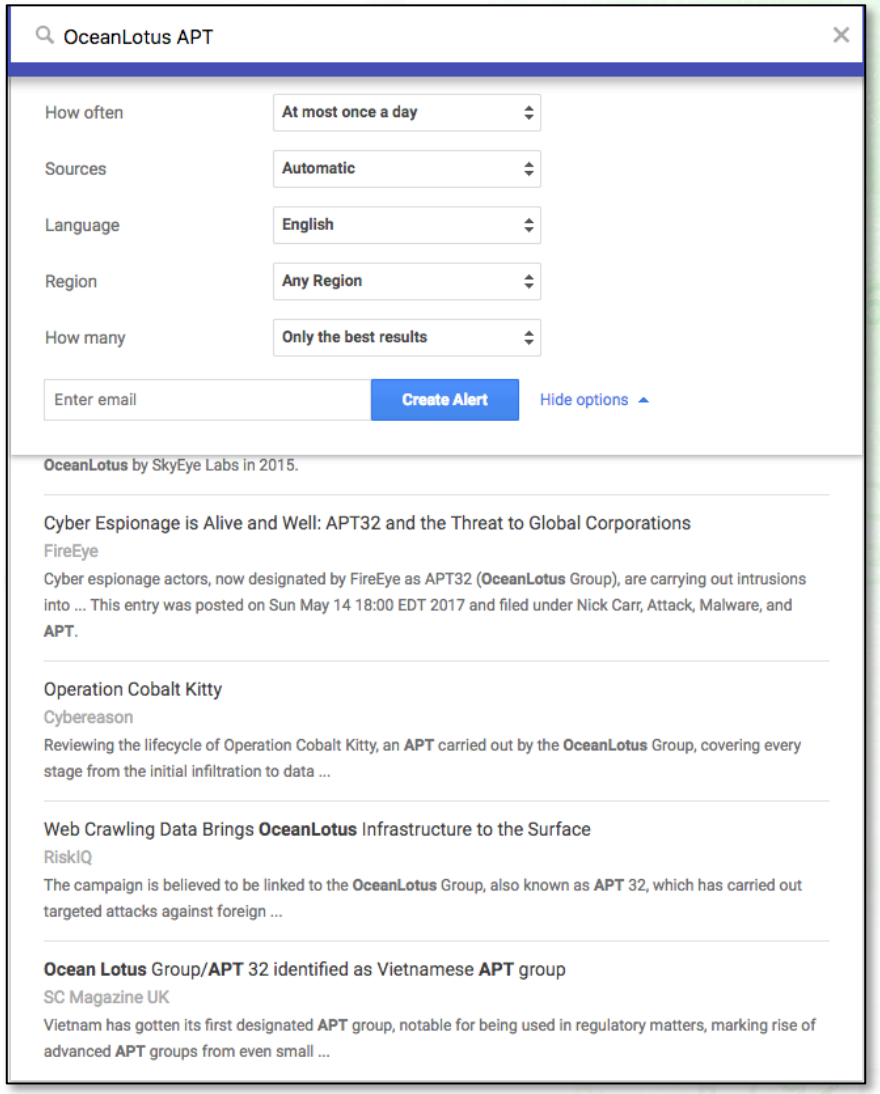


# Methodology - Collect

Besides using spiders, researchers can choose RSS or similar tools.

**RSS Tool**


**Google Alerts**



# Methodology - Classify

Classify filtered OSINT data

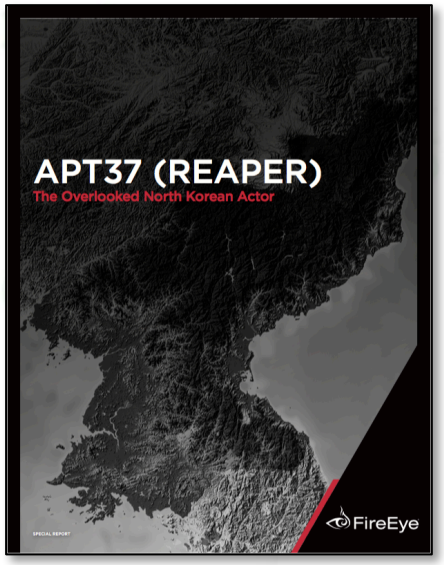
- Threat activities, incidents
  - Malspam, targeted attack, cybercrime, APT
- Threat analysis
  - Ransomware, malicious miner, exploit kit, bankbot, etc.
  - Vulnerability or exploitation.

Reports from security vendors are more valuable, because they include more technical details and even indicators, which benefit further threat hunting.

# Methodology - Structure

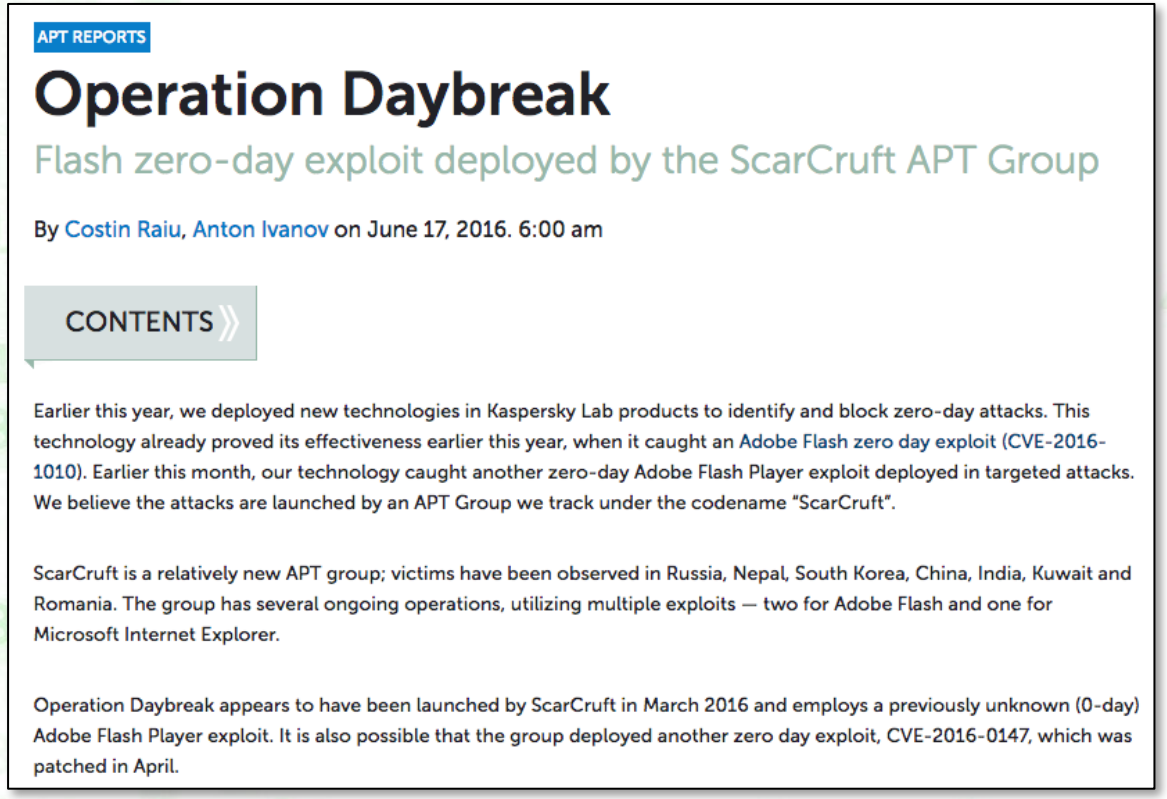
Retrieve information from OSINT data and summarize it.

Based on the STIX, we can easily to describe it and make it simpler.




| Threat Actor |
| --- |
| alias name |
| intent |
| state region |
| language |
| target |
| TTPs |
| ... |

# Methodology - Structure



APT REPORTS

## Operation Daybreak

### Flash zero-day exploit deployed by the ScarCruft APT Group

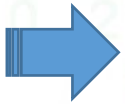
By Costin Raiu, Anton Ivanov on June 17, 2016. 6:00 am

CONTENTS

Earlier this year, we deployed new technologies in Kaspersky Lab products to identify and block zero-day attacks. This technology already proved its effectiveness earlier this year, when it caught an Adobe Flash zero day exploit (CVE-2016-1010). Earlier this month, our technology caught another zero-day Adobe Flash Player exploit deployed in targeted attacks. We believe the attacks are launched by an APT Group we track under the codename "ScarCruft".

ScarCruft is a relatively new APT group; victims have been observed in Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations, utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer.

Operation Daybreak appears to have been launched by ScarCruft in March 2016 and employs a previously unknown (0-day) Adobe Flash Player exploit. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.




| Campaign |
| --- |
| time range |
| target |
| TTP |
| ... |

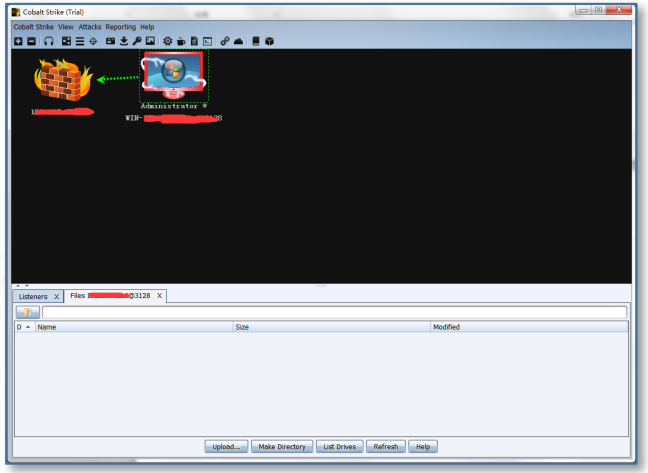
# Methodology - Structure


Blog Home > Unit 42 > Sofacy Uses DealersChoice to Target European Government Agency

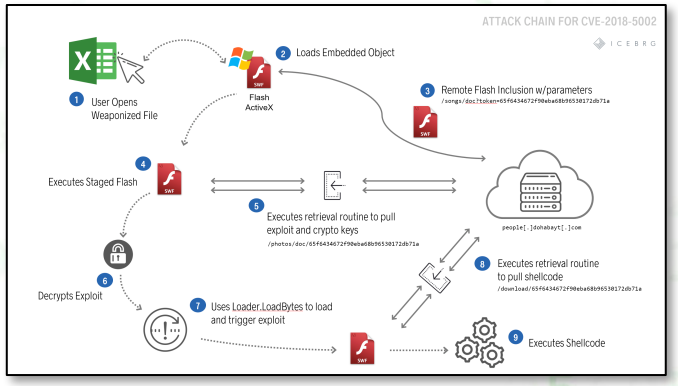
**Sofacy Uses DealersChoice to Target European Government Agency**

By Robert Falcone
March 15, 2018 at 1:00 PM
Category: Unit 42 Tags: DealersChoice, European Government Agency, Sofacy

14,816 5






## Indicators of compromise:

### Malicious IPs and hostnames:

- 212.7.217[.]10
- reg.flnet[.]org
- webconncheck.myfw[.]us

### MD5s:

3e5ac6bbf108feec97e1cc36560ab0b6
a6f14b547d9a7190a1f9f1c06f906063
e51ce28c2e2d226365bc5315d3e5f83e
067681b79756156ba26c12bc36bf835c
f8a2d4ddf9dc2de750c8b4b7ee45ba3f
8844a537e7f533192ca8e81886e70fbc

# Methodology - Structure

**objects & relations**


**alias name**

| | | | | | |
|---|---|---|---|---|---|
| 海莲花 | OceanLotus<br>APT32<br>Cobalt Kitty<br>APT-C-00<br>SeaLotus | 海莲花组织是由360最早披露的一个APT组织，其自2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。<br>2014 年 2 月以后，OceanLotus 进入攻击活跃期，并于 2014 年 5 月发动了最大规模的一轮鱼叉攻击，大量受害者因打开带毒的邮件附件而感染特种木马。<br>至17年该组织的攻击依然存在。<br>FireEye后续也称其为APT32，其针对多个行业的私营企业，外国政府、持不同政见者和记者实施攻击，其还广泛使用失陷的网站来攻击受害者。其拥有一套功能完备的恶意代码，并结合商业工具实施攻击。<br>参考：<br>https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html<br>https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/ | 中 | 2012 | 2018 | 该组织拥有非常高的社会工程学技巧，并且常用鱼叉攻击和水坑攻击，并且会利用和修改公开的攻击工具和开源项目。常用PowerShell脚本、COM scriptlets，恶意代码使用C++编写，也有C#编写的恶意代码。<br>战术：<br>1. 邮件鱼叉攻击，附带包括伪装成文档的PE文件、HTA文件、 |

**state region, languages, TTPs**

# Methodology - Analysis

We need to do further analysis:

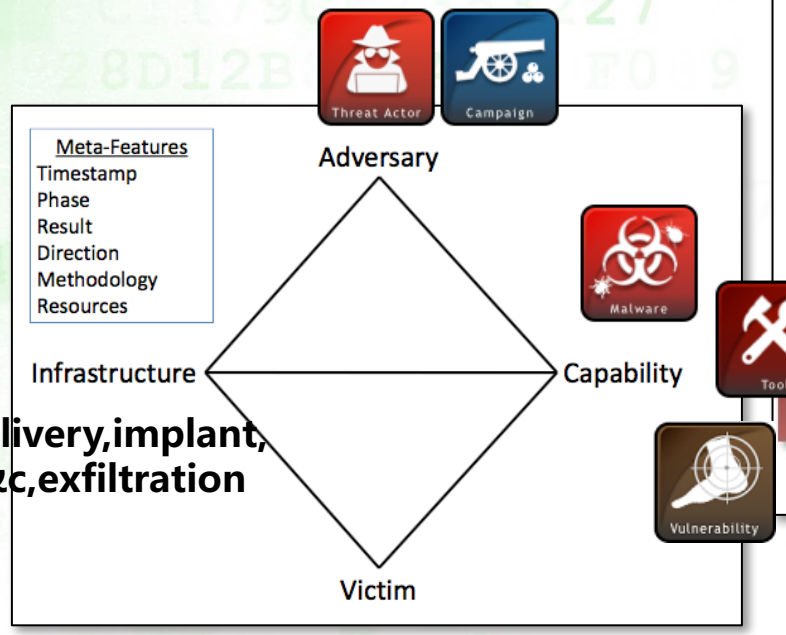
- Check the OSINT is accurate or not.
  - Reported threat actor is really THE ACTOR?
  - Uncovered a new actor or overlapped with the old ones?

- Check the IOCs, sometimes we found these happens in the report:
  - Hash string lost 1 byte
  - subdomain of legal website mixed in the C&C domain list, may cause false positive

- Update the actor's TTP & profile.
- Found the relations & overlapping based on the OSINT and internal threat data

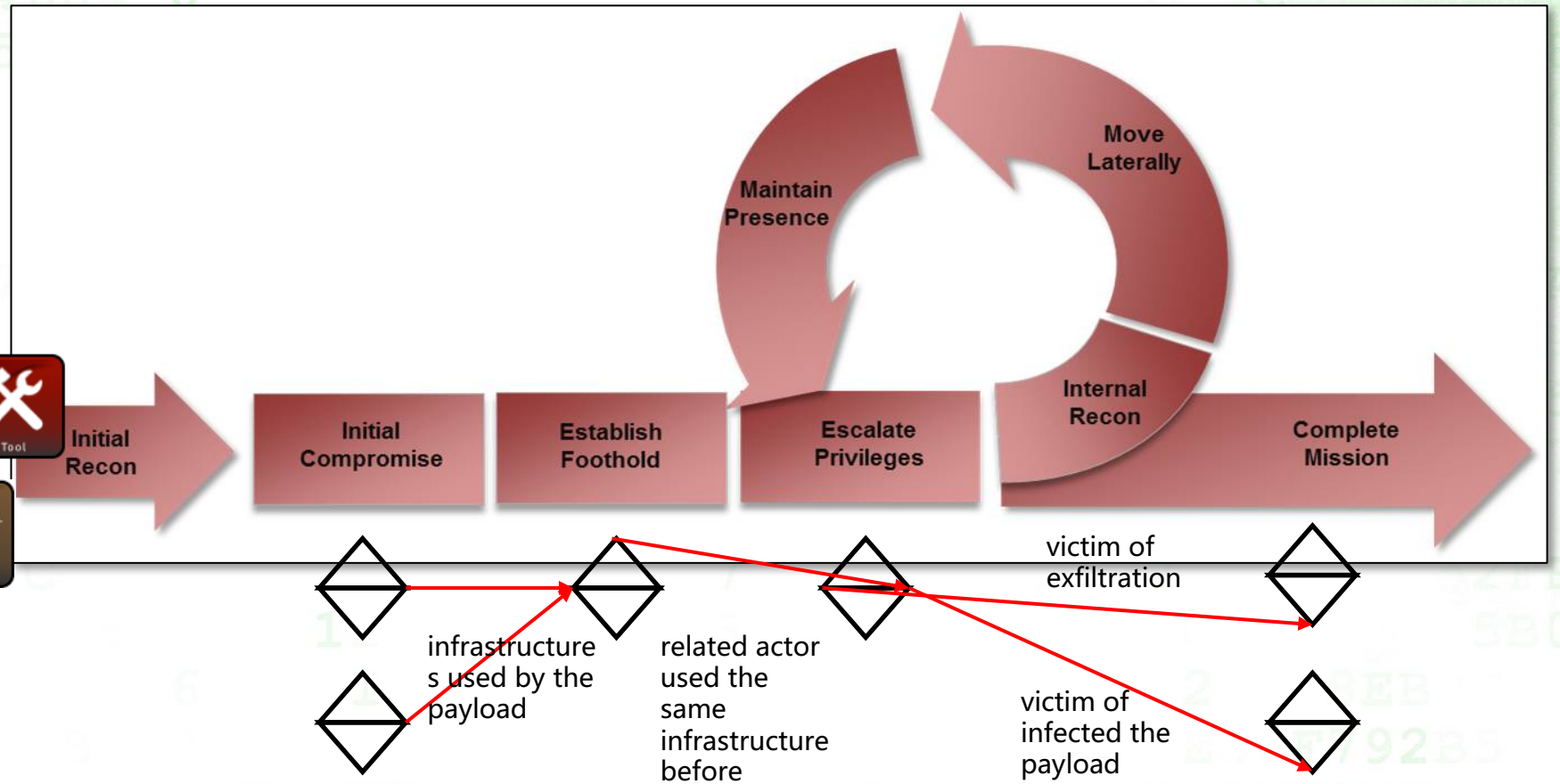
# Methodology - Analysis

Diamond Model in the attack lifecycle.




**delivery,implant, c&c,exfiltration**

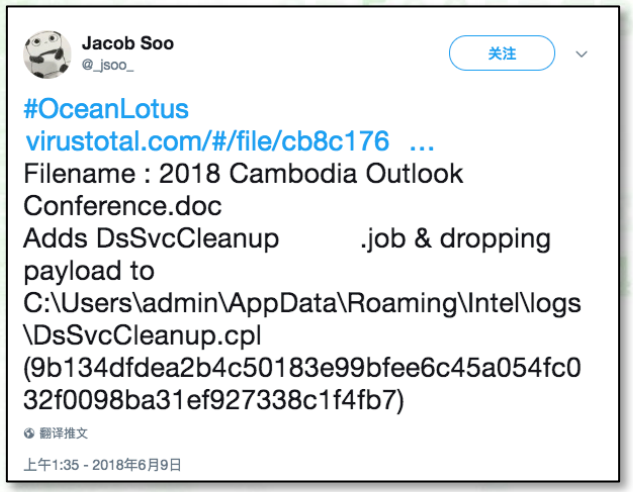
**region,industry,role**



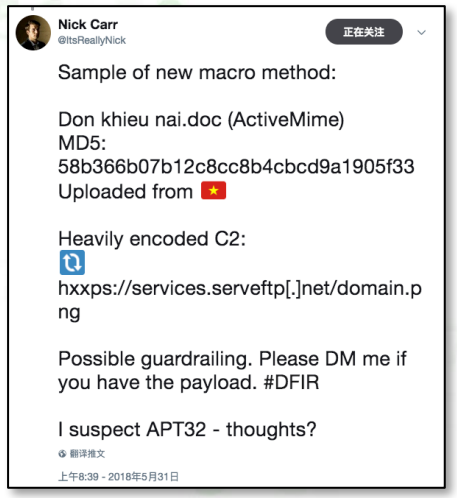

source：http://www.iacpcybercenter.org/wp-content/uploads/2015/10/cyber_attack_lifecycle.jpg

# Example - OceanLotus

Decoy document tagged OceanLotus(aka APT32) from Twitter



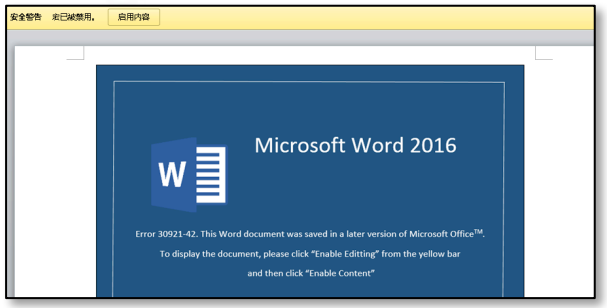

exploit document




malicious macro

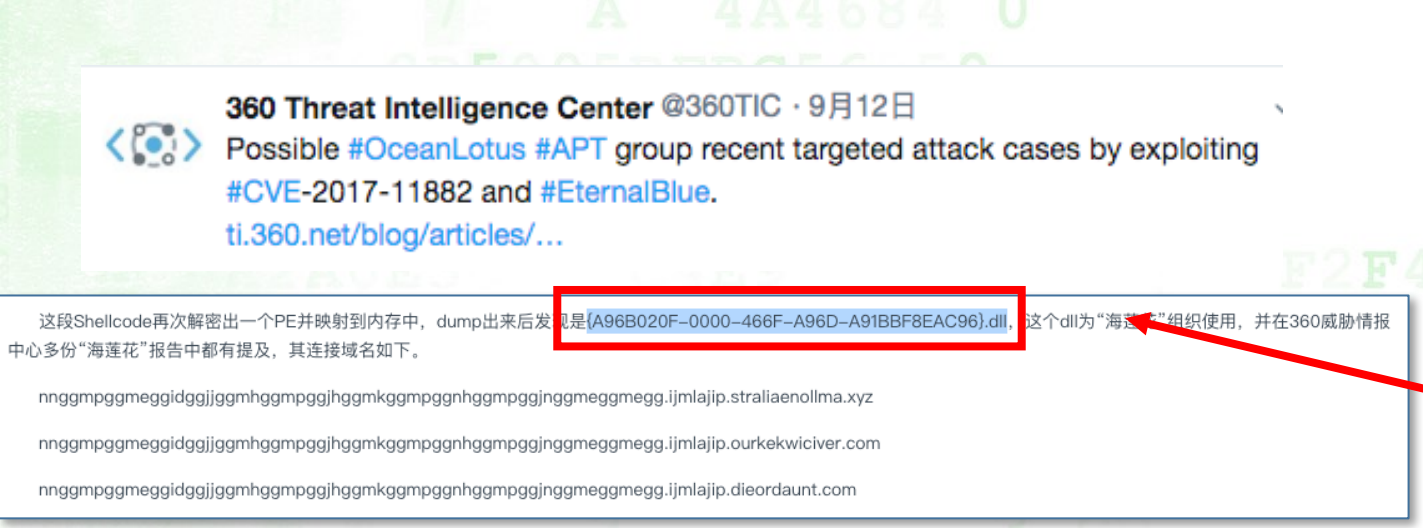
Shellcode load an dll has same export name


https://ti.360.net/blog/articles/oceanlotus-with-cve-2017-8570/



# Example - OceanLotus

OceanLotus uses this DLL module in several activities.




https://ti.360.net/blog/articles/oceanlotus-targets-chinese-university/


https://ti.360.net/blog/articles/oceanlotus-with-cve-2017-8570/

# Example - OceanLotus

## Update TTPs

```
sub_8           proc near               ; CODE XREF: seg000:0000002F↑p
                pop     edi
                mov     ebp, [edi]
                add     edi, 4
                mov     esi, [edi]
                xor     esi, ebp
                add     edi, 4
                push    edi

loc_16:                                 ; CODE XREF: sub_8+22↓j
                mov     eax, [edi]
                xor     eax, ebp
                mov     [edi], eax
                xor     ebp, eax
                add     edi, 4
                sub     esi, 4
                xor     eax, eax
                cmp     esi, eax
                jz      short loc_2C
                jmp     short loc_16
; ---------------------------------------------------------------------------

loc_2C:                                 ; CODE XREF: sub_8+20↑j
                pop     ebp
                jmp     ebp
sub_8           endp ; sp-analysis failed

; ---------------------------------------------------------------------------
                call    sub_8
; ---------------------------------------------------------------------------
                dd 9833D978h
                dd 983DD778h
                dd 98DB9335h
                db  25h ; %
```

```
if ( !RegCreateKeyExA(
        (HKEY)0x80000001,
        "Software\\Classes\\CLSID\\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}",
        0,
        0i64,
        0,
        0xF003Fu,
        0i64,
        (PHKEY)NumberOfBytesWritten,
        0i64)
  && !RegCreateKeyExA(
        (HKEY)0x80000001,
        "Software\\Classes\\CLSID\\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\\InprocServer32",
        0,
        0i64,
        0,
        0xF003Fu,
        0i64,
        (PHKEY)NumberOfBytesWritten,
        0i64) )
{
```

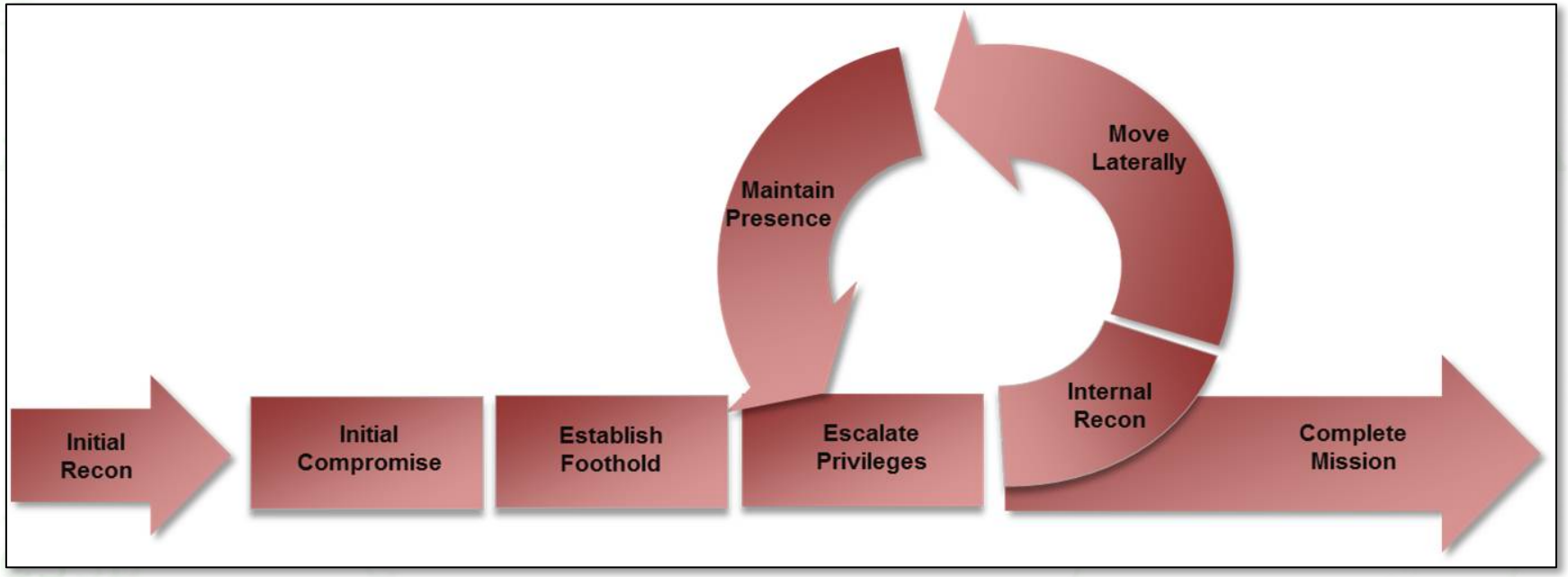
| | |
|---|---|
| Initial Access | Spear Phishing |
| Payload Execution | multiple stage script<br>PowerShell<br>Cobalt Strike |
| Persistence | Hijack CLSID |
| Defense Evasion | Bypass Applocker<br>• Google Update（old）<br>• Flash Player（new）<br>• Word（new） |
| C&C/Exfiltration | • DNS tunnel<br>• Cobalt Strike beacon with Malleable-C2-Profiles |

```
push    ebp
mov     ebp, esp
push    edi
push    offset LibFileName ; "wwlib.dll"
call    ds:LoadLibraryW
mov     edi, eax
test    edi, edi
jz      loc_300016DD

                        ; CODE XREF: sub_30001573+178↓j
push    ebx
push    esi
mov     esi, ds:GetProcAddress
push    offset aFmain   ; "FMain"
push    edi             ; hModule
call    esi ; GetProcAddress
push    offset aWdcommanddis_0 ; "wdCommandDispatch"
push    edi             ; hModule
mov     ebx, eax
call    esi ; GetProcAddress
push    offset aWdgetapplica_0 ; "wdGetApplicationObject"
push    edi             ; hModule
mov     dword_30003010, eax
call    esi ; GetProcAddress
```

```
http-get {

    set uri "/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books";

    client {

        header "Accept" "*/*";
        header "Host" "www.amazon.com";
```

# Methodology - Analysis

MITRE Adversarial Tactics, Techniques & Common Knowledge in the attack lifecycle.




Spear Phishing
Watering Hole

Fileless, Scriptlet
Bypass UAC
Bypass Applocker

HTTP/HTTPS/FTP/SMTP
DNS Tunnel
Cloud service
Cloud disk

source：http://www.iacpcybercenter.org/wp-content/uploads/2015/10/cyber_attack_lifecycle.jpg

# Example - Analysis

**Actors use their own tacticals and techniques.**
Comparison of delivery from spear-phishing email.

| | OceanLotus | DroppingElephant | Darkhotel | APT-C-01 | Group 123 | APT28 |
|---|---|---|---|---|---|---|
| decoy document | √ | √ | √ | √ | √ | √ |
| RAR/SFX | | | | √ | | |
| phishing link | | | | | √ | √ |
| link to compromised website | | | | | √ | √ |
| drive-by download | | √ | | | | √ |

# Example - Analysis

Comparison of establishing foothold/ 1st implant payload

| | OceanLotus | DroppingElephant | Darkhotel | APT-C-01 | Group 123 | APT28 |
|---|---|---|---|---|---|---|
| exploit document | √ | √ | √ | √ | √ | √ |
| DDE | | | | | | √ |
| malicious macro | √ | √ | √ | | | √ |
| HTA | | | | √ | | |
| scriptlet | √ | √ | | | √ | √ |
| PowerShell | √ | √ | | | √ | √ |
| LNK | | | | √ | | |
| PE | √ | | | √ | | |

# Example - Analysis

Major techniques used for the payload.

| | OceanLotus | DroppingElephant | Darkhotel | APT-C-01 | Group 123 | APT28 |
|---|---|---|---|---|---|---|
| C/C++ | √ | √ | √ | √ | √ | √ |
| .Net | | √ | √ | | | |
| PowerShell | √ | √ | √ | √ | √ | |
| AutoIt | | √ | | | | √ |
| Delphi | | | | | | √ |
| Cobalt Strike | √ | | | | | |
| Open Source Code | √ | √ | | | | √ |

| | OceanLotus | DroppingElephant | Darkhotel | Group 123 | APT28 |
|---|---|---|---|---|---|
| Bypass Applocker | √ | | √ | | |
| DLL Hijack | √ | | √ | | |
| UAC Bypass | √ | | √ | | |
| Image Steganography | | | √ | √ | √ |
| PE ReflectiveLoader | | √ | | | |
| job schedule | | √ | | | |
| CLSID hijack | √ | | | | |

# Example - Analysis

Infrastructures used for C&C or exfiltration

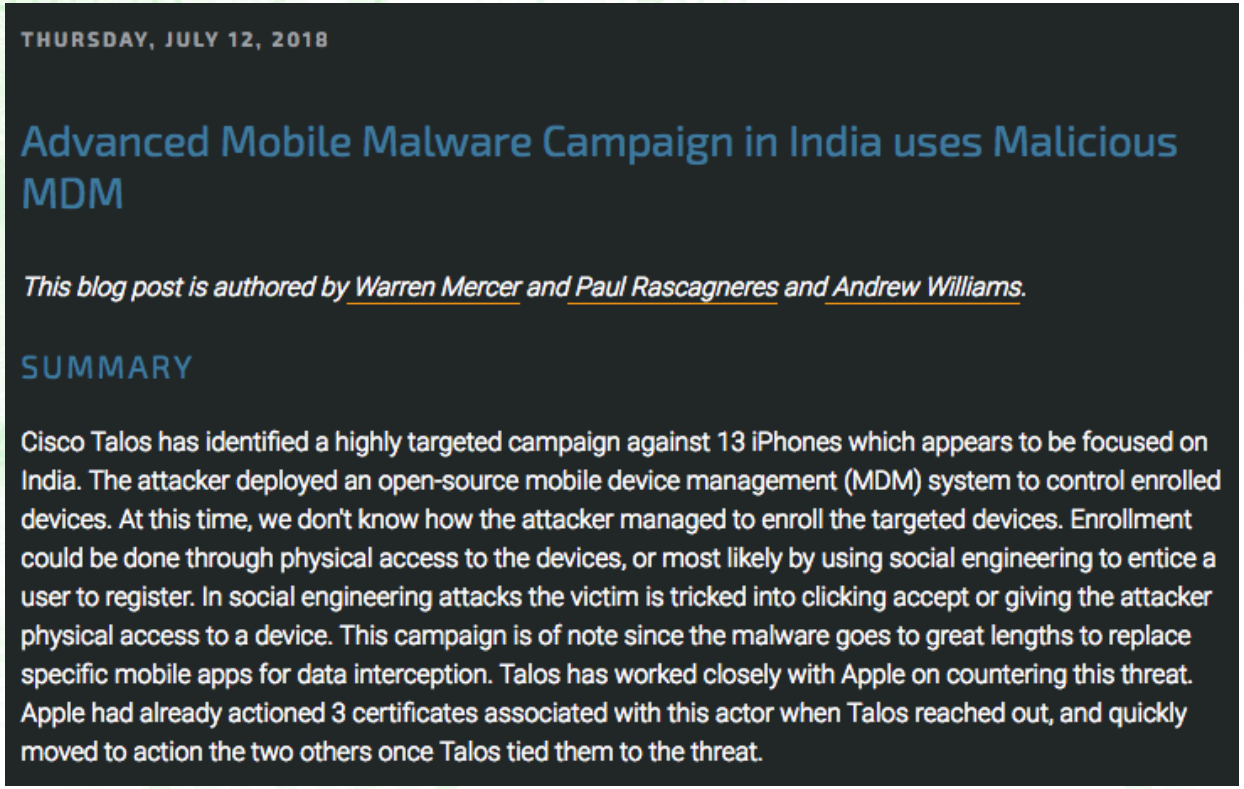
| | OceanLotus | DroppingElephant | Darkhotel | APT-C-01 | Group 123 | APT28 |
|---|---|---|---|---|---|---|
| domain registration | √ | √ | √ | | | √ |
| DDNS | | | | √ | | |
| Cloud Storage | | | | | √ | |
| DGA | | | | | | |
| DNS Tunnel | √ | | | | | |
| Compromised website | | | | | √ | √ |

# Methodology - Analysis

We construct APT actors TTP & Profiles as objects and relations, it can easily find the relation and overlapping based on the graph database and theory.

- relations of observed data （Internal graph analysis tool from 360 Netlab）
  - hash, IP, domain
  - PDNS, Whois registration
- relations of actors and its indicators, aim to find the related technique details. ( neo4j demo )
  - actor and its alias name
  - payload used
  - infrastructure used
  - etc.

# Example1 – actors overlapping & relations



THURSDAY, JULY 12, 2018

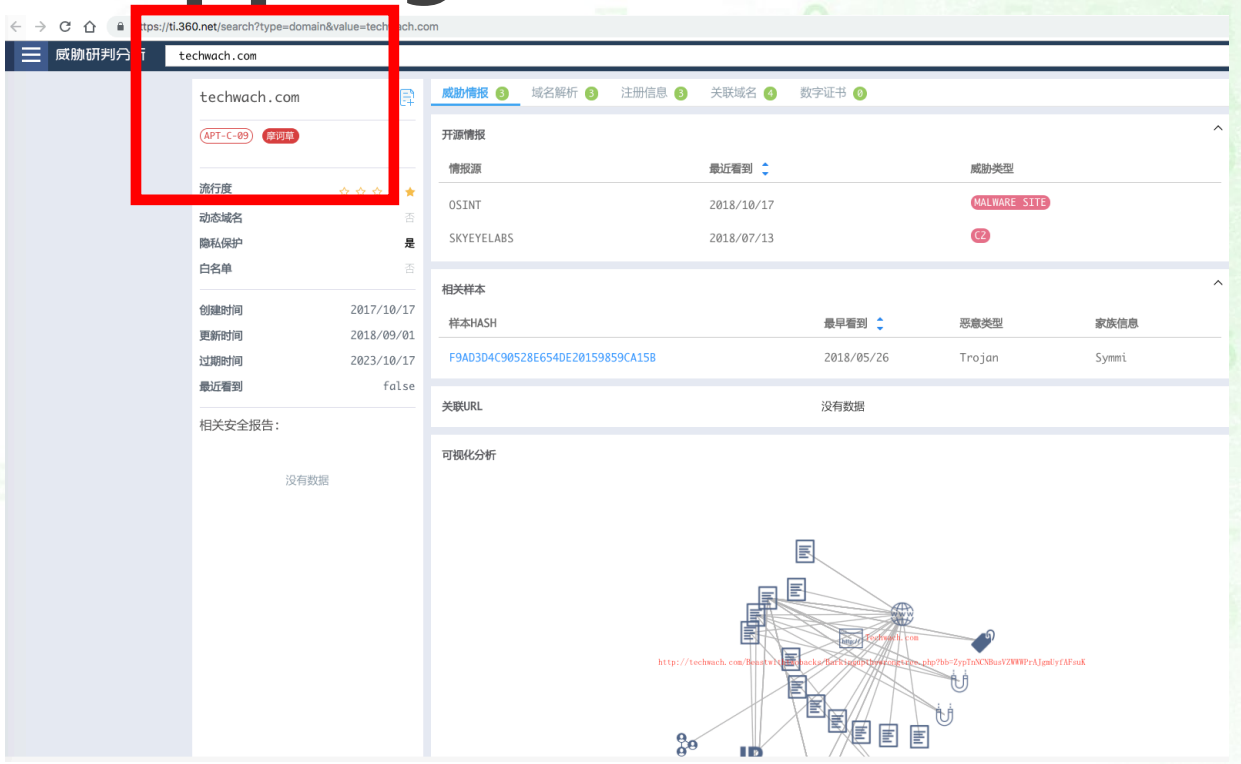
## Advanced Mobile Malware Campaign in India uses Malicious MDM

*This blog post is authored by Warren Mercer and Paul Rascagneres and Andrew Williams.*

### SUMMARY

Cisco Talos has identified a highly targeted campaign against 13 iPhones which appears to be focused on India. The attacker deployed an open-source mobile device management (MDM) system to control enrolled devices. At this time, we don't know how the attacker managed to enroll the targeted devices. Enrollment could be done through physical access to the devices, or most likely by using social engineering to entice a user to register. In social engineering attacks the victim is tricked into clicking accept or giving the attacker physical access to a device. This campaign is of note since the malware goes to great lengths to replace specific mobile apps for data interception. Talos has worked closely with Apple on countering this threat. Apple had already actioned 3 certificates associated with this actor when Talos reached out, and quickly moved to action the two others once Talos tied them to the threat.

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

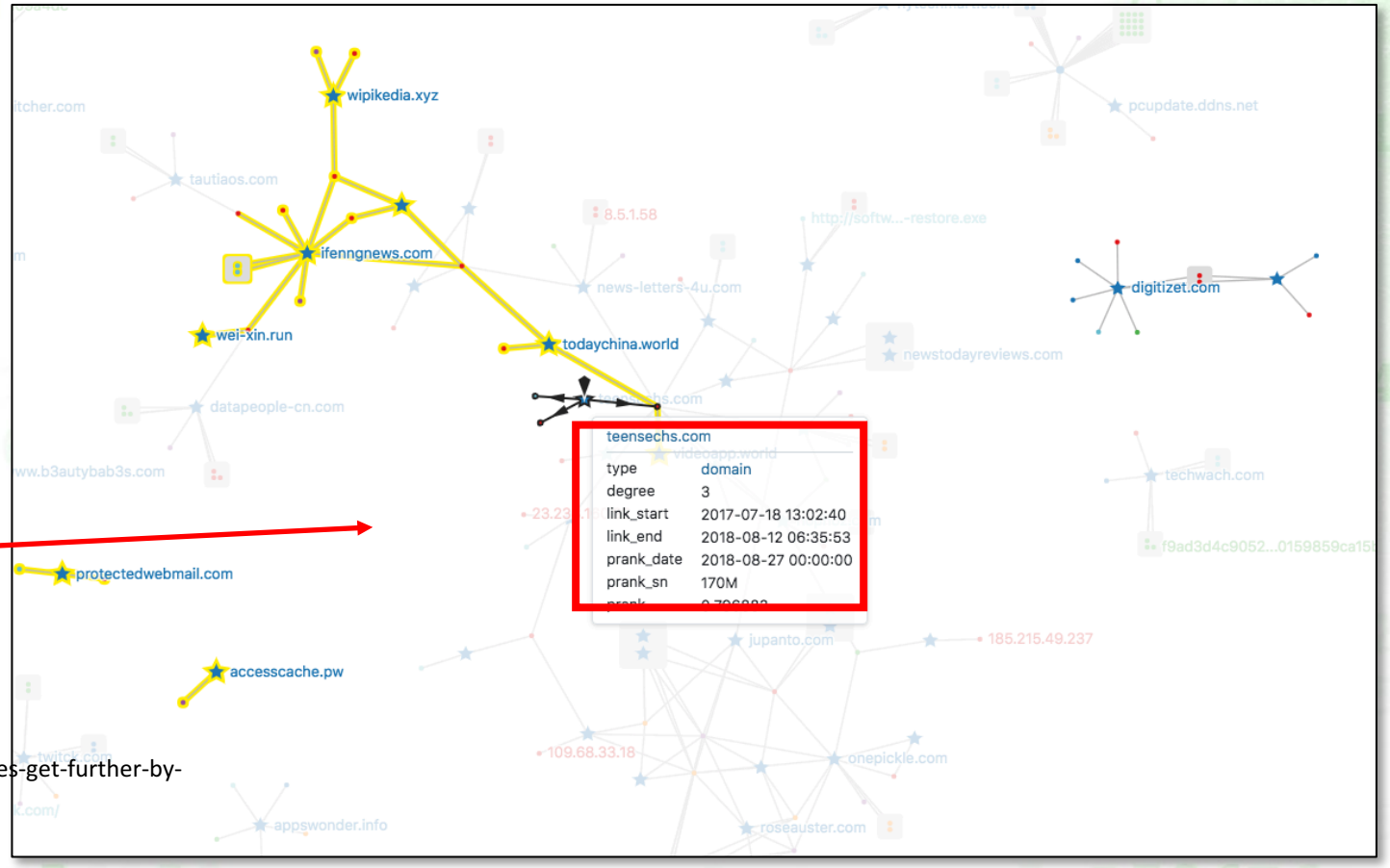



# Example1 – actors overlapping & relations

C2 Addresses:

adhath-learning[.]com
stepontheroof[.]com
ns1[.]b3autybab3s[.]com
stilletowheels[.]com
b3autybab3s[.]com
fierybarrels[.]com
mail[.]cooperednews[.]info
ns2[.]cooperednews[.]info
teensechs[.]com
newstodayreviews[.]com
ns2[.]softwares-free[.]com
www[.]fierybarrels[.]com

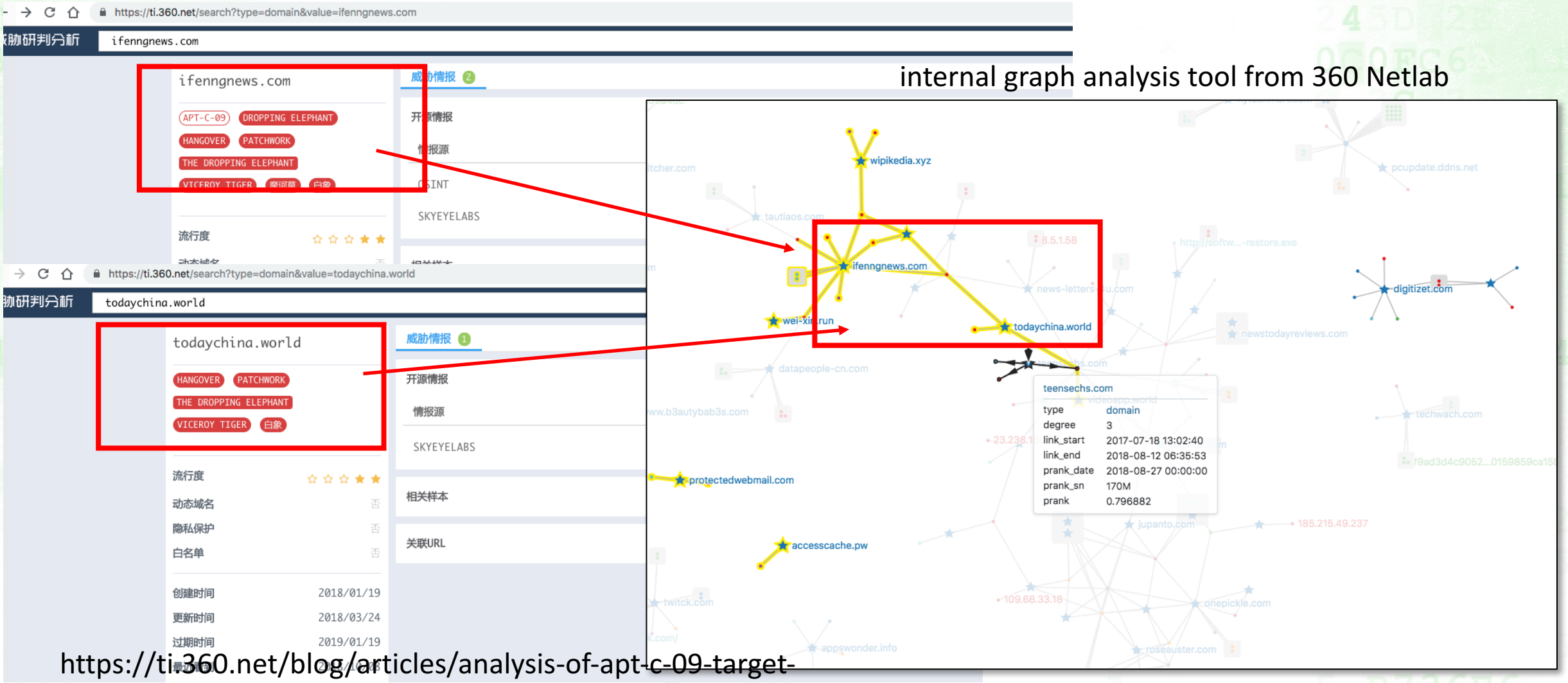
internal graph analysis tool from 360 Netlab




https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

# Example1 – actors overlapping & relations

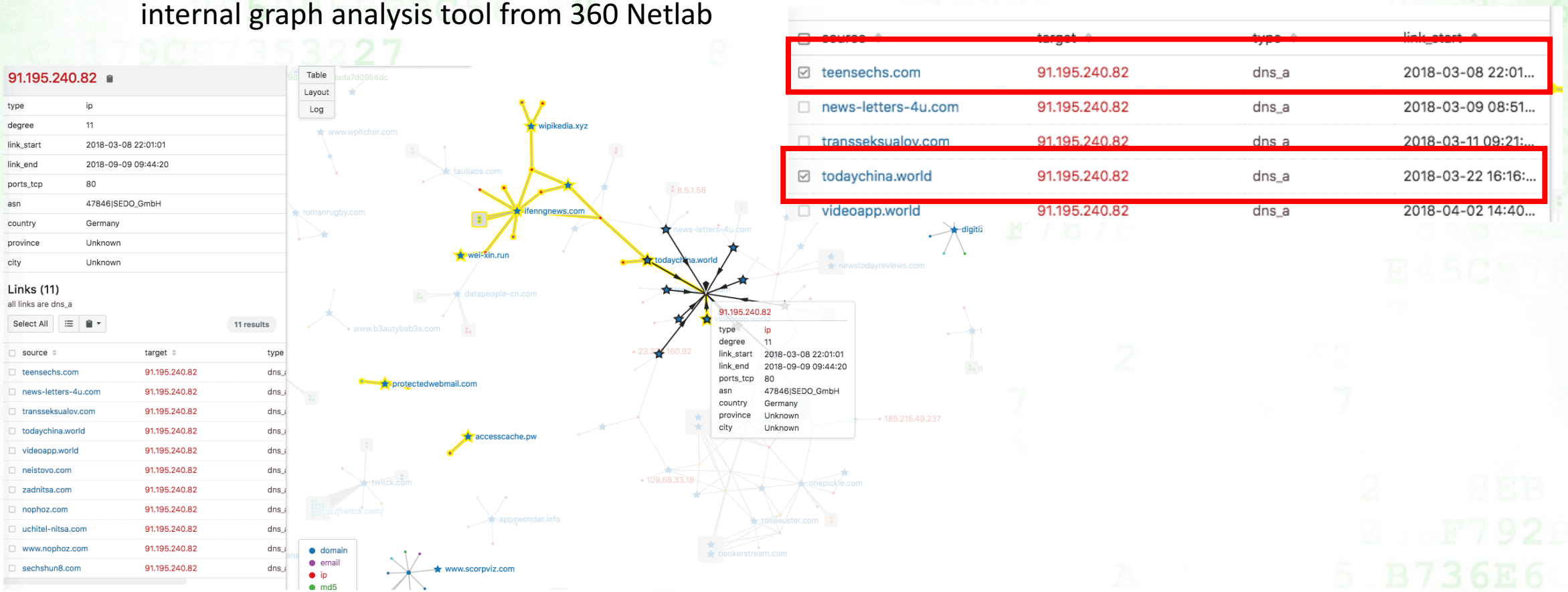
internal graph analysis tool from 360 Netlab




https://ti.360.net/blog/articles/analysis-of-apt-c-09-target-china/

# Example1 – actors overlapping & relations

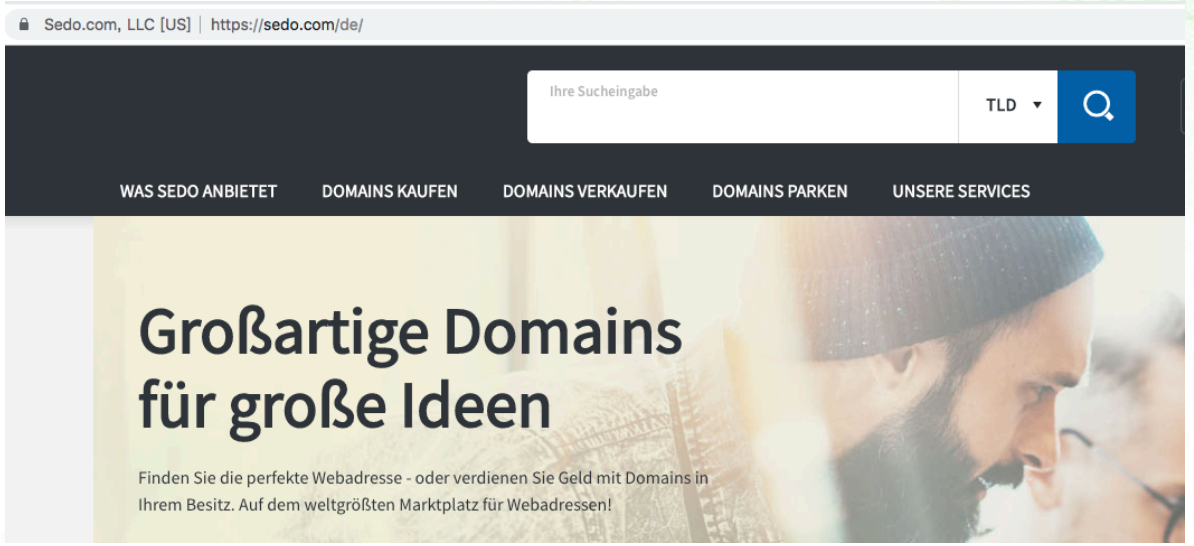
internal graph analysis tool from 360 Netlab



# Example1 – actors overlapping & relations

The IP address(91.195.240.82) belongs to SEDO GmbH, a Germany domain service provider.

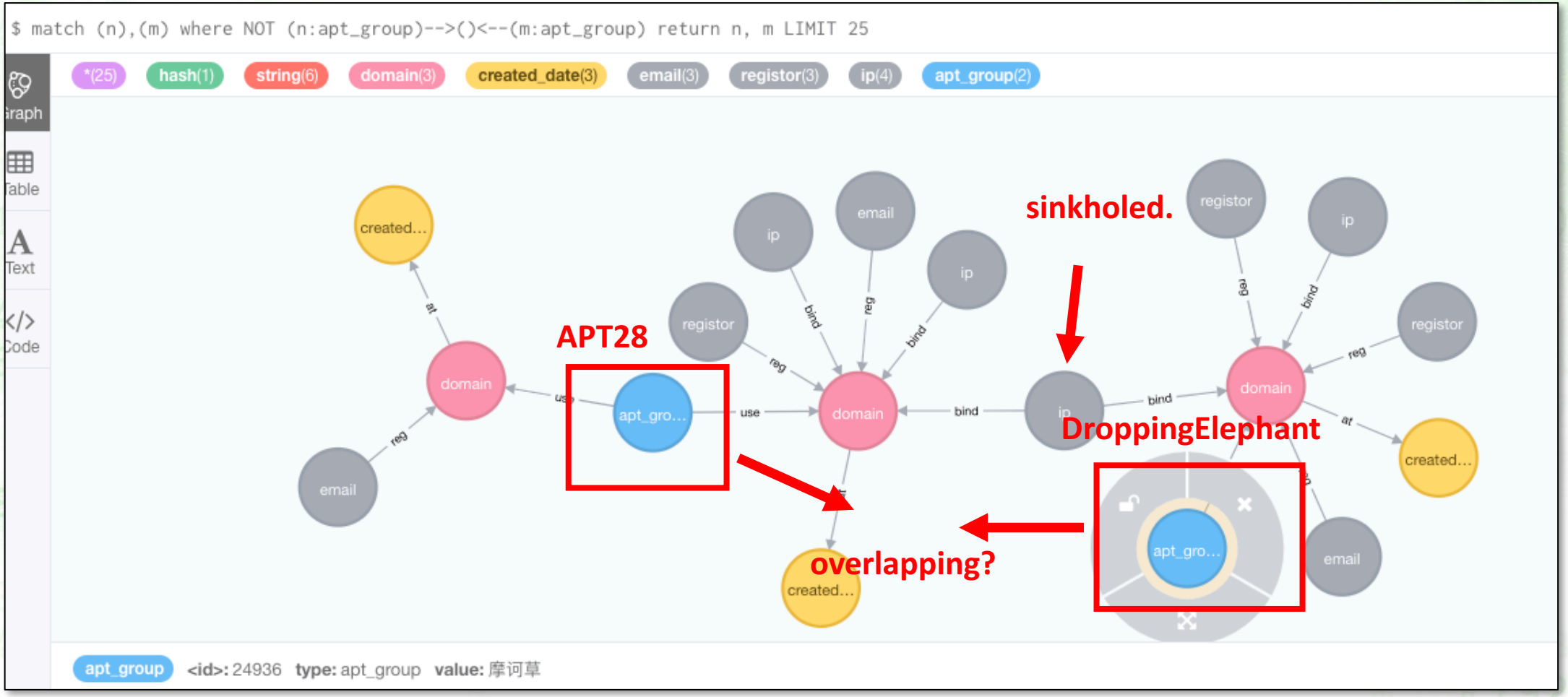
| | |
|---|---|
| **Address type** | IPv4 |
| **ASN** | AS47846 SEDO GmbH |
| **Organization** | SEDO GmbH |
| **Route** | 91.195.240.0/23 |



# Example1 – actors overlapping & relations

| | Confucius | Dropping Elephant | Bahamut |
|---|---|---|---|
| Target | South Asia | China, South Asia | South Asia,<br>Middle East |
| Target platform | PC， Android | PC， Android | Android |
| Payload | Delphi | Delphi， C# | |
| Initial Compromised | Social media | Spear Phishing, Social media | Spear Phishing, Social media |

# Example2 – actors overlapping & relations



# Summary

Leveraging OSINT give us a more comprehensive insight on APT groups.

We believe that APT groups have limited resources and time. They may reuse some custom tools or infrastructures.

OSINT can help us correlate evidence of the actor and complete the puzzle.

# Summary

Twitter： @360TIC


Blog：

https://ti.360.net/blog/

Wechat account

# THANKS