Wave Your False Flags

Deception Tactics Muddying Attribution in Targeted Attacks
Hello False Flags! The art of deception in targeted attack attribution

Juan Andrés Guerrero-Saade
@juanandres_gs
Senior Security Researcher
Kaspersky Lab

Brian Bartholomew
@Mao_Ware
Senior Security Researcher
Kaspersky Lab
Attribution

**Common Threads to Pull on**
- Compile times
- Activity timelines
- Strings
- Debug path
- Resource language
- Tasking / targeting
- C2 infrastructure
- Backend connections
- Malware families
- Code reuse
- Password / key reuse
- Motivation

**Why is Attribution a Problem?**
- Lack of intelligence training
- Limited visibility
- Reputation
- Political fallout
- It's no secret anymore

All Can be Manipulated!
Why is Attribution a Problem?

Lack of intelligence training

Limited visibility

Reputation

Political fallout

It's no secret anymore
Common Threads to Pull on

- Compile times
- Activity timelines
- Strings
- Debug path
- Resource language
- Tasking / targeting
- C2 infrastructure
- Backend connections
- Malware families
- Code reuse
- Password / key reuse
- Motivation

All Can be Manipulated!
We don’t do attribution...for reasons that should become obvious with this talk.

But in order to make our case, we are going to mention examples of conventional or specialized wisdom that point certain campaigns and threat actors towards certain countries.

Let's call it the "Attribution Grapevine"
Cloud Atlas (AKA - Inception)

- Spinoff from Red October
- Eastern European based
- Relies on cloud based services
- Concerted effort to deceive investigators
- Still active today
- Targeting RU based entities mainly

The ‘TurDuckEn’ of APT

- Spanish document name
- Arabic strings in Blackberry malware
- Hindi strings in Android malware
- “God_Save_The_Queen”
- Home routers popped in South Korea
- Chinese malware deployed at one point
- Purposely set clocks wrong
Cloud Atlas
(AKA - Inception)

Spinoff from Red October

Eastern European based

Relies on cloud based services

Concerted effort to deceive investigators

Still active today

Targeting RU based entities mainly
In there?
The ‘TurDuckEn’ of APT

- Spanish document name
- Arabic strings in Blackberry malware
- Hindi strings in Android malware
- “God_Save_The_Queen”
- Home routers popped in South Korea
- Chinese malware deployed at one point
- Purposely set clocks wrong
ARE YOU SERIOUS?
Wild Neutron

Sure, let's sprinkle some language in there

- Romanian for 'goodbye'
- Transliterated RU for 'success'

Attempts to incriminate researchers
Stolen digital certificates

The real messy bit...
Wild Neutron Hacker Group Victims

Kaspersky Lab discovered the return of the infamous Wild Neutron Hacker Group, also known as “Jrijob” and “Morpho”. In 2013 this group was spotted attacking companies like Apple, Facebook, Twitter and Microsoft. In a recent attack the group targeted multiple new companies in 11 countries and territories around the world.

Kaspersky Lab products successfully detect and block the malware used by the Wild Neutron Hacker Group.

Read more on Securelist.com
Lazarus Group

Weak attempt at blending into hacktivism

- Principes and Hastati
- Guardians of Peace
- Who Am I? Crew

Why weak?

Hacked By GOP
Sofacy

Traditionally considered Russian based

Plethora of 0 days at disposal

Targets include media, CT, foreign govs

Massive infrastructure

Large amount of resources

Love to mess with people
Shift in TTPs

Pre-2015:
- Stealthy
- Careful
- Standard espionage actor

2015-Present:
- Careless
- Brazen
- Sloppy OpSec

Targeting expanded to media, policy influencers, dissidents, and democratic elections

Deception / information operations began

Coincided with Ukraine conflict and economic struggles
Targets / Compromises

Ukraine gov, elections, infrastructure
German Bundestag / Parliament
Warsaw stock exchange
US media outlets
French media
CENTCOM
Saudi MoFA (suspected)
WADA / TAS-CAS
DNC / DCCC / Podesta / Bradley Foundation
Personas

Cyber Berkut

Cyber Caliphate

Yemen Cyber Army

Guccifer 2.0

DCLeaks

Fancy Bears Hack Team

@ANPoland
APT-on-APT Action

The Illust... DuQu 2
- Big bad APT
- Stacking Odays
- Memory resident
- Coordinated exfiltration
- "Persist on a network, not on a machine"

But... does that sound like Wang Dong?

TigerMilk
- Targeted campaign against a single country
- No solid attribution leads
- Custom malware for clunky memory injection
- Big gains for small gains

Does anyone recognize this certificate?

Big Bad Stuxnet (A/B)
The Illest... DuQu 2

Big, bad APT

Stacking Odays

Memory resident

Coordinated exfiltration

'Persist on a network, not on a machine'

But... does that sound like Wang Dong?
TigerMilk

Targeted campaign against a single country

No solid attribution leads

Custom malware for clunky memory injection

Big guns for small gains

Does anyone recognize this certificate?

Big Bad Stuxnet (.A/.B)
Does anyone recognize this certificate?
Big Bad Stuxnet (.A/.B)
TigerMilk

Targeted campaign against a single country

No solid attribution leads

Custom malware for clunky memory injection

Big guns for small gains

Does anyone recognize this certificate?

Big Bad Stuxnet (.A/.B)
**Turla**

Popular belief is this is Russian
One of the most advanced APTs
Been around since 1997
Very in tune with what's going on

**Faking Dragon**

Began messing with investigators and researchers

Stage 1 - Wipbot

Stage 2 - Quarian? WTF?

Used already compiled malware

Meant to send researchers down rabbit hole

Had to use rare stage 2 - APT1 wouldn't work

Other theories:
- Turla is Chinese
- Turla is selling other vics to China
- Turla is working with China
Turla

Popular belief is this is Russian

One of the most advanced APTs

Been around since 1997

Very in tune with what's going on
Faking Dragon

Began messing with investigators and researchers

Stage 1 - Wipbot

Stage 2 - Quarian? WTF?

Used already compiled malware

Meant to send researchers down rabbit hole

Had to use rare stage 2 - APT1 wouldn't work

Other theories:

• Turla is Chinese
• Turla is selling other vics to China
• Turla is working with China
“Turla Dragon” - Infrastructure

Beijing, China
Faking Dragon

Began messing with investigators and researchers

Stage 1 - Wipbot

Stage 2 - Quarian? WTF?

Used already compiled malware

Meant to send researchers down rabbit hole

Had to use rare stage 2 - APT1 wouldn't work

Other theories:
- Turla is Chinese
- Turla is selling other vics to China
- Turla is working with China
I DON'T THINK SO

TIM
What Level of Attribution is Needed?

Government

vs.

Private Sector

vs.

Media
Government

Most fidelity needed
Unit or individual attribution
Conducts offensive operations
Sanctions / Indictments / Demarche
Private Sector

Individual attribution is sexy, but not needed

Attribution needed for resource direction

Focus on countries where business is
Media

Any level WANTED

#1 question asked...Who dunnit?

Worried about the 'who' and not the 'why'

Immature orgs can be pressured
Conclusions
Threat Intelligence is not the same as IT or IR, looking at different things from a different perspective and experience
Historical context is irreplaceable in Threat Intel
There are uniquely positioned entities that do attribution. We are not them.
Takeaways
What happens to 'hacking back' if you can't pinpoint your target?
To what extent do you need attribution?
Is clustering of activity or group definitions enough to combat the threat?
What ACTIONABLE intelligence are you providing?
Hello False Flags! The art of deception in targeted attack attribution

Juan Andrés Guerrero-Saade
@juanandres_gs
Senior Security Researcher
Kaspersky Lab

Brian Bartholomew
@Mao_Ware
Senior Security Researcher
Kaspersky Lab