Prepared for Black Hat Webcasts

February 2017

Attribution – the good the bad and the ugly

Andrew van der Stock

Chief Technology Officer
Doing appsec since 1998

OWASP Board member
OWASP ASVS
OWASP Top 10 2007
OWASP Dev Guide

Family, cats, WRC nut

Agenda

Attribution

- What is attribution
- Why would you want to do attribution?
- The difference between intelligence and actionable facts
- Attribution markers - TTP

The ugly

- Naming groups
- Naming individuals
- Naming nation states
- Where to go from here

The good - attribution


What is attribution

Why would you want to do attribution?

Identify common patterns

Campaigns
Incidents
Motives

Tools
Techniques
Procedures

Help understand:

Targets of exploitation
Why they are there
How they move laterally
Persistence techniques
How they hide
How they exfiltrate

Differences between intelligence and actionable facts

Intelligence

Shared threat intelligence

Unusual and curious activities

Campaigns

TTP

Threat actor profiles

Actionable facts

Incidents

Observations

Analysis of malware

Analysis of logs

Timeline analysis

Time of day analysis

IOCs

Exploit targets

Compromised C&C server(s)

… still no names, no addresses

Attribution markers - TTP

If the same family of malware or tools or practices appears, you have a similar threat group

If they always compromise in the same or very similar ways, you might have the same or similar threat group

If they trained in the same way under the same person, it might not be the same threat group

If they use many different methods of attacking you, and these are all different, it's difficult to attribute to the same group except by time lines and targets of exploitation

The bad

Naming groups

Firms, often for marketing purposes, will attribute a set of TTPs to a single group

It's common marketing practice to give groups a name like Equation Group, Fancy Bear, Cozy Bear, or Rocket Kitten

It's better to use naming schemes like APT-2017-43

Limits unconscious bias

Curtails conscious bias

The ugly

Naming individuals

The family of Sunil Tripathi – the missing student who was wrongly identified as a suspect in the Boston bombing and whose body was this week recovered from a river – have expressed thanks for messages of support they said poured in from around the world.

Officials in the US state of Rhode Island confirmed on Thursday that the body of a man that was found in a river running through the city of Providence was that of 22-year-old Mr Tripathi.

Naming individuals

Doxing individuals has a long and sad history

Nearly always wrong

Can be devastating to those caught by the doxing

When is it right to name an individual?

What level of certainty do you need?

Are you in a position to do something about the individual?

Naming nation states

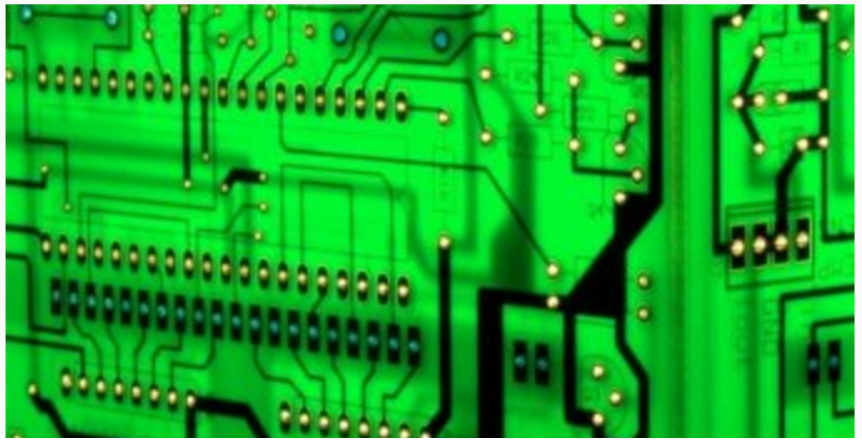
China blamed for 'massive' cyber attack on Bureau of Meteorology computer

By political editor Chris Uhlmann

Updated 2 Dec 2015, 8:28pm

China is being blamed for a major cyber attack on the computers at the Bureau of Meteorology, which has compromised sensitive systems across the Federal Government.

Multiple official sources have confirmed the recent attack, and the ABC has been told it will cost millions of dollars to plug the security breach, as other agencies have also been affected.



Naming nation states

This is a fairly common practice with certain firms.

When VPS cost nothing and it's trivial to break into millions of compromised servers, how certain can you be?

What can you do about it if the attacker is a nation state?

Leave this to nation states

Where to go from here

Attribution can be useful

Find like incidents

Search for similar IoCs

Clear out attackers more rapidly

Understand their motives

Guesses at future attacks based on past history

Share knowledge with others

Attribution can be harmful

Wastes time

Opportunity cost of chasing down false leads

Could be wrong

Could be harmful

Thank you!

Andrew van der Stock,

CTO

Andrew@ThreatIntelligence.com

P: +61 422 644 792