



# Cyber Threats to the G20

---

2018 SANS CTI Summit  
Lincoln Kaffenberger  
IMF

# Agenda

- IMF and G20 Background and Overview
- Research Findings
  - Historic G20 Cyber Threat Incidents
  - External Threat Information
- Analysis of Findings
- Threat Scenarios and Recommendations
- Lessons Learned

# Disclaimer

---

The views expressed herein are those of the speaker and should not be attributed to the IMF, its Executive Board, or its management

# whoami?

---

- Lincoln ([@LincolnKberger](#)): Threat Intelligence Officer with the International Monetary Fund.
- Background:
  - ~10yrs in U.S. Army doing Military Intelligence.
  - ~3yrs doing Strategic Cyber Intel

# IMF Overview

## ABOUT THE IMF

### About the IMF

The International Monetary Fund (IMF) is an organization of 189 countries, working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world.

Created in 1945, the IMF is governed by and accountable to the 189 countries that make up its near-global membership.



**IMF != World Bank**

**IMF is a member of the G20**

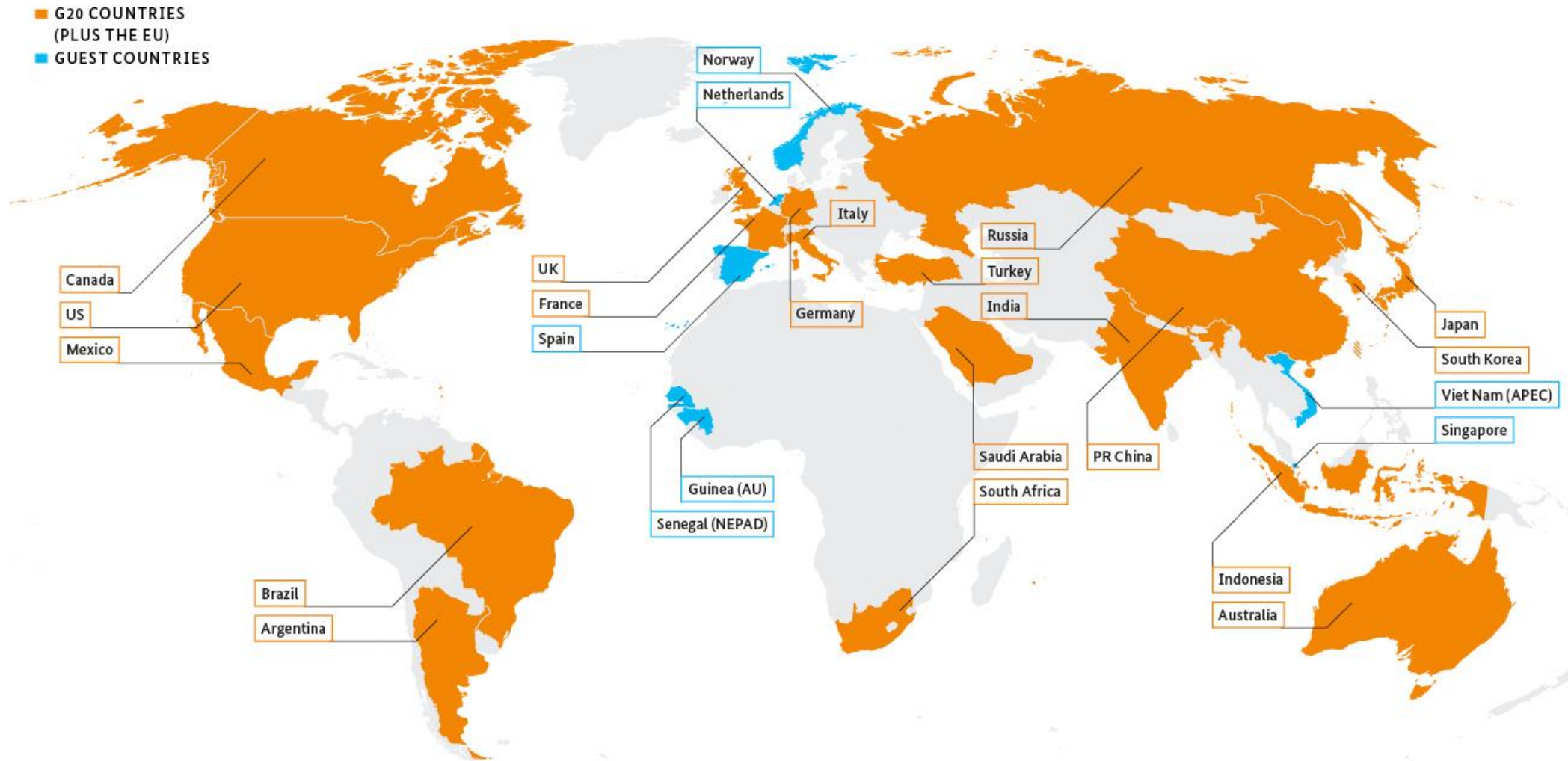
# Background

---

- G20 Leaders' Summit identified as a HIGHER threat than Annual or Spring Meetings
- Conducted a detailed analysis on the threat posed to attendees of the pre-Summit working groups and ministerial meetings



# G20 Overview - Members





# G20 Overview - Events

---

## 12 Separate Working Groups

- *Agriculture Working Group*
- *Anti Corruption Working Group (ACWG)*
- *Development Working Group*
- *Employment Working Group*
- *Framework for Growth Working Group*
- *Global Partnership for Financial Inclusion*
- *Green Finance Study Group*
- *HealthWorking Group*
- *International Financial Architecture Working Group*
- *Sustainability Working Group (Energy and Climate)*
- *Trade and Investment Working Group*
- *Task Force Digital Economy*

Two Tracks – Leaders (Sherpa) and Finance

Every Leaders' Summit concludes w/ a **Communique** – important final declaration

IT Setup:

-separate network setup for Summit



**G20 GERMANY 2017**  
HAMBURG



# “Hackers” target the G20 a lot....right?



### U.S. State Department email system hacked during G20 meeting in Australia



18  
Like

On Nov. 16, the U.S. State Department suddenly shut down access to their unclassified email system after what appeared to be a cyber-attack from external sources. The attack also hit the U.S. agency at the same time that world leaders were together in Brisbane, Australia for this year's meeting of the G20 group of economic powers, possibly sending a message to the U.S. that their actions against sovereign countries or global citizens was being noticed.



# Research Findings

## Historic G20 Themed Phishing Events

Date	Incident	G20 Date	Timing
Jan 2011	Spear phishing emails – G20 themed subjects	South Korea – Nov 2010	After Leaders'
Jan 2011	Spear phishing emails (2 <sup>nd</sup> time) – G20 themed subjects	South Korea – Nov 2010	After Leaders'
Aug 2013	Spear phishing emails to targeted list of 200+ G20 attendees	Russia – Sep 2013	Prior to Leaders'
Mar 2014	Spear phishing emails – G20 themed subjects from an APT	Australia - Nov 2014	In between Leaders'
Nov 2014	Spear phishing email sent to seven G20 users	Australia - Nov 2014	Prior to Leaders

Zero targeted phishing or USB vs G20 personnel in 2016/2017 season.

***What is a big assumption here?***

# Analysis

## G20 Cyber-attack References

Negligible indication of targeting 2017 G20

### APT Calc Team Suspected in Cyberattacks on G20

By Joshua Phillips, The Epoch Times  
August 27, 2013 3:04 pm Last Updated: December 15, 2013 6:45 pm



Participants of G20 Finance Ministers and Central Bank Governors meeting attend the plenary session in Moscow, Russia, on July 19, 2013. Hackers are targeting G20 attendees. (Killer Kudryavtsev/AFP/Getty Images)

### G20 2014 Summit Lure used to target Tibetan activists

BY ESET RESEARCH POSTED 14 NOV 2014 - 03:29PM

GOVERNMENT



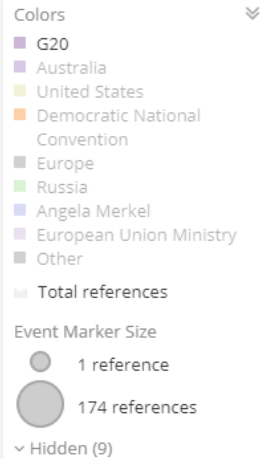
### G20 world leaders' personal details leak a 'huge embarrassment', says Labor

Shadow immigration minister Richard Marles calls on Australian government to explain why world leaders were not notified of the breach when it occurred last November

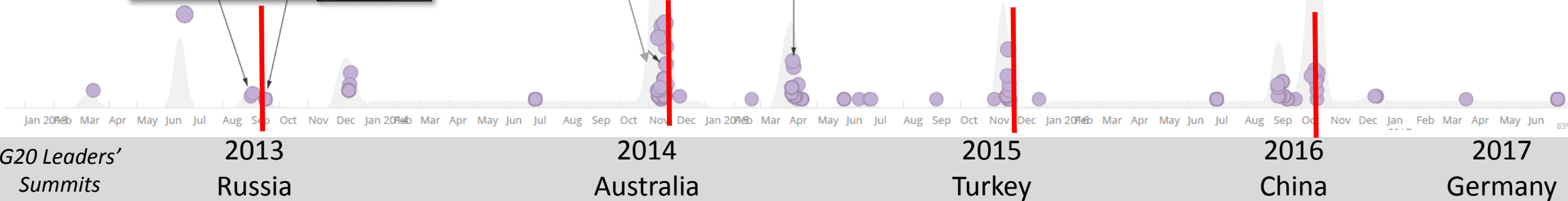


### HACKERS DESCEND ON THE G20 SUMMIT IN CHINA, CONDUCTING OVER 133,000 MALICIOUS CYBER ATTACKS

Posted by Dean Alvarez - October 7, 2016 in EDITOR'S NEWS 0 Comments



Russia bid to bug No 10 aides with Trojan horse gifts: Free phone chargers and USB drives at G20 summit were plot to tap into secrets





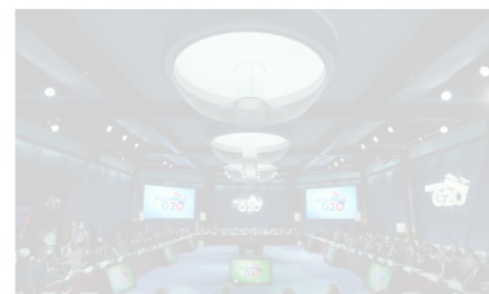
# Analysis

## G20 Cyber-attack References

Negligible indication of targeting 2017 G20

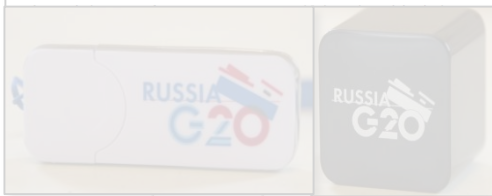
### APT Calc Team Suspected in Cyberattacks on G20

Joshua Kessler, The Epoch Times  
10/17/2013 3:54 pm, Last Updated: December 15, 2013 8:45 pm



Participants of G20 Finance Ministers and Central Bank Governors meeting ahead of the primary session in Moscow, Russia, on July 18, 2013. Hackers are targeting G20 attendees. (G20 Security/Reuters/PHOTO Images)

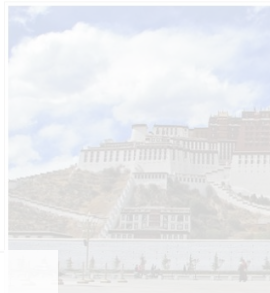
Russia bid to bug No 10 aides with Trojan horse gifts: Free phone chargers and USB drives at G20 summit were plot to tap into secrets



### G20 2014 Summit Lure used to target Tibetan activists

BY ESET RESEARCH POSTED 14 NOV 2014 - 03:29PM


GOVERNMENT



### Cyber attack against G20

NOV  
18  
2015

From Twitter by @InsideCyber

 @insidecyber "#Russia backs norm barring industrial-espionage hacking at #G20 summit <https://t.co/00KZIIIG7OW> #infosec."

From Twitter by @InsideCyber on Nov 18, 2015, 22:45

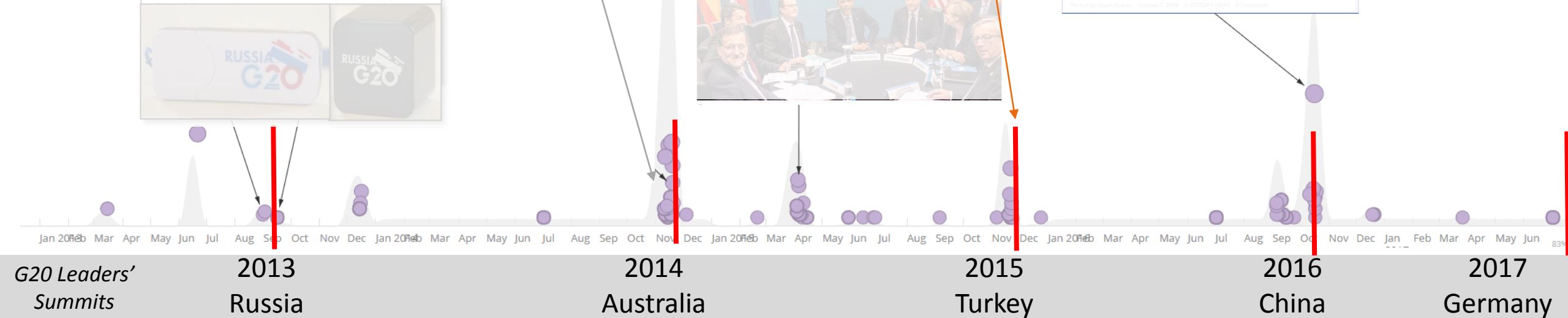
Resolved <https://t.co/00KZIIIG7OW> to [insidecybersecurity.com](https://insidecybersecurity.com)

<https://twitter.com/InsideCyber/statuses/667111470178660352> • 6+ references



HACKERS DESCEND ON THE G20 SUMMIT IN CHINA, CONDUCTING OVER 133,000 MALICIOUS CYBER ATTACKS

Posted by Dawn Aronson, October 5, 2016, in EDITOR'S NEWS, 10 Comments



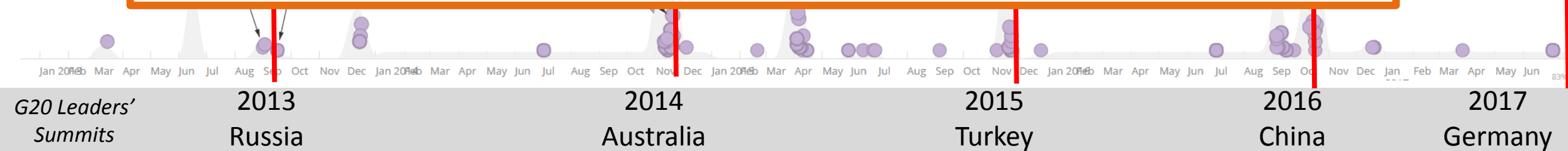
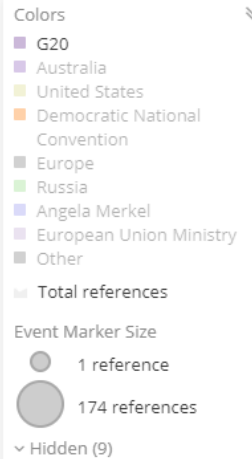
# Analysis

## G20 Cyber-attack References

Negligible indication of targeting 2017 G20

*“no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.”*

Source: Point 24 from 2015 G20 Communique



# Analysis – Analysis of Competing Hypothesis

## 3 Hypotheses to explain dip in activity:

1. Increased Stealth

2. Stopped Attacking

3. Changed to MITM

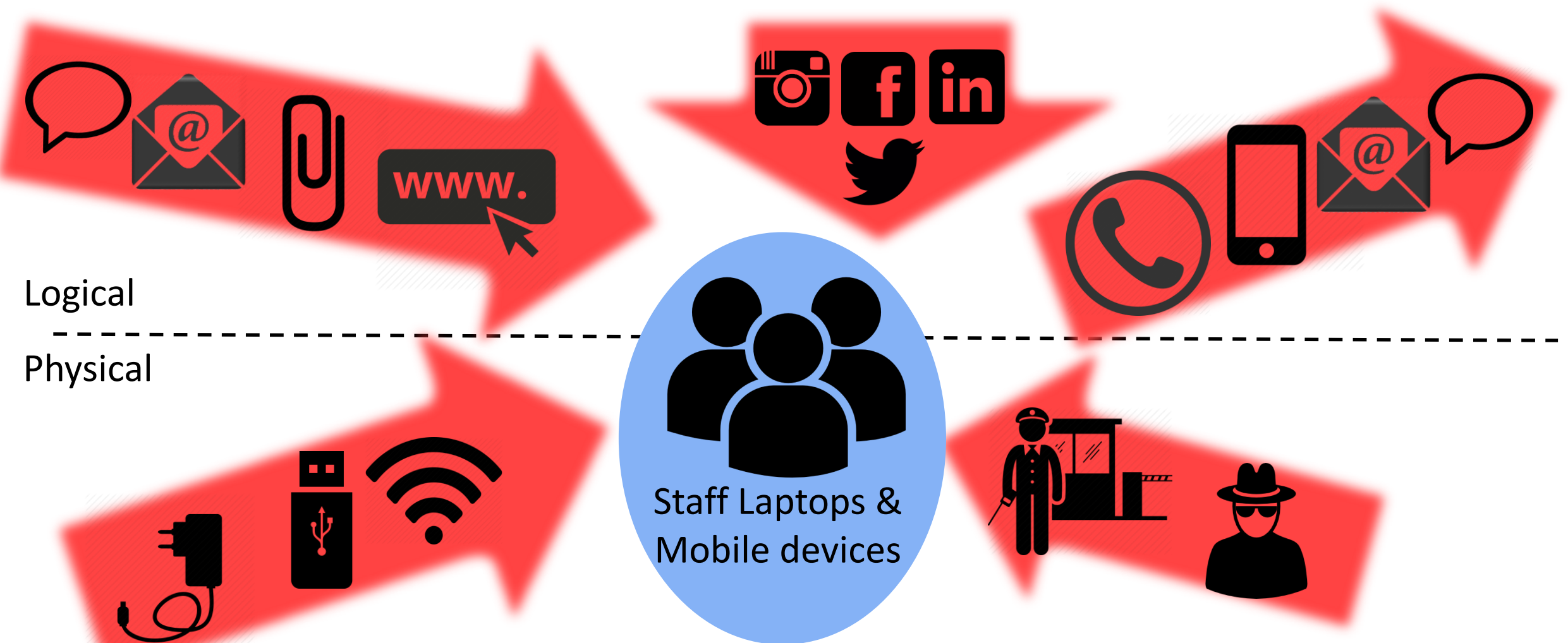
Conclusion: Adversaries either stopped attacking or changed to MITM to gather information.

Sort Evidence By: <div>Order Added</div>		Type of Calculation: <div>Weighted Inconsistency Score</div>	Duplicate Matrix		Hide/Show Columns	Hide Tutorial			
		Type	Credibility	Relevance	H: 1	H: 2	H: 3	H: 4	P
					Attackers increase stealth of cyber attacks and continue to focus on compromising devices	Attackers choose to attack less	Attackers change tactics - MITM through telecom passive recon rather than attacking devices		
		Weighted Inconsistency Score ↕			-2.121	-1.414	-1.414	-0.0	
		Enter Evidence							
E15	G20 Network attacked 133k times in 2016 - Web attacks and DDoS		LOW	LOW	C	C	N	NA	
E14	2015 G20 Communique states the members will oppose industrial espionage hacking		HIGH	MEDIUM	CC	C	CC	NA	
E13			HIGH	HIGH	N	N	N	NA	
E12			HIGH	MEDIUM	N	N	N	NA	
E11	Lack of current cyberattack related info on Recorded Future		LOW	MEDIUM	C	C	C	NA	
E10			HIGH	HIGH	N	N	N	NA	

Picture of ACH done in PARC ACH 2.0.5 software

# Threat Scenarios and Recommendations

Created Threat scenarios based upon the threat analysis with recommendations for attendees





# Conclusions and Impact

---

Wrote long form report

- ***and somebody actually read it!***

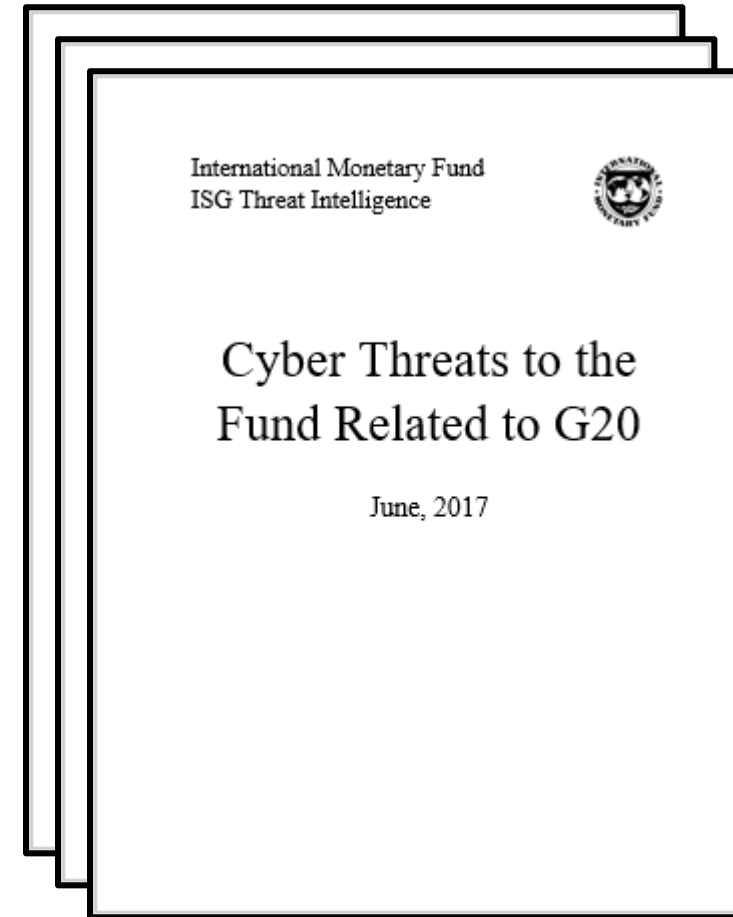
*Some* recommendations taken

Monitored during the event

- nothing anomalous

Debriefed attendees upon return

- nothing out of ordinary



**Conclusion: Assessment was right.**


# Then...

**proofpoint™**

PRODUCTS ▾SOLUTIONS ▾THREAT CENTER ▾PARTNERS ▾SUPPORT ▾☰

## TURLA APT ACTOR REFRESHES KOPILUWAK JAVASCRIPT BACKDOOR FOR USE IN G20-THEMED ATTACK


AUGUST 17, 2017 Darien Huss




### Overview

Proofpoint researchers have observed a well-known Russian-speaking APT actor usually referred to as Turla using a new .NET/MSIL dropper for an existing backdoor called JS/KopiLuwak. The backdoor has been analyzed previously [11] and is a robust tool associated with this group, likely being used as an early stage reconnaissance tool.


### MOST RECENT




5 DAYS AGO  
Kovter Group malvertising campaign exposes millions to potential ad fraud malware infections




1 WEEK AGO  
Threat Actor Profile: TA505, From Dridex to GlobelImposter



2 WEEKS AGO  
Retele banking Trojan leverages EternalBlue exploit in Swiss campaigns



3 WEEKS AGO  
German elections are on September 24, but spammers have already cast their votes



1 MONTH AGO

# Lessons Learned

---

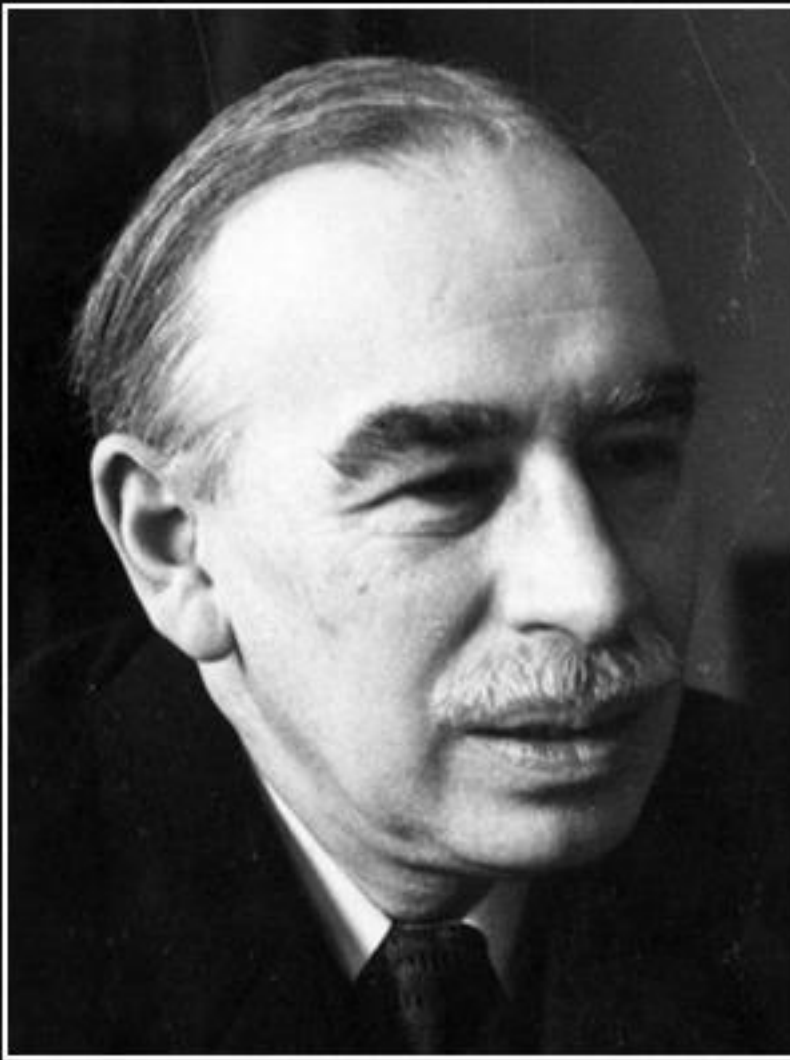
## Sustain

- Using SATs (ACH) – helped make analysis more deliberate
- Interact directly with the business/customers
- Conduct follow-up w/ attendees upon their return
- Work closely with various cyber threat intel providers

## Improve

- Begin the analysis and discussion with business earlier
- Identify assumptions early on
- Leverage sharing communities to validate analysis and increase potential data sources
- **Consider the geopolitical situation – non-cyber, strategic analysis – better indicator of cyber attacks**

# Questions?



The difficulty lies not so much in  
developing new ideas as in escaping  
from old ones.

— *John Maynard Keynes* —

AZ QUOTES