Cyber Threats to the G20

2018 SANS CTI Summit
Lincoln Kaffengerer
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

IMF Overview

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 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

https://www.g20.org/Webs/G20/EN/G20/Participants/participants_node.html
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
“Hackers” target the G20 a lot….right?

G20 Conference Gives Hackers High-Profile Targets

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

Hackers descend on the G20 summit in China, conducting over 133,000 malicious cyber attacks

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Incident</th>
<th>G20 Date</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2011</td>
<td>Spear phishing emails – G20 themed subjects</td>
<td>South Korea – Nov</td>
<td>After Leaders’</td>
</tr>
<tr>
<td>Jan 2011</td>
<td>Spear phishing emails (2\textsuperscript{nd} time) – G20 themed subjects</td>
<td>South Korea – Nov</td>
<td>After Leaders’</td>
</tr>
<tr>
<td>Aug 2013</td>
<td>Spear phishing emails to targeted list of 200+ G20 attendees</td>
<td>Russia – Sep 2013</td>
<td>Prior to Leaders’</td>
</tr>
<tr>
<td>Mar 2014</td>
<td>Spear phishing emails – G20 themed subjects from an APT</td>
<td>Australia - Nov 20</td>
<td>In between Leaders’</td>
</tr>
<tr>
<td>Nov 2014</td>
<td>Spear phishing email sent to seven G20 users</td>
<td>Australia - Nov 20</td>
<td>Prior to Leaders</td>
</tr>
</tbody>
</table>

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

What is a big assumption here?
Analysis

APT Calc Team Suspected in Cyberattacks on G20

G20 2014 Summit Lure used to target Tibetan activists

G20 world leaders’ personal details leak a ‘huge embarrassment’, says Labor

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 Leaders’ Summits

2013 Russia

2014 Australia

2015 Turkey

2016 China

2017 Germany

https://app.recordedfuture.com/live/sc/52k3GI3Gs78f
**Analysis**

**G20 Cyber-attack References**

Negligible indication of targeting 2017 G20

**Cyber attack against G20**

From Twitter by @InsideCyber

@InsideCyber "#Russia backs norm barring industrial-espionage hacking at #G20 summit https://t.co/00KZIIG7OW #infosec."

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

Resolved https://t.co/00KZIIG7OW to insidecybersecurity.com

https://twitter.com/InsideCyber/statuses/65711470178660352 • 6+ references

**G20 Leaders’ Summits**

2013 Russia

2014 Australia

2015 Turkey

2016 China

2017 Germany

https://app.recordedfuture.com/live/sc/52k3GI3Gs78f
“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 Communiqué
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.

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

Logical

Physical

Staff Laptops & Mobile devices
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...

Then...

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 —