The News is OSINT

Ashley Holtz, with contributions from:

Elizabeth Bujwid & Victoria Law
Important Note

Intel isn’t one-size fits all, all recommendations and observations are personal opinions and may not apply to your organization.
Why is news better OSINT now than it was 10 years ago?

• Better technology – online & digital news, standard feed formats, NLP tech
• Today’s news is more cyber-aware, more cyber reports
• It’s harder to keep cyber secrets - easier to discover widespread attack trends
• News is social – reactions are public and create pivot signals & selectors
What does publicly-reported news tell us about cyber attacks and trends?

<table>
<thead>
<tr>
<th>DATA FROM CSIS WITH ADDITIONS FROM OUR RESEARCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>EACH EVENT TAGGED WITH SOURCE/TARGET COUNTRY, ATTACK TYPE AND TARGET SECTOR</td>
</tr>
</tbody>
</table>

566 DATA POINTS 2006-2019

https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
Government vs. Private Sector Targeting

- **Government**
- **Government-Related**
- **Private**

---

<table>
<thead>
<tr>
<th>Year</th>
<th>Government</th>
<th>Government-Related</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Variance in Reported Attack Types
Notable Attack Category Trends: Society & Individuals

**Surveillance & Monitoring**

- USA
- Unknown
- Russia
- North Korea
- Iran
- China

**Influence OPs**

- Unknown
- United Arab Emirates
- Russia
- Iran
Notable Attack Category Trends: Cyber to Physical

ICS

2008 2013 2015 2017 2019

USA
Unknown
Syria
Russia
North Korea
Iran
Eastern Europe
China

Financial Fraud


Unknown
Russia
North Korea
Israel
China
Notable Attack Category Trends: Disruptive Attacks

Ransomware & Wiper

DDOS & Outage

- USA
- Unknown
- Russia
- North Korea
- Iran
- China
Notable Attack Category Trends: Email and Web

Email-based Attacks (Phishing, BEC)

Web Compromise, Defacement
Notable Attack Category Trends: Data Theft

Govt Data Theft, Spying, Espionage

IP Theft, Industrial Espionage (Non-Govt)

- Wikileaks
- USA/UK
- USA
- Unknown
- Taiwan
- Shadow Brokers
- Russia
- North Korea
- Morroco
- Lebanon
- Iran
- Germany
- France
- Egypt
- Vietnam
- Unknown
- Russia
- North Korea
- Iran
- China
Attackers targeting US, Aggregate 2006-2019
Chinese Targeting Trends: Concentrating and projecting power

- Long Range Planning, Made in China 2025
- China 2017 Cybersecurity Law
- Foreign & Domestic Influence
China-Attributed Attack Targets 2010-2019
Chinese TTP Trends

- Website Compromise, Outage, Defacement
- Surveillance & Monitoring
- Spying, Espionage, Govt Data Theft
- PII Theft & Data Exposure
- Military Activity
- IP Theft & Industrial Espionage (Non-Govt)
- IOT
- ICS
- General Attack/Targeting
- Financial Fraud
- Email-based attacks (phishing, BEC)
- DDOS & Disruptive Attacks
- Attacks against creds
Chinese TTP Trends

US – China Cyber Agreement

- Website Compromise, Outage, Defacement
- Surveillance & Monitoring
- Spying, Espionage, Govt Data Theft
- PII Theft & Data Exposure
- Military Activity
- IP Theft & Industrial Espionage (Non-Govt)
- IOT
- ICS
- General Attack/Targeting
- Financial Fraud
- Email-based attacks (phishing, BEC)
- DDOS & Disruptive Attacks
- Attacks against creds

Trends
- US – China Cyber Agreement
- Chinese TTP

Collecting and Analyzing News Items
<table>
<thead>
<tr>
<th>What news sources are the best OSINT?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media, Forums, Chat: Reddit, Twitter, Telegram</td>
</tr>
<tr>
<td>Local &amp; International Papers &amp; Web News</td>
</tr>
<tr>
<td>Think tanks &amp; Academic Research</td>
</tr>
<tr>
<td>Policy documents &amp; blogs</td>
</tr>
<tr>
<td>Law blogs, court cases, legislation</td>
</tr>
</tbody>
</table>
How do I organize news in my pipeline?

- Major headlines (Local & Intl)
- IOC’s & Pivot Terms
- Low fidelity signals
- Org-specific Google Alerts
- Social Media/Forums/Chat
Ye Olde Google Alert

Alerts
Monitor the web for interesting new content

- **How often**: At most once a day
- **Sources**: Automatic
- **Language**: English
- **Region**: Any Region
- **How many**: Only the best results

Search query: site:nbcnews.com "breaking news"
Case Study: Social Media

News reports via social media
Resource: Omnisci Tweet Map

- [https://www.omnisci.com/demos/tweetmap](https://www.omnisci.com/demos/tweetmap)
- ~1% of tweets are geo-tagged, visualize and filter them here
Filter for Language, Location and Date

“Undetermined” = unclassifiable, but usually interesting (English slang, localized dialects)
Pivoting Opportunities

- Search Twitter & other social media sites with top hashtags
- Use hashtags as keywords in search engine search against recent news articles, translate results
- Look for trends on other services
We're investigating a significant spike in potentially spoofed Internet-wide port scan traffic. This thread will be updated as the situation develops.

Related:

Wew okay, so there's some REALLY bizarre internet-wide scan traffic happening right now in @GreyNoiseIO. It started two/three hours ago, quieted down for a few minutes, then just started up again. I'm going to do my best to stream of conscious what's going on while we dig in:

Show this thread
Jan 3 Traffic increases, Greynoise.io

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Value</th>
<th>% Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>74123</td>
<td>682%</td>
</tr>
<tr>
<td>115</td>
<td>TCP</td>
<td>36772</td>
<td>1175%</td>
</tr>
<tr>
<td>123</td>
<td>TCP</td>
<td>34871</td>
<td>3006%</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>70007</td>
<td>924%</td>
</tr>
<tr>
<td>194</td>
<td>TCP</td>
<td>36313</td>
<td>1211%</td>
</tr>
<tr>
<td>7547</td>
<td>TCP</td>
<td>37787</td>
<td>2937%</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>68391</td>
<td>1834%</td>
</tr>
<tr>
<td>554</td>
<td>TCP</td>
<td>38303</td>
<td>2347%</td>
</tr>
</tbody>
</table>
Jan 3
Anomalies, Greynoise.io

<table>
<thead>
<tr>
<th>Port / Protocol</th>
<th>Unique IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 / TCP</td>
<td>79820</td>
</tr>
<tr>
<td>25 / TCP</td>
<td>62976</td>
</tr>
<tr>
<td>47721 / TCP</td>
<td>20</td>
</tr>
<tr>
<td>21 / TCP</td>
<td>67307</td>
</tr>
<tr>
<td>53 / TCP</td>
<td>20960</td>
</tr>
<tr>
<td>5060 / TCP</td>
<td>38672</td>
</tr>
<tr>
<td>22 / TCP</td>
<td>76101</td>
</tr>
<tr>
<td>36081 / TCP</td>
<td>26</td>
</tr>
<tr>
<td>7 / TCP</td>
<td>38208</td>
</tr>
</tbody>
</table>
News Topic: Health Crisis
DON'T PANIC... YET —

China locks down 35M people as US confirms second coronavirus case

It’s an emergency in China, but not yet for the rest of the world, WHO says.

BETH MOLE - 1/24/2020, 1:30 PM
Fear of coronavirus fuels racist sentiment targeting Asians

By SUHAUNA HUSSAIN | STAFF WRITER  |  FEB. 3, 2020  |  5 AM
A troubling off-shoot of the coronavirus outbreak has started to emerge: racist comments and behavior against China and people of Asian descent.
Corpses and mob violence: How China’s social media echo chamber fuels coronavirus fears

By Joanna Chiu  Vancouver Bureau
Wed., Feb. 5, 2020  5 min. read
It’s a phish!

https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/
News Topic: Internet & Service Outages
Partial internet disruption registered in Iran

Network data from the NetBlocks internet observatory confirm disruptions to mobile networks in Iran on the morning of Wednesday, 25 December. The outage has partial impact and is ongoing at ...

Major internet disruption registered across Iran

Network data from the NetBlocks internet observatory confirm disruptions to multiple fixed-line and mobile providers in Iran on the morning of Thursday, 19 December. The outage had partial but severe ...
Social media partially unblocked in Iraq after 50 days

Network data from the NetBlocks internet observatory confirm that Twitter, Facebook and Instagram, and messaging apps have been restored for many users across Iraq on 21 November 2019. The services ...

Twitter, Facebook and Instagram restricted in Venezuela on day of planned protests

Data from the NetBlocks internet observatory confirm that Venezuela’s state-run internet provider ABA CANTV (AS8048)
How is news OSINT?

Today’s headlines are tomorrow’s phishing campaign lures

Geopolitical context adds data points to attribution exercises

News can inform TTP’s to research and provide pivot points