# Quantifying Threat Actors with Threat Box

**medium.com**/@andy.c.piazza/quantifying-threat-actors-with-threat-box-e6b641109b11

September 18, 2020

## Responses

### What are your thoughts?

### There are currently no responses for this story.

### Be the first to respond.

“Which threat actor should I care about today?” That was a question from my client for a few months that sort of plagued my team. The CISO always engaged in the briefing material our team presented, and he seemed to enjoy our discussions about various threat actors, but we always came back to questions about racking and stacking groups. It was an interesting challenge and I am lucky to have been a part of an awesome team that worked together to develop the first iteration of the Threat Box model.

From that initial framework, I modified category the definitions and scoring criteria, added modifier categories, and conducted threat analysis for three notional organizations that would serve as the backdrop for my second SANS research paper, Quantifying Threat Actor Assessments.

## Why Not an Existing Threat Model

There are a lot of great risk models available on the internet. There are some decent threat models too. Most notable is the threat modeling approach covered in the SANS CTI course (FOR578) and discussed in Katie Nickels’ webcast “The Cycle of Cyber Threat Intelligence”, which looks at an organization through the lens of the data they hold and the actors that traditionally target those data types. I love this model and I think it is a critical part of CTI analysis. However, it does not present well for an executive board for a large organization and it doesn’t address ranking the actors. It does serve as an awesome feeder model to identify which groups to process and present on the Threat Box.

The primary mission of Threat Box is to ingest a mountain of historical reporting, process it through a structured analytical framework to evaluate intentions and capabilities, and output a single slide for executives. None of the existing models hit that requirement, so we created our own model.

## Threat Box Categories and Scoring

Starting out, the intent of the model was to assess threat actor intentions and capabilities. But the intentions and capabilities to do what? To conduct cyber attacks against our organization. Okay. But what kind of attacks? Threat Box addresses four categories of attack:

- **Espionage** — attacks impacting the **Confidentiality** of data or systems
- **Destructive** — attacks impacting the **Integrity** of data or systems
- **Disruptive** — attacks impacting the **Availability** of data or systems
- **Cyber-Crime** — attacks intended for **near-term financial profit**

There's a discussion here that's important to consider. It can be difficult to decide which category ransomware campaigns fall into. My recommendation: if the ransomware campaign appears to be a legitimate extortion attempt, that reporting supports the actor's cyber-crime score. If the campaign appears to be purely destructive in nature, it supports the actor's destructive score.

Intellectual property theft is another discussion point. I consider IP theft as a form of espionage since it doesn't necessarily lead to immediate financial gain. On the flip side, an actor that breaks into an organization and steals intellectual property to immediately sell to another party, that breach would support the cyber-crime score.

## Intent & Willingness

Threat actors are assessed for their intentions to carry out these attacks against the targeted organization to answer, "**Why would this actor target this organization with this type of attack?**" The Intent score is balanced by the Willingness Modifier, which attempts to answer, "**What constraints may impact the actor's intent?**" This modifier considers existing legal, political, and economic dependencies that may lower the threat. For example, there is a pretty low likelihood that the UK will hack the NSA for intelligence they can likely get through their FVEY relationship.

> **Intent: Why would this actor target this organization with this type of attack?**

**5 —** *Target-Specific Data:* $ACTOR targets $ORG based on an objective that can only be achieved within $ORG's network

**4 —** *Ideology Association*: $ACTOR targets $ORG based on its association with a specific ideology (e.g., USG, war, etc.)

**3 —** *Sector Association*: $ACTOR targets $ORG based on its association with a specific business sector (e.g., finance, energy, government)

**2 —***Regional Association*: $ACTOR targets $ORG based on its regional area of operations (e.g., North America, Middle East, etc.)

**1 —** *Target of Opportunity*: $ACTOR targets $ORG simply as a target of opportunity

> **Willingness modifier: What constraints may impact the actor's intent?**

**-0:** Strained diplomatic relations/previous hostilities/significant economic disruption perceived by $ACTOR from $ORG's operations

**-1:** Moderate relations with the U.S. and moderate economic dependencies between $ACTOR interests and $ORG's operations

**-2:** Strong diplomatic, economic, and security ties with the US

## Capabilities & Novelty

Each actor is assessed for their known capabilities for each attack category to answer, "**what evidence is available that this actor is capable of this attack type?**" The *Capability* score is balanced by the *Novelty Modifier* that adjusts the *Capability* score by trying to answer, "**what indication of advanced skills are evident?**" The reality is that threat actors don't bring out the big guns (custom malware and zero days) when the front door is open. This is why the *Capability* score focuses on whether or not the actor has a demonstrated history with an attack type rather than trying to assess their skill level. The *Novelty* modifier was my attempt to give some credit to the Blue Teamers to be able to defend against common TTPs and malware families, while also giving some credit to the adversary that has demonstrated the ability to write custom toolsets and move quietly in an environment.

> **Capability: What evidence is available that this actor is capable of this attack type?**

**5 —** *Significant Capability*: Significant evidence that $ACTOR previously conducted this type of activity; multiple trusted sources confirmed

**4 —** *Credible Capability*: Credible evidence of operational capability; moderately confirmed

**3 —** *Limited Capability*: Some evidence of operational capability; limited sources

**2 —** *Possible Capability:* Very limited evidence of operational capability; feasibility confirmed

**1 —** *Not Capable*: No evidence of operational capability; feasibility unconfirmed

> **Novelty modifier: What indication of advanced skills are evident?**

**-0:** Custom toolset per campaign with demonstrated living off the land capability

**-1:** Limited availability/high-cost toolset used in multiple campaigns

**-2:** Toolset generally available

Well, there is the scoring criteria and the categories that make up the Threat Box threat assessments. Let's talk about applying the model to organizations in the next section.

> **PRO-TIP: Build your threat assessments on existing threat intelligence to prevent the What-If Monster from devouring your team. There is no room for Mr. Tin Foil in threat intelligence.**

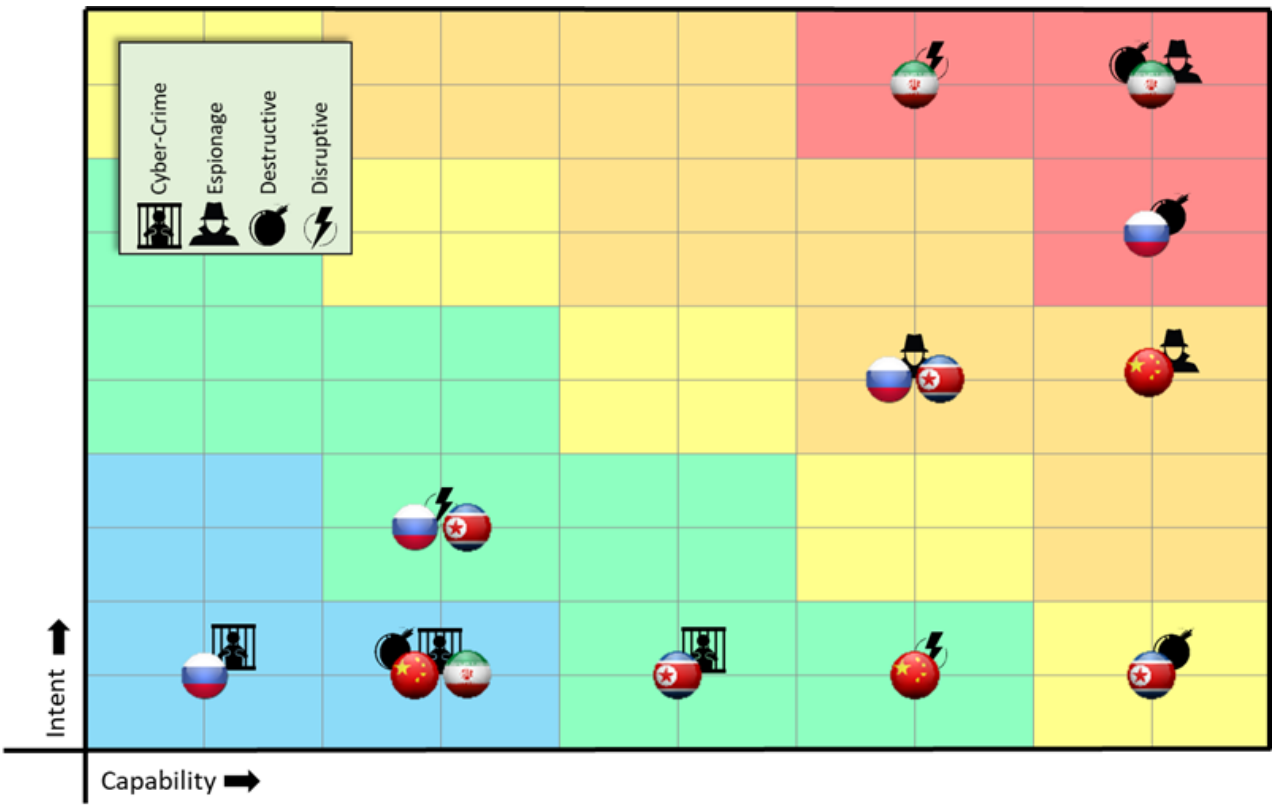
## The Notional Targets and Threat Box Assessments

For my research, I wrote three mock profiles for fake organizations. The idea here is to demonstrate that the model works for any business sector. The scores presented below were calculated by myself using a few open-source repo's of threat reports that I'll include at the bottom of this page. As with all things in infosec, I suspect we'll have some disagreement how these scores washed out. I look forward to that discussion.

## American Oil (AmO)

American Oil is a Texas-based oil company operating ICS manufacturing and operations in the US and Saudi Arabia. A threat analyst at AmO reads a large body of reports on Iranian capabilities, including FireEye's *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware*. The analyst translates the statement "Iran's desire to expand its own petrochemical production and improve its competitiveness in the region" into an intention score of three (3) for "Sector Association." The actor is motivated through their national strategy to compete in the business sector. The briefer's threat assessment may sound something like:

Based on historical events, Iran presents the greatest threat in the categories of destructive attacks and espionage. The infamous Shamoon attack that wiped out tens of thousands of systems at Saudi Aramco facilities in 2012 was the work of the Iranian group known as APT33 (Osborne, 2018). Additionally, FireEye identified APT33 phishing campaigns that targeted oil and petrochemical companies in the Middle East and Saudi Arabia in May 2017 (O'Leary, Kimble, Vanderlee, & Fraser, 2017). It is a national goal of Iran's Deputy Oil Minister, Marzieh Shadaei, to strengthen Iran's petrochemical companies so they "can easily be ranked high on the list of the world's largest petrochemical exporters" (Financial Tribune: First Iranian English Economic Daily, 2016). With both the intention and capabilities to conduct espionage and destructive attacks against energy-sector companies operating in the Middle East and Saudi Arabia, Iran is clearly a 5x5 threat to this fictional American Oil company.




AmO's Threat Box

## United States Government Financial Organization (USGFO)

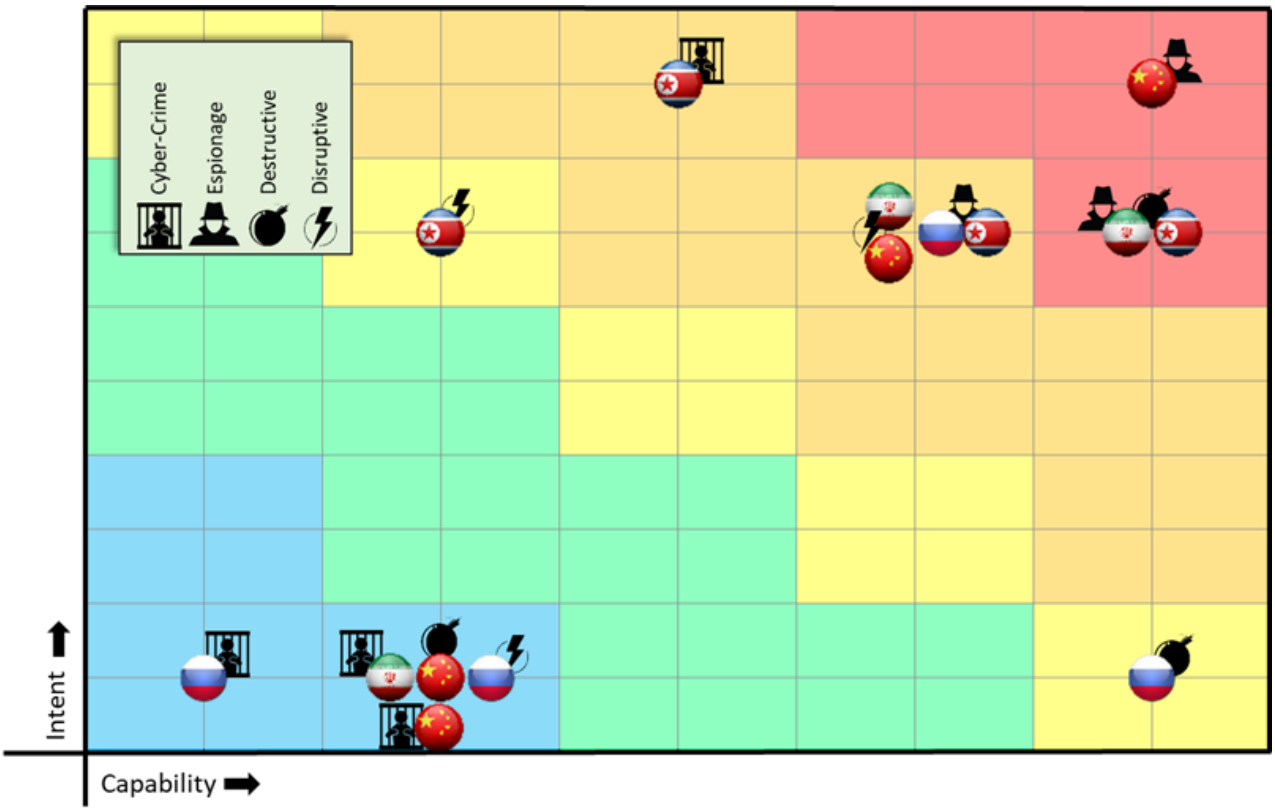
A Washington, DC-based federal agency that processes financial payments for all USG services that are provided to the public.

> **PRO-TIP: I use bold text when prepping briefer notes in case someone else briefs my material, they'll know which elements to ensure they stress.**

China has a long history of conducting bulk theft of sensitive data, including PII and financial records. Their activity has led to the United States' aggressive legal response, which includes multiple Department of Justice indictments against Chinese hackers for the **Anthem medical records theft in 2015** (Department of Justice, 2019) and the **Equifax breach in 2017 (Barret & Zapotosky, 2020**). The FBI has even arrested some of the hackers responsible for the **OPM breach** (Chalfant, 2017). With this record of aggressive large-scale thefts against U.S. institutions, **China is a 5x5 threat to the USGFO for espionage**.

While **not commonly thought** of as a **disruptive** attacker, China's early entrance into the hacking scene began in **1999 with website defacements in the U.S.** after the U.S. accidentally bombed the Chinese embassy in Belgrade (Denning, 2017). Since **the USGFO maintains a public-facing website**, China's **disruptive score** against USGFO received an **intent rating of 4** for ideology association and a **capability rating of 4** for credible capacity.

China received **a willingness modifier of zero** since China has **proven their willingness to carry out these types of attacks**.

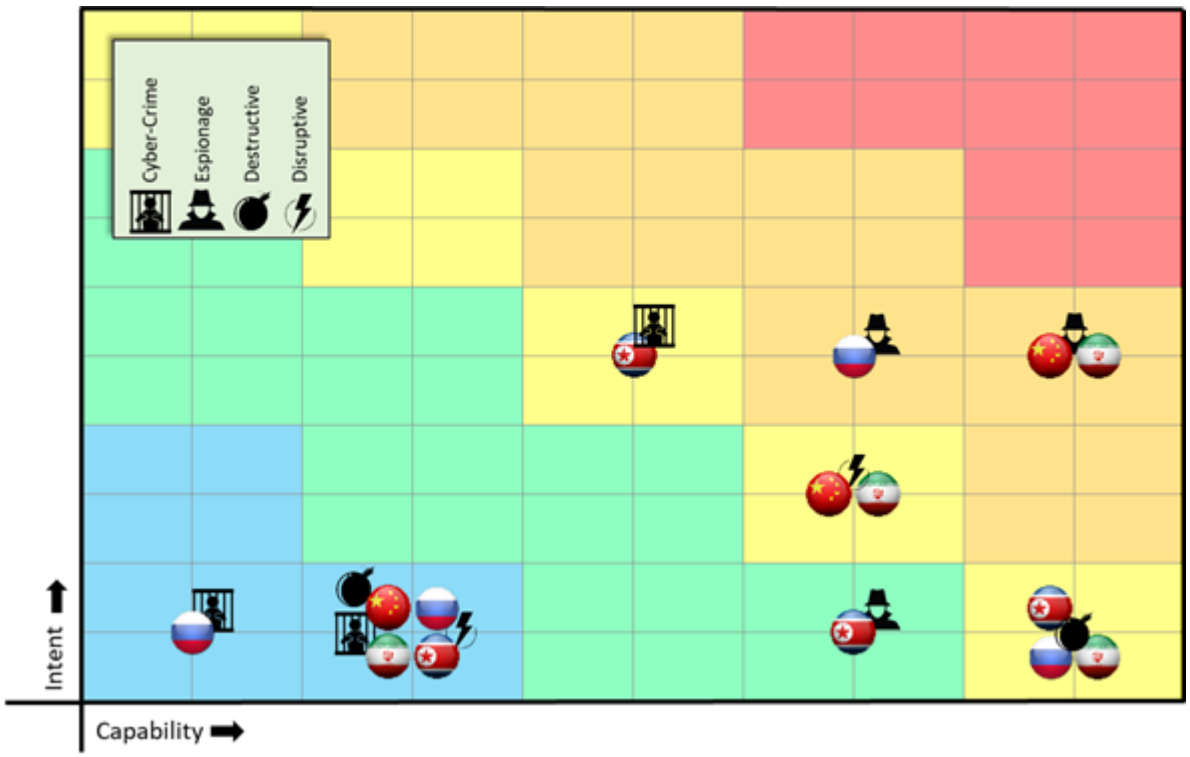



USGFO's Threat Box

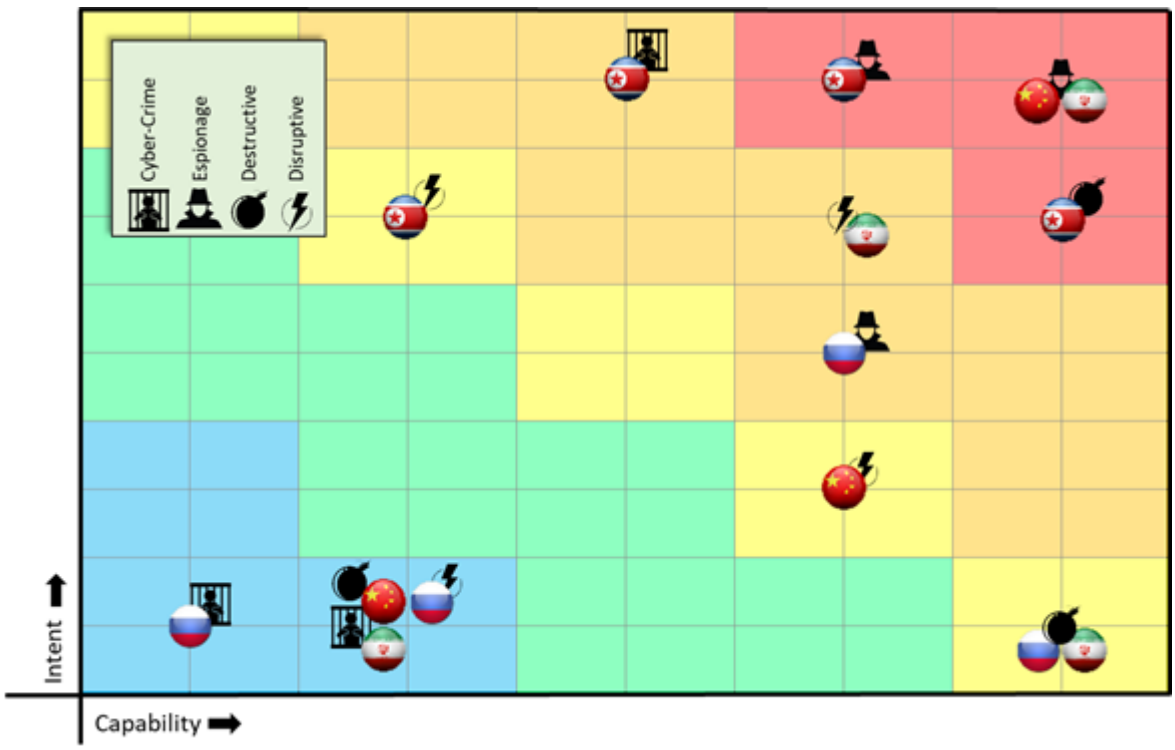
## Information Technology Company (ITCO)

A California-based tech company that offers multiple online services, such as cloud computing and storage, and sells proprietary IT hardware. ITCO conducts two separate Threat Box assessments: one for their **core business network (Enterprise)** and one for the **Services segment** of their network.

The ITCO services Threat Box presents far higher scores than their enterprise Threat Box since the ITCO threat team assessed that threat actors' intentions to target customer data are increased based on ITCO's diverse customer base. As an example, organizations from multiple targeted industries store sensitive corporate data in the ITCO Cloud Services environment. China became a 5x5 threat of espionage based on their Cloud Hopper campaign, where they infamously compromised multiple cloud service providers to steal data from customers of those providers (Stubbs, Menn, & Bing, 2019).




ITCO's Enterprise Threat Box




ITCO's Services Threat Box

## Working with an Awesome Team

All intelligence products should be a team effort, but the Threat Box is 100% a team sport. From the initial ask from our CISO, I had the absolute pleasure of working with, arguing with, and collaborating with an awesome team of really, really smart analysts: Brandy Harris, Jay Kiser, Zack Plunkert, Mike "The 0Day" O'Dea, and Cam Kennedy. As a team,

we worked through building the original model, setting up a framework to rate the actor groups, and conducting the research necessary to complete the assessments for our client. The team has gotten a bit smaller with time, but we are still producing a version of this product for our client each month and we get requests to add it to other briefings and supporting material. Without this team and our shared experience, I could not have built on the model to research and write my SANS paper.

> PRO-TIP: Analyst teams need to have enough trust in each other to be able to constructively argue and challenge each other's positions — and still go get coffee as colleagues afterwards.

## Closing it Out

Hopefully this article isn't a complete mess. If it is, give the full paper a read instead. But here's the basic process as a recap:

1. Read a LOT of reporting,
2. Determine if the reports are discussing espionage, destructive, disruptive, or cyber-crime attacks,
3. Determine the Intent score, consider the Willingness modifier,
4. Determine the Capability score, adjust for the Novelty modifier,
5. Map the actor's scores on the model.
6. Rinse, repeat, and get coffee with your awesome team.

## References and Resources

I had the privilege of discussing my research on the SANS ISC podcast — which is still an absolutely insane honor to me.

## SANS ISC Stormcast: Daily Network Security News Summary; Cyber Security Podcast

### SANS Daily Network Security Podcast (Stormcast) for Thursday, September 17th 2020

#### isc.sans.edu

Here's a link to the full paper:

## SANS Institute: Reading Room - Threat Intelligence

### Featuring 15 Papers as of May 20, 2020 Quantifying Threat Actor Assessments SANS.edu Graduate Student Research by Andy…

#### www.sans.org

Here's a link to my first paper, ATT&CKing Threat Management:

## ATT&CKing Threat Management

### It would be really awesome to map out the most common techniques used by threat actors and prioritize those for…

**medium.com**

Go read everything Katie Nickels has written and check out the SANS webcast I mentioned above, "The Cycle of Cyber Threat Intelligence".

## The Cycle of Cyber Threat Intelligence - SANS Institute

### Too often, our community thinks of cyber threat intelligence (CTI) as just a finished product (or even just an…

**www.sans.org**

Here is a great resource to get a lot of threat reports from one location:

## Threat Actors (powered by MISP)

### Please enable JavaScript to use all features of this site. The following table provides a mapping of the actor groups…

**malpedia.caad.fkie.fraunhofer.de**

The good folks at MITRE ATT&CK have a decent list of actor reports too.

## Groups

### Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110 APT3 is a China-based threat group that researchers…

**attack.mitre.org**

## Supporting References

https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

https://financialtribune.com/articles/energy/41665/call-for-restoring-past-petrochemical-status

https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

https://www.washingtonpost.com/national-security/justice-dept-charges-four-members-of-chinese-military-in-connection-with-2017-hack-at-equifax/2020/02/10/07a1f7be-4c13-11ea-bf44-f5043eb3918a_story.html

https://thehill.com/policy/cybersecurity/347897-fbi-arrests-chinese-national-linked-to-opm-hack-malware-report

http://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469

https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

Written by

## Andy Piazza

**I enjoy writing, mentoring, and sharing knowledge. Read my full bio in my whoami article https://medium.com/@andy.c.piazza/whoami-a5410956fffb**

## More From Medium

## Microsoft Seriously Beefs Up Security in Windows Server 2019

PCMag in PC Magazine


## How to Truly Secure Your Online Accounts—Going Beyond Password Protection

BidiPass in BidiPass

## Basic SSH Security

Josh Rollins in Emacs

## Hackers are Ready to Exploit Zero-Day Flaws; Companies are Slow to Act

ReadWrite in ReadWrite

## Discover Medium

**Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch**

## Make Medium yours

**Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore**

## Become a member

**Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade**