MIS|TI™ PRESENTS

InfoSecWorld

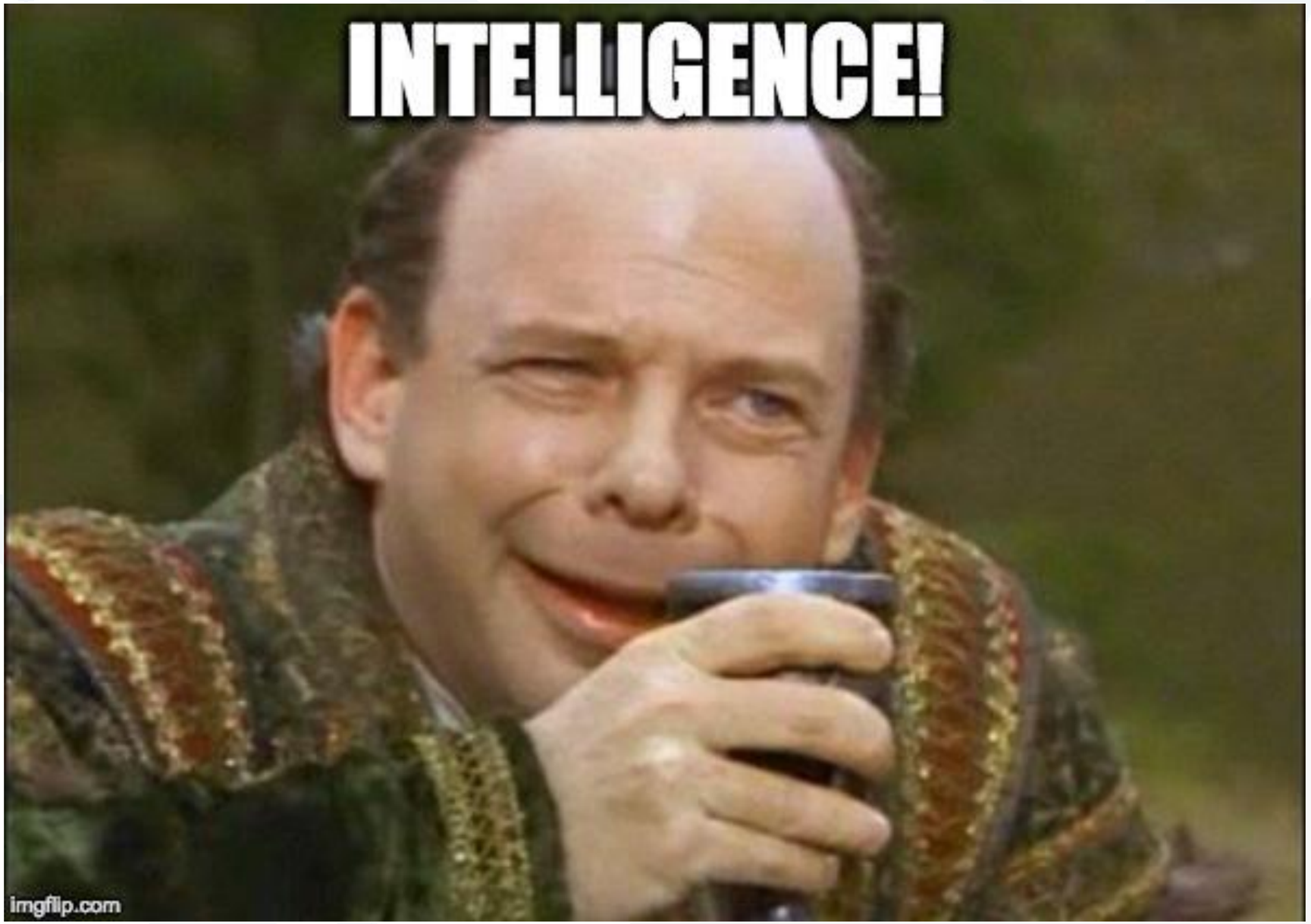
Conference & Expo 2018

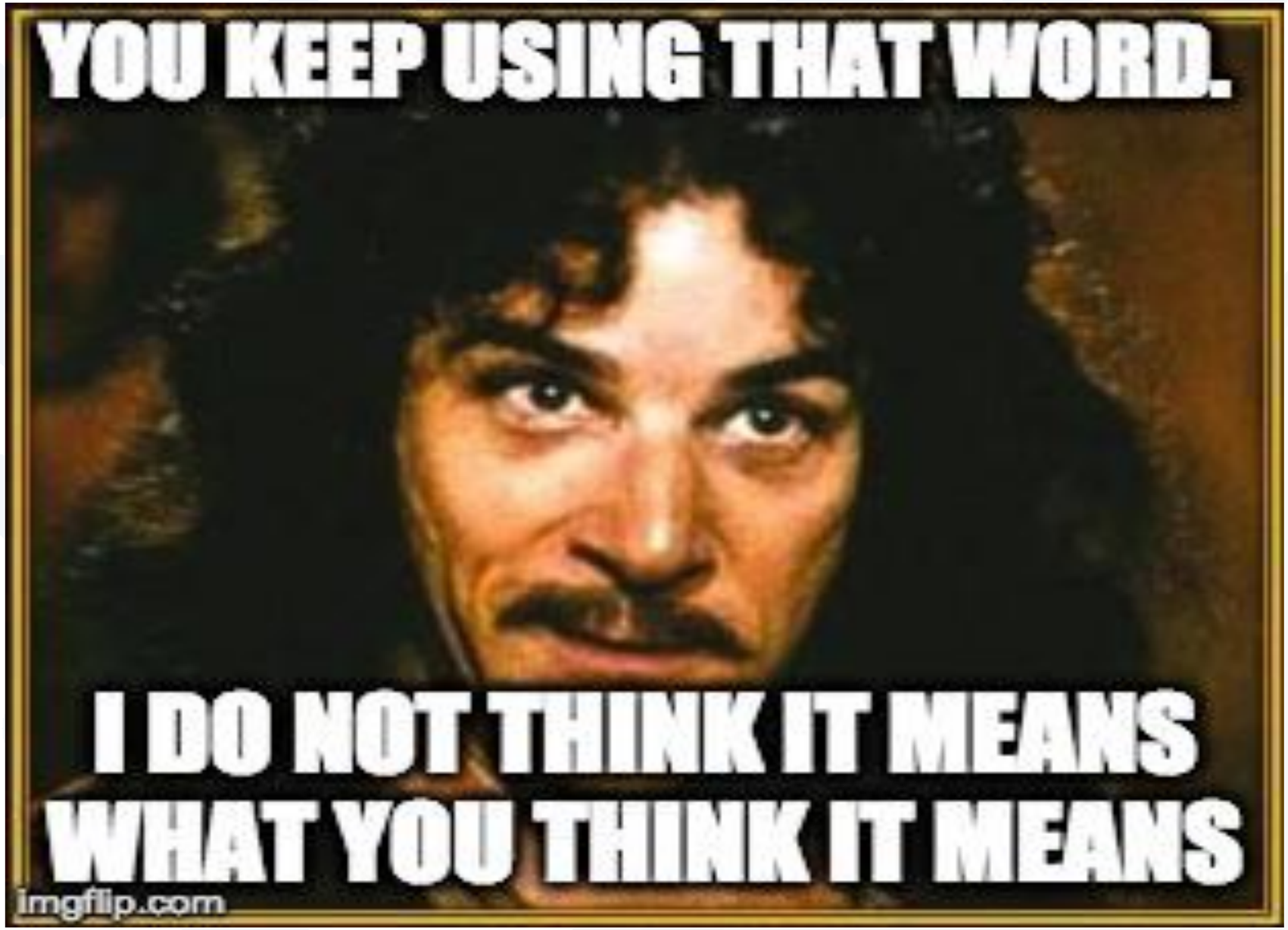
HACKING INTELLIGENCE:

THE USE, ABUSE, AND MISAPPROPRIATION OF INTEL FOR FUN AND (MOSTLY) PROFIT

Mark Arnold, Navisite

Will Gragido, Digital Guardian


INTELLIGENCE!
imgflip.com


YOU KEEP USING THAT WORD.
I DO NOT THINK IT MEANS
WHAT YOU THINK IT MEANS
imgflip.com

Intelligence Bias

SEMANTIC BIAS: NAMED ENTITY RESOLUTION (NER) IN SOCIAL MEDIA (WATERS, 2016)

בְּרֵאשִׁית בָּרָא אֱלֹהִים אֵת הַשָּׁמַיִם וְאֵת הָאָרֶץ׃

In the beginning, God created the heavens and the earth.

In the beginning, see God, the heavens, and the earth. GT

Au commencement, Dieu créa les cieux et la terre.

Au commencement, voyez Dieu, les cieux et la terre. GT

"Questions about fairness and bias in machine learning are tremendously important for our society, We have a situation where these artificial intelligence systems may be perpetuating historical patterns of bias that we might find socially unacceptable and which we might be trying to move away from."

- Arvind Narayanan, an assistant professor of computer science and an affiliated faculty member at the Center for Information Technology Policy (CITP) at Princeton University, as well as an affiliate scholar at Stanford Law School's Center for Internet and Society.

COGNITIVE BIAS: REDDIT READ IT WRONG (2013)

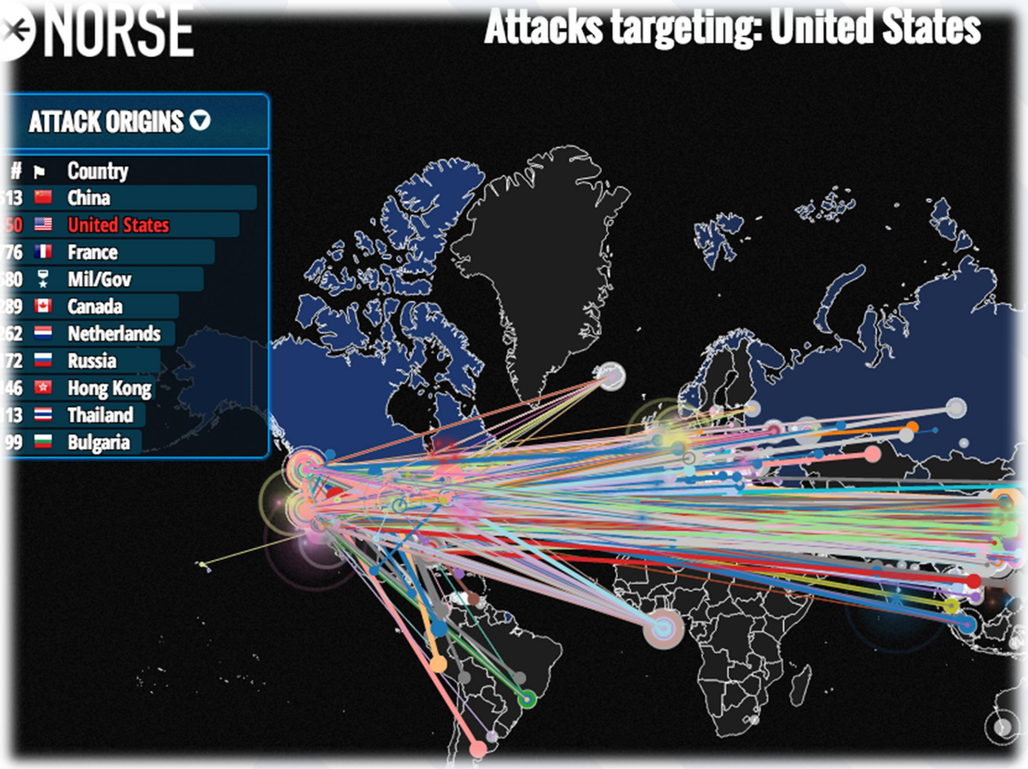
"We were very worried about Sunil and about each other because of how fast completely unsubstantiated claims were spreading."

- Sangeeta Tripathi sister of Sunil Tripathi

POLITICAL BIAS: NOT YOUR AVERAGE BEARS

"I really hope you've missed me a lot. Though I see they didn't let you forget my name." - Guccifer

ABSOLUTE BIAS: FALL FROM GRACE (2016)



The Growing Cyber threat from Iran, a.k.a. The Initial Report of Project Pistachio Harvest report was deemed “deeply biased” and “headline-grabbing” based on false data.

- Brian Krebs


"…If you're not reading the intelligence you're flying blind…"
– Jeh Charles Johnson, 4th United States Security of Homeland Security
InfoSecWorld
Conference & Expo 2018

FOLLOWING SUIT…WE'RE GOING TO TRY AND ANSWER THE FOLLOWING

1. What is "intelligence" as it is defined by the military and intelligence communities?
2. Why in the last decade has "doing" intelligence become so important to SMBs and enterprises alike?
3. Intelligence Tradecraft – are the organizations seeking to "do" intelligence prepared, equipped, and capable of conducting tradecraft successfully?

INTELLIGENCE DEFINED

”

1. *Dictionary of United States Military Terms for Joint Usage* (Revision of February 1957)
   "Intelligence - the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to planning.”

2. *A Training Handbook*
   "Intelligence-The product resulting from the collection, evaluation, collation, interpretation, [and] analysis of all available information concerning the intentions, capabilities and objectives of other countries which are significant to a government's development and execution of plans, policies, decisions, and courses of action.”

TYPES OF INTELLIGENCE AND INTELLIGENCE GATHERING DISCIPLINES

Intelligence Gathering Disciplines

1. **HUMINT**
   - Collected by and from people on the ground
2. **GEOINT / IMINT**
   - Collected via satellite, aerial photograph, and mapping & terrain data
3. **MASINT**
   - Measurement and signal intelligence
4. **OSINT**
   - Collected from open sources
5. **SIGINT**
   - Collected from intercepted signals
6. **TECHINT**
   - Collected by analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions.
7. **CYBINT/DNINT**
   - Collected from cyber space
8. **FININT**
   - Collected from the analysis of monetary transactions

WHAT LEAD TO THE EXPLOSIVE POPULARITY OF INTELLIGENCE SECURITY AND WHY ARE ORGANIZATIONS PURSUING IT EN MASSE?

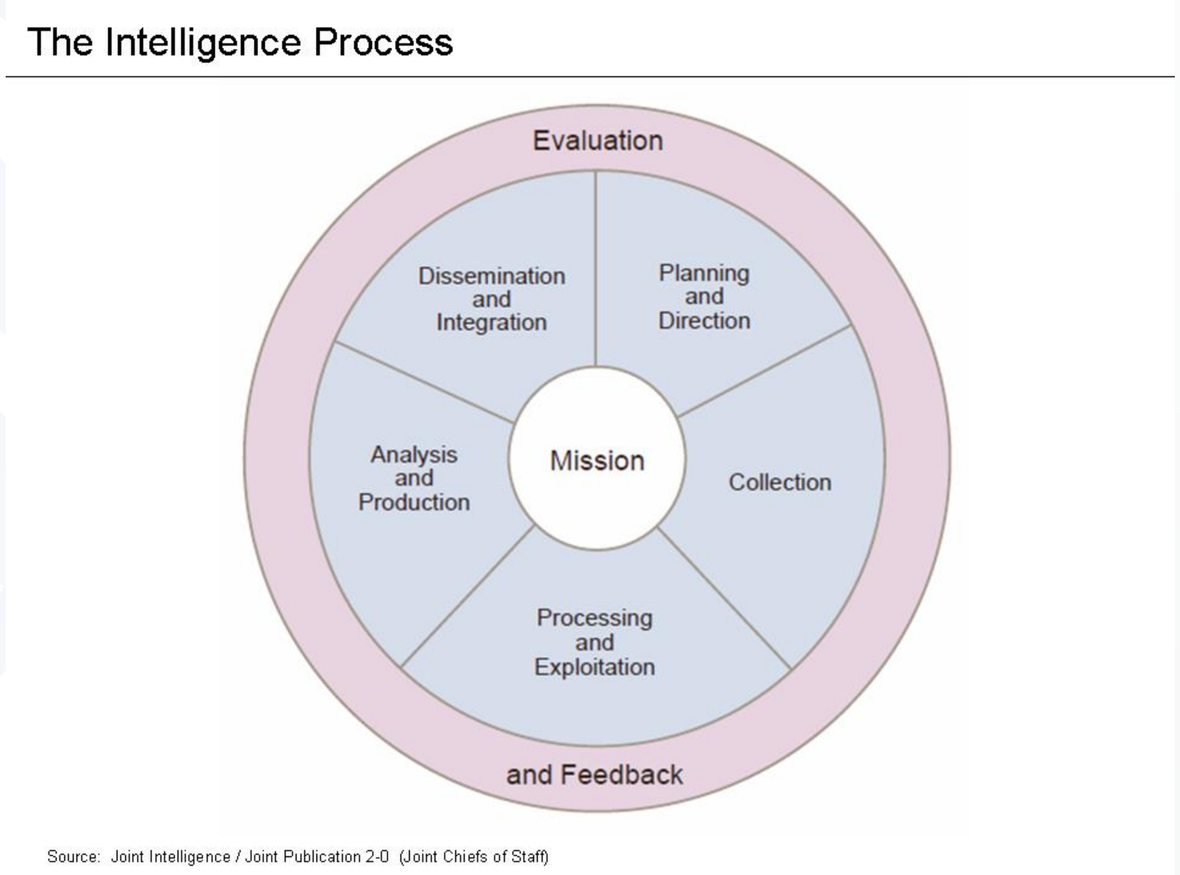
- Generic “hacker” / “miscreant” behavior?
- Evolution and maturity of cyber criminals (advent of traditional organized criminal organizations entering “cyber”)?
- Advanced Persistent Threat (APT)?
- Nation State proxy?
- Nation State?
- Overly aggressive marketing entities?

EFFICACY: ORGANIZATIONS “DOING” INTELLIGENCE GOOD, BAD, UGLY?

- Are organizations endeavoring to “do” intelligence doing so successfully?
- The numbers (DBIR for example), would suggest that we’ve got some work to do….
- Are they equipped properly?
- Are their results differentiating? Do they show in quantifiable and qualitative ways that their efforts are paying dividends?
- This goes for vendors of threat intelligence too…

INTELLIGENCE TRADECRAFT

- What is “tradecraft”
  - (DoD/IC) tradecraft can be defined as:
    - Techniques, methods, and technologies used in espionage.
  - In information / cyber security circles it can be defined as:
    - Techniques, methods, and technologies used in defending organizations, personnel, and their interests against adversaries – internal and external alike



INFORMATION / CYBER SECURITY TRADECRAFT

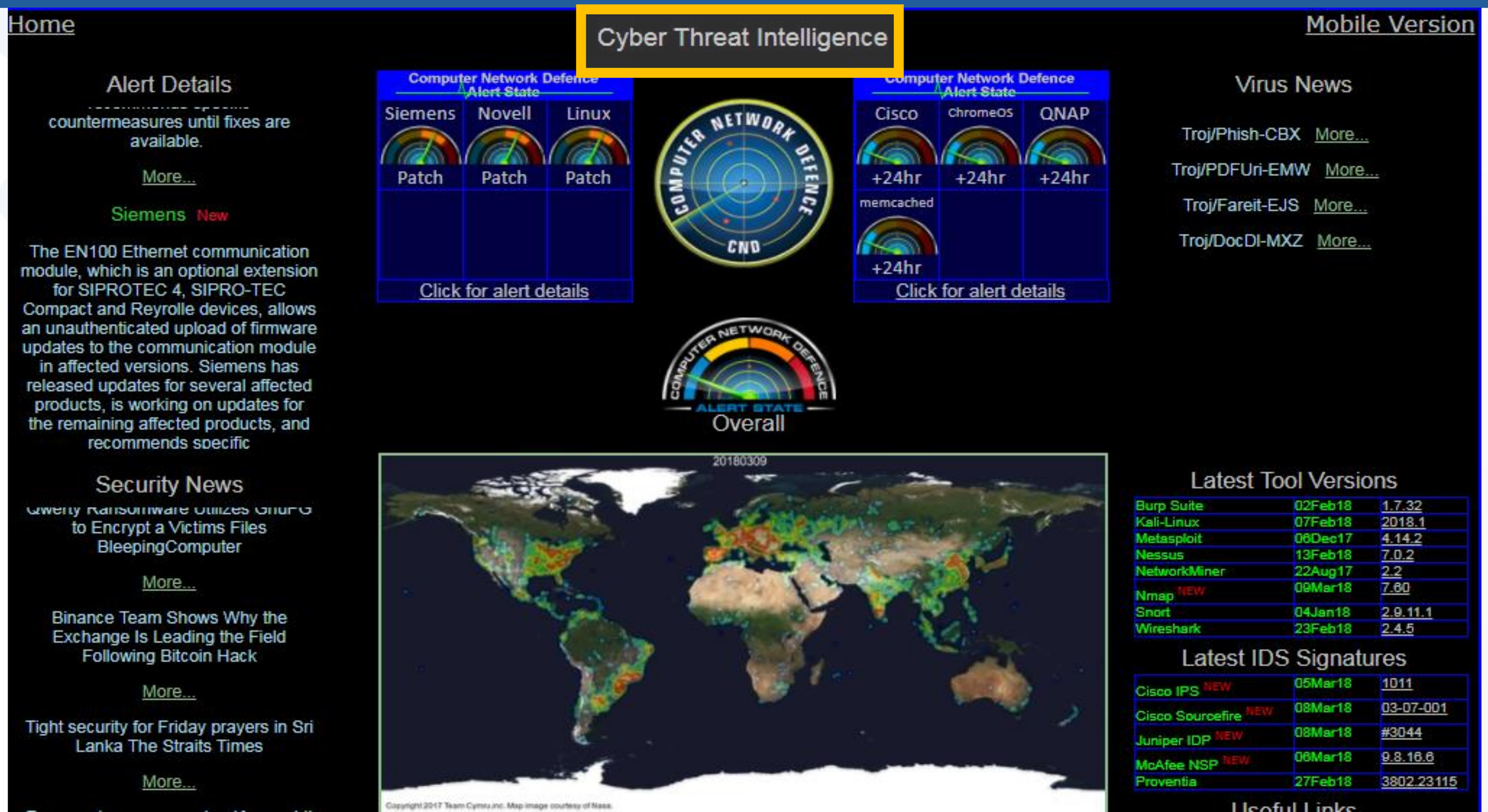
- Understanding of the “Intelligence” life cycle
- Priority Intelligence Requirements (PIR)
- Collections process flow
- Collections tools and targeting
- Hunting
- Understanding and incorporation of TTPs, IOCs, IOAs
- Adversarial profiling
- Organizational & personnel profiling
- Understanding of which intelligence gathering disciplines play a role in “cyber” for the lay person
- Understanding of to taxonomical models
- Glossary terms
- Analytic techniques
- Production workflows
- Deliverable production and dissemination

ALL THE THREAT THINGS. ALL THE PROMISES

"I saw your InfoSecWorld interview. I liked how you guys discussed understanding effectiveness of an ecosystem against weaponized intelligence specific to that organization or ecosystem. At **<vendor>** we've seen our innovative platform help with that. The architecture allows for the safe execution of real attack behaviors, and while we have content available for organizations to sequence the actions into behavior for launch, we also allow for intel from organizations like **[SourceA]** or info from an **[SourceB]** to be weaponized."

InfoSecWorld
Conference & Expo 2018

DOES YOURS LOOK LIKE THIS?



Hacking Intelligence?

FRIENDS WITH BENEFITS

- Hub & Spoke
- Source/Subscriber
- Peer-to-peer

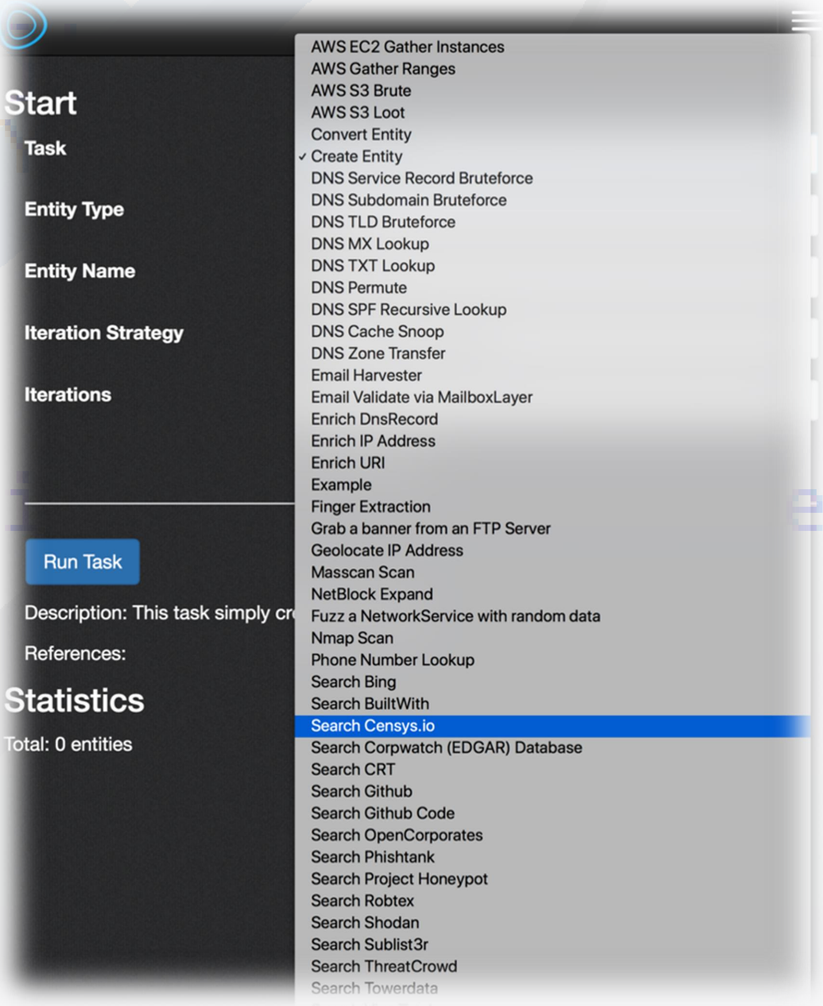
CLOSED SOURCE: TRUST NO ONE, ROLL YOUR OWN

Without understanding context, **relevance**, accuracy, or known associations, however, you can’t see the broader picture…

OPEN SOURCE: DIY

SHODAN
Computer Search Engine

censys



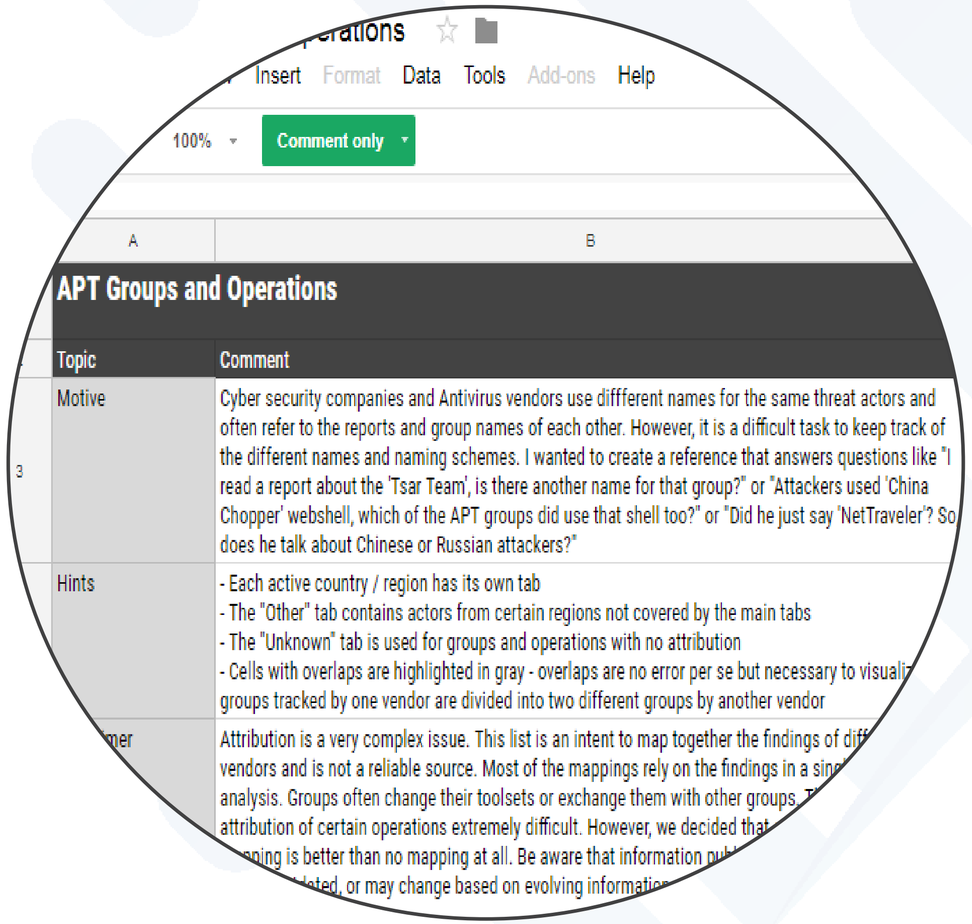
LOCAL HELP: REGIONAL INTELLIGENCE RESOURCES

THE EXCHANGES

OPEN THREAT EXCHANGE

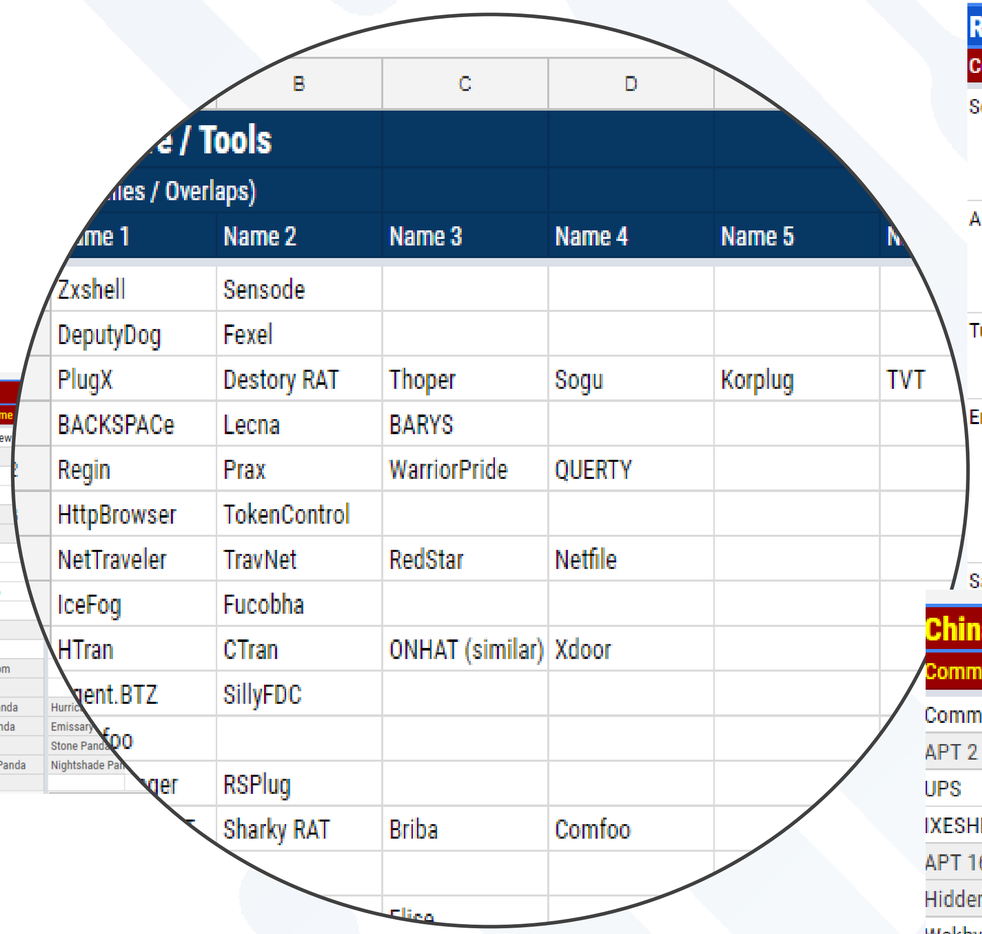
facebook ThreatExchange

CROWDSOURCED INTEL?: PRUDENT? RESPONSIBLE?



DOC DISCLAIMER - Attribution is a very complex issue. This list is an intent [sic] to map together the findings in a single incident analysis

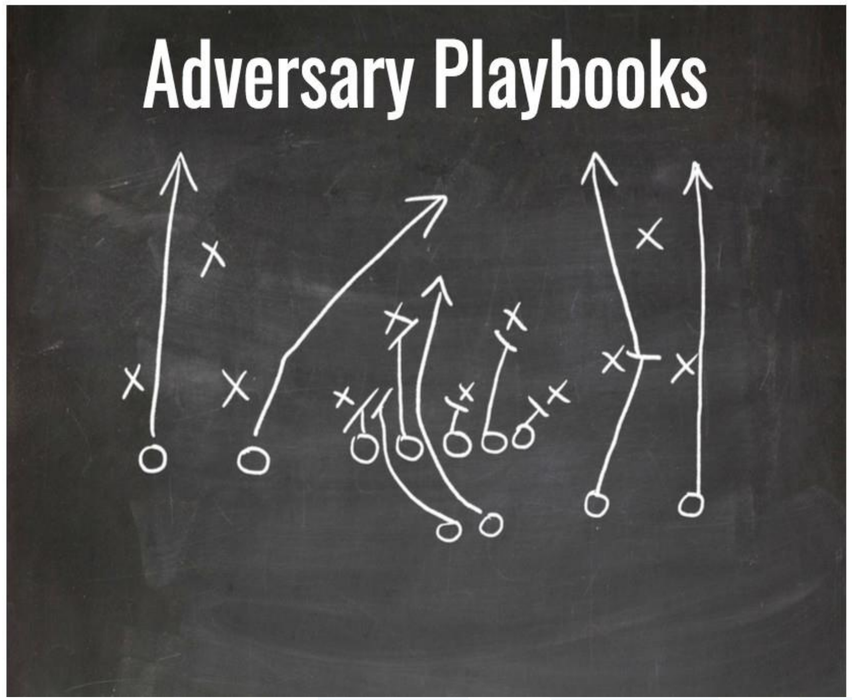
CROWDSOURCED INTEL: PRUDENT? RESPONSIBLE?



Russia								
Common Name	Other Name 1	Other Name 2	Other Name 3	Other Name 4	Other Name 5	Other Name 6	Other Name 7	Other Name 8
Sofacy	APT 28	Sednit	Pawn Storm	Group 74	Tsar Team	Fancy Bear	Strontium	Swallowtail
APT 29	Dukes	Group 100	Cozy Duke	EuroAPT	Cozy Bear	CozyCar	Cozer	Office Monkeys / TEMP.Monkeys
Turla Group	Snake	Venomous Bear	Group 88	Waterbug	Turla Team	Krypton	Uroburos	SIG23
Energetic Bear	Dragonfly	Crouching Yeti	Group 24	Koala Team	Bersek Bear	Anger Bear		
Sandworm	Sandworm Team	TEMP.Noble	Electrum	TeleBots	Quedagh	BE2 APT		

China									
Common Name	CrowdStrike	IRL	Kaspersky	Dell Secure Works	Mandiant	FireEye	Symantec	iSight	Cisco (VRT/Sour
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36
UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6
IXESHE	Numbered Panda			TG-2754 (tentative	APT 12	BeeBus		Calc Team	Group 22
APT 16					APT 16				
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8
Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18				
Axiom					APT 17			Tailgater Team	Group 72
Winnti Group	Wicked Panda								
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13
Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30				
PLATINUM									
Lotus Blossom			Spring Dragon						
APT 6					APT 6				

FUTURE OF INTELLIGENCE: ADVERSARY PLAYBOOKS (HOWARD, 2018)



The norm of the day is to share indicators of compromise about adversaries with little or no context about the sequence of events or the motivations. Most of us have no idea if we have multiple controls in place down the kill chain for specific adversaries. We kind of treat security controls as giant sets of prevention and detection instead of focusing on the adversaries that are attacking us

- Rick Howard, CSO Palo Alto Networks

unit42

PLAYBOOK VIEWER

PLAYBOOKS

OILRIG

SOFACY

Sofacy (also known as Fancy Bear, APT 28, STRONTIUM, Pawn Storm) is a highly active actor with a Russian nexus. They have been active since the mid 2000s, and have been responsible for targeted intrusion campaigns against various industry vertical such as but not limited to Aerospace, Defense, Energy, Government and Media. Extensive observation and research of Sofacy's activities over time indicated a profile closely mirroring the strategic interests of the Russian government. More recently, this group has been attributed to the GRU, Russia's premier military intelligence service as reported by the US intelligence community within several declassified public documents.

This adversary has been observed to have access to a wide range of implants, such as Coreshell, XAgent, Xtunnel, SofacyCarberp, as well as a variety of malware for non Windows platforms such as Linux, macOS, IOS, Android, and Windows Phones. They are also known for registering domain names closely resembling domains of legitimate organizations they are planning to target. Often times, credential harvesters may be deployed onto these sites in order to gather credentials to be repurposed for post-exploitation operations.

Several high profile intrusions have been publicly linked to the Sofacy group, such as the German Bundestag, France's TV5Monde TV station, the Democratic National Committee, the World Anti-Doping Agency, and the Ukrainian military.

January 2018 t

Intrusion Set: Sofacy **Campaigns:** 1 **Indicators:** 11

RECON	WEAPONIZATION	DELIVERY	EXPLOIT	INSTALL	COMMAND
Identify business relationships	Acquire and/or use 3rd party infrastructure services	Conduct social engineering or HUMINT operation	Authorized user performs requested cyber action	Hidden Files and Directories	Remote File Copy
	Remote access tool development	Spear phishing messages with malicious attachments		Process Injection	Data Encoding
	Install and configure hardware, network, and systems	Acquire and/or use 3rd party infrastructure services		Rundll32	Standard Application Layer P
	Obfuscate or encrypt code	Remote access tool development		Software Packing	

HOW TO HACK INTELLIGENCE

- Best Practice – Better than best
  - Attacker Ghost Stories (Mubix)
  - Nightmares of a Pentester (Nickerson)

SOURCES | REFERENCES

- Brown, Rebekah and Roberts, Scott. *Intelligence-Driven Incident Response: Outwitting the Adversary*. Minneapolis: O'Reilly, Sebastopol 2017
- Gragido and Pirc. *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011*
- Christopher Nickerson. Nightmares of a Pentester. Accessed, March 1, 2018 *http://www.securitytube.net/video/14978*
- Robert Fuller. Attacker Ghost Stories accessed March 1, 2018 *https://www.youtube.com/watch?v=yxhQF6E8kO0*
- Sergio Caltagirone. "Why Threat Intelligence Sharing is Not Working: Towards An Incentive-Based Model" accessed March 13, 2018. http://www.activeresponse.org/threat-intelligence-sharing-not-working-towards-incentive-based-model/
- Layton, R., and Paul A. Watters, eds. *The Automating of Open Source Intelligence* Waltham, Syngress, 2016.

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Mark Arnold, Navisite

Will Gragido, Digital Guardian