vb 2019 LONDON 2 – 4 October 2019

KING OF THE HILL
NATION-STATE COUNTERINTELLIGENCE FOR VICTIM DECONFLICTION

Juan Andres Guerrero-Saade
Chronicle, USA

jags.sec@gmail.com

ABSTRACT

Cyber situational awareness is the ultimate outcome of mature threat intelligence. Though we normally think of threat intelligence as a defender's practice, extensive study of advanced cyberespionage operations reveals that attackers are engaged in a similar activity. Defenders apply threat intelligence insights to ensure that attackers don't gain persistent access to their enterprise machines. Similarly, attackers monitor for the presence of other threat actors to ensure that they're the sole owners of a given victim box. While allied organizations engage in a bureaucratic process of victim deconfliction, it turns out that adversarial organizations have turned to embedding anti-virus-like techniques into their malware in order to do the same. This paper will focus on in-the-wild examples of these techniques and provide a conceptual framework for understanding adversarial deconfliction and its ramifications.

INTRODUCTION

Increased public scrutiny over the past decade has pulled the curtain back from broad features of the digital espionage arms race. This has astronomically increased our overall awareness of the breadth of active operations. However, salient features of professional-grade digital subversion operations remain shrouded in mystery. Our collective understanding lacks specificity when it comes to motivators, edge cases, power dynamics, operational paradigms, and strategic considerations. If anything, the parallel rise of an industry of attack mimicry[1] has led us further astray by falsely assigning the simplicity of pre-arranged microcosmic engagements to unexpected macro-scale in-the-wild operations. The reality of intra- and inter-national operations[2] entails multitudinal complexities befitting of an arm of intelligence, military strategy, and international relations.

Beyond first impressions, we find that the simplest aspect of digital espionage may in fact be the tooling itself, the very artefacts over which the malware analysis industry routinely obsesses. Depending on the calibre of threat actor, the tooling will range from astounding technical pirouettes to barely functioning slapdash code. It turns out that both extremes can result in either mission failure or success – effectively decoupling the quality of the tooling from the mission's outcome. Flying in the face of the natural inclinations of a predominantly technical industry, we will instead focus on the operational paradigms and attacker dynamics that impel, shape and limit the more organized tranche of operations we observe in the wild (ItW). Let's briefly discuss how institutional paradigms shape

[1] Under benign monikers like 'penetration testing', 'red teaming' or 'offensive security'.
[2] Be they enablers of espionage, sabotage, psychological or 'hybrid warfare'.

operational dynamics and focus on one particularly elusive tenet observed by a subset of actors, deconfliction.

ACTIONS MIRRORING STRUCTURE

To better understand professional operations, we are required to acknowledge the heterogeneity of a field of actors with diverse motivations, institutional practices, cultures and interests. Not only do these actors operate differently – displaying diverse procedural propensities and tooling preferences – they also operate within an established institutional paradigm. Just because the means of spying are new doesn't mean that technical operators will get to trample established institutional practices, reinvent collection priorities, or subvert the political stability of their sponsor organization. While threat intel analysts may recoil at the seemingly superfluous addition of an another layer of complexity, institutional paradigm is a factor in threat actor decision making and we'd do well to observe it to the degree that it's discernible from an outsider's vantage point.

The operating thesis is that adversary behaviours reflect their institutional configuration[3]. As such, threat intelligence analysts may profile an institutional paradigm based on observable features of an adversary's operations. The inverse principle applies as well. Understanding an institutional tenet followed by the adversary should allow us to predict and prescribe in-the-wild concerns and subsequent decision making. While the first formulation was explored in a previous paper on adopting behavioural profiling for threat actors, the latter inversion is the thesis belying this paper. Let's discuss examples of the former as a backdrop for the inverted thesis.

A diverse operations space

We must resist the temptation to gentrify the threat actor menagerie. Western actors involve readily relatable mores but the heterogeneity of known threat actors involves a far wider gamut of organizational dynamics. In some cases, the operational means and motivators stand in direct opposition to familiar Western principles. Juxtaposed with bureaucratic restraint, the foreign cadres of digital spies often resort to unbridled opportunism. Covertness and prolonged access – cornerstones of the seasoned threat actor – are sometimes sacrificed in favour of garish attention-seeking displays of newfangled 'ability'.

Whether temporarily disabling a movie studio or denying access to online banking across a region, petulant displays of newly acquired capabilities have earned disproportionate attention from an international business community concerned with the fragility of essential systems and the 'irrationality' of their destabilizers. As low-tier operational capabilities proliferate, technical hegemony is effectively combated with nefarious audacity and a disconcerting comfort with occasionally spectacular failure. It's reasonable to speculate that non-Western clusters of nation-state activity[4] should also reflect the cultural, political and socioeconomic idiosyncrasies of their provenance[5].

[3] A thesis discussed at greater length in a previous paper [1].

[4] 'Nation-state activity' hereafter serving as an umbrella term for multiple operational arrangements, including in-house or directly state-sponsored, nation-state adjacent, or criminal-opportunistic offensive activities that align with political requirements.

[5] As responsible analysts, we must consider the possibility that these 'observations' merely reflect our own biases – retroactively assigning cultural patterns and institutional motivations entirely foreign to the operators involved. No amount of rhetorical handwringing should do away with this lacuna of understanding, analogous to the late Wittgensteinian anxiety over an observer's inability to discern whether a third party is *following* a pattern or merely acting in *accordance* with it from an observer's perspective. We forge ahead with the uncertainty rather than cheaply resolve it.

We could decide to interpret the Chinese-adjacent clusters' propensity for state-enabled intellectual property theft as unfolding from a sociocultural fabric whose notion of ownership centres around the effective production of an item and not the original inception of its design [2, 3][6]. Alternatively, prolific intellectual property theft may be the result of established political-economic incentives that arise in a state with customary direct ownership and intervention in 'private' enterprises – not to mention the state's emphatic engagement in a global competition for economic expansion.

In practice, the recurring appearance of poorly segmented operations where state-sponsored threat actors engage indiscriminately in both espionage operations and intellectual property theft operations could lend credence to that institutional dynamic. But perhaps that's simply affirming a reductionist bias where we could be witnessing a dynamic arising from the extensive use of external groups[7] feeding multiple appetites (i.e. reliance on mercenary groups for state espionage who happen to moonlight in IP theft for enterprise clients).

Blended resources

Russian threat actors present another organized cluster of activity that exhibits unusual operational dynamics. This cluster includes well-established government threat actors like Turla[8] and the infamous 'Hades'[9] [5] cluster. Beyond these more-or-less official umbrella actors, there's an established history of 'blended operations' involving criminal elements reporting to state officers or acting on behalf of state interests. Perhaps this dynamic is symptomatic of a 'Mafia state' [6] where the interests of organized crime and the state are largely the same. Or maybe we are seeing the effects of a school of intelligence that regularly employs leverage on compromised individuals to incite cooperation.

Russian operations involving criminal operators or 'contractors' were reported as early as the mid-1980s. At the time, West German hackers were observed stealing information from US institutions and selling it to the KGB. The episode was epitomized in Clifford Stoll's seminal tale [7] of chasing hackers across the Lawrence Berkeley National Laboratory networks. His ingenuity – at a time before most conventional network defence systems were available – not only led to the capture of Markus Hess and his co-conspirators [8] but also established multiple links to the KGB buyers, including the involvement of a Hungarian intermediary acting on fabricated stolen information.

More recent examples gained notoriety due to recent criminal indictments leading to new additions to the FBI's Most Wanted hackers list:

First, Latvian-born Russian national Alexsey Belan [9] was indicted for his alleged cooperation with two Russian agents to hack *Yahoo Mail* in 2013. *Yahoo* revised original estimates of affected user

[6] Including explicit monetary incentives for the improvement of production processes with outright disregard for patents in the pursuit of state interests.

[7] Considering the possibility that these 'external outfits' were intentionally created to cultivate distance equivalent with plausible deniability.

[8] Turla (a.k.a. Snake, Uroburos, Venomous Bear, MOONLIGHT MAZE and KRYPTON) has been operating for more than two decades with a variety of toolkits [4].

[9] The Hades cluster includes the better-known Sofacy (a.k.a. APT28, Fancy Bear, STRONTIUM) threat actor, whose storied past includes the hack-and-leak operations around the 2016 US elections. I use *Kaspersky*'s umbrella term 'Hades' specifically because it covers newly discovered subteams, including on-the-ground (i.e. in situ) teams. The Dutch arrest of one of these teams during an operation provides us with a de facto recognition of the involvement of Russian state operatives in the Hades cluster. Artifacts collected during the arrest reportedly correlate with multiple previously known Sofacy attacks.

accounts to three billion [10]. Belan had previously been indicted for unrelated computer crimes such as holding databases for ransom and identity theft. There's speculation [11] that these early indictments motivated Belan's recruitment by Russian security services to conduct the *Yahoo* hack.

Similarly, in 2015 the FBI announced a three-million-dollar reward for any information that could lead to the arrest of Evgeniy Bogachev. The latter gained infamy for his development of GameOver ZeuS, a widespread crimeware botnet used primarily for banking fraud and ransomware distribution. Bogachev's criminal empire alone warranted law enforcement scrutiny. Yet, a less reported dimension of the GameOver ZeuS operation is its selective use for espionage operations in specific localities. In 2015, *Fox-IT* researchers reported [12] that the botnet was leveraging specific queries on Georgian, Ukranian and Turkish victim systems. The queries were intended to collect documents with classification markings and information related to local intelligence services.

Whatever institutional paradigm may be fostering these dynamics, Russian groups display a peculiar propensity for employing resources blended from multiple spheres. They exhibit fluid interplays between in-house talent, contracted private talent and criminal elements in order to conduct official operations. That same institutional fluidity finds creative expression in the operational aftermath where pilfered materials are leveraged to cause mayhem in unexpected ways: disguising their provenance, abusing public trust, and enlisting unwitting cooperators to amplify effective distribution. Perhaps we should attribute their creative modus operandi to a well-established school of espionage unrestricted by convention in accomplishing its goals. Or perhaps we are meant to believe these operations are entirely the work of 'patriotic hackers' [13] who, like artists [14], wake up with the sudden inspiration to hack in a manner aligned with Russian state interests.

AN INVERTED APPROACH

Each cluster and region tempts us with multiple analytical paths (i.e. interpretative assignations). However, we cannot avoid the possibility of bias distorting the analytical product, particularly when it comes to attribution-based oversimplifications[10]. If our intention is to discern an organizational order and principled influence, we should examine a case where organizational structure is known to exist in the first place and tenets are observed by direct admission of the subject of study. In other words, rather than looking for guiding principles where there may be none, let's start with a principle that a subset of actors has admitted to working towards and trace its manifestation in operations observed in the wild.

A discreet struggle with principles

For example, notable Western nations contend with observance of: the rule of law, civil rights, democratic principles, preassigned jurisdictions and areas of operation, international alliances and treatises, tooling equities and priorities, possible economic ramifications, the adverse effects of inadvertent civilian and private-sector oversight, considerations of proportionality and collateral damage, and respecting the autonomy of corporate intermediaries who may wittingly cause mass technical interference[11]. Recognized arms of said governments implicitly inherit these principles through established practice, institutional oversight, and a bureaucratic segmentation of operations.

[10] Exceedingly common in our field, where attribution is based on a combination of fungible indicators and gut feeling. The country provenance is then used to make statements about entire nations as singular homogeneous entities. Accuracy seldom makes an appearance at this level of anecdotal abstraction.

[11] As in the case of service providers who decide to roll out defence measures to protect their customer base en masse.

In the case of Western state-sponsored threat actors, the aforementioned principles may prove the single greatest strictures of their operational paradigm. Where some believe that the covertness of digital operations relaxes the concern for democratic principles, when it comes to this cluster of actors, evidence largely points to the contrary[12]. Observed principles are expressed in the form of self-imposed technical limitations. One example is the use of seemingly arbitrary *kill switches* in exploits and malware execution (i.e. malware designed to stop operating at a date relative to an administrative handover). Another example involves disinfecting victims when they appear to operate from within a given nation's IP range.

Restrained actors have arbitrarily capped aggressive exploit-based spreaders with nearly unlimited potential by coding self-imposed 'hop limits'. This practice may well account for the stark difference in results between the NSA's use of the ETERNALBLUE SMB exploit[13] as opposed to that of the Lazarus Group[14]. Tooling with abilities intentionally limited by developers or operators is indicative of a higher-order decision-making process than that exhibited by nations whose sole consideration is whether something *can be accomplished* and not whether the means entail potentially extensive consequences. While likely most bureaucratically constricted, Western actors have managed to dominate the digital operations space through a combination of ingenuity and sheer technical superiority.

In an unfortunate turn of events, some of the most organized actors have also been subject to a greater number of leaked internal materials. These materials supplement proactive public engagements and public oversight. The inner workings of organizations like the NSA's Tailored Access Operations (TAO[15]) and the CIA's Information Operations Center (IOC [16][16]) were largely opaque beyond scarce public speeches by high-ranking officials fighting back against increasingly negative or unbalanced public narratives [18–20]. The result is a slightly less veiled understanding of the concerns, capabilities, limitations, and extensive bureaucracy involved in internal decision making.

Some of these same operations were independently discovered and expertly analysed before relevant documents were available to taint public observations. This presents us with an opportunity to assess both the perpetrators' intent in following a given tenet and whether we can perhaps discern some of the in-the-wild expressions of that tenet. The particular principle we'll be focusing on is *deconfliction*.

DECONFLICTION AND INFORMATION ASYMMETRY

In the most straightforward sense, deconfliction refers to the coordination of movements in order to avoid unintended collisions. Coordinating the flight plans of commercial aeroplanes is a form of deconfliction. Similarly, satellite orbital paths require planning to avoid undesirable encounters. In these cases, the incentive for all actors to collaborate proactively is clear: ensuring mutual safety and long-term operational viability. Yet, deconfliction isn't always so straightforward.

[12] As in-the-wild operations designed and carried out long before the private sector began scrutinizing APT malware displayed seemingly arbitrary self-imposed limitations more likely symptomatic of the overbearing involvement of a cadre of lawyers and bureaucrats in the decision-making process. For example, 2009–2010 samples of Stuxnet's USB spreader rate-limit to three infections before self-deleting [15].

[13] Undiscovered or unreported as of the time of writing.

[14] The latter's reuse of WannaCry resulted in a global crisis of rampant infections antithetical to the presupposed purpose of the payload as ransomware, netting negligible gains relative to the size of its victim base.

[15] Now more generically renamed to Computer Network Operations (CNO).

[16] Now enhanced by a larger 'Digital Directorate' [17].

Deconfliction in the military space finds ever increasing complexity depending on the number of factions involved. For example, a country's ground forces and air support require coordination to avoid the latter accidentally bombing the former's location. When a theatre of war involves multiple allied nations, more complex situations arise, requiring better coordination, up-to-the-minute updates, and overall caution to avoid unintended conflicts, skirmishes or harm among coalition forces conducting separate missions in close proximity.

Deconfliction is far more complicated when it involves military actors on opposing sides of a conflict. One might wonder why deconfliction would be necessary in this scenario. One example is a proxy war – where one actor supports a nation's incumbent forces and another supports rebel forces. While the locals may be in direct opposition, sponsor countries will likely avoid direct confrontations that might spark a greater direct conflict between said supporting nations[17].

While there's a clear incentive to avoid direct confrontation between supporting nations in a proxy conflict, information asymmetry is also necessary. Where allied nations are somewhat more comfortable informing their coalition counterparts as to their whereabouts and mission objectives, proxy-support nations are naturally disincentivized to share their plans openly as doing so is tantamount to tipping their hand to opposition forces. Necessary information asymmetry is precisely where the complexity of deconfliction rises exponentially beyond that of aircraft logistics.

Coordination between law enforcement agencies (LEAs) can serve as a prime example. In abstraction, it may appear as if a regional or activity-based segmentation of jurisdictions should be sufficient to deconflict operations across departments. A crime that occurs in Miami-Dade county belongs to the local police department; a drug trafficking case belongs to the Drug Enforcement Agency. However, in practice, overlaps are inevitable. For example, investigating the activities of a drug cartel operating within the United States could simultaneously involve:

- Local police from multiple municipalities, both local and international
- Federal investigators with a superseding jurisdiction (e.g. FBI, DHS)
- Regulatory organizations focused on the proliferation of arms (e.g. ATF)
- Federal law enforcement focused on drug trafficking and distribution (e.g. DEA)
- Financial regulators focused on money laundering and tax evasion (e.g. IRS-CI, among others)
- External-facing intelligence agencies with macro collection capabilities and a wider understanding of the players involved (e.g. NSA, CIA).

These larger cases[18] will ultimately be assigned a presiding or coordinating agency given their scale. Ideally, that organization will manage the access and information flow of the multiple organizations involved and coalesce the findings. Sensitivities remain as different LEAs seek to protect their sources and methods, even from one another.

Alongside a wide gamut of innovative collection mechanisms, these organizations are likely to resort to confidential informants, embedded undercover agents, voluntary tips, and foreign sources. All of the aforementioned sources require tactful management to ensure both the value of the intelligence

[17] A scenario played out in the recent Syrian conflict as American and Russian forces attempted to support opposing forces, presumably without wanting to engage one another directly [21].
[18] Which may be professionally referred to as a 'jurisdictional clusterf-ck'.

gathered as well as the safety of the source. Given the notorious reach of drug cartels, what organization would comfortably share information about embedded sources to wide distribution?

Even among allied forces, the possibility of unwitting information leaks, corruption and infiltration makes limiting information sharing essential to prolonged operational viability. But how, then, can we assure that a DEA raid won't inadvertently remove another organization's crucial confidential informant from play? Or that an IRS criminal investigation won't get in the way of CIA efforts to track the spread of illicit gains to more unsavoury international actors? There is no easy answer.

This problem has spawned a variety of cultural efforts and system-based solutions, both internal and commercial. Culture reform attempts to incentivize tighter-knit inter-agency cooperation are likely to involve cross-embedding agents in different organizations to familiarize them with individuals, processes and counterparts so that information can flow more naturally. Alternatively, the systems approach seeks to make all information streams from different agencies available with relative immediacy to analysts across different organizations. These streams may include raw information collected, related analyses, and even leads to other interested departments. The hope is that, in the end, the net positives of information sharing outweigh the potential liabilities of careless handling or an insider threat compromising sources.

Two additional complex cases of deconfliction are worth mentioning:

Humanitarians have become all too familiar with issues of deconfliction as they attempt to provide aid and relief in active theatres of war. While most responsible nations would welcome this information (e.g. the location of an ad-hoc hospital or refugee camp), there's an implicit expectation of good faith. Sadly, not all actors observe humanitarian principles, and so a complex calculus of selective information sharing for survival is placed squarely in the hands of those seeking to help where it's needed most.

Additionally, in the case of the upper echelon of international intelligence services, true covert operations require absolute deniability. While common sense may dictate that a team operating behind enemy lines inform 'friends' and local counterparts, some operational objectives cannot afford the luxury of indiscriminate information sharing. Those cases may prove the most interesting yet. These 'edge-cases' of deconfliction in covert operations will come to bear heavily as we transition this concept into fifth domain terms.

DESIGNING DIGITAL OPERATIONS

Digital espionage operations differ greatly from their analogue counterparts in a variety of ways. While it remains important to view digital espionage through the lens of espionage proper[19], fundamental features of the fifth domain[20] break down attempts to metaphorize digital operations in terms of physical attacks. Relevant among these features are notions of *speed*, *range*, *medium dependence*, and most importantly, *default discreetness*. Once past the preparation stages, digital operations benefit from great speed and near unlimited range in contrast to their kinetic counterparts.

Additionally, digital operations are largely dependent on the medium that connects the operators with their targets – likely the public Internet, in its connective patchwork of private service providers and infrastructure, stitched together with the target's immediate infrastructure topology and systems.

[19] More substantially argued in [22].
[20] Features of the fifth domain described in [1] pp.2–6, §Epistemology of the Fifth Domain.

Also, most digital operations are discreet by default – requiring intentional effort, substantive technical failures or incompatibilities, or some form of interference to announce the presence of an ongoing or concluded operation. Physical analogies often fail to accurately reflect the aforementioned fundamental features of these operations but they weigh heavily on the applicability of deconfliction.

Consider a digital espionage operation carried out by a mature threat actor, '*actor A'*, against an unwitting target, '*target P'*. After adequate preparation, *actor A* infects a consumer-grade router, a smartphone, and a computer associated with *target P*. Given the specifics of the operation, *actor A*'s mission objectives involve prolonged collection and covertness – i.e. persist for as long as necessary without getting caught. The information security industry is likely to fixate on the breach (i.e. *Actor A* has successfully infected these devices) or on the persistence (i.e. *Actor A*'s implants were active for six months without detection or response). However, in the process of accomplishing the mission, *actor A* has to observe a multitude of concerns in a dynamic environment:

- Are there security products involved at any point in the 'stack'?
  - Along the route? At the perimeter? Within the perimeter? Or on the devices themselves?
  - Are security providers already alerted to the nature of this user as a high-profile victim? (e.g. a previous attack on this particular victim was previously observed)
- Are there medium restrictions?
  - Is the connection metered, such that the victim might notice a spike in Internet cost due to the volume of exfiltrated traffic?
  - Might the connection become unstable or be severed? Will unusual activity alert a service provider along the route?
  - Does the target's pattern of life place restrictions on connectivity? (e.g. the target hides in the jungle and travels once a week to connect to the Internet at a nearby village for an hour)
- Are other actors interested in this target?
  - If the target is interesting to *actor A*, they're likely to be of interest to other threat actors with similar remits.
  - Is there evidence of the presence of other threat actors on the same devices?
  - Is the target of interest to a local government or an entity in control of their connective medium? Is their connection being monitored already?

These diverse considerations fit into an important operational calculus that *actor A* must undertake to weigh the operational risk, return on investment, and the likelihood of mission success within requisite terms[21].

This operational calculus is not simple as it does not revolve around *target P* alone.

[21] Concern for the mission requirements of covertness and prolonged access speaks to the nature of the particular actor in question. As we know, lesser actors are perfectly happy with smash-and-grab operations – with success measured in successful exfiltration of sensitive materials despite getting caught, outed, and eventually removed.

- **Shared tooling:** Given the nature of *actor A*'s investment in a complex espionage platform intended to serve multiple targets, discovery in *target P*'s environment could result in loss of visibility or operational viability for unrelated *targets Q, R, S,* etc.
- **Infrastructure practices:** Given the peculiar manner in which *actor A* registers and maintains their infrastructure[22], discovery in *target P*'s environment could result not just in a loss of visibility but in a setback in procuring and maintaining infrastructure that suits *actor A*'s established practices.
- **Target of interest (enemy, external):** As mentioned before, the target may be of interest to an enemy service. Perhaps the local government considers *target P* a vital figure and monitors their communications, Internet connections and traffic. Is the relevant infrastructure at risk of arousing suspicion on a broader level? Would that discovery put other ongoing operations in *target P*'s region at risk?
- **Target of interest (enemy, internal):** Is the target infected by another threat actor, the unfriendly *actor E* from a neighbouring country? Depending on the maturity of *actor E*, might their toolkit be in a position to monitor the activities of *actor A*[23] or inadvertently collect relevant artefacts? Alternatively, is *actor E* so careless and loud as to incite an incident response effort that would lead to the collateral discovery of *actor A*'s toolkit as well?
- **Target of interest (ally, external):** Does access to *target P* require leveraging routes, infrastructure, or methods shared with a nation allied with *actor A*? Would discovery of *actor A*'s activities jeopardize the friendly *actor F*'s infrastructure, methods, or ongoing operations in the region?
- **Target of interest (ally, internal):** Adding to the aforementioned concerns, is it possible that *target P* is already under the active surveillance of the friendly *actor F?* Does the friendly *actor F* have primacy of jurisdiction over *target P* by virtue of their locality or involvement in specific activities? Would discovery of *actor A*'s toolkit create international friction by overstepping into *actor F*'s jurisdiction or remit?

Now consider a second intrusion: our *actor A* engages *target Q*. The nature of this mission differs in that espionage is not the sole objective. By the nature of *target Q*'s position, *actor A* intends to leverage this access for a secondary effect. For example, *target Q* manages a system within a radar station in an enemy country and *actor A*'s ultimate intention is to enable an episodic degradation of that radar system in the event of a potential – but as yet unscheduled – armed conflict. The aforementioned considerations are supplemented with operational measures intended to ensure prolonged access: *actor A* might choose to create alternative means of access to the system, limit the volume of exfiltration to the bare minimum, or leverage a passive backdoor designed to lie entirely dormant until awakened by a specific mechanism.

The cost of awareness

The possibility of discovery by *targets P* or *Q* and their local associates presents another concern: raising local awareness. While a target's value may be evident to the attackers, the targets

[22] One might imagine we are dealing with an actor that knows to register and maintain their infrastructure in advance, with trusted providers, establishing domain/IP reputation, etc.
[23] For a discussion of the complex dynamics of fourth-party collection, refer to [23].

themselves may not know that they are desirable targets or that they're vulnerable to digital operations. While that awareness is unlikely to raise the target's defensive posture to a degree such that *actor A* wouldn't be able to reinfect these systems or ultimately carry out their operations by other means, the increased operational cost, potential publicity, or potential diplomatic fallout is undesirable.

Additionally, as threat intelligence producers, we are keenly aware of the effects that third-party intermediaries can have on these operations. After 2010–2011, threat actors had to add the presence of private threat intelligence brokers into their operational calculus. Personal security products (PSPs) such as anti-malware products, perimeter defence systems and logging solutions located in the target's environment are designed not only to provide the target organization with visibility into a past or ongoing attack but are also likely to be uploading telemetry and samples offsite to their respective backends.

Furthermore, there are less obvious organizations now playing a larger role in this space: the service providers that compose the essential connective tissue on which these operations are carried out. These include the service providers enabling the command-and-control, staging and exfiltration servers that enable the threat actor's operations, the ISPs providing the target's Internet, and the software providers that support the target's chosen flavour of operating system. Each of these is now more likely to implement security measures, collaborate with security companies, or arbitrarily decide to roll out mitigations for the general safety of their overall install base.

Threat actors continue to adapt in response to this multi-layered assault on their operational procedures. Mitigations include adapting their infrastructure practices to use new protocols, avoid single points of failure, encrypt data in transit and at rest, or rely on alternative infrastructure arrangements. On the endpoint, some have chosen to design implants that adapt to weaknesses specific to the PSP in place, relying on commodity malware as a first stage, or taking a multi-tiered approach[24]. Where resources are abundant, advanced frameworks are placing greater emphasis on residing in memory or firmware to abuse natural blindspots[25].

It's important to remember that even the best threat actors aren't 'masters of the universe'. The greatest operational gadgetry can be foiled by trivial inconveniences: a machine is taken offline, reformatted or replaced, credentials are changed, a piece of hardware breaks down and is replaced, an Internet service bill is not paid, an intermediary provider experiences an outage, a rival government takes down the Internet across the target region during a conflict, etc.

The number of unforeseeable factors is staggering. Technological wizardry of modern espionage operations fills us with a sense of wonder akin to that of a magic show – but much like a Penn and Teller show, we should remember that no matter how grandiose the magic trick, if a stage light falls on Penn or Teller mid-show, the magic trick is rendered moot. Operators are, more often than not, likely to succeed with the right preparation and tooling, but we'd do well to remember the realities and constraints under which they operate.

[24] A good example of this approach is spelled out in the architecture of HackingTeam's implants: the initial infection is an initial 'scout' module with limited functionality that surveys the infected system. If the victim is validated and the environment is safe, the implant can be upgraded to an 'elite' infection with fully fledged capabilities. Finally, a final tier was suggested – the 'ghost' implant would maintain a foothold in a victim system that's no longer actively being monitored, allowing for easy reinfection without taking up a slot in HackingTeam's limited implant licensing model.

[25] Particularly for the increasingly popular 'light touch' (i.e. lazy) EDR solutions that do next to nothing in memory.

Parsing digital deconfliction

Honing in on the concept of digital deconfliction, the attempt to avoid the friction of cohabitation may prove particularly daunting. A failure of physical deconfliction is painfully obvious: two aircraft attempting to inhabit the same space at the same time will be destroyed. Failures of digital deconfliction provide no such obvious or immediate tell. Modern computers are designed to run countless processes simultaneously and discreetly. Even where two processes interfere with the system in conflicting ways, the machine may malfunction but it won't necessarily point to a piece of malware as the source of that failure. Deep technical savvy[26] is likely required to identify the root cause. *Default discreetness* is the chief fifth domain antagonist of digital deconfliction.

Threat *actor A* is looking to avoid undesirable overlaps. Broadly, there are two overlaps to be concerned with: those with enemy actors and those with allies. The former is effectively equivalent to the fear of fourth-party collection and is outside of the scope of this paper[27]. The latter overlaps – those between 'friendly' actors – are interesting in that they illustrate a nuanced intersection between principled needs, superseding requirements, and pragmatic approaches. They are only made more complex by the nature of international alliances, jurisdictional ambiguities, shared equities, and the aforementioned *default discreetness* of the fifth domain.

Intelligence-sharing alliances (ISAs)

The remit of local intelligence services in the early 20th century was comparatively simple. An understanding of regional boundaries and sentiments, local actors, limited access to materials, and the manner and means of foreign influencers allowed a competent intelligence service to scope and prioritize the concerns of their respective region. The *acceleration*[28] of modern society imposes drastically different circumstances and priorities for modern intelligence services. The interconnectedness of the 21st century entails a lack of conceptual and material boundaries, an increased availability of materials, resources and information and, more importantly, a missing hierarchy of distressing conditions[29]. In our time, there's no such thing as a *local* intelligence service; all modern intelligence requirements are effectively global in scope.

While technology allows the reach of well-resourced and competent intelligence services to scale massively, analytical expertise, thematic and regional understanding, and local resources and influence do not scale. As such, allied countries do well to avail themselves of intelligence-sharing alliances of varying sizes and scopes in order to effectively scale their ability to process the deluge of

[26] The story of the Stuxnet discovery comes to mind. Iranian systems showing 'blue screens of death' (BSOD) indicated a conflict. But it took a technical expert like Sergey Ulasen (at the time at *VirusBlokAda*) to root out the culprit and recognize an ongoing operation. Yet, while a rash of BSODs pointed at a noteworthy operation, plenty of other malfunctions occur without a nefarious culprit to identify other than perhaps a poorly coded system driver.

[27] See [23].

[28] Borrowing the Heidegerean concept – as notably reframed by Kevin Aho – as 'the frantic pace of modern life' after the industrial revolution. Aho focuses on the psychological effects of acceleration on the individual, in the forms of sensory overload, nihilism, and a *lack of existential distress* in our busy modern lives. Let us bastardize this concept by broadening its scope to that of an entire society and consider the operative implications thereby inherited by its intelligence apparatus [24].

[29] In our time, a disagreeable opinion by a popular figure, a shooting massacre in a neighbouring state, a terrorist attack in a nearby country, or the early cancellation of a popular show are all likely to spark an intermittent wave of frenzied high-engagement, low-cost social concern without lasting consequence. That same fever pitch is likely replaced within a day or a week by the next concerning episode(s), effectively rendering moot the hierarchy of these events as lasting concerns.

information required to serve 'all problems, everywhere, all the time'. In order to be effective, information-sharing alliances require some semblance of coordination, cooperation, shared resources, and planning.

Multinational ISAs make it possible to subdivide intelligence collection and analysis by leveraging local resources and sharing the collected data and intelligence byproduct with other members that lack those capabilities or resources relative to that region or area of expertise.

Let's imagine a simple bi-national ISA:

Country A neighbours Latin America and has a history of established asset networks in the region, as well as relevant-language-speaking regional experts. *Country B* neighbours Eastern Europe and has similar resources specific to that region. If each focuses on their nearby region with their respective institutional strengths to collect relevant information and produce intelligence, the resulting information and intelligence byproduct can be made available to both actors (to an established degree) and benefit both with wider coverage of regions they wouldn't otherwise be suited for, without doubling efforts or expending resources inadequately.

Country A has a regional advantage and institutional history for tracking illicit arms trading, while *country B* is positioned to monitor money laundering hubs and ports of entry to the continent. Once again, primary focuses and regional inclinations arise that can ultimately strengthen both countries by means of sharing and coordination. Additionally, *country A* has access to specialized local resources, such as an unparalleled cutting-edge tech sector, while *country B* lacks that access but is positioned to leverage those resources at key regional junctures.

This simplified scenario should allow us to evaluate some modes of coordination and nuances therein. The collection priorities are simple. Each country has a region that they're suited to collect on and analyse, thereby setting an easy jurisdictional demarcation based on locality. Additionally, their respective areas of interest are likely interconnected – as the illicit arms trade originating near *country A* is likely to partially leverage the money laundering resources and points of entry more readily accessible to *country B* – prompting a mutually beneficial cooperation on the overlapping subject. With this mutual interest, there's motivation to make the technological resources that are natively available to *country A* available to *country B* in order to enhance the collection capabilities they'll both subsequently enjoy.

So far, our fictional ISA is well poised for effective coordination. As the cooperation is established, the manner in which resources will be shared can be determined. One possible configuration is for *country A* to allow *country B* to purchase high calibre equipment normally restricted to local use so that *country B* can run operations independently using this equipment and make the results of their collection available to *country A*. Alternatively, *country A* can suggest a shared equity program wherein both countries leverage the equipment, adding their respective strengths. The shared equity in turn is limited to their specific shared interests and operations and the information collected is made available to both countries.

Herein, we encounter an oft-ignored nuance of digital operations. As third-party observers, threat intelligence producers discover and classify clusters of activity made coherent by shared tools, techniques, procedures, and targeting priorities. These clusters are named and tracked under a given moniker. Subsequent analyses (particularly in public reductivist discourse) display a propensity to equate these named clusters with a given country and further simplistic conclusions are drawn

thereafter[30]. These conclusions are not only spurious by virtue of a poor grasp of country-level nuances but further misguided by the implicit expectation that a given cluster of activity equates to a single country or a single organization.

Segmenting, sharing, transferring and discerning equities

Equities broadly defined[31] are an important part of the sharing dynamic between allied governments involved in an ISA. While information and intelligence are the desired byproduct of an ISA, sharing or transferring equities presents an opportunity to exercise soft power, empower a partner, and maximize collection capabilities. Shared equities will ideally streamline coordination and deconfliction efforts by designating a specific platform for a task or region, thereby providing some visibility and predictability into its subsequent use.

Stated more plainly, *actor A* and *actor B* agree to use *platform X* to conduct their espionage operations in the Middle East. This 'regional equity' designation means that, despite the availability of other platforms, both countries will resort to this specific platform to carry out those operations, thereby simplifying deconfliction as *platform X* will be able to account for (and deduplicate) designated tasking. An equity could also be assigned to tracking a specific subset of activities: *countries A* and *B* designate *platform Y* to tracking money laundering efforts by Eastern European groups. Alternatively, a larger suite of tools can be designated as a shared equity for a larger ISA (i.e. allied *countries A, B, C* and *D* share access to *platform Z*).

This final example configuration involves the further added benefit of making development efforts across the cooperating countries in an ISA compatible with *platform Z* by design, thereby simultaneously adding to the capabilities of all countries involved and deduplicating efforts across many possible operations (e.g. if *country C* designs an excellent anti-forensic tool compatible with *platform Z*, *countries A, B* and *D* can make use of that tool without developing their own). Further standardization of design abstractions in a long-established ISA would allow an ease of compatibility with past and future tooling, infrastructure and ingestion.

From the perspective of the threat intelligence analysts attempting to cluster, track, and possibly attribute these operations, shared equities present multiple non-trivial challenges. Not only will different operations by multiple countries blend together based on shared infrastructure, exploits and development frameworks, but a lack of visibility into the composition of an ISA and its jurisdictional assignations over time leads to a further pitfall. What happens when a larger ISA decides to reassign an area of interest (and its relevant equities) to a different member state? If *platform X* is reassigned from *countries A+B* to *countries B+C* instead, would observers have any means to determine this change? Long-term static assignations are another implicit trap of the attribution-prone analyst.

Equity sharing is not enough

While sharing equities is a promising avenue for deconflicting allied operations, jurisdictional segmentation and pre-assigned equities do not account for important overlap-prone scenarios. The organizations involved are intended to pierce and leverage information asymmetry for the benefit of

[30] In the vein of: 'the Lazarus Group reflects the North Korean regime's interest in tracking defectors'.
[31] The term 'equities' has entered common infosec parlance with the recent disclosure of the 'vulnerability equities process' (VEP). While VEP deals primarily with vulnerabilities as the name implies, equity herein refers more broadly to development frameworks, exploits, physical interdiction tools, infrastructure practices, and other equipment leveraged by government CNO teams.

their respective national interests. Intelligence organizations benefit their 'customers'[32] by providing assessments of nebulous or intentionally duplicitous situations. The information they collect and the intelligence they produce form part of that same desirable product in the eyes of a foreign intelligence service and must be guarded to assure *advantage* in that information-asymmetrical space.

Even within the closest and most historically successful intelligence-sharing alliance imaginable, no organization with a decent counter-intelligence practice would disclose the breadth of its collection, or the specifics of its tasking, with another intelligence service[33]. This means that no ISA has complete information over the breadth of operations covered by its constitutive countries and the success of its coordination efforts towards digital deconfliction are likely to fall short.

Nations with established practice in fifth domain operations are likely to leverage their wealth towards fulfilling good counter-intelligence practice – specifically, the need to compartmentalize and diversify operational methods and practices. In digital operations, that extends beyond needing to diversify the agents and analysts involved, also diversifying the implant frameworks, exploits and infrastructure, *as well* as their developers and providers. Though costly and redundant, this effort avoids systematizing a single point of failure into *all* operations in a given domain[34]. No spited developer, compromised operator, glorified sharepoint admin or misguided provider is in a position to burn the breadth of the organization's operations. Similarly, our research efforts may hinder clusters of activity of varying sizes, but they will not affect the breadth of operations of these organizations and ISAs.

The blindspots created by that compartmentalization have a direct negative effect on deconfliction efforts as no group of individuals can assure that tasking across organizations or countries isn't overlapping. Even where strict activity-type demarcations are set (i.e. 'We are the only organization that tracks drug traffickers'), how does one account for dual-hat targets? Surely, some money launderers are also involved in drug trafficking.

We must also remember that targets are dynamic entities. Setting a regional demarcation (i.e. 'We are the only ones tasked with monitoring targets in Syria') conflicts with that dynamism. What happens with targets that cross borders frequently or travel internationally? What about when they travel and set up shop in a region tasked to another organization? And if that's considered a conflict, should the target be disinfected? Should the implant cease to operate? Or is the distinction too pedantic for us to care?

[32] The political decision makers, tasking organizations, and ultimate recipients of their intelligence product.

[33] If only to avoid inheriting the counter-intelligence failures of that sister organization.

[34] The storied past of the Equation Group (EQGRP) presents examples of both systematic failure and compartmentalization success. In brief, the former involves the standardization of a custom cryptographic library for use across EQGRP's malware frameworks. While this is a response to the understandable concern of a signals intelligence agency over the use of poor crypto implementations that may render its collection vulnerable to enemy services, the sustained use of that library meant that once a single EQGRP implant was discovered, seasoned researchers could identify artefacts from more than a decade of EQGRP operations.

At the same time, the EQGRP's discovery by researchers and subsequent leaks of internal development materials showcase the diversification of methods and tools employed by the organizations involved and the resilience that method affords them. While EQGRP is commonly (and naively) simplified to equate with NSA's TAO, discussions in the CIA's Vault7 leak actually point to the discovery of EQGRP tools in 2015 as a collection of tools used by at least two groups at two organizations, and not fully equivalent to either organization. Moreover, both organizations have showcased parallel capabilities undisrupted by the EQGRP discovery and subsequent leaks.

The purpose of the aforementioned (possibly caricaturesque) examples is to illustrate the practical limitations of coordination among intelligence-sharing partnerships. These limitations – alongside the briefly mentioned concern for fourth-party collection – are likely to push these threat actors to adopt a more involved approach to deconfliction.

A BATTLE WITH DEFAULT DISCREETNESS

The advent of general-purpose computing delivered multi-use devices capable of thousands of complex operations at speeds beyond the ability or comprehension of their users. In order to make these devices accessible to common users with no background or interest in their underlying intricacies, modern operating systems were designed to provide an intuitive user experience that prolongs engagement. The OS will quietly execute untold numbers of operations unbeknownst to the user. When software isn't designed specifically to interact with the user via an obtrusive graphical interface, the common user is unlikely to know of its existence on their machine at all. To the common user, these myriad processes default into discreetness.

Most malware takes advantage of this de facto quality. Once a system is successfully infected, the user is unlikely ever to independently discover the implant's presence[35]. Over the past three decades, the anti-malware industry has developed around the premise of providing a 'second pair of eyes' on the system and attempting to detect and remediate the presence of undesirable software. These personal security products (PSPs) would eventually become the natural antagonists of intelligence organizations attempting to operate covertly. However, PSPs were not the only antagonists in that space. As in any other field of intelligence, rival intelligence organizations would continue to be a source of concern in the fifth domain – raising the possibility of fourth-party collection, discovery and subsequent tracking of digital operations, or repurposing of equities after deployment.

Implant framework developers could get their hands on most PSPs by their very nature as commercial products and develop against their engines and detection mechanisms. Eventually, the better engineered nation-state frameworks would come to adapt their traits to operate around the target's PSP of choice in foreseeable manners[36]. However, they would not have that luxury with rival intelligence services. The default discreetness enjoyed by covert actors would show itself to be an indiscriminate advantage, hiding in the brush without knowing what other enemies lurk nearby. Organized actors would need to leverage situational awareness of the capabilities of foreign actors to take informed decisions in the field and maintain their upper hand in the fifth domain.

From the vantage point of nation-state sponsored threat actors, situational awareness of fifth domain operations could be collected out-of-band (through all-source intelligence[37]) or reactively (by repurposing intelligence produced by counterparts tasked with defending government networks from attacks by similar actors). This approach leverages a general awareness of past or currently active operations by known actors in case they just so happen to inhabit the same victim machine. However,

[35] Discounting cases where malware is specifically designed to announce its presence, to elicit a ransom or announce an intentional disruption.

[36] The dynamic nature of supported software entails the possibility of a drastic engine update, new detection capabilities, or newly distributed static or behavioural signatures that would flag general traits or specific components of an active implant as suspicious or malicious.

[37] Including but not limited to accounts from assets or defectors, SIGINT collection, or targeting the developers and operators of foreign services.

this approach alone has obvious limitations – it relies on previous knowledge and is not responsive to the target environment. A third approach is necessary.

The alternative is to emulate some of the features of the dreaded PSPs to monitor the target box after infection[38]. Three techniques come to mind: (1) static detection by means of specific indicators of compromise (IOCs), (2) behavioural analysis, and (3) polling system information to later monitor on a backend system. At their core, the better modern anti-malware solutions opt for a combination of all three, building additional 'bells and whistles' on top. Of these three options, leaks suggest that approaches (1) and (3) have been adopted by different organizations:

An example of static detection by scanning for IOCs on a victim box was first pointed out by *CrySyS Lab*'s Boldizsár Bencsáth [25] as part of the ShadowBrokers dump of Equation Group files. Bencsáth notes that 'Territorial Dispute' (or TeDi) includes a series of simple tools and scripts to check for specific hard-coded IOCs. This presented an interesting opportunity to attempt to identify the actors tracked by EQGRP operators up to the time of the leak. *CrySyS Lab* identified a number of known actors under the numbered signatures[39], this effort was extended by *Chronicle*'s Uppercase researchers as well as *Kaspersky Lab*'s GReAT. Many indicators remain unidentified, in part due to the basic nature of the indicators available, as well as visibility limitations, particularly with regard to older operations.

The inclusion in the toolset of a file called 'drv_list.txt' showcased an acute paranoia of cohabiting with rootkits – likely a remnant of a bygone era before *Microsoft* enforced driver code signing. It also includes PSPs, common or defunct *Windows* utilities, and false positives. 'Drv_list' is particularly interesting as it not only includes filenames but also instructions for the EQGRP operators to follow if they encounter any of these files on victim boxes[40].

Contemporary criticism of static-based anti-virus efforts[41] applies to Territorial Dispute. The TeDi method will only detect the presence of already known or identified enemy components. There's also a propensity for false positives, as malware components so often adopt system component filenames and paths to attempt to hide from PSPs. The most glaring problem with the static approach is made painfully obvious by the ShadowBrokers leak itself: by hard coding IOCs, a concerned threat actor could tip its hand as to the state of its situational awareness into enemy digital operations and allow an enemy group to work around it[42]. While less than ideal, the presence of signatures from multiple EQGRP components old and new – like EXPANDINGPULLEY (EP) and DANDERSPRITZ (DS) – suggests a reliance on this rudimentary approach for far longer than one might expect.

The Snowden trove included a series of enlightening slides from the Canadian SIGINT agency CSEC[43]. These slides are a particular favourite among threat intelligence researchers as they include

[38] Keeping in mind that many actors have already adopted multi-stage deployments, beginning with a validator-style implant meant to fingerprint the environment before a next-stage payload is effectively deployed.
[39] The main signatures are identified under a nomenclature of 'SIGxx', digits ranging from 1 to 45, and include rudimentary IOCs like filenames, paths and registry keys.
[40] Some of the more interesting findings based on this file will be discussed in §'Observations on In-the-Wild Deconfliction'.
[41] So often misapplied to contemporary anti-malware solutions, which largely do not rely on these basic engines.
[42] Or, in this case, allow researchers to piggyback on that rare glimpse into a SIGINT behemoth's threat intelligence cache.
[43] Communications Security Establishment Canada, now Communications Security Establishment (CSE).

explicit references to some known actors alongside their cryptonyms, like SNOWGLOBE[44]. The authors also included a description of the system CSEC maintained to track these actors [26]. In broad strokes, the slides showcased JSON output collected by plug-ins[45] leveraged via implants on victim systems. The design explicitly states that the 'real work' is done on the backend, basically describing the same architecture as what the industry refers to as 'cloud AV'. REPLICANT FARM appears to be one such backend system, which processes the data and applies verdicts for different 'modules', separated by actor abbreviations.

The absence of the behavioural approach (2) is notable but not surprising. Behavioural monitoring and the application of heuristic signatures is perhaps the most valuable and promising approach developed by the anti-malware industry. However, it often requires the costly[46] development and maintenance of clunky kernel-level components. The resulting instability of messing with the *Windows* kernel[47] is likely one of the reasons that anti-virus solutions gained such a bad reputation for system instability. An attacker attempting to replicate this functionality would likely misfire in unpredictable ways, expanding the footprint of the malware and requiring near constant maintenance. While deconfliction and avoiding fourth-party collection are important principles for developed threat actors, they do not supersede the main function of the operation as a prolonged covert collection effort.

OBSERVATIONS OF IN-THE-WILD DECONFLICTION

This circuitous exploration of threat actor behaviour in the wild was intended to illustrate how a principle observed by a subset of threat actors might be expressed in observed operations. As in all things regarding covert operations, assigning specific intent is tricky and often inexact. In the particular case of deconfliction among allied Western actors, we have the added benefit of reading the explicit concerns of some of the developers and operators behind these operations. But we shouldn't get hung up on this analytical 'low hanging fruit'. As is so often the case with leaks, we often forget our strengths and the particulars of our own visibility and practice as we accept that which we were never meant to see with morbid fascination.

By their own admission, allied Western threat actors observe a principle of deconfliction to guide their operations. It's very much a principle and not a strict rule, nor a perfectly instituted operational tenet. After all, it's hard to avoid cohabiting on a *box* when one can't get a reliable accounting of the presence or absence of others on that target system. I'm sure that as pressure on these digital operations mounts from the research community – alongside that of enemy services – even greater emphasis is being placed on operational security. These actors are getting dramatically harder to track. One can assume that less public observers are also plagued by that same obscurity.

[44] Equivalent to 'Animal Farm', a threat actor observed using six different custom malware families, including Babar, Bunny (a.k.a. 'EvilBunny' or internally 'BugsBunny'), Casper, Dino, Nbot and TaFaCalou (or Transporter).
[45] A handful of plug-ins are listed as part of target recon and OpSec modules whose output ultimately contributes to the actor tracking backend, these include some network monitoring as well as rootkit and implant detection.
[46] Likely why many (but not all) 'EDR' solutions appear to shirk this approach entirely, creating 'lightweight' agents that promise better performance while drastically handicapping their ability to detect complex implants. This should be a serious concern for defenders as the market appears to prefer these solutions without realizing that they're drastically degrading their endpoint visibility just as most threat actors adopt more inventive infection mechanisms, such as trampolining directly into memory residence.
[47] Due to *Microsoft*'s (and now *Apple*'s) neglect to provide adequate APIs for security solutions to collect telemetry and poll the kernel in standard and safe ways.

By way of a conclusion, rather than further 'waxing lyrical' regarding the concept of deconfliction, I would instead prefer to point out a handful of interesting observations regarding the study of TeDi as a 'crib sheet' for one of the greatest global intelligence service's digital situational awareness. Albeit outdated, TeDi is a glimpse into the successes and shortcomings of what's likely the organization with the greatest visibility and telemetry into digital operations worldwide. As an industry developing knowledge *in parallel*, we should take note – pat ourselves on the back where appropriate, and be humbled where otherwise.

In brief, a few notable takeaways perhaps worthy of further study:

A fundamental problem unresolved

The presence of the TeDi 'drv_list.txt' (hereafter 'Driver List') file is interesting not just for its extensive list of leads into potentially significant pieces of malware that EQGRP operators encountered on the boxes of their victims, but also because there's some vague degree of guidance attached to every entry. Most filenames are actually accompanied by the instruction 'UNKNOWN – PLEASE PULL BACK'. This brings us to confront an interesting shortcoming in the black-box analysis of software, one that the anti-malware industry is all too familiar with: that there's simply no tell-tale characteristic of maliciousness inherent within all malware. Maliciousness, or undesirability, is not a feature imprinted on the constitutive genes of a program.

For the past five years, 'hot startups' bathing in venture capital funding have reiterated a naive approach to 'besting' AVs: that we can simply rely on 'machine learning' or 'artificial intelligence' to unburden us of the need to classify software with malicious intent. Taken in good faith, the vision appears to be that some perfect model will emerge that hones in on previously unseen shared patterns of characteristics between clusters of malicious software, perhaps in the appearance of certain API combinations, or strange file structures, or some other as yet unidentified seed of badness. Years later, we've come to see these startups[48] either fail, pivot, or patch their performance failures with generic detections so paranoid as to become a meaningless stream of false positives.

Ultimately, this attempt at automatic classification of intent appears to be the anti-virus equivalent of phrenology – 'by measuring the subject's head, we can clearly see that the ridges on the side of the cranium suggest a proclivity for criminality'.

Perhaps we can take solace in seeing that the EQGRP operators were just as baffled in their attempts to classify and understand the wealth of new drivers, libraries and executables that they encountered on their target's machines. Going so far as to roll back a successful infection at the sight of what they considered an unknown file – which we now know in some cases was just a common utility for burning CDs or mounting ISOs. While the numbered SIGs suggest a discerning understanding of activity clusters, the far larger Driver List points to the extreme care of the EQGRP operators not to land on a system that may compromise their operations. There's no doubt that this level of care played a role in their ability to operate since a suspected 1996 without being publicly outed or discovered for nearly two decades.

[48] In the best-of scenario, that VC runway ultimately allowed a newcomer to stealthily rebuild the same anti-malware technology as every other solution already in the market, with the aid of more modern marketing, while casting stones at every product they would go on to emulate.

Burned either way

Continuing on the subject of Driver List, this innocuous 244KB text file should be recognized for the sheer weight of its disclosure potential. The ShadowBrokers used the 'Equation' name to provide immediate public context to their leak. By tying their leaked materials to GReAT's 2015 discovery of EQGRP in the wild, the ShadowBrokers could immediately command the morbid fascination of the industry without having to fight to have their warez recognized for their rarity and value. One might be tempted to wonder how the value of this trove could have been established had it not been preceded by that landmark discovery.

Had GReAT not discovered EQGRP on the 'Magnet of Threats', it turns out that all that the ShadowBrokers would have had to do is to release the 'drv_list.txt' file. At the very top of the Driver List's more than 5,000 entries is a listing of implant file names directly correlated with their respective cryptonyms. Considering that GReAT found more than a decade's worth of EQGRP operations by sigging based on one driver discovered on a single overpopulated target[49], releasing 'drv_list.txt' alone would have been enough to overwhelm the research community with discoveries and burn a sizable amount of the EQGRP toolkit.

Wherefore art thou, Regin?

While the indicators in TeDi show a breadth of knowledge and concern for other actors and operations, it also includes some conspicuous gaps. Chief amongst these is the absence of the Regin Supra Threat Actor[50]. Regin being equivalent to WARRIORPRIDE and DAREDEVIL, is our observer's umbrella term for implementations of the Wzowski API used as a compatibility framework across Five Eyes to facilitate joint development.

Moreover, code similarity connects Regin samples consistently to the 'cni-1.dll' library included in the ShadowBrokers trove. Code from this same library serves as a transitive connector with the EQGRP toolkit, whose components also share this code in different ways. Despite these links establishing the EQGRP operators' awareness of the existence of Regin, this threat actor is completely absent from both TeDi's numbered SIGs as well as the more comprehensive Driver List. For comparison, TeDi tracks other likely shared equities (like Stuxnet). The absence of Regin is perhaps a testament to the larger organization's commitment to compartmentalizing operational details to avoid a single point of failure scenario for this and other parallel equity frameworks likely at play.

Shady neighbours

On a similar note, the general absence of the Lamberts from the numbered SIGs is also interesting. However, they're not entirely absent. The Driver List actually contains small references to very old Lambert components. Notably, it appears that the EQGRP is not aware of all (or most) of the

[49] A notable instance of collateral discovery on an improperly deconflicted target.

[50] As described in our work on GOSSIP GIRL, Supra Threat Actor (STA) is used to denote a cluster of activity that reflects the collaborative efforts of multiple threat actors (countries or organizations) as denoted by the use of a compatibility framework that allows multiple development platforms to function together. In the case of the GOSSIP GIRL STA, code similarity, plug-in development and shared exploit implementations evidenced the involvement of five distinct clusters (Equation, Flame, Stuxnet, Duqu and FlowerShop). In the case of Regin, we not only have the explicit disclosure of Five Eyes joint development from the CSEC slides (identifying the equivalence between CSEC's [and DSD's] WARRIORPRIDE and GCHQ's DAREDEVIL) but also through code similarity analysis that connects Regin and Equation malware (as well as 'cnli-1.dll' from the ShadowBrokers leak, likely the Wzowski API library itself).

Lamberts components. Beyond how old[51] these components are in comparison to other entries, it's interesting to note that while the Driver List classifies Gold Lambert components as 'FRIENDLY TOOLs', the subsequent appearance of Orange Lambert components falls under the more common 'UNKNOWN TOOL'.

Stylish frienemies

Finally, as we've discussed the possibility of shared or outsourced equities, it's interesting to note development patterns among some of the actors tracked by the EQGRP. Multiple non-Five Eyes but allied actors are present in the TeDi numbered SIGs. Looking at Flame and Animal Farm[52], a particular trait stands out: the use of an embedded Lua VM for modularity and extensibility. Lua is a lightweight embedded scripting language and its use in malware is relatively rare. However, it appears consistently among a notable subset of advanced threat actors whose toolkits have been publicly acknowledged as controlled (at least partially) by foreign nations, and yet whose developers showcase native English and common development traits. Widening our view beyond TeDi, we see the emergence of other more ambiguous nation-state toolkits (old[53] and new[54]) with similar proclivities. Rather than clumping these obviously diverse operations into a single cluster, we should instead consider the possible involvement of a 'digital quartermaster' arrangement in equity sharing at play with for both near and distant neighbours.

REFERENCES

[1] Guerrero-Saade, J. A. Draw me like one of Your French APTs – Expanding Our Descriptive Palette for Cyber Threat Actors. Virus Bulletin 2018. https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Guerrero-Saade.pdf.

[2] Thomas, K. China's post-WTO intellectual property system. 2008 (p.16). http://eprints.nottingham.ac.uk/12621/1/518837.pdf.

[3] Gale, B. The Concept of Intellectual Property in the People's Republic of China: Inventors and Inventions. The China Quarterly, No. 74, 1978. Cambridge University Press. https://www.jstor.org/stable/652695.

[4] Guerrero-Saade, J. A.; Raiu, C.; Moore, D.; Rid, T. Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

[5] How the Dutch foiled Russian 'cyber-attack' on OPCW. https://www.bbc.com/news/world-europe-45747472.

[51] Samples dating back to the mid-2000s.

[52] More recently connected by French authorities with DGSE operations and yet treated as an unknown or outside discovery by the CSEC slide deck developers – perhaps showcasing genuine compartmentalization between information assurance teams and those familiar with equities leveraged by allies in lesser-trust ISAs, wherever those equities may originate.

[53] TORCH RELAY (unpublished) showcasing the oldest use of an embedded Lua VM for a targeted nation-state operation, pre-dating the oldest Flame samples by three years and using a slightly older version of Lua than any in the aforementioned operations.

[54] Project Sauron (a.k.a. Strider or RemSec) discovered by *Kaspersky* and *Symantec* in 2016 and showcasing the use of a Lua VM modified in house to natively handle foreign characters [27, 28].

[6] Wikileaks: Russia branded 'mafia state' in cables. https://www.bbc.com/news/world-us-canada-11893886.

[7] Stoll, C. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Doubleday, 1989.

[8] 2 W. Germans Get Suspended Terms as Computer Spies. LA Times. https://www.latimes.com/archives/la-xpm-1990-02-16-mn-667-story.html.

[9] Wanted by the FBI: ALEXSEY BELAN. https://www.fbi.gov/wanted/cyber/alexsey-belan.

[10] Stempel, J.; Finkle, J. Yahoo says all three billion accounts hacked in 2013 data theft. Reuters. https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

[11] Collins, K. Russia is recruiting the FBI's most-wanted hackers. Quartz. https://qz.com/934432/russian-intelligence-recruited-alexsey-belan-and-evgeniy-bogachev-fbis-most-wanted-hackers/.

[12] Sandee, M. GameOver ZeuS. Backgrounds on the bad guys and the backends. https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends-wp.pdf.

[13] 'It's our time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. Meduza. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

[14] Putin Compares Hackers To 'Artists,' Says They Could Target Russia's Critics For 'Patriotic' Reasons. RFE/RL. https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html.

[15] Falliere, N.; O'Murchu, L.; Chien E. Stuxnet Dossier. 2011 (p.10). https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[16] Gellman, B.; Nakashima, E. U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show. Washington Post. August 2013. https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[17] Lyngaas, S. Inside the CIA's new Digital Directorate. FCW. October 2015. https://fcw.com/articles/2015/10/01/cia-digital-directorate.aspx.

[18] Blackhat 2010 Keynote: General Michael Hayden – https://www.youtube.com/watch?v=pKZDYgj0KTA.

[19] Blackhat 2013 Keynote: General Keith Alexander – https://www.youtube.com/watch?v=xvVIZ4OyGnQ.

[20] USENIX Enigma 2016: TAO Chief, Rob Joyce – https://www.youtube.com/watch?v=bDJb8WOJYdA.

[21] Press Gaggle by Press Secretary Josh Earnest en route Washington, D.C., 9/29/2015. September 29, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/30/press-gaggle-press-secretary-josh-earnest-en-route-washington-dc-9292015.

[22] Guerrero-Saade, J.A. Ethics and Perils of APT Research: An Unexpected Transition into Intelligence Brokerage. Virus Bulletin Conference Proceedings (2015). https://www.virusbulletin.com/virusbulletin/2016/01/paper-ethics-and-perils-apt-research-unexpected-transition-intelligence-brokerage/.

[23] Guerrero-Saade, J.A.; Raiu, C. Walking In Your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell. Virus Bulletin Conference Proceedings (2017). https://www.virusbulletin.com/virusbulletin/2017/10/vb2017-paper-walking-your-enemys-shadow-when-fourthparty-collection-becomes-attribution-hell/.

[24] Aho, K. Acceleration and Time Pathologies: The Critique of Psychology in Heidegger's Beiträge. Time and Society, 16:25-42, (2007).

[25] Bencsáth, B. et al. Territorial Dispute – NSA's perspective on APT landscape. 2018. https://www.crysys.hu/files/tedi/ukatemicrysys_territorialdispute.pdf.

[26] Pay attention to that man behind the Curtain: Discovering aliens on CNE infrastructure, CSEC Counter-CNE, Target Analytics Thread, SIGDEV Conference, 2010. https://www.youtube.com/watch?v=YcR9k8o4I0w.

[27] The Project Sauron APT. Kaspersky. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf.

[28] The Project Sauron APT. Technical Analysis. Kaspersky. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190156/The-ProjectSauron-APT_Technical_Analysis_KL.pdf.