WAVE YOUR FALSE FLAGS! DECEPTION TACTICS MUDDYING ATTRIBUTION IN TARGETED ATTACKS

Brian Bartholomew & Juan Andres Guerrero-Saade
Kaspersky Lab, USA

Email {brian.bartholomew, juan.guerrero}@kaspersky.com

ABSTRACT

This paper takes a comprehensive look at the current state of attribution in targeted attack research and at deliberate attempts by the adversary to obstruct this process. The paper includes common bases for attribution, practical and methodological complications, and examples of purposeful abuse by sophisticated threat actors in the wild.

INTRODUCTION

Attribution is often the most prominent point of interest and contention when it comes to threat intelligence, both for direct recipients and the general public alike. Despite this pervasive interest, the attribution phase of the analysis cycle is little understood and the complications that arise therein are often ignored. Similarly, the value of attribution remains largely unquestioned. We will not argue that attribution provides no value. However, a thorough study of the methods for arriving at attribution and the data available to reach these conclusions will reveal the shaky foundation of attribution in threat intelligence and hopefully prove a cautionary tale for threat intelligence producers as well as recipients making decisions on the basis of attribution claims. At a time when 'hacking back' is discussed as a legitimate option for victims, and governments are willing to take heavy-handed geopolitical retribution on the basis of threat intelligence products, misattribution can have a hefty cost.

Moreover, attackers aware of the reactions taken by victim nations and companies in the face of audacious attribution claims may seek this tertiary effect purposefully. Acknowledging the space for error in attribution, threat intelligence circles often raise this possibility under the vague threat of 'false flag operations'. However, little has been provided publicly to substantiate this possibility. As part of our work in *Kaspersky Lab*'s *Global Research and Analysis Team* (*GReAT*), we have been uniquely positioned to witness both general and specific cases of manipulation of indicators by attackers of medium-to-advanced skill attempting to mislead researchers and other nosy onlookers. Rather than resort to innuendo, we will provide multiple and diverse examples of manipulation that showcase the abuse potential currently being exploited by attackers in the wild.

By substantiating the case for false flags, we intend to raise a general awareness of the complications involved in investigating targeted attacks. We hope that these cautionary tales will also reach the consumers of threat intelligence products to temper their expectations and reactions to attribution claims and hopefully dull the edge currently leveraged by cunning attackers interested in casting blame for their nefarious activities onto unsuspecting nation states or unrelated threat actors.

What follows will cover the general approach to attribution and its basis. We will then present overviews of multiple examples of purposeful manipulation of attributory indicators to showcase different forms of manipulation, each displaying varying degrees of cunning and success potential. Armed with these examples, we will explore general and methodological complications. Finally, we discuss some general reflections to further a deeper discussion of the value and risks of attribution for consumers and producers alike.

ATTRIBUTING TARGETED ATTACKS

The expression 'attribution is hard' is often bandied about, either apologetically or in jest. It's easier than explaining that, in fact, attribution relies on a combination of fungible technical indicators, mistakes, overlaps, and luck. Sloppy or careless operators (such as those nation-state actors who believe they can act with impunity) are wont to provide more data than they should, like debug paths and language strings, or to reuse infrastructure from previous attacks, which allows researchers to group them into a threat actor cluster. Sometimes our luck is such that an IP address will point us at an incriminating location or we find a widely reused handle rife with personal information. Other times, there are little to no indicators pointing us in any particular direction. Attribution is an important part of the threat intelligence (TI) process but it isn't one that can always be fulfilled with any certainty.

Though the analysis process adapts and changes on a case-to-case basis, we can discuss the most common bases for attribution claims encountered during targeted attack research. What follows should impress the reader as to the inexactitude and need for interpretation in every step of the attribution process. Heaping several of these indicators together may paint a more cohesive picture but it is nonetheless a series of intuitions ideally (but not always) pointing in the same direction. The question to keep in mind is 'what makes a satisfactory attribution claim?', particularly the sort with such certainty as to justify further action (be it legislative, political, law enforcement, or retaliatory CNA)[1].

Timestamps

A great benefit of the Portable Executable file format is the inclusion of compilation times. Though these can be altered with ease, many samples include original timestamps. Beyond an obvious indication of an actor's longevity, timestamps allow for an understanding of specific campaigns as well as the evolution of an actor's toolkit throughout the years. With a large enough collection of related samples, it's also possible to create a timeline of the campaign operators' workday. Where these operate in any professional setting or with any semblance of discipline, it's possible to match the normal peaks and troughs of a workday and pinpoint a general timezone for their operations.

[1] A topic further addressed in the final section of this paper.

Strings, debug paths, and metadata

Malware binaries often include several artifacts of their construction in the form of strings and debug paths. Even perfectly innocuous strings used to describe the normal operations of a backdoor can give away impressions of the malware authors. The most obvious is their preferred language, particularly when it comes to rare languages in the targeted attack landscape, but also indicating language proficiency with broken English showcasing the colloquial shortcomings of the coder. Among these strings, a favourite of TI researchers is the debug path: a string describing the folder structure leading up to files from the time of development that made its way into the final binary. Debug paths most often reveal a username but may also (in the case of organized coders) reveal internal naming conventions like internal tool, project or campaign names.

Another telling resource is the presence of metadata both in malware binaries as well as dropper files like decoy or macro documents. From time to time, binary resources will contain language IDs that reflect the configuration of the developer's system in telling ways, perhaps pointing to the system's native language. Phishing documents are also often riddled with metadata. Disciplined actors regularly employ virtual machines with nondescript usernames and software registrations, usually reflecting the use of pirated software with common file attributes or resources pointing to generic, publicly traded exploit kits. However, metadata will occasionally include original user handles and unintentional save state information that points to the actual author's machine.

Infrastructure and backend connections

A preferred method for grouping targeted attack activity together is through cataloguing of the malicious use of network infrastructure. Command-and-control infrastructure can be costly and difficult to maintain, with the added complication that availability may be disrupted by researchers, law enforcement, or a spooked system administrator (in the case of compromised infrastructure). Even well-resourced attackers have a tendency for reusing command-and-control or phishing infrastructure. For threat intelligence teams building databases of targeted attack-related infrastructure, this is often the most telling sign of an attacker resurfacing or retooling. In rare instances, multiple attack groups may go after the same vulnerable server (particularly with teams that insist on using compromised infrastructure rather than mounting their own) but this remains rare enough to be an outlier. The trend at this time remains that even in cases of infrastructure reuse between teams, these occur within the same threat actor cluster (as in the case of multiple independent 'Chinese-speaking' threat actors getting their hands on the same zero-days, some overlapping infrastructure, or sharing lateral movement tools – a situation that speaks more to the tasking arrangement or 'community' of attackers in this cluster than to a breakdown in attribution methods).

In the case of researchers with a privileged point of view, such as those working with email services, ISPs, or those providing support for a compromised server, backend connections can be a serendipitous and often telling attributory indicator. What we mean by 'backend connections' are connections that take place when an attacker retrieves data from an exfiltration server or email account, prepares a staging or phishing server, or checks in on a compromised domain to assure its continued availability. Attackers almost always use Tor or some other anonymizing service to mask this connection but mistakes happen more often than not. The mistake will likely provide researchers with an IP or a region telling of the native operations of the attacker.

Toolkits

Malware families

Although even the most advanced threat actors may rely on publicly available tools, most take the time to build their toolkits and develop custom backdoors, lateral movement tools, and exploits. Knowing the value of what they've developed, actors will jealously guard their toolkit, thereby allowing researchers to hone in on a threat actor by the presence of a tightly controlled malware family. In simpler terms: if Snake is present then it looks like Turla; if WildPositron malware is found then it's probably Lazarus, and so on. It's important to remember that 'malware ownership' isn't static. Just as the malware itself develops over time, the ownership may be transferred. It can be shared with other teams in the same cluster, developers may leave or set up their own shops, or source code may leak through a variety of circumstances.

Code reuse

In cases where an actor has been exposed or has found other motivations for a top-down retooling, code reuse can indicate a relationship between currently used tools and their predecessors. Coders can be quite lazy and even when the intention is a full retooling, malware developers will often reuse specific functions or pieces of code that have worked well in the past. This means that the avid researcher or obsessive yara rule writer may be able to hone in on these traits and connect new and old campaigns, or even seemingly unrelated threat actors.

Passwords

A similar circumstance applies to the reuse of passwords. These may be the passwords to email accounts used for phishing or exfiltration, accounts on compromised servers, or hard-coded passwords in malware components. A recent example saw a threat actor deploying droppers with password-protected resources that contained the actual payload in an attempt to thwart sandboxes and automatic detection systems. The hard-coded password protecting the resource was the same even when different, seemingly unrelated malware families were being dropped, thus allowing researchers to tie the two malware families to the same actor. This also applies to hard-coded encryption keys in different malware families or campaigns.

Exploits

Finally, zero-day exploits are a great source of excitement in research circles these days. The presence of an '0-day' immediately sets an actor apart from the run-of-the-mill attackers, thus justifying greater researcher involvement.

Though exploits may be repurposed or acquired from public sources, a greater emphasis on responsible disclosure has limited the availability of the latter by dissuading the release of fully developed ‘proof-of-concept’ code that may aid attackers in leveraging newly discovered exploits[2]. That said, many advanced attackers have exploit developers in house, with some threat actors unleashing a seemingly unlimited supply of exploits where needed.

With a given exploit being an arcane and jealously guarded weapon in the attacker’s arsenal, home grown implementations of an exploit allow researchers to group together diverse malware families or separate campaigns to a given cluster. When a specific implementation of a zero-day appears in separate unrelated instances within a given timeframe (even long after the zero-day was identified and patched), it signifies code sharing likely pointing to the same actor or activity cluster. Despite discussions of parallel discovery [2] of exploits by different vulnerability researchers in a given timeframe, exploit implementations differ. However, this does not entirely discount the possibility of a double-dealing seller in the black or grey market or other unexpected threat actor interactions like exploit repurposing, as evidenced with Equation team’s reuse of CVE-2013-3918 within a couple of days of its initial use by the Aurora actors [3]. One also cannot discount the nefarious possibility that a disclosed exploit repository itself has been hacked, as this represents a boon for an advanced attacker with indisputable return on investment.

Tasking

A final oft ignored tell of targeted attacks are the chosen targets themselves as they represent the intent propelling forward a well resourced espionage operation. Though many indicators may be faked or altered, the dynamic between attacker and victim is harder to hide or directly manipulate as it involves ‘real-world’ publicly known circumstances or geopolitical conflicts. The threat intelligence space represents an unprecedented circumstance in which an unrelated third party with an unexpected vantage point can have situational awareness over large swathes of the targets of a secretive intelligence organization. For research teams with gifted analysts, this insight allows for attacker profiling. A possible outcome is the mapping of a campaign to a geopolitical or regional situation that may point in the direction of a given perpetrating organization or nation. Or in the case of a resurgent retooled threat actor, witnessing them revisiting the ‘old favourites’ can be a telling sign connecting a new actor with a known cluster of activity, particularly when the new attacks leverage previously pilfered insights into the victim’s network or ‘pattern of life’.

However, the study of tasking alone is largely interpretative and faces common pitfalls derived from cognitive biases and geopolitical oversimplifications, already familiar to intelligence analysts. Further complications arise from the particularities of certain targets and attackers alike. For example, some targets are so attractive by their very nature and position as to attract the interest of several different actors simultaneously. Also, certain threat actor configurations break this paradigm entirely, as will be discussed further in the next section.

A CUNNING MENAGERIE IN THE WILD

In order to delve into specific examples, we require two distinct allowances from the reader:

- The first regards the use of attribution examples. As should have become apparent by now, attribution claims are far from certain and often sparsely substantiated. As part of a company and a research team that is cautious to remain attribution agnostic, we toe this line respectfully and with good reason. In the process of discussing in-the-wild examples of manipulation of attribution leads, it may be necessary to point to commonly held beliefs or rumours as to the provenance of certain threat actors in order to showcase where the indicators falter. We ask the reader to treat these as what they are: rumours heard through the attribution grapevine, the sort of RUMINT that associates a threat actor with a country, region, or organization. *These are not our own assertions or claims. We remain steadfast in our conviction of the complexities of the attribution problem and would prefer not to be quoted by overzealous readers as asserting attribution claims that are not our own*. At times our own research may support these intuitions but we do not go so far as to make these attribution claims our own.
- Secondly, despite the liberties provided by an academically toned industry publication, we remain bound by corporate realities, respect for the research methods of collaborators, and, most of all, legal constraints. As such, we may not always be able to provide full disclosure of indicators involved in certain findings. As we do not seek to recreate the process of each investigation, we feel these are not vital to convey the main thrust of our argument, which is that intermediate-to-advanced threat actors are aware of attribution methods and are already attempting to manipulate researchers to expend limited resources chasing ghost leads. Where gaps arise, let us relegate these accounts to camp fire re-tellings among friends.

We thank the reader for these allowances, providing a lacuna between authors and content, in order to further a wider discussion about the complexities of attribution that could not happen otherwise.

On language – Cloud Atlas

In December 2014, *Blue Coat* exposed a newly discovered malware framework dubbed ‘Inception’ [4, 5], which was later attributed to a new actor named ‘Cloud Atlas’ [6]. Cloud Atlas is believed to have been born from a previous actor tracked as ‘Red October’ [7]. Whether Cloud Atlas is the same actor or a spin-off of the original, this case posed some interesting analytical problems when it came to attribution. The current belief is that both teams are likely Eastern European-based and most likely Russian-speaking. Cloud Atlas may be a spin-off from the original group following conflicts arising from the annexation of Crimea in the spring of 2014.

[2] An example is the quick adoption by DarkHotel of a Flash zero-day found in the reckless full release of the HackingTeam trove [1].

During the investigation of this new campaign, various oddities were discovered that seemed to disprove the belief that Cloud Atlas was Eastern European. It was only after analysing these breadcrumbs in conjunction with each other that the determination was made that Cloud Atlas was most likely 'muddying the water' in order to make attribution more difficult. Targeting seemed to fit the original campaign, as the majority of attacks were heavily focused on Russia, specifically government and diplomatic entities. Very similar, if not identical lure documents were used in the two campaigns. Also, the implementation of compression algorithms was nearly identical in both, with the Cloud Atlas version showing slight improvement. But this is where the similarities stop, and the weirdness starts:

One of the early lure documents discovered in this campaign pertained to Russian government officials but was titled in *Spanish*. Further analysis of metadata from the original lure document showed it was created on a native Spanish speaker's system. Initially, this caused a bit of confusion, but it was later determined that the lure document was most likely stolen from an advisor in the Spanish Embassy in Moscow and repurposed for use in attacks.

The infrastructure used by Cloud Atlas to manage victim data and implants was also interesting. The actors used a large pool of IP addresses in a 'round robin' fashion to access the cloud-based provider used to host payloads and store exfiltrated data. Geolocation of the IP addresses showed the actors as mainly originating from *South Korea*. Later analysis revealed that these IP addresses were mostly compromised home routers which contained a small proxy implant.

Focusing on language clues left behind in the malware caused further attribution issues, as conflicting indicators were peppered into the mobile implants:

- *Arabic* strings in the *BlackBerry* version
- *Hindi* characters in the *Android* version
- *God_Save_The_Queen* was found in the *BlackBerry* version
- 'JohnClerk' was found in the project path for the *iOS* version

The presence of these various conflicting strings in different versions of the malware could either mean that the actors borrowed code from various sources to use in their implants, or that the strings were purposely placed to misguide researchers.

During the investigation, many researchers were running the various samples found in the wild in an effort to solicit a second-stage binary from the actors. In multiple instances, an implant was served up to researcher machines that did not fit the typical Cloud Atlas framework. This implant showed characteristics of malware traditionally considered Chinese and used a command-and-control domain that was inactive at the time. The belief is that the actors recognized researcher systems in their logs and instead of serving the normal second-stage binary, they instead provided a 'fake', unrelated piece of malware to cause confusion.

Blue Coat researchers did an excellent job in their original paper describing the various paths attempted for attribution, only to hit a dead end or to find nonsense data. This is a great example of how certain APT actors are aware of the indicators we as researchers tend to latch onto, and are already purposely modifying those characteristics.

On tasking – Wild Neutron

Wild Neutron[3] is a crowd favourite when it comes to complicated attribution research, complete with apocryphal tales and red herrings. Wild Neutron first rose to prominence in 2013 [8], though evidence shows the group was active as early as 2011. Their reputation is in large part thanks to their ambitious targeting, bagging whales like *Apple*, *Facebook*, *Microsoft* and *Twitter*. Their arsenal included multi-platform malware [9], a Java zero-day (CVE20130422), and a penchant for well-chosen watering-hole sites. After close to a year of silence, Wild Neutron returned for a 2015 campaign, this time with a stolen digital certificate and a still undiscovered Flash zero-day exploit. Throughout, attribution has been a maze of contradictory indications and false starts that continue to elude researchers.

Some of the simpler misleads are found in the *Windows* malware where language strings were found both in Romanian ('*la revedere*' meaning 'goodbye') and Russian ('*uspeshno*', a transliteration of 'successfully'). Other leads include a false connection to a well known researcher, connections to apparent scam artists, investment funds, and even a seemingly successful cryptocurrency scam[4]. But Wild Neutron presents a deeper challenge for analysts than this particular hodgepodge of indicators, one that speaks to the possible nature of the threat actor as a mercenary entity. Usually a situation so convoluted would find some semblance of resolution by looking at the victim spread, the sort of organizations and entities targeted by the threat actor. In this case, the victim spread does little to assuage our uncertainty.

Looking at Wild Neutron's targeting, no one clear nexus of interest is apparent:

- Large company groups involved in M&A
- Real estate companies
- Bitcoin-related companies
- Investment firms
- IT companies
- Healthcare companies
- Law firms
- Developers (iOS and Linux)

With victims in over 11 countries[5] and multiple verticals, we can perhaps assume several different and possibly overlapping nexuses of interest that may suggest multiple tasking entities or diverging mission imperatives. Another noteworthy observation

[3] Also known as: Morpho, Butterfly, ZeroWing, or Jripbot.

[4] These attributory hypotheses and the supporting indicators are presented in the *Kaspersky Private Intel Report* on Wild Neutron pushed to subscribers in July 2015.

[5] Visibility courtesy of the *Kaspersky Security Network* (*KSN*) and *Kaspersky* sinkholes of Wild Neutron command-and-control infrastructure.

is the lack of victims in diplomatic or government institutions, a customary vertical for a threat actor of this calibre. This stands in juxtaposition to what is presumably counterterrorism tasking with the compromise of the Ansar alMujahideen forum. Researchers concluded that the tasking was in line with a mercenary arrangement, taking tasking from different entities and imperatives, including a financial incentive to pilfer tradeable financial information on mergers and acquisitions. This type of threat actor, while unlikely to remain rare, by its very nature dismantles our ability to form a generalized attributory claim on the basis of tasking alone.

On hacktivism

The following examples are not intended as a particular criticism of hacktivist tendencies themselves, but rather point to the abuse potential in the prevalence of hacktivism as a commonplace element in the Internet. Threat actors interested in misleading the public and researchers alike with their disruptive activities stand to benefit from doing so under the cover of a hacktivist group. They are thereby afforded a cover of expected anonymity, plausible deniability, and the inherent legitimacy of an Internet-age societal force springing forth from a ground swell of 'community sentiment' (even when said community is nowhere to be found).

The following two threat actors have attempted this with varying degrees of success:

Lazarus[6] the Weak

The Lazarus Group [10] represents a cluster of activity stretching back as far as 2009. From that time the group has engaged in a series of infamous attacks, most notably the devastating wiping attack on *Sony Pictures Entertainment* (*SPE*) in 2014. Our findings[7] tied this cluster together to contain a series of malware families and campaigns suspected of sharing the same provenance but not previously technically correlated. Looking at these different campaigns, we see a pattern emerge characterized by the use of unheard of hacktivist groups as self-assigned perpetrators of each attack. In the case of *SPE*, the group was 'Guardians of Peace' or GOP. We are meant to believe this is an established hacktivist group despite lacking a visible presence or pedigree before or after the attack.

Similarly, the 2012 attack on the Korean newspaper *JoongAng Daily* [11] that reportedly disrupted operations was plastered with the motto 'Hacked by IsOne', an unheard of attacker. 2013 saw wiper attacks on South Korean institutions [12] using malware designed to overwrite files with Roman army terms 'HASTATI' and 'PRINCPES'[8] before corrupting the drive's Master Boot Record. Interestingly, these attacks were claimed by two unheard of groups, the 'New Romantic Cyber Army Team' and the 'WhoIs Team' [14].

Despite media coverage, the Lazarus Group's insistence on employing cover groups has done little to persuade onlookers for long as to the provenance of these attacks. This is due, in large part, to the supposed perpetrators' complete lack of pedigree or prevailing Internet presence. Their lifespan is only that of the attack in question. With no entity to trace, follow, or interrogate, attention quickly turns to the more obvious perpetrator of these attacks. However, this misleading tactic has been better employed by another threat actor.

Sofacy the Strong

One of the most interesting groups in recent years has been Sofacy[9]. Sofacy is widely believed to belong to a Russian intelligence organization, although this is still a subject of debate. The group has vast resources at its disposal and has produced copious numbers of zero-day exploits, especially in the last three years. Targeting for Sofacy has changed over the years in parallel with the Russian political climate and has included foreign government agencies (intelligence, military and civilian), suspected terrorism targets, media outlets (both foreign and domestic), non-governmental organizations (NGOs), and energy-based companies to name a few. What's most interesting about this group is their effectiveness at conducting deception operations in an effort to afford their sponsors some level of plausible deniability. We will address three instances in which Sofacy is believed to have employed a false front in order to mask its true intentions. As mentioned before, due to the sensitivity of specific data and sources, we will not reconstruct our investigations to prove these are, in fact, acts of Sofacy, but rather present the narrative in the hope of supporting a wider debate.

CyberBerkut

In March 2014, a supposedly Ukrainian-based, pro-Russian separatist group calling itself CyberBerkut rose to prominence by conducting various attacks against the Ukrainian government and other entities supporting Ukraine during the annexation of Crimea [15]. The group was extremely active in 2014 and 2015, targeting not only local Ukrainian government and infrastructure, but also NATO resources, US defence companies, and the German Bundestag to name a few. While the group operated under the guise of being part of the larger Anonymous collective, further research has indicated that this may not have been the case. Some researchers in the community have indicated that a connection between Sofacy and CyberBerkut exists [16], with others going as far as stating they are one and the same. When looking at the timeline of events leading up to the annexation of Crimea and the conflict in Donbass, one can certainly make the argument that the actions of CyberBerkut align closely with Russian interests.

On 22 February 2014, then President Viktor Yanukovych was ousted by the Ukrainian parliament. Yanukovych eventually fled and later surfaced in exile in southern Russia. Following this, on 25 February, the special police forces in Ukraine known as 'Berkut' were dissolved by parliament. In the following weeks, unidentified gunmen, widely believed to be Russian soldiers,

[6] Also known as DarkSeoul, Operation Troy, WildPositron and TEMP.Hermit, or in relation to the malware families Destover, Duuzer, Hangman, and SpaSpe.

[7] Initially presented at the 2016 Kaspersky Lab Security Analysts Summit (SAS) in collaboration with *AlienVault Labs*' Jaime Blasco.

[8] As noted by *FireEye* researchers, probably a misspelling of 'Pricipes', a term for spearmen or swordsmen [13].

[9] Also known as APT28, Tsar Team and Pawn Storm, among others.

seized control of various checkpoints and airports throughout Crimea. Around the same time (3 March 2014), the domain cyberberkut[.]org was created and the group made its first public appearance. Before this date, there is no known data showing that the group or its members existed in any capacity. This becomes relevant when looking at the other examples given later in this section, as hacktivist groups tend to have some kind of history supporting their lineage.

Some of CyberBerkut's attacks also coincidentally targeted the same victims as Sofacy. In January 2015, CyberBerkut conducted attacks against multiple German government websites, including the German Bundestag [17]. Subsequently, in May 2015, the Bundestag was also attacked by what was later confirmed by the German government as Sofacy [18]. While it is not uncommon for two actors to target the same victim, the argument could be made that both attacks were conducted by the same actors, or possibly that some type of 'trade-off' occurred between the two.

CyberCaliphate

On 24 December 2014, a new pro-ISIS hacktivist group by the name of CyberCaliphate announced its presence by taking control of the *Albuquerque Journal*'s mobile application and broadcasting propaganda to its subscribers [19]. Then, on 12 January 2015, CyberCaliphate seized control of the United States Central Command (USCENTCOM)'s *Twitter* and *YouTube* accounts [20]. In February 2015, they proceeded to compromise *Newsweek*'s *Twitter* account [21] and also sent propaganda text messages to subscribers using *WBOC Maryland*'s text alert system [22]. Following these attacks, in April 2015, the group lashed out again, this time against a French television station, *TV5 Monde* [23], where they were able to block broadcasts for 11 stations and seize control of the TV station's social media accounts.

While initial speculation pointed to this being yet another pro-ISIS group attempting to spread their propaganda to the masses, further research turned up interesting data that potentially pointed to a Russian entity, specifically Sofacy, as the real culprit. First, there was no evidence of the group's existence prior to the initial attacks in January. As stated previously, it is not typical for a hacktivist group to have no pedigree or lineage prior to a large defacement such as USCENTCOM. Secondly, *FireEye* later revealed that the IP address of the website where data from the *TV5Monde* hack was published was part of the same netblock of previously known Sofacy infrastructure [24]. Additionally, other sources have shown that the registrant information used to register the group's official domain cyb3rc[.]com is linked to other well-known Sofacy domains.

While the exact motivation is unknown, it is believed that CyberCaliphate was created to provide the Sofacy actors a way to conduct psychological operations against certain targets of interest while providing a level of plausible deniability. Whatever the case may be, if it weren't for a couple of small errors on the part of the actors, CyberCaliphate could have remained a useful front for their operations.

Yemen Cyber Army

In the wake of the success of the CyberCaliphate campaign, another hacktivist group emerged: Yemen Cyber Army (YCA) appeared in May 2015. As with the other two groups, YCA also had no prior history and its members were completely unknown. They proclaim to be a hacktivist group operating out of Yemen, specifically supporting the Houthi movement and possessing strong anti-Saudi sentiments.

Saudi Arabia mounted a bombing effort in March 2015 against Yemen to suppress the ongoing Houthi forces that were overtaking Yemen's government in Sana'a. Shortly after this campaign in April 2015, the website of the London-based *AlHayat* newspaper was defaced by YCA. Subsequently, in May 2015, the Saudi Ministry of Foreign Affairs was also hacked by YCA and thousands of internal communications were published on *Wikileaks*. Many researchers currently believe YCA is an Iranian-led front to cause damage and spread propaganda against the Saudi government, but after investigating the group and its activities further, a new theory has surfaced, indicating that this is potentially another campaign orchestrated by Sofacy. While there is no solid proof showing that this is, in fact, Sofacy and not Iran, we point to factors that may shed some light in favour of the former.

First, it is important to understand the relationship between Russia and Saudi Arabia. Saudi is arguably one of the top nemeses of the Russian government, dating as far back as the 1980s when Saudi supported the Mujahideen during the Soviet-Afghan war. Saudi is a key US ally in the Middle East and also allied with other countries in the region that do not hold close diplomatic relations with Moscow. In February 2015, Saudi deployed fighter jets to Turkey for use in ground-based operations in Syria to support the militant opposition. Also during this time, Russia openly accused Saudi of depressing oil prices in an effort to tank the Russian economy.

All of this speaks to the potential motive of why Russia would be very much interested in damaging the Saudi government.

Around the same time, in February 2015, Sofacy was discovered using a zero-day exploit against a select few targets, one of these being the Saudi Embassy in Ukraine. This exploit was used in the wild only by Sofacy until April 2015, when *Microsoft* finally patched it. The very limited use of this exploit during this time frame, combined with the fact that the Saudi Embassy was actively being targeted, shows a very real possibility that Sofacy had access to the Saudi Ministry of Foreign Affairs networks as early as February 2015.

Another interesting tie to Sofacy is a domain that was established by YCA in June 2015 (wikisaleaks[.]com). This domain was registered using privacy-protected services, but digging behind the protection revealed that the email registrant used for this domain was 'nghockeng@yandex.com', the same as was used to register three other domains utilized by YCA (yemenica[.]com, yemenica[.]org, and yemenica[.]net). While this specific registrant has never directly been tied to known Sofacy domains, the use of *Yandex* email accounts is a favourite for the group. Also interesting are the nameservers used for wikisaleaks[.]com. This domain utilizes nameservers from orderboxdns[.]com, which is also a highly favoured provider for Sofacy. Further digging revealed that the domain is being hosted at 87.236.215.129. While this IP address has never been used by Sofacy before, the subnet is also a favourite of the group's. The following are some other IP addresses in the same subnet used by Sofacy in past attacks:

87.236.215.13 87.236.215.60 87.236.215.99
87.236.215.102 87.236.215.132 87.236.215.134
87.236.215.143 87.236.215.246

As stated above, while none of these observations represent the proverbial 'nail in the coffin', in combination they strengthen the claim that Sofacy could be behind YCA, just as it has been with the prior two campaigns. Another possibility is that Sofacy could be providing information and assistance to an Iranian-based group as they may share an interest in damaging the Saudi government. Whatever the case, Sofacy has displayed a predilection and gift for running effective deception campaigns against targets of interest, and is likely to continue to do so.

On blame shifting

The following threat actors have chosen a different tactic. Rather than persuade researchers into thinking that their attacks are the work of a different category, lesser calibre player, these threat actors instead attempt to cast the blame onto another recognizable nation-state actor. The attempts are presented in rising order of perceived effectiveness.

Duqu 2.0

The formidable Duqu was first discovered in 2011 by *CrySyS Lab* and extensively researched by *GReAT*. The initial notoriety of Duqu was largely due to the malware's relationship to Stuxnet, with specific modules displaying traits of shared development indicative of the Tilded platform. But Duqu is most admirable for its audacity, as displayed by the choice of infecting a Hungarian digital certificate authority in order to solve an operational requirement. Appreciative of *GReAT*'s admiration, as conveyed through more than half a dozen blog posts and extensive analysis, the legendary threat actor resurged by hand-delivering a vastly improved version of the malware to our doorstep. This time around, Duqu was equipped with up to three zero-day exploits including a kernel exploit (CVE-2015-2360), memory-resident malware signed with a stolen digital certificate, and a unique persistence philosophy cognizant of the victim as a network rather than a collection of independent victim machines [25]. Other unwitting recipients of this gift included venues for P5+1 talks, industrial control systems-related companies, and telecommunications providers [26].

Duqu 2.0 is entirely modular, spanning upwards of 100 plug-in variants, with separate modules to handle specific operations like communications with command-and-control infrastructure and tunnelling directly into the victim's LAN. Among the latter is an NDIS filter driver internally named 'termport.sys'[10], whose functionality is toggled by packets that include the hard-coded magic string, 'romanian.antihacker' in the 32-bit driver. The 64-bit version, on the other hand, uses 'ugly.gorilla': a reference to a member of Comment Crew/APT1 [27]. Wang Dong, known by the alias 'Jack Wang' or the handle 'Ugly Gorilla', was one of the five PLA officers indicted [28] by a US grand jury in 2014 on 31 criminal counts related to computer abuse activities. Though APT1/Comment Crew remains active to this day, presumably with Wang Dong amongst its ranks, the idea that they are behind the Duqu 2.0 attacks is patently ridiculous.

Apart from a series of attributory indicators pointing in an entirely different direction, the APT1 group would have needed to get their hands on the original Duqu source code given the structural similarities in some modules of the new platform. The more likely explanation is that the threat actor noted the greater risk posed by a device driver (compared to the memory-resident modules) and peppered some false flags to misguide incident responders. By citing a publicly indicted member of a well known and widely reported APT crew, the Duqu developers may have mislead an IR team whose technical expertise in the area of threat intelligence amounted to *Google* searching binary strings with no greater awareness of the threat landscape to draw from.

TigerMilk

The mysterious TigerMilk[11] actor is a thus far unattributed, privately reported discovery. The campaign started in early 2015, targeting Peruvian institutions and entities exclusively for a period of six months. The attacker used a commonplace exploit (CVE-2012-0158) in conjunction with a curriculum vitae stolen from a local victim in order to infect users with custom credential-stealing malware. The position-independent backdoor was injected into processes like explorer.exe and various browsers. In 64-bit systems, the malware would spawn a separate desktop with its own infected explorer.exe to avoid suspicion. However, in operation the malware was clunky and caused perceptible instability so neither the development nor the intended functionality were indicative of a sophisticated actor. So why mention TigerMilk?

The one particular feature of TigerMilk that makes it noteworthy is its use of a notorious digital certificate. Every backdoor deployed is signed with the same stolen *Realtek* certificate[12] as Stuxnet(.a/.b). The samples were compiled and signed long after the certificate's validity expired[13], thereby obviating its use as a means of bypassing execution controls. As such, the only imaginable value of signing these samples with this particular certificate is to fool incident responders and researchers into casting blame on the notorious Stuxnet team for an attack on Peruvian military and government institutions. Moving beyond this basic deception, the true unresolved mystery of TigerMilk is: how did this new actor get its hands on this specific certificate?

The man behind the curtain

One of the most advanced and prolific known threat actors is the Turla group. They have existed in some shape or form since at

[10] The filename at time of deployment was changed to 'portserv.sys'.

[11] The private TigerMilk report was pushed to *Kaspersky Intel Report* subscribers in November 2015.

[12] Serial number: 5e 6d dc 87 37 50 82 84 58 14 f4 42 d1 d8 2a 25.

[13] 12 June 2010.

least 2006, but some speculate that their true origins may be as much as a decade earlier. It's widely accepted that Turla is a state-sponsored actor originating from Russia. What makes Turla so fascinating is the group's attention to detail, operational security, and advanced tactics for victim data exfiltration. During one specific incident in November 2012, the Turla group showed their willingness to engage in deception tactics when cornered.

Turla compromised a handful of victims during this campaign, but one particular European victim proved especially enticing. The group had deployed their typical first-stage malware, Wipbot, on the victim's system and began their normal routine of collection and monitoring. At some point, the victim became suspicious and decided to engage their incident response (IR) team to investigate their network and determine the source of nefarious activity. The IR team began their normal process of surveying the system and running various investigative tools, however, they did not pull the system offline. Turla became aware that they would soon be discovered. At this point, most actors would simply uninstall their malware from the victim and move on. Instead, Turla decided to have a bit of fun with the IR team in an attempt to cover their tracks.

They proceeded to utilize Wipbot to download and install a second-stage binary. But this was no ordinary Turla malware, rather they installed a somewhat rare, already compiled piece of Chinese malware by the name of Quarian. The Quarian malware communicated back with infrastructure located in Beijing, which was neither under Turla's control nor related to previous Turla operations. They then proceeded to uninstall the Wipbot malware and erase their tracks from the victim systems.

This proved to be a great move on their part, as the IR team spent countless hours tracking down the Quarian malware and assuming the victim had been targeted by a Chinese-based APT group. Because they used a lesser-known piece of malware, the investigators first had to identify the family, then dig through the sprawling infrastructure in search of some level of attribution. All of this work was obviously pointless and served as a fantastic smoke screen for Turla's retreat.

A COMPLICATED LANDSCAPE

Beyond the particulars of an investigation or the cunning of a given actor, attribution suffers from a variety of complications ranging through varying external motivators, inherent limitations, and methodological disparities across vendors and research teams. This merits a more high-level discussion of conditions complicating attribution in targeted attacks. The intended takeaway is that attributory analysis is far from straightforward, largely hermeneutic, and in no way a standard practice at this time.

General complications

Your sexiest attribution, please

The private threat intelligence production landscape involves various intertwined forces that arise from an interplay between private industry, private and public consumers, and public attention. Various motivations arise within this interplay, most notably that of the value of media attention and *free PR*, which has proven a notable motivator for the rise of threat intelligence production in the anti-malware industry. While some TI teams have arisen out of the need for in-house elite researchers to deal with sophisticated attacks, many have followed from the realization that TI products garner heavy media attention with inherent marketing value. Judgment for this tactic is dampened by recognition of its value in motivating the awareness and adoption of the need for mature threat intelligence in an industry where even corporate giants and leaders in technology products have been less than willing to devote even meagre resources to tackle a complex, demanding, and ever-evolving problem.

However, as is often the case with easy value-added ventures, abuse is quick to follow, as immature threat intelligence producers (often never-before-seen start-ups) have taken the stage with bombastic, absurd, and unverifiable attribution claims for the sake of headline stories that bring their companies to momentary prominence. These stories will serve as an excuse to approach or even extort potential victims-cum-customers whose dismayed IT teams are forced to spend precious limited resources chasing down nebulous leads for the sake of due diligence to reassure an anxious C-suite of the continued integrity of their systems, reputation and intellectual property. These tactics have borne ephemeral fruit not only with claims of sophisticated attacks but also presumed breaches, larger-than-life credential dumps, and ghost botnets.

This is not the only case where an eager but sometimes technically naïve media machine is abused to the detriment of the threat intelligence production landscape. In an effort to foster a sense of balanced debate, media outlets have entertained any sign of contention in the research community, lending credence to doubt even where there is little ambiguity and breeding a class of pundits charitably referred to as professional *cyber-truthers*, who have built careers on the basis of sparsely substantiated contrarian attributory claims. While legitimate disagreement in the research community should not be diminished, we should also acknowledge the prevalence of sniping between competing vendors, the anti-anti-malware peanut gallery, and other skeptics eager to disparage popular research at face value.

In response, larger outfits are increasingly adopting a closed-door approach to the distribution of threat intelligence products, or the partial withholding of significant details intended solely for paying customers – an approach with obvious benefits and latitude for expression, but one that's also prone to validation issues as the value of the research product cannot be verified by qualified third parties[14]. On the off-chance that a given vendor's products prove dubious or inconsequential for a single-source consumer, this can lead to an erosion of trust in threat intelligence as a whole.

The one-eyed man is king

The very nature of threat intelligence results from a fascinating injection of third-party observers into the dynamic between an attacker and victim, often by chance. This serendipitous

[14] Discussed as a validation crisis likely to arise in threat intelligence [29].

interplay may be the result of a contractual placement of defence solutions in the victim's network, the maintenance of service infrastructure (as in the case of ISPs and webmail, cloud or storage providers), or by stumbling upon attack artifacts found on multi-scanners, staging servers, or through their foolishly wide distribution, in the case of hamfisted attackers.

The implicit takeaway is that the position of the threat intelligence producer will shape the nature of the research by virtue of limited visibility. All possible producers inevitably suffer from varying degrees of limited visibility. This often means that two different similarly positioned companies possess different incomplete parts of the same operation, that endpoint security companies see payloads with no network traffic, that ISPs see network traffic and victimology but no payloads, and so on. To then claim perfect awareness over a given campaign will prove short-sighted folly, given that little deters the same actors from continuing their efforts, often retooling and targeting the same victims. Failures become apparent as alternate reports contain vaguely overlapping IOCs that showcase the incompleteness of a single-source report and extended campaigns against a given victim may abuse previously unseen attacker capabilities possibly witnessed by other vendors.

Analyst training

An often ignored facet of the threat intelligence production cycle is the role of the analyst whose purpose is to coalesce various sources of information, arrive at various conclusions, and vet the overall logic of the finished product. Sadly, at this stage in the rise of the threat intelligence industry, deficient hiring practices overemphasize specialized technical knowledge and eschew generalist broad-thinking capabilities, often assuming technical candidates will bring these in tow. This is seldom the case, as showcased by talented malware reverse engineers who don't consider themselves 'threat hunters', as well as by outlets promulgating technical malware breakdowns who fail to identify the connection of these artifacts with larger campaigns.

Threat intelligence analysts often suffer from deficient training in conventional intelligence analysis. Industry forums and conferences are heavily populated with trainings and ample resources aimed at fostering skills such as reverse engineering and 'threat hunting' that are essential to the production process, but among these little is exclusively aimed at fostering the broad-thinking methodologies necessary to turn technical indicators and victimology into a reliable estimative and actionable consumable product. Many military and intelligence metaphors and models are suggested at this stage but these are still reliant on the ability of the analyst to weigh different possibilities and scenarios, keeping excitement for a given theory at bay, and allowing for accurate estimative language to make its way to the final recipient.

In simpler terms, it's necessary to state that a hunch is a hunch, that some conclusions are sparsely sourced or cannot be independently arrived at, or that no conclusion can be made at this time. There exist a handful of exemplary threat intelligence veterans whose familiarity with previous operations allows them to express high accuracy intuitions that speak to the provenance of targeted attacks; the remainder of us mere mortals must be able to follow the logical foundations of a theory to arrive at an accurate action plan that can independently be sustained by the consuming IT and IR teams.

METHODOLOGICAL COMPLICATIONS

Scope

Even among seasoned threat intelligence producers, significant disagreements arise. Investigating a targeted attack is a largely hermeneutic endeavour as researchers interpret sparse fragments and indicators to understand the means, capabilities and (hopefully) the intentions of the attackers. A common pitfall arises from a lack of consensus on whether a given threat actor is defined by a shared toolkit, overlapping infrastructure, or similarities of tasking. The disagreement is most visible in disparate naming schemes across vendors, an issue that isn't as superficial as picking a shared name when differences in visibility are coupled with one vendor's insistence to categorize an actor by their shared use of a given lateral movement tool while another vendor focuses on a cluster of phishing infrastructure. The issue extends beyond mere preference to reflect a heterogeneous understanding of the scope and intended functionality of threat intelligence products.

Functionality

Further complications arise when considering the variable intended functionality of threat intelligence products. Is the intended purpose PR value, enterprise defence, or cyber situational awareness? Each of these is a legitimate purpose but not all are equally served by the same product. We touched upon the complications that arise with seeking PR value, which tends to require audacious attribution claims that stand in conflicting opposition to the alternatives mentioned. A product intended to support an audacious claim particularly through wide and loud distribution will cripple its own actionable value as it spooks the attacker. The likely reaction is also a general retooling that cripples any prolonged awareness or ability to track a known determined malicious actor.

On the other hand, defending an enterprise network gains little from country-level attribution claims. By its very nature, the institution is endowed with little latitude to retaliate against a nation state no matter what the injustice of a cyber-espionage or sabotage campaign. Defending the enterprise requires campaign-level understanding that includes an awareness of infection vectors, toolkits, and attacker standard practices. Loosening the grip of a specific campaign will then allow the victim enterprise to switch to tracking the threat actor or related actor cluster in preparation for the future attempts that will almost certainly come.

Finally, in the case of the larger project of cyber situational awareness, there are requirements that sometimes stand in juxtaposition to both the media imperatives and the defence of any particular entity. With the most cunning and resilient actors, tracking may well require an infection not to be cleared immediately, so as not to spook the actor being hunted.

Understanding that some threat actors are so cunning and well resourced that playing network 'whack-a-mole' is unlikely to deter them in the least, researchers stand to benefit from quiet observation and the deployment of radical tailored defence solutions rather than the simple disinfection of a given machine. Though this approach may be shocking to those critics who consider the single role of anti-malware to be that of machine disinfection, it is important to consider the heavy weaponry commanded by actors of this calibre. Exemplary 'god mode'-style zero-day exploits are a concern for an entire software ecosystem and not just a single victim. In turn, these require a large-scale immune response, beginning with the discovery and understanding of the technique leveraged, propelled in priority by its abuse in the wild, and only then postulated for resolution by the software behemoths that support the relevant codebase. The role of the anti-malware industry here extends beyond simple metrics and immediate customer obligations to that of defenders of the larger ecosystems in the face of unscrupulous actors.

Given an understanding of how the intended audience shapes the research imperative and thereby the consumable product, there is a need for research teams to define their intended audience during the production cycle itself and not after.

REFLECTIONS

Threat intelligence has true value beyond the current hype of an emerging pocket in the information security industry. As showcased by the multiple examples presented of abuse in the wild, there is a need for professionals whose job it is to understand the apex predators in the malware ecosystem. In juxtaposition to IT and IR teams whose overlapping responsibilities in responding to attacks are sometimes considered capable of obviating the need for TI, the latter is the sole producer of the historical context that helps mitigate the attackers' potential ability to manipulate responders into chasing down ghosts, by virtue of familiarity and a broad-thinking methodology. In place of a summary conclusion, we instead leave open questions in need of deeper reflection, on the part of both producers and consumers of threat intelligence, to serve as our final takeaways in furthering a much needed conversation.

What is solid attribution?

Considering the common bases for attribution, limitations in visibility specific to each research camp, and requirements specific to each type of customer, what could possibly make a satisfactory attribution claim? We must ask ourselves if there can even be such a thing. In a hypothetical scenario where we have packets captured en route (as in the common jab 'PCAP or GTFO'), could it not be a backdoored system being used to proxy through? Where we catch a nation-state operator red-handed, would we not need an understanding of the provenance of their tasking? More realistically, there will never be a solid enough attribution claim for everyone to get behind. Rather, the combination of multiple indicators helps an analyst make an educated determination of the trustworthiness or accuracy of a claim. This further highlights the importance of estimative language that allows others to make strategic decisions based on preferably unbiased facts with the analyst's opinion as a guide.

What is actually needed?

A more sobering metric for attribution claims rests in understanding the action capability of the intended recipient. What can a single non-governmental entity do with the name of a nation-state operator? How does it bolster its defensive stance against further attack to be told which Chinese citizen to peg on its dartboard? On the other hand, a government (whose recourse includes diplomatic, legal, and even retributory CNO) stands to benefit from the greatest possible level of fidelity in attribution. The question 'what do you actually need?' has to be answered in relation to 'who are you meant to be serving?'. The guiding principle remains the production of actionable intelligence and not the feeding of 'cyber-voyeurism' and grandstanding.

Who can really do attribution?

The attribution limitations do not apply to all producers equally. If a 'PCAP' is considered the ultimate measure of attack fidelity, then what entity is more supremely positioned to perform attribution than the modern SIGINT agencies? These 'gods of the wires' are positioned in such a way as to enact near perfect recall when an attack is discovered, either by snooping on the wires or having 'popped' the routers in a country of interest. In true Greek irony, the Cassandras of the modern age are hamstrung by their own Apollonian curse: as intelligence agencies they are blessed with the ability to see but not to publicly substantiate, the gift to attribute without being believed.

Who are you hacking back?

Finally, for anyone holding out hope that anything like 'cyber-retribution' can ever legitimately enter the stage for private entities, we hope to have provided enough reason for ample skepticism. In a world where solid attribution claims in the private sector are unlikely, how does one go about 'hacking back'? Moreover, with cunning attackers manipulating victims into casting blame towards an unrelated entity, who's to blame when misattribution leads to a retributory attack on another blameless victim?

REFERENCES

[1] Darkhotel's attacks in 2015. Securelist. August 2015. https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/.

[2] Schneier, B. Simultaneous Discovery of Vulnerabilities. Schneier on Security. February 2016. https://www.schneier.com/blog/archives/2016/02/simultaneous_di.html.

[3] Equation Group: Questions and Answers. Securelist. February 2015. https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

[4] Fagerland, S.; Grange, W. Blue Coat Exposes ‘The Inception Framework’; Very Sophisticated, Layered Malware Attack Targeted at Military, Diplomats, and Business Execs. Blue Coat Labs. December 2014. https://www.bluecoat.com/en-gb/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware.

[5] Fagerland, S.; Grange, W. The Inception Framework: Cloud-Hosted APT. Blue Coat Systems. https://www.bluecoat.com/documents/download/638d602b-70f4-4644-aaad-b80e1426aad4/d5c87163-e068-440f-b89e-e40b2f8d2088.

[6] Cloud Atlas: RedOctober APT is back in style. Securelist. December 2014. https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style.

[7] The “Red October” Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies. Securelist. January 2013. https://securelist.com/blog/incidents/57647/the-red-october-campaign.

[8] Romang, E. http://eromang.zataz.com/2013/02/20/facebook-apple-twitter-watering-hole-attack-additional-informations/.

[9] Romang, E. http://eromang.zataz.com/2013/03/24/osx-pintsized-backdoor-additional-details/.

[10] Guerrero-Saade, J. A.; Raiu, C. Operation Blockbuster revealed. A glimpse at the spider web of the Lazarus Group APT campaigns. Securelist. February 2016. https://securelist.com/blog/incidents/73914/operation-blockbuster-revealed/.

[11] AFP. South Korea Says North Was Behind Cyber Attack on Newspaper. Security Week. January 2013. http://www.securityweek.com/south-korea-says-north-was-behind-cyber-attack-newspaper.

[12] Schwartz, M. J. South Korean Bank Hackers Target U.S. Military Secrets, Dark Reading. 2013. http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?.

[13] Pidathala, V.; Sai Omkar Vashisht, S. O.; Khalid, Y.; Singh, A. More Insights on the recent Korean Cyber Attacks (Trojan.Hastati). FireEye. March 2013. https://www.fireeye.com/blog/threat-research/2013/03/more-insights-on-the-recent-korean-cyber-attacks-trojan-hastati.html.

[14] South Korea Under Cyber Attack. North Korea suspected of carrying out major cyber attack against Seoul-based banks and broadcasters. NK News. March 2013. https://www.nknews.org/2013/03/south-korean-banks-broadcasters-paralyzed-by-cyber-attack/.

[15] CyberBerkut. Wikipedia. https://en.wikipedia.org/wiki/CyberBerkut#Activity.

[16] Lehtiö, A. Twitter. https://twitter.com/lehtior2/status/672351924734312448.

[17] Crauß, U. Cyber-Angriff auf Kanzleramt und Bundestag. Die Welt. January 2015. http://www.welt.de/politik/deutschland/article136114277/Cyber-Angriff-auf-Kanzleramt-und-Bundestag.html.

[18] Wagstyl, S. Germany points finger at Kremlin for cyber attack on the Bundestag. FT. http://www.ft.com/cms/s/0/668a131e-1928-11e6-b197-a4af20d5575e.html#axzz4CQg3T78B.

[19] Malone, P. Hoax or cyberattack? ABQ Journal’s mobile app hacked. The Santa Fe New Mexican. December 2014. http://www.santafenewmexican.com/news/local_news/hoax-or-cyberattack-abq-journal-s-mobile-app-hacked/article_32f895fa-79e4-5b13-9f6e-a43a4d2bc8da.html.

[20] CNN Staff. CENTCOM Twitter account hacked, suspended. CNN Politics. January 2015. http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/.

[21] Mosendz, P. Newsweek Twitter Account Hacked by Group Claiming ISIS Affiliation. Newsweek. 2015. http://www.newsweek.com/newsweek-twitter-account-hacked-isis-affiliated-group-305897.

[22] WBOC Victim of Another Cyber Attack. WBOC. February 2015. http://www.wboc.com/story/28070058/wboc-text-alerts-cyberattacked.

[23] ISIS-allied hackers claim worrying new attack. CBS News. April 2015. http://www.cbsnews.com/news/french-tv-network-tv5-monde-hacked-by-cybercaliphate-in-name-of-isis/.

[24] Leyden, J. Russia’s to blame for pro-ISIS megahack on French TV network. The Register. June 2015. http://www.theregister.co.uk/2015/06/10/russian_trolls_staged_tv5monde_megahack_shocker/.

[25] The Duqu 2.0 Technical Details. Securelist. June 2016. https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

[26] Duqu 2.0: Reemergence of an aggressive cyberespionage threat. Symantec. June 2015. http://www.symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat.

[27] Critical Lessons from 15 Years of Industrial Control Systems Vulnerabilities. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[28] Wanted by the FBI: Wang Dong. https://www.fbi.gov/wanted/cyber/wang-dong/view.

[29] Guerrero-Saade, J. A. The Ethics and Perils of APT Research: An Unexpected Transition into Intelligence Brokerage. Proceedings of the 25th Virus Bulletin International Conference, 2015. http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf.