2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Silent Battles: Towards Unmasking Hidden Cyber Attack

Robert Koch
Fraunhofer FKIE
Bonn, Germany
Robert.Koch@fkie.fraunhofer.de

Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
Mario.Golling@Unibw.de

Abstract: When looking at the media, it can easily be seen that new cyber attacks are reported on a regular basis. The corresponding effects of these attacks can be manifold, ranging from downtime of popular services affected by a rather trivial Denial-of-Service attack, to physical destruction based on sophisticated cyber weapons. This can also range from single affected systems up to an entire nation (e.g., when the cyber incident has major influence on a democratic election). Some of these attacks have gained broader public attention only by chance. This raises the fundamental question: do some cyber activities remain hidden, even though they have a significant impact on our everyday lives, and how can such unknown cyber involvements be unmasked? The authors investigate this question in depth in this paper.

The first part of the paper analyzes the characteristics of silent battles and hidden cyber attacks – what needs to be considered on the way towards a better detection of hidden cyber attacks? After that, an evaluation of the current cyber security landscape is provided, summarizing what developments we can see and what we can expect. Based on this, the complexity of detecting hidden cyber attacks is discussed and we ask the question: why does detection fail and how can it be improved?

To investigate this question, the capabilities of the attackers are examined and are reflected in a 3-Layer Vulnerability Model. It is shown that a traditional Cyber Kill Chain is not sufficient to detect complex cyber attacks. Therefore, to improve the

detection of hidden cyber attacks, a new detection model based on combining the 3-Layer Vulnerability Model and the Cyber Kill Chain is proposed.

Keywords: *cyber war, cyber defense improvement, attack model, detection requirements, detection transitions, Cyber Kill Chain, 3-dimensional detection model*

1. INTRODUCTION

Whether we consciously perceive it or not, whether we want to admit it or not, our everyday life is entangled with information technology (IT). Today, IT is a corner stone for our daily office work and is even a prerequisite for administrative tasks at public authorities. It covers areas from transportation and telecommunication up to industrial control systems and the financial sector. In short, today's world is more cyber-dependent than ever. However, due to (i) its economic potential, but also because of (ii) the alleged and at least partially achievable anonymity, (iii) regularly occurring security vulnerabilities, and (iv) the lengthy international prosecution of cyber crimes, the Internet offers a considerable potential for abuse. To counter this abuse, various protection systems and programs have been published and established over the past decades. In parallel, the fundamentals of the Internet, such as standards and protocols, have also been improved or developed from scratch to reduce the risks involved with a broad usage of the Internet. Despite these efforts, the economic losses remain very high. In this regard, corresponding estimates are often problematic, due to (un)available data, the expected number of unreported cases and the complexity of indirect costs. A recent estimate by RAND, which was published as part of their "Cyber Risk Calculator", states that "the global cost of cyber crime has direct gross domestic product (GDP) costs of $275 billion to $6.6 trillion and total GDP costs (direct plus systemic) of $799 billion to $22.5 trillion (1.1 to 32.4 percent of GDP)" [1]. The authors emphasize the high sensitivity of the numbers regarding the input parameters. Nevertheless, even the "most favorable" case reveals the enormous loss that results from cyber incidents. According to McAfee [2], for instance, the global cost of cyber crime has now reached as much as $600 billion - about 0.8 percent of the global GDP. As already mentioned, such estimates are extremely difficult to perform, usually due to a lack of sufficient data. For many reasons, such as the fear of reputation loss, companies are often cautious whether to report cyber attacks or not. Even today, reporting obligations are limited to a few areas such as critical infrastructure. This also hampers the detection of cyber attacks. In various reports, cyber security companies have regularly warned that insufficient detection procedures can be expected in areas that report little or even no cyber attacks.

In practice, this fundamental problem becomes even more difficult once different groups and abilities of attackers, and the associated challenges of detection, are taken into account. In recent years, extensive measures for the preparation of the battlefield can be observed. In particular, the Snowden Leaks [3] and the Vault 7 [4] and 8 [5] files have revealed details about comprehensive programs for the manipulation of hardware, software and standards. Some of those attacks have gained broader public attention only by chance. This raises the fundamental question of whether some cyber activities may remain hidden even though they have a significant impact on our everyday lives, and how as yet unknown cyber involvements can be unmasked. In numerous cases, cyber attacks remained unrecognized for a long time, often to the surprise of the victim.

A. On Silent Battles and Their Relevance - A Brief Review

The element of surprise, that is the ability to conduct an attack without warning, is one of the central and therefore most discussed aspects of military theoreticians in general. According to the Prussian general and military theorist Carl von Clausewitz (one of the most well-known analysts of normative behavior and trends in military affairs and military history), the concept of war, therefore the act of violence to the opponent in order to the fulfill one's own will [6] requires first and foremost the pursuit of relative superiority [7]. For this in turn, the surprise of the enemy [8] is more or less always of utmost importance. Without surprise, superiority (the crucial point) is actually unthinkable [8]. Thus, surprise is the precondition for superiority, which in turn is the greatest precondition of victory [8]. Where both (surprise and superiority) succeeds, confusion, and broken courage of the opponent are the consequences [8]. These considerations are similar, for example, with those of Sun Tzu, another well-known military theorist. For Sun Tzu, in the fight, direct actions lead to confrontation, surprising actions lead to victory [9]. Although there are roughly 2,500 years between Sun Tsu and today, little has changed. Silence is the prerequisite for surprise, which in turn is a prerequisite for superiority. Superiority, after all, is the most general principle of victory.

B. Silent Battles - A Definition of Terms

The term Silent Battle therefore has several facets. Based on the aforementioned considerations, we define the term Silent Battle with regard to cyber activity as

- a hostile encounter or engagement between opposing parties (nations, organizations, military forces)
- characterized by an absence or near absence of "noise" or "sound".

This may in particular be due to the fact that the engagement (i) remains hidden (i.e., no actions have been discovered, no effects can be observed) or (ii) allows no attribution

(thus no legally consistent link to the opposing party can be established), or (iii) is not relevant for the public (e.g., no media coverage) or (iv) is not disclosed (e.g., because a company prefers to keep an attack secret so as not to upset its customers).

C. Silent Battles in the Cyber Domain

At this point, in the context of hidden cyber attacks, one also has to raise the question, whether "noise" can also be used to distract attention. Concerning this matter, a look at the cyber incidents of recent years reveals that Distributed Denial-of-Service (DDoS) attacks seem to be used to mask the actual attack in order to divert the IT security department. For example, a comprehensive study of DDoS attacks published by Kaspersky in 2015 came to the conclusion, that "74% of attacks that lead to a noticeable disruption of service coincided with a different type of security incident, such as a malware attack, network intrusion or other type of attack" [10]. On the other hand, other companies disagree and present different results of the analysis of data available to them. With respect to DDoS attacks covering other breaches, Verizon made a humorous comparison to the government covering up evidence of alien visitation: it is often heard but not so easy to prove [11]. Based on their evaluation, "this year's data set only had one breach that involved a DoS, and in that one, the breach was a compromised asset used to help launch a DDoS, not the other way around" [11]. These essentially different results with respect to the same elementary attack vector, namely DoS, show the challenge of analyzing the cyber security environment. Therefore, Silent Battles in the cyber domain *may* be accompanied by noise like DDoS, but of course they do not have to be. Accordingly, aspects like this must also be taken into account when identifying opportunities for hidden cyber attacks, and other attack vectors must be considered as differentiated.

D. Structure of the Paper

To investigate the question whether some cyber activities may remain hidden even though they have a significant impact on our everyday lives or how yet unknown cyber involvements may be unmasked, the paper is structured as follows: an analysis of the evolution of the cyber security landscape is presented in Section 2, highlighting different aspects of what we know, and what we can expect. In order to develop new ways of detecting hidden attacks, Section 3 applies a 3-Layer Vulnerability Model to investigate potential attackers, their capabilities, and their characteristics. To clarify the particularities, some examples are discussed and a possible usage of the characteristics in order to identify hidden attacks is presented. Based on this theoretical foundation, Section 4 proposes a first model for the identification of hidden attacks. For this purpose, some Lemmata regarding observable respective useful properties are motivated and introduced before a three-dimensional extension of the current Cyber Kill Chain is proposed in order to improve the identification of hidden cyber attacks. Finally, Section 5 summarizes the key aspects of the paper and presents our

next steps, including the evaluation of a prototypical implementation of our model by using suitable datasets.

2. EVOLUTION OF THE CYBERSECURITY LANDSCAPE

In order to identify further characteristics such as the importance of noise in the context of cyber attacks, the next step is to look at what we currently know about cyber attacks and the developments in this area of the last few years.

A. What We See

As there is nowadays a variety of reports on an annual, half-yearly or quarterly basis available, as well as occasion-related publications, only a few key findings and observations of selected recent reports, which are most important for the paper, are summarized here.

As companies like Verizon, Symantec, IBM or Kaspersky have huge "sensor networks" available like, for example, the evaluation of data generated by nodes which are equipped with endpoint protection, a good picture of different developments and incidents can be generated. However, it must not be forgotten that due to the complexity of the cyberspace and its systems, each and every system can only provide its viewpoint, which depends on many factors. Results of different systems can support each other, but also quite different results can be achieved, as in the aforementioned example of the DoS attacks.

Of course, the basic risk posed by cyberspace today is not only addressed in the reports of IT companies alone. Having a look at The Global Risks Report 2019 published by the World Economic Forum, data fraud or theft and cyber attacks are placed 4th and 5th on the Top 10 risks in terms of likelihood, with rising cyber dependency as one of the main risk-trends in 2019 [12]. Various reports underline the fact that a cyber incident is coming, and it is therefore essential for the companies to prepare themselves accordingly (e.g., see [11, 13]). As Verizon highlights, state institutions are in a particularly bad situation: "Depending on function, government entities may be targeted by state-affiliated groups, organized crime or employees" [11].

One phenomenon that has been observable for a long time is highlighted: the discrepancy between the perception of the threat of cyber attacks and the lack of *strategically* addressing the threat. While many companies are aware of the danger, it is rarely considered a strategic priority [14]; this also holds for the industry and the area of operational technology (OT), where for example "only 23% are compliant with minimal mandatory industry or government guidance and regulations" [15]. The

risk increases all the more because of the increasing convergence of IT and OT and the growing use of Industrial Internet of Things (IIoT) devices [13].

This dangerous discrepancy can also be explained by the fact that cyber attacks are still a "mystery" for companies. For example, Accenture analyzed that for 71% of their respondents, cyber attacks are still a "bit of a black box; we do not quite know how or when they will affect our organization" [13]. On the other hand, if one looks at the professionalism of current attacks, this situation is particularly worrying. For example, the malware Triton (also called Trisis or Hatman [16]) was specifically targeting Safety Instrumented Systems (SIS), systems which enable the controlled shutdown of industrial processes when unsafe operating conditions are detected. While this malware was found in at least one critical infrastructure facility [13], the necessary knowledge and capacity to build such malicious programs is available to an increasing number of players [17, 18].

In this context, not only direct attacks are an increasing challenge, but especially attacks executed by exploiting the networks of third- or fourth-party supply chain partners. Here, a broad range of attack techniques is already in use. Accenture emphasizes, that they "have collected intelligence on recent campaigns that highlight the challenges of combating weaponized software updates, prepackaged devices, and supplier ecosystems as these all fall outside the control of victim organizations" [13]. Recent vulnerabilities with global impact like Meltdown and Spectre exacerbate the situation (see [19]), as periods of widespread vulnerability disclosure provide opportune times for actors to distribute malicious communications to users anticipating updates [13]. As a result of that, even the traditionally good advice to keep the patch level of the systems as up-to-date as possible is reaching its limits and requires practical precautions. For a better understanding of the threat, an evaluation of the attack path taken can be useful. By identifying the different steps and analyzing their characteristics, new detection opportunities may be discovered which later can be used to detect and possibly mitigate future cyber attacks [11].

From a more technical point of view, after a slight decline in 2017, significantly more malicious software was identified again in 2018 [20]. Due to the "success" for cyber criminals in 2017, an increasing number of ransomware campaigns could be observed in 2018 [20]. While these numbers are not surprising, the increasing proportion of encrypted cyberattacks is more interesting; the proportion of encrypted traffic in the Internet has been increasing for years. This follows the publication of the Snowden documents, and follows efforts from Google and projects such as Let's Encrypt [21] (now reaching a level of almost 70 percent [20], and for Google services even more than 90 percent [22]). Cyber criminals are also increasingly using encryption to disguise malicious traffic [20], another example of the dual use challenge [23].

As a result, larger companies are increasingly using Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)-Scanning technologies. This in turn weakens the security of the encrypted link and introduces new attack vectors (see [24]). The fact that security systems can be the attack vector itself is shown by numerous examples from recent years. For example, Tavis Ormandy has repeatedly demonstrated how antivirus software could be exploited for attacks due to programming errors (see [25]), while the Snowden documents have revealed numerous examples of the deliberate weakening and incorporation of backdoors in firewalls [26].

B. What We Know

Thanks to some whistleblowers like Snowden, some light was shed into the shadow of the real cyber security situation, which goes well beyond what one can read from logs of systems and reports of companies and authorities. Of course, the use of such sources always requires a reality check and a certain dose of skepticism, because it is also conceivable that deliberately generated leaks may well have the goal of disseminating false information. From a scientific point of view, there was nothing really unexpected within the disclosures of Snowden. However, the whole dimension of surveillance, and thus the severe infiltration of security systems, hardware, firmware, software and even algorithms was somehow surprising and disturbing. The documents contained, for example: information about programs for firmware persistence implants with backdoor capabilities like JETPLOW [27]; BIOS persistence implants like SOUFFLETROUGH [27] for the installation in firewalls; or hardware implants like GODSURGE [28] which exploits the Joint Test Action Group (JTAG[1]) debugging interface of the server's processor.

Other interesting information was the disclosure known as the Vault 7 breach[2], containing information on the capabilities and hacking activities of the CIA [29]. Important details disclosed related to programs like MARBLE [30] which aim to obfuscate the source of a program or even try to motivate a false attribution, WEEPING ANGEL [31], a tool to exploit Smart TVs for the purpose of intelligence gathering, or programs which aim at the steering system of cars.

Another important area is the comprehensive analysis of incidents that initially did not necessarily have to be caused by cyber means. For example, having a look at the Ukraine's power outages in December 2015 and 2016, the suspicion of a cyber attack emerged quickly after the incidents, but only extensive investigations revealed the exact occurrence and the complex attack path [32]. Taking the many pieces of the jigsaw puzzle that results from the disclosures, leaks, and recent research suggests the approximate extent of the threats in cyberspace.

1 IEEE 1149.1
2 Disclosed by Joshua Adam Schulte.

C. What We Expect

When considering what must be expected, and what may be already applied in the real-world, news reports and stories, scientific work and the associated discussions must be taken into account, and evaluated holistically. A prominent example are hardware backdoors built into products like processors or server boards. While a lot is written about the possible endangerment, and research papers pertaining to reversing the x86 processor microcode and prototypically implementing microcoded Trojans into the AMD K8 & K10 processors [33] are available, actual real-world cases are rare. An interesting but controversial example was the discussion on a hardware backdoor in the Microsemi ProASIC3 processor. While the researchers found some processor commands onboard the chip which could be used as a backdoor [34], industry argued that these functions were only undocumented debugging functionality to be used by the chip developers for testing purposes. On the one hand this can be true, but on the other hand, for a sensitive or classified application, it is a dangerous attack vector, regardless of what you call it.

In October 2018, there was a new and much more public discussion based on an article published by Bloomberg Businessweek called "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" [35]. Bloomberg claimed that China implemented tiny Trojan hardware into Supermicro servers at manufacturing time, and that government contractors and companies like Apple had been affected. Even after the immediate and vehement contradiction of the alluded companies and institutions, Bloomberg stood by their statement [36]. An analysis of the rare available technical details, completed by the Security Research Computer Laboratory of the University of Cambridge, concluded that an attack in the described manner is technically feasible [37].

Regardless of whether the case described by Bloomberg has taken place in this way, the threat of corresponding attacks is obvious, as they can be attractive for state actors because of their relatively simple feasibility, the complex and low detection options and, if properly carried out, the good opportunities for plausible deniability.

The identified attacks against the supply chain executed by nation-state threat groups like the Chinese cyber espionage group PIGFISH or the Russian BLACK GHOST KNIFEFISH group [13] and the introduction of malicious software and backdoors into industrial control systems and critical infrastructure, underlines the severe, real threat and demonstrates the further preparation of the battlefield [17].

3. DETECTING HIDDEN CYBER THREATS

Due to the complexity and rapid development of cyberspace, an attacker has numerous attack vectors from various areas available that are difficult to detect.

A. Why Detection Fails

The use of singular detection techniques like antivirus or intrusion detection systems (IDS) is not enough for adequately detecting cyber threats nowadays. Even though heuristics and detection methods such as behavior-based detection are constantly being improved, attackers are able to avoid the protective mechanisms on a large scale again and again. Detection becomes particularly difficult if tools and malicious code are specifically developed or adapted within the scope of targeted attacks.

To identify attack vectors, weak links and also detection opportunities, a kill chain can be used for the analysis. A kill chain is a phased-based model to describe the stages of an attack (see [38]). By analyzing them, weaknesses can be identified, and subsequently can be hardened. The basic steps of a common kill chain are shown in Figure 1.

FIGURE 1. COMPONENTS OF THE KILL CHAIN

For a better application to cyber threats, Lockheed Martin proposed the so-called Cyber Kill Chain for identification and prevention of cyber intrusions activity by identifying what the adversaries must complete in order to achieve their objective [39].

The proposed Cyber Kill Chain contains seven steps, namely (1) Reconnaissance: harvesting email addresses, conference information, etc., (2) Weaponization: coupling an exploit with a backdoor into a deliverable payload, (3) Delivery of the weaponized bundle to the victim via email, web, etc., (4) Exploitation of the vulnerability to execute a code on the victim's system, (5) Installation of malware on the asset, (6) Command & Control channel installation for remote manipulation of the victim and finally (7) Actions on Objectives to accomplish the intruder's original goals [39]. Figure 2 summarizes the attack steps.

FIGURE 2. CYBER KILL CHAIN BY LOCKHEED MARTIN [39]

While this model and the different steps are stringent and well understandable, the current Cyber Kill Chain still does not seem to be sufficient for the detection of sophisticated cyber attacks. As mentioned above, the attack path and characteristics of an attack are often still not really known to the companies respectively defenders [13]. While a basic model of cyber attacks like the Cyber Kill Chain can be helpful there, such a simple, one-dimensional model is often not able to describe and eventually identify especially sophisticated cyber attacks for two basic reasons: the companies can overlook the respective indicators or they may not even be able to look for them; and/or cyber campaigns may inflict several different targets and specific attack steps may only be executed against selected ones. On the other hand, the composition, characteristics and transitions of the attack steps may not be exact enough or may even be faulty, depending on the adversary and their available attack techniques. For example, if an adversary is able to introduce the vulnerability they want to exploit by using a supply chain attack, at least steps 1 to 3 of the Cyber Kill Chain, depending on the implementation and the used trigger maybe even up to step 6, must *not* be executed.

Therefore, an extension which better reflects the attackers capabilities and the cyber security- respectively vulnerability-ecosystem is required to improve detection chances.

B. Vulnerability Model

A basically 3-Layered Model can be used to describe the different kinds of vulnerabilities and their specific characteristics. In their publication "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Gosler et al. proposed a 6-Tier Cyber Threat Taxonomy to describe the capabilities of potential attackers [40]. The fundamental distinction of the attackers is based on the level of skills and breadth of available resources, building the different Tiers as follows (see [40]):

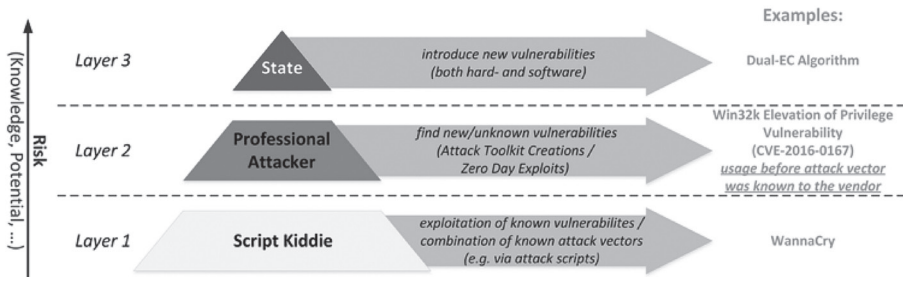
- Tiers I and II attackers primarily exploit known vulnerabilities;
- Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to discover new vulnerabilities in systems and to exploit them;
- Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to actually create vulnerabilities in systems, including systems that are otherwise strongly protected.

The original model of the Task Force used the six Tiers presented, and grouped them into three layers. For the further considerations, the use of the respective three layers is sufficient:

- Layer 1 for the exploitation of known vulnerabilities;
- Layer 2 for finding new, yet (publicly) unknown vulnerabilities; and
- Layer 3 for deliberately introduced vulnerabilities.

The model is visualized in Figure 3.

FIGURE 3. 3-LAYER VULNERABILITY MODEL BASED ON [40]



To gain a better understanding of the peculiarities of the different levels, some examples of corresponding vulnerabilities are described:

Layer 1 Vulnerabilities are the exploitation of publicly known shortcomings, which are already published, for example, by the Common Vulnerabilities and Exposures (CVE) database provided by the MITRE Corporation, including an identification number, a description, and at least one public reference [41].

Due to public knowledge of the vulnerabilities, a good defense against them *should* be possible. Typically, details of vulnerabilities will not be announced until several weeks after discovery so that developers of the affected product have time to generate and publish a patch. In practice, however, such known vulnerabilities can be exploited quite often. This can be due to a variety of reasons, for example, poor system maintenance if available patches are not installed in time. On the other hand, it may also happen that for detected and published vulnerabilities no more patches are provided., because the product is no longer supported by the responsible company ("end-of-life", EOL) or the company possibly no longer exists. In the area of operational technology (OT) such as industrial control systems (ICS) but also with devices of the so-called Internet of Things (IoT), it still happens again and again that discovered vulnerabilities cannot be closed because of insufficient system resources or other limiting factors. Certifications can also cause significant delays in deploying and installing patches, for example, in the medical area or in avionics, where any changes to the system, including patching, may require re-certification [42].

For these reasons, even the Layer 1 vulnerabilities can create significant trouble in everyday life. A prominent example is the ransomware WannaCry, which hit enterprises and institutions all over the world in May 2017 [43]. Its impacts included the taking offline of 61 National Health Service hospitals in the UK, production stops at car factories in France and Japan, and several further significant disruptions. While there was already a patch available for the exploited ETERNALBLUE[3] vulnerability [44], the ransomware particularly affected the older Windows XP/Server 2003 systems for which no patch had been published until the consequences of the worm run. Anyway, it was "just" the exploitation of a known vulnerability, but based on the aforementioned reasons, with very bad effects. At least, even if no patch is available, or in a case where it cannot be applied, the knowledge of a vulnerability can be used to prevent an exploitation by other means, for example mitigating the risk of an unpatched vulnerability by preparing respective firewall or IDS resp. intrusion prevention system (IPS) rules, etc.

Layer 2 Vulnerabilities are new, yet publicly unknown vulnerabilities which are found by techniques like code analysis, reverse engineering or fuzzing. Depending on the kind of vulnerability, it can have a quite different value, ranging from a few dollars up to 2 million dollars. A vulnerability of a less common system, or one which only generates a DoS-condition, is of course not so valuable like, for example, a remote code execution for Apple's macOS. While most companies have bug bounty programs nowadays where researchers are rewarded when submitting new identified vulnerabilities, it can be much more lucrative to sell them to companies like ZERODIUM which are working in a gray area, buying 0day vulnerabilities from researchers and selling them, to, e.g., governments. Based on the possible destructiveness of 0days, there is a debate in numerous countries whether or not governments should retain or disclose such vulnerabilities. Owning a corresponding arsenal is the prerequisite for being able to conduct cyber attacks reliably and at any time. Accordingly, they are of great importance for governments, but also in the context of organized crime and other areas, which promotes the corresponding market and trade. In this context, the RAND Corporation published the analysis of a data set of information about 0day vulnerabilities and exploits regarding the life status, longevity, and collision rates [45].

At this point, the increasingly important role of so-called 1days should be mentioned. 1days are vulnerabilities that have *just* been published. While in the optimal case, the corresponding patches are already provided and possibly even installed by automatic mechanisms, the reasons given above always result in a window of opportunity, where the corresponding patches have not yet been installed in a number of systems and therefore still can be exploited. For capable attackers, these are low hanging fruits; e.g., CrowdStrike published an evaluation that Russian hackers require only about *18*

3 The vulnerability was stolen from the NSA by the Shadow Brokers in 2016 and published by them in April 2017.

minutes to infiltrate a computer network [46]. Furthermore, new companies and offers are emerging in this area, with very fast development and provision of 1day exploits right after the release of the vulnerabilities.

Layer 3 Vulnerabilities are the culmination of the opportunities available to attackers as they offer assured access combined with a very low detection risk. This is achieved by intentionally introducing vulnerabilities into products, often without the provider of the product learning about them. The most dangerous manipulations at this level are involving algorithms and even standards. An example in this context is the Dual-EC algorithm, which was provided by the NSA with a kleptographic backdoor. This example also highlights the small number of players who are able to perform this kind of high-level attacks. In addition to the required mathematical knowledge [47], information is also needed on the corresponding influence, in this case this was on a standardization body. Other Layer 3 attacks can involve the manipulation of hardware, for example, by adding backdoors to chips or adding malicious components to a system like that highlighted in the discussion earlier in this paper on the article from Bloomberg Businessweek [35]. Recent attacks on the supply chain, which are increasing rapidly, underline the corresponding risk and may open up opportunities for sophisticated cyber attacks [48]. The complexity of today's supply chains makes it easier to attack them. At the same time, proving a manipulation can be difficult, even after a detection, as the discussion on the Microsemi ProASIC3 has shown. Thus, at least in certain cases, by appropriate reasoning, even in the case of discovery, a malicious intent may be denied, which may be another incentive to perform such manipulation.

Based on this 3-Layer Vulnerability Model, the respective attackers and their capabilities can also be described, and opportunities of detection and defense can be discussed.

C. Detection Opportunities

Taking the characteristics of the vulnerability model into account and combining them with the Cyber Kill Chain approach, new detection opportunities arise which may be useful to build new and more powerful and effective detection systems.

The fundamental detection challenge of sophisticated, and therefore quite often hidden cyber attacks, is as follows: due to the large and ever increasing amounts of data, as well as the complexity of the systems and the speed in cyberspace, a high degree of automation of the evaluation is required. On the other hand, attack vectors which are to be expected for sophisticated attacks, are often not recognizable by today's systems, which merely evaluate the data traffic by using different techniques. This includes, for example, signatures and heuristics for data classification, the evaluation

of the process flow or user behavior to identify malign programs, threats and activities. While this may be sufficient for identifying and preventing Layer 1 attacks, already protection against Layer 2 attacks is only possible to a limited extent when using these techniques, and regularly ineligible for Layer 3 attacks. One of the main problems is that important elements of the attack path of sophisticated attacks cannot be identified "by cable," for example, social engineering attacks (in the sense of the original social engineering with direct interaction [49], not in the sense of indirect vectors like spear phishing emails where there is no direct social interaction between the involved parties). Regardless, even in the case of Layer 3 attacks, interaction with systems and networks is required sooner or later, otherwise, it would not be a cyber attack.

The related actions of sophisticated attacks often stay under the radar of current detection technology, as they are specifically adapted or even designed for the respective target. However, adding knowledge about the attacker and their capabilities, as well as adding additional sources for the evaluation, means that different measures can be taken to retrospectively identify evidence of a sophisticated, yet hidden cyber attack.

FIGURE 4. ENRICHMENT OF THE DATA TO BE EXAMINED DEPENDS ON THE LEVEL OF THE ATTACKER.

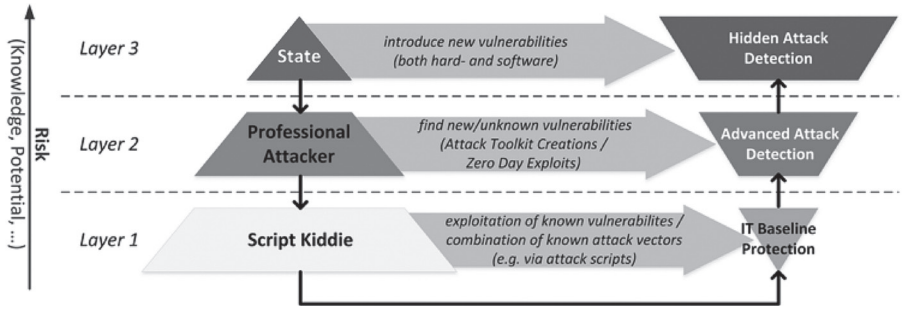


Figure 4 highlights the basic idea of the hidden cyber attack detection: depending on the Layer of the attacker, additional resources are included into the evaluation, indicated by the opposing surfaces; the more hidden the cyber attack, the broader the information base must be. For example, if there are indications that an attacker has Layer 2 capabilities, additional sources of information can be evaluated and existing data can be re-evaluated. For example, the detection threshold of a system can be adapted and possible anomalies can be recalculated, or external sources of information like news about leaks and vulnerabilities can be consulted for the evaluation. In order to model this, some expectations regarding the opponent have to be defined.

4. TOWARDS UNMASKING HIDDEN CYBER ATTACKS

To enable a retrospective identification of hidden cyber attacks, we propose a new evaluation scheme based on the combination of Cyber Kill Chains and the 3-Layer Vulnerability Model, therefore resulting in a 3d-detection model consisting of the respective Cyber Kill Chains on each Layer and linked with a corresponding timeline on each Layer.

A. Behavioral Rule

In order to implement a corresponding evaluation, it is necessary to create a basis of how the cyber attacker may move. The following Lemmata are proposed; note, that an adversary may try to use this knowledge when choosing her means to again reduce the probability of detection of a cyber attack. Nevertheless, this again may affect other detectable traces by non-controllable side-effects, including changes on the 0day-market, or resulting in an increased operational risk.

1. Vulnerabilities of higher levels are normally only used if there are no vulnerabilities at a lower level available with the same probability of success and the same detection risk.
2. The attacker is more willing to deploy a 0day the lower the risk of detection and the higher the need for operational protection.
3. In times of increased tensions, the direct use of higher-level vulnerabilities is more likely.
4. The attacker prefers the use of unpublished vulnerabilities discovered by others to the exploitation of their own ones, as long as the operational protection requirements allow this.
5. The attacker is more willing to deploy 0days of Layer 2 the older they are, taking their limited life time, decreasing value and higher probability of detection into account.
6. One-shot Layer 3 Vulnerabilities which are exposed with their use, are only deployed in an emergency.
7. Layer 3 Vulnerabilities are all the more likely and more regularly used, the lower the probability of detection of the overall deployment process (including communication channels) and the higher the plausible deniability is.

For the implementation of the respective decisions, the cyber risk must be calculated. Therefore, a quantitative approach is required; currently, we are assessing different quantitative security risk analysis models as well as calculations and experiences in the field of cyber insurance, and we examine how the characteristics of our model, respectively the Lemmata, can be integrated.

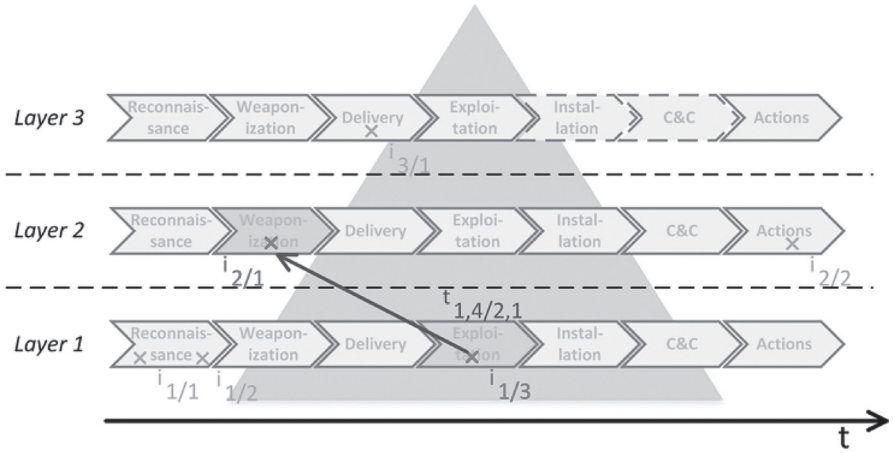
Furthermore, we implemented a matrix that reflects the custom Cyber Kill Chains of each layer. For each layer and each step, characteristics are defined which trigger a further evaluation of another Cyber Kill Chain step and Layer, typically going back in time on the new Layer. Here, sensitivities and threshold values can be adapted for the next evaluation step. There are also characteristics which trigger further evaluations of another step of the current Cyber Kill Chain, or even within the current steps. As the full set of definitions in the transition matrix is a centerpiece of the prototype currently being implemented, and due to the limited space, we are not yet fully presenting the transition matrix at this point. This will be part of our further work. However, for a better understanding of the task and functionality of the transition matrix, two examples of corresponding transitions, respectively actions, are provided:

- Adaptation of thresholds for a re-evaluation of IDS logs in order to detect very slow scans of a network, which remain normally below the detection threshold. For example, one can think about actions like a scan with "paranoid timing" by the network scanner nmap[4]: nmap `-T0`, moving the search window from a Delivery Step back to a Reconnaissance Step. Note, that the effects in the evaluation are based on the change of the associated conditional probabilities and not resulting from the mere change in the sensitivity of the analysis, therefore they are also *not directly visible* in this example.
- Moving the search window from the Exploitation Step on Layer 1 to the Weaponization Step on Layer 2 based on unexpected system behavior or program crashes.

Such a transition is visualized by the arrow going from $i_{1/3}$ to $i_{2/1}$ in Figure 5, and which denotes the selection of $t_{1,4/2,1}$, moving the window of the search from Exploitation Step on Layer 1 to the Weaponization Step on Layer 2 because of identified, abnormal and suspicious system behavior.

4 Note, that this example is for illustration – as the parameterization of nmap is well-known, changing the search pattern wrt. the timing options of nmap is not enough to improve the detection quality significantly.

FIGURE 5. EXEMPLARY VISUALIZATION OF THE 3D-DETECTION SCHEME FOR THE RETROACTIVE IDENTIFICATION OF HIDDEN CYBER ATTACKS. I REPRESENTS INDICATIONS ON THE RESPECTIVE LAYER AND COMBINED WITH THE EVENT NUMBER, AND T REPRESENTS TRANSITIONS, GOING FROM ONE LAYER TO ANOTHER AND COMBINED WITH THE STEPS OF THE RESPECTIVE CYBER KILL CHAINS. NOTE, THAT THE TIMELINE BETWEEN THE DIFFERENT LAYERS IS *NOT* SYNCHRONIZED.



B. System Composition

Based on the presented Behavioral Rules, a new detection system is proposed as follows: adapted to the respective target network and the systems, the regular information sources such as logs and IDS messages are evaluated in order to recognize steps such as reconnaissance and delivery. Raw data, flows, log entries as well as already processed data, e.g., from an integrated security information and event management (SIEM) system, can be used.

Second and of particular importance, a basic set of "non-wire" and indirect data sources is continuously evaluated for every single Layer, searching for step-specific indications and information of attack. This data is filtered and ranked based on the system environment and stored into a database. These consulted data sets involve, for example, surveillance of pastebin websites and respective forums for the appearance of new leaks, information on vulnerabilities or disclosures, and monitoring of the 0day market and its price development. Information about for instance, operating systems and vulnerabilities of applications which are not used in the system environment are dropped. This database is crucial for the 3d-detection scheme, as a holistic overview is required to identify possible clues related to cyber attacks.

Figure 5 outlines the basic searching process. Based on indicators in the different levels and layers, the probability of transitions are calculated on the basis of the

respective cyber risk and according to the defined rules. By the identification of possible transitions, the elements of the potential, multilayer attack paths are dumped for the further, manual evaluation.

5. CONCLUSION AND FURTHER WORK

The entire world is becoming increasingly networked and dependent on the cyberspace. Because of its properties such as a certain degree of anonymity, the cyber arena is more and more interesting for a variety of actors, from script kiddies to nation states. Therefore, a lot of attacks may be seen in cyberspace. Or not. Some of the known attacks have gained broader public attention only by chance. This raises the fundamental question whether some cyber activities may remain hidden even though they have a significant impact on our everyday lives - how can yet unknown cyber involvements get unmasked? If you look at the data and compare it with the possibilities of various attackers, the assumption is reinforced that more incidents may have a (yet undiscovered) cyber background.

The reason detection of sophisticated cyber attacks fails is caused by corresponding steps which are not executed “over the wire”, at least not over the wire of the attacked company, and which are therefore not detectable for conventional systems. Using a 3-Layer Vulnerability Model, the attackers can be characterized based on their capabilities and available attack vectors. By evaluating methods for the analysis of the attack path, it became clear that they are not sufficient to investigate complex attacks, and thus are not suitable for discovering them. To improve the detection of sophisticated cyber attacks and to move towards the identification of yet unknown, hidden cyber attacks, we propose a three-dimensional model based on the combination of the 3-Layer Vulnerability Model and Cyber Kill Chains.

Currently, we are completing a prototypical implementation of our model by using the KNIME Analytics Platform. The next step is building up the required databases, before different data sets can be evaluated. For this purpose, first the databases are filled with the identified information types and sources for the respective Layers and attack steps, and then the logs and system data of selected networks in which cyber attacks were discovered after a long time will be imported. Based on that, the search and evaluation process of the proposed three-dimensional detection scheme will be analyzed to identify necessary adjustments of the cyber risk and transition calculations, as well as the algorithms for adapting the sensitivity of the sensory. As this process requires real-world data of complex networks, we invite companies interested in cooperation and evaluation of their networks and systems to contact us,

as having a broad dataset is crucial for enabling the detection scheme. Of course, the used data will be anonymized appropriately.

While the first prototypical implementation will only be able to retroactively identify indications of hidden cyber attacks, the ultimate goal is to minimize the necessary time window required for the process, and to investigate which indicators can also be used to detect an ongoing campaign or campaign under preparation. For that purpose, machine learning techniques will also be applied; a prerequisite, however, is the access to sufficient data sets and their evaluation and marking.

REFERENCES

[1] P. Dreyer, K. Jones, Theresecand Klima, J. Oberholtzer, A. Strong, J. W. Welburn, and Z. Winkelman. *Estimating the global cost of cyber risk: methodology and examples*. RAND Corporation. Technical Report; 2018.

[2] J. Lewis *Economic impact of cybercrime - no slowing down*. McAfee; 2018. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

[3] D. P. Fidler. *The Snowden Reader*. Indiana: Indiana University Press; 2015.

[4] WikiLeaks. *Vault 7: Cia hacking tools revealed*. 2017. Available: https://wikileaks.org/vault8/.

[5] WikiLeaks. *Vault 8*. 2017. Available: https://wikileaks.org/vault8/.

[6] Carl Philipp Gottlieb von Clausewitz, *Vom Kriege, Book 1, Chapter 1*, Bassford, Christopher, 1832. Available: https://www.clausewitz.com/readings/VomKriege1832/_VKwholetext.htm .

[7] Carl Philipp Gottlieb von Clausewitz, V*om Kriege, Book 3, Chapter 8*, Bassford, Christopher, 1832. Available: https://www.clausewitz.com/readings/VomKriege1832/_VKwholetext.htm.

[8] Carl Philipp Gottlieb von Clausewitz, *Vom Kriege, Book 3, Chapter 9*, Bassford, Christopher, 1832. Available: https://www.clausewitz.com/readings/VomKriege1832/_VKwholetext.htm.

[9] S. Tzu, The art of war. In: Mahnken TG, Maiolo JA. (eds). *Strategic Studies, A Reader*. 2nd edn. New York: 2008. p28.

[10] Kaspersky Lab. *Denial of Service: how businesses evaluate the threat of DDoS attacks*. Kaspersky Lab. Technical Report; 2015.

[11] Verizon. *Data breach investigation report*. Verizon. Technical Report; 2018.

[12] W. E. Forum *The global risks report*. 14th edition. Switzerland: World Economic Forum. Cologny/Geneva, Switzerland, Technical Report; 2019.

[13] J. Ray, H. Marshall, R. Coderre, E. Cody, and J. Jean *Cyber threatscape report 2018 - midyear cybersecurity risk review*. Accenture Security. Technical Report; 2018.

[14] Ponemon Institute. *2018 Study on global megatrends in cybersecurity*. Ponemon Institute LLC. Technical Report; 2018.

[15] W. Schwab and M. Poujol, *The state of industrial cybersecurity 2018*. Kaspersky Lab. Technical Report; 2018.

[16] M. Dudek. *TRISIS / TRITON / HatMan Malware Repository*. Available: https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN.

[17] R. Koch and M. Golling, The cyber decade: cyber defence at a x-ing point. in *2018 10th International Conference on Cyber Conflict (CyCon)*. IEEE, 2018, p. 159–186.

[18] M. Giles. *Triton is the world's most murderous malware, and it's spreading*. Available: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/.

[19] C. Canella, J. Van Bulck, M. Schwarz, M. Lipp, B. von Berg, P. Ortner, F. Piessens, D. Evtyushkin, and D. Gruss, A systematic evaluation of transient execution attacks and defenses. *arXiv preprint* arXiv:1811.05441; 2018.

[20] SonicWall. *2018 Sonicwall cyber threat report mid-year update*. SonicWall Inc. Technical Report; 2018.

[21] Internet Security Research Group. *Let's Encrypt Stats*. Available: https://letsencrypt.org/stats/.

[22] Google. *HTTPS encryption on the web*. Available: https://transparencyreport.google.com/https/overview?hl=en.

[23] Cisco Systems. *Cisco 2018 Annual cybersecurity report*. Cisco Systems Inc. Technical Report; 2018.

[24] US-CERT. *Alert (TA17-075A) https interception weakens TLS security*. Available: https://www.us-cert.gov/ncas/alerts/TA17-075A.
[25] T. Ormandy Sophail: *A critical analysis of Sophos antivirus*. Proc. of Black Hat USA; 2011.
[26] Canadian Journalists For Free Expression. *Snowden archive*. Available: https://www.cjfe.org/snowden.
[27] Electronic Frontier Foundation. *NSA ANT Catalogue*. Available: https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa\s\do5(a)nt\s\do5(c)atalog.pdf.
[28] Infosec Institute. *A close look at the NSA monitor catalog - server hacking*. Available: https://resources.infosecinstitute.com/close-look-nsa-monitor-catalog-server-hacking/.
[29] J. Assange. *Vault 7: CIA hacking tools revealed*. Available: https://wikileaks.org/ciav7p1/.
[30] WikiLeaks. *Marble Framework*. Available: https://wikileaks.org/vault7/#Marble.
[31] WikiLeaks. *Weeping Angel*. Available: https://wikileaks.org/vault7/#Weeping.
[32] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the cyber attack on the Ukrainian power grid*, Electricity Information Sharing and Analysis Centre. Technical Report; 2016.
[33] P. Koppe, B. Kollenda, M. Fyrbiak, C. Kison, R. Gawlik, C. Paar, and T. Holz, Reverse engineering x86 processor microcode. *Proceedings of the 26th USENIX Security Symposium*. USENIX Association; 2017. p.1163–1180.
[34] S. Skorobogatov and C. Woods, Breakthrough silicon scanning discovers backdoor in military chip. *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2012.p. 23–40.
[35] J. Robertson and M. Riley. *The Big Hack: How China used a tiny chip to infiltrate U.S. companies*. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
[36] J. Naughton. *The tech giants, the US and the Chinese spy chips that never were... or were they?* Available: https://www.theguardian.com/commentisfree/2018/oct/13/tech-giants-us-chinese-spy-chips-bloomberg-supermicro-amazon-apple.
[37] T. Markettos. *Making sense of the Supermicro motherboard attack*. Available: https://www.lightbluetouchpaper.org/2018/10/05/making-sense-of-the-supermicro-motherboard-attack/.
[38] J. A. Tirpak. *Find, Fix, Track, Target, Engage, Assess. Air Force Magazine. 2000*;83 (7): 24–29. Available: http://www.airforcemag.com/MagazineArchive/Documents/2000/July.
[39] LM Corporation. *The Cyber Kill Chain*. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[40] J. R. Gosler and L. von Thaer, *Task force report: resilient military systems and the advanced cyber threat*. Washington, DC: Department of Defense, Defense Science Board; 41, 2013.
[41] The MITRE Corporation. *Common vulnerabilities and exposures (CVE)*. Available: https://cve.mitre.org/.
[42] R. Koch and T. Kühn, Defending the grid: backfitting non-expandable control systems. *2017 9th International Conference on Cyber Conflict (CyCon)*. IEEE, 2017. p. 1–17.
[43] Q. Chen and R. A. Bridges, Automated behavioral analysis of malware a case study of WannaCry ransomware. *arXiv preprint* arXiv:1709.08753; 2017.
[44] N. Grossman. *Eternalblue - everything there is to know*. Available: https://research.checkpoint.com/eternalblue-everything-know/.
[45] L. Ablon and A. Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Rand Corporation; 2017.
[46] CrowdStrike. *2019 Crowdstrike global threat report - adversary tradecraft and the importance of speed*. CrowdStrike. Technical Report; 2019.
[47] D. J. Bernstein, T. Chou, C. Chuengsatiansup, A. Hülsing, T. Lange, R. Niederhagen, and C. van Vredendaal, *How to manipulate curve standards: a White Paper for the Black Hat*. Cryptology ePrint Archive. Report 2014/571; 2014.
[48] Accenture. *Cyber threatscape report 2018 - midyear cybersecurity risk review*. Accenture. Technical Report; 2018.
[49] K. D. Mitnick and W. L. Simon. *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley & Sons; 2011.