https://doi.org/10.53656/str2024-3-3-mod

Research Results
Резултати от научни изследвания

MODERN SCIENTIFIC PROACTIVE CYBER COUNTERINTELLIGENCE STRATEGIES FOR ADVANCED PERSISTENT THREATS EARLY WARNING

Petar E. Manev
University of Library Studies and Information Technologies – Sofia

Abstract. The article presents a modern scientific proactive cyber counterintelligence concepts and strategies for applying advanced persistent threats early warning approach. The research reviles some of the main challenges and problems that the cyber security domain faces with respect to evolving and advanced cyber threat actors. The research exposes the main gaps in detection mechanisms of the cyber defense industry and landscape and based on that presents some relevant concepts and strategies. This includes assumptions, challenges, concepts and strategies. Based on actual experience from different cyber activities such as threat hunting, incident response and NATO live fire cyber security and cyber defense exercises, the author provides a wide approach for addressing those gaps and generates the possible strategies for applying advanced persistent threats early warning concepts and methodologies.

Keywords: cyber security; cyber-attack; cyber defense; early detection strategies

Introduction

Digital communications and systems are the norm in modern day society. Widely adopted and ever expanding, that communication domain inherits natural challenges in terms of cyber defense. The execution of cyber-attacks can no longer be confined to a specific geolocation and no longer poses the predictability of geo directionality as the actual breach can happen from within an organization as well as from outside. In many cases public infrastructure such as Gdrive or DroBox can also be used to launch or facilitate cyber-attacks. The main point discussed in the article addresses a rising trend of sophisticated and very aggressive and disrupting cyber-attacks by persistent actors that can target critical communication infrastructure with the aim of permanently disabling functional operations or existence of a specific organization or cyber communication area of control. Due to the nature and dedication of threat actors these types of attacks can be considered existentially threatening. That's why generating new scientific con-

cepts and strategies for defending in more effective way modern cyber nets need applying multi-dimensional strategies. So new concepts of multilateral approach are needed.

Quite normally most research and publicly available information, the analysis of the activities of a threat actor is post factum. In other words, a breach and objectives already occurred. Detection principles based on those analysis, naturally, can confine the actual defense response and methodology of protection to what is known. This article aims at providing a suggestive practical approach for an early detection strategies and mechanisms regardless of that fact in cases where the final objective is disruption of critical infrastructure operations.

A guiding concept for this research is exactly that, the assumption that the most successfully executed attacks are the ones that have not been found, detected or have been found but details about the information are not publicly disclosed. Thus not making it easy to analyze and develop detection concepts, strategies and mechanisms.

Any cyber-attack goes through a life cycle just as any threat actor, advanced or not, has certain techniques and or procedures and tools it is using. Those can change in terms of actual time and tools but the principle is the same. This is reviewed and used in the article as a non-deterministic approach of helping the suggested detection methodology. The article also provides sub examples of such detection approach and methodology.

Main components and definitions

Cyber lateral intelligence. This is the process utilized by an attacker that has already established a foothold inside an entity or organization – to discover, target, attack and exploit high value targets inside the organization – in order to achieve its goals. In other words – the final objective.[1]

Counter cyber lateral intelligence. This is the process of countering the intelligence or reconnaissance activities above in order to prevent the attacker from achieving its goals.[2]

Preemptive cyber intelligence. This is the process of doing in advance procedures and cyber analysis in order to highlight a potential breach that is about to be engaged in an attack or imminently exploit the actual threat actor's objective. This process can also be part of a network defense activity – active hunting.[3]

An Advanced Persistent threat (APT) is defined by National Institute of Standards and Technology as follows: *"An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually ex-filtrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives."*[4]

An adversary has a dedicated team, organization, and motif. One of the most difficult APT groups to defend against can be the ones that are not influenced by monetary value – those APT teams do it for pride or to prove a point of expertise – recognition & achievement, politically motivated – hacktivism or acting on behalf of a country/motherland – state actors, patriotically motivated.

Since there is no financial game at play, the dedication and thus capabilities in terms of persistence of those groups is endless and limitless.

In that line of view, in a lot of cases, the time factor – time to start the operation – may not be relevant. In other words, there is enough time for preparation and defining subsequent targets and decision making is not influenced by cost.

Life cycle of an attack

Even with the obvious advantage of the above – the process of achieving those goals needs to go through its respective phases. Lockheed Martin has defined those as follows: reconnaissance, weaponization, deliver, exploitation, installation, command and control, actions on objective.[5] Each phase has its viable possibility associated with it of the APT actor being uncovered. Those hints (giveaways) can vary: from mentions or hints (by mistake or on purpose) in social media accounts, for example X, Linkedin, Instagram and others, to talking about it in friendly circles and dark forums, to actually being discovered by the defending side.

Techniques Tactics Procedures

An attacking side or actor in most cases uses certain actions and procedures that can be grouped and categorized. One of the most widely used knowledge base for techniques, tactics and procedures (abbreviated as TTPs) used by malware adversaries is produced by MITRE.

"MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge."[6]

Diamond model of intrusion analysis

A framework model for analyzing and detecting activities of malware actors was developed and proposed by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz in a 2013, U.S. Department of Defense technical report titled "The Diamond Model of Intrusion Analysis" (Caltagirone, Pendergast & Betz 2013). "…*the model describes that an adversary deploys a capability over some infrastructure against a victim*" (Caltagirone, Pendergast & Betz 2013). The model is depicted in the Fig. 1.

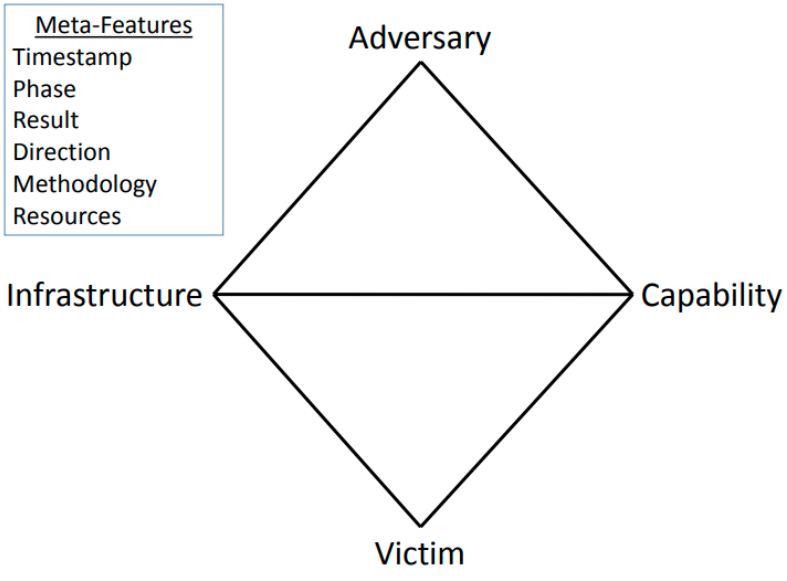

Figure 1. Diamond model for intrusion detection

Dwell time

Dwell time is the period of time between when an attack starts/begins and has been detected. The time range itself can vary depending on a multitude of factors including geographical location, culture, target and objective. The median dwell time however is in a constant decline as reported by different security vendors.

Average dwell time as recorded by Mandiant Solutions is shone on the Fig. 2:

Global Median Dwell Time, 2011-2022

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	416	243	229	205	146	99	101	78	56	24	21	16
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

Figure 2. Median dwell time trends – Mandiant[7]

Thus, in most cases we can conclude that in general the attackers are forced into achieving their objective with higher pace due to improving technology and

knowledge of the defenders. Which in turn can result in an advantage for the defenders as the short dwell time means more verbosity, more movement and communication in a shorter period of time – which ultimately exposes TTPs easier.

Types of APTs

One factual point that exists is that there are many APT groups – both known and unknown. Each APT group has specific targets that can vary by size, culture, language, organization etc. Thus each APT group has tactics and strategy that may be known, little known or unknown. Which has the expected effect of increasing the difficulty of detection and establishing effective strategy to do so in different types of organizations and cultures.

Known Knowns – APTs APTs we are aware of and understand their TTPs	**Known Unknowns – APTs** APTs we are aware of but do not understand their TTPs
Unknown Knowns – APTs APTs we understand but are not aware of their TTPs	**Unknown Unknowns – APTs** APTs we neither aware of nor understand their TTPs

Figure 3. Types of APTs and their TTPs (Author)

APTs targets

Considering the above a target can be anything beyond the obvious gains in terms of – political, military or personal efforts. In other words, a target and the reason for targeting can be unknown.

Attribution

Nowadays it is extremely difficult to attribute and prove beyond doubt that something happened in the cyber medium coming specifically from an individual, team, organization, department or military unit. There are many questions that need yes or no type of answers that are impossible to prove beyond doubt in a court of law. If a web page is visited from a house‘s public IP address, in a home for example, for an investigating organization – it is often impossible to determine:

1. If the web page visit was done by a specific person, a member of the family or when a guest was visiting, by the guest.

2. It is also impossible to confirm 100% the exact device that the web page was visited.

3. It is also impossible to confirm if it was done intentionally – someone purposefully typed in the address in the browser or click on a web page address vs someone was mislead to click by a phishing mail/advertisement vs if the device that the web page visit was made for was beyond doubt hacked and it was actually done by the hacker

Assuming it is possible to indisputably find and prove the above in many cases it is still not enough to bring the perpetrators to justice (assuming non state sponsored APT groups) due to government, geopolitical regulations and political or strategic views. One simple reason can be that there simply might not be extradition policy between different governments depending on the specific case or in case perpetrators are located in a different country. This means – even if proven and discovered – the APT groups activity or the activity of its members will not necessarily seize. Thus contributing to the problematic of minimizing the volume of attacks.

The Network

One indisputable fact is that when communication is happening in the cyber security domain – communication, in its main component, preceding, during and post the attack must happen over the network communication medium. There simply is no other way of doing it.

In some cases when targets are highly secure and air gapped, the communication activities can only be observed inside that air gapped environment, inside that security domain. In such cases once the actor is inside the domain – it still evolves and communicates over the network.

In one such case, in an effort to contain and defend against intrusions, external media devices were forbidden: *"The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further. ... The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services."*[8]

In such cases the unwanted activity can still be observed on the network but in a lateral/internal way – post breach. Thus leaving the network as the only possible medium of communication.

Missed APT attacks

Every successful APT group attack has a preemptive stage before the actual deployment or take over happens. The prelude or the communication prior to the actual trigger is usually missed.

In the most difficult, dangerous and destructive operations of APT groups – the goals are actually non profit/non financial and non espionage. Example: critical infra take down or take over – complete communication or operational functioning capability take down of an organization. Such cases are more common than expected, anticipated or thoughts. The take down of the Viasat network Service

provider is one such example: *"Viasat told Reuters the outage affected satellite modems owned by tens of thousands of customers in Europe. Some of those modems are still offline at time of writing, according to the report, and bringing them back online is going to be a fairly involved process."*[9]

Important point to consider is that threat actors can purposefully destroy devices to take down an organization's infrastructure and operations. Just recently, a well-known vendor advised customers to replace their physical devices because patching the software vulnerability was not possible.

Challenges

Omission of some basic cyber warfare principles are usually leading to a blind spot in the security controls, objectives and the security deployment goals. Most defensive protections are often enough influenced:

– by fear/anxiety/anticipation or political goal
– commercial perspective – cost of deployment
– reactive deployment – based on response from a current or ongoing breach

These basic principles of those deployments – contradict and are poised to miss out the basic principle of determination of the not for profit, non-espionage APT groups objectives and goals.

Security controls

In such and other cases where critical network communication devices like routers, switches, firewalls, VPN concentrators are targeted specifically, endpoint detection and response (EDR) cannot help organizations defend against threat actors. This is why it's so important that organizations implement a layered defense that pairs EDR with network monitoring – especially on critical infrastructure. Only when they have network visibility can organizations rapidly detect threats – and this is critical to mitigate the damage that can be done following a successful attack.

Another major blind spot is actually monitoring edge or legacy devices where endpoint detection cannot be installed. For example, SCADA devices, medical and pretty much a big chunk of the Military, Industrial, Medical and Automotive devices domains. Very often there are Common Vulnerabilities and Exposures (CVE) of such systems being unearthed and disclosed. One such example is CVE from Fortiguard – Cyber Security company located in Sunnyvale, California.[10]

Some network security monitoring vendors are already actively noting the problem, for example Stamus Networks[11].

A big point to consider is vulnerabilities or breaches that we do not know about or that are not public. Hence amplifying the already perilous necessity to be able to monitor all communication aspects, the very minimum – of critical network communications infrastructure.

Additional aspect that brings yet another challenge is that one cannot protect what one doesn't know is there. In other words one cannot protect and monitor devices that are unknown and exist in the organization. Often such devices like bring your on device (BYOD).

Wrong Assumptions

Opponents.There may be opponents and or APT groups that are unknown including their respective goals and objectives. Do not assume all your opponents are known and or find-able.

Time. Understanding the time of operations and activities that an organization must defend itself from is essential for success. The fact that a person or organization does not do operations during Sunday, during Christmas time off or during New year does not mean the opponent will do the same. On the positive side though – if there is any unusual communication during that time – it would have a better chance to be picked up by the defending side.

Underestimating your opponent. One of the biggest mistakes that can be made and in many cases is still done towards an opponent is to underestimate the capabilities or determination.

Lack of visibility – overestimating your defenses. Lack of visibility from a security perspective can result in overestimating the capabilities of the existing cyber defense deployment.

Defense perimeter and criticality. Know your cyber defense perimeter. This part very often comprises the essence of the blind spot. It is the age of IT/IoT/Mobile networks. Often enough many organizations do not have a robust way of identifying, inventorying, reporting and analyzing all devices or communication points on the network. In other words the basic question : ***"What and how many devices reside in different parts of my network"*** cannot be answered with 100% certainty. This is even more amplified during crisis situations like natural/ industrial disasters or military conflicts.

There are critical devices present in the communication domain that are in many cases often unknown – example legacy and unmigrated systems or test and non-production systems that do hold critical data that allows an attacker to use it and leverage privileged access to actual production critical systems. One such example case was reported by Microsoft Corporation in January 2024.12

Early warning strategies and concepts

Critical systems monitoring strategy. Map out the most critical systems monitoring. Those are systems that when offline or unavailable – the organization or the bigger information system – ceases to function. Concentrate the following methodology on communication coming towards those types of systems.

The concept of early warning signals can be observed on the network some time before the APT enters its actual Actions Objectives stage from the Lockheed Martin Cyber Kill Chain. Mainly two big parts that follow.

1. Communication from new sender

The basic principle of visualizing the event from a security perspective is a new sender on the communication medium – communication from a new sender.

One example of such activity in the realm of cyber security can be communication from a Newly Registered Domain (NRD) to and from a critical system or device.

NRD by itself alone does not mean something is good or bad. It is just a piece of information. Often enough used by threat actors utilize this method as the domain used in its communication is new and its analysis from a security perspective has not been done yet by the security vendors.

One of the challenges with analyzing or even finding NRDs is that the availability of the data that the domain was registered today for example - depends entirely on the Domain Name Registrar for the country where that domain was registered.

There are also possibilities to use NRD as a subdomain of a very legitimate public service – like Google/Cloudflare/Microsoft and by using custom domain names under those registrars.13

2. Previously unseen/unique Communication

The basic principle of visualizing this communication event from a security perspective is a new previously unseen communication – uniquely new communication event.

Detection concepts

The above would allow for high level break down of detection events with the following four cases, based on two major types of communication – encrypted and unencrypted:

1. new unique unencrypted communication to and from critical system;

2. new unique encrypted communication to and from critical system;

3. new unique unencrypted communication & new sender to and from critical system;

4.new unique encrypted communication & new sender to and from critical system.

The detection concepts above are not meant to provide a single linear detection event but rather allow for a detection formula methodology for an early detection possibility that is a prelude to a final stage of an attack. Thus allowing a defending team to apply the strategies of thwart the objective of an elusive threat actor that has already managed to bypass existing cyber defenses.

Actual example

This is a simpler method where any new previously unseen communication can be hashed and documented and only new ones each time period/day can be observed.

"*Knowing when certain communication metadata pieces are being seen on the network for the first time provides a big advantage to any hunter. Here, the analyst may view first time sightings of domain queries, HTTP hosts, JA3, JA3S, SMB file transfers, TLS certificates, TLS SNI, and more*." (Manev 2023).

An effective example of a process of preemptive Counter-cyber Intelligence for Early Detection of Advanced Persistent Threat is summed up by this review blog (Manev 2023). Its concept, in essence, is analyzing a combination of new and previously unseen and newly registered domain communication.

This can further be enhanced and optimized for critical network equipment via exclusively looking into communication to and from that specific part of the network medium.

Some formulas based on using world renowned and famous Suricata14 Network Security monitoring engine can be as follows below. The one below are queries in the Kibana, Lucene query syntax, based on data in Elasticsearch15 database. Those queries can easily be adjusted to other databases or Security Information and Event Management (SIEMs) systems. A few examples follow:

Seek and display all encrypted connections based on combination of NRD and previously unseen labeled network flows:

*event_type:flow AND metadata.flowbits:*stamus.nrd.entropy* AND metadata.flowbits:*stamus.sightings* AND app_proto.keyword:tls*

Seek and display all connections based on a combination of NRD and previously unseen labeled network communication based on HTTP where the data transferred is more than 10Kbs. The point of the formula here is that HTTP is clear text and it should really not happen to and from critical devices in the organization.

*event_type:http AND metadata.flowbits:*stamus.nrd* AND metadata.flowbits:*stamus.sightings* AND app_proto.keyword:http AND flow.bytes_toclient:>10000*

Seek and display all unencrypted, HTTP based communication based on combination of NRD and previously unseen labeled network flows where an executable was downloaded:

*event_type:alert AND metadata.flowbits:*stamus.nrd* AND metadata.flowbits:*stamus.sightings* AND alert.signature:*exe* AND http.status:200*

The formulas above can be further developed to cover more different types of communication from critical infrastructure devices in order to improve the concepts and strategies.

Conclusion

Uncovering unwanted actions of a little known adversary or a multitude of adversaries is not an easy task. It never was. The basic unconditional truth and end result is that at some point of time, unavoidably a threat actor must communicate over the network medium. The communication can be to either fetch more information

from a central server (Command and Control), to deploy more tools or simply to check in and acknowledge that the environment is still breached and available.

The proposals in this article aim at providing a basis for a working foundation, concepts and strategies that can match, highlight and expose the actions of a malware actor before it starts executing their final objectives – thus preventing (further) breach or disaster. The proposed measures range from understanding and better evaluating an organization's exposure to actual examples of working queries that have a capability to generically expose unwanted behavior that can be or may lead to an advanced persistent threat actor lurking in the environment.

Acknowledgments and funding

The report was prepared with the financial support of the National Science Program "Security and Defense", financed by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No. 731 of 21.10.2021.

NOTES

1. Author's definition.
2. Author's definition.
3. Author's definition.
4. https://csrc.nist.gov/glossary/term/advanced_persistent_threats, Sources: NIST SP 800-137 from NIST SP 800-39, available 27.02 2024.
5. MARTIN, L., 2024. The Cyber Kill Chain®. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (27.02.2024).
6. *https://attack.mitre.org/,* available 27.02.2024.
7. https://inthecloud.withgoogle.com/mandiant-m-trends-2023/download.html, available 27.02.2024;
   https://www.mandiant.com/m-trends, available 27.02.204.
8. https://www.wired.com/2008/11/army-bans-usb-d/, available 27.02.2024.
9. https://www.pcmag.com/news/report-nsa-investigates-viasat-hack-that-coincided-with-ukraine-invasion, avaliable 27.02.2024 .
10. https://fortiguard.fortinet.com/psirt/FG-IR-24-015, avalable 27.02.2024 .
11. https://www.stamus-networks.com/blog/the-rise-of-network-infrastructure-attacks-and-what-to-do-about-them, avalable 27.02.2024.
12. https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/, avalable 27.02.2024.
13. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-alternate-domain-names.html, avalable 27.02.2024.
14. https://suricata.io/, avalable 27.02.2024.
15. https://www.elastic.co/elasticsearch, avalable 27.02.2024.

REFERENCES

CALTAGIRONE, S.; PENDERGAST, A. & BETZ, C. 2013. *The Diamond Model of Intrusion Analysis. Available at:* https://apps.dtic.mil/sti/pdfs/ADA586960.pdf (27.02.2024).

MANEV, P., 2023. Threat Hunting for Unknown Actors & Threats using NRD and Sightings. Available at: https://www.stamus-networks.com/blog/threat-hunting-for-unknown-actors-threats-using-nrd-and-sightings, (27.02.2024).

MARTIN, L., 2024. The Cyber Kill Chain®. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (27.02.2024).

✉ **Petar E. Manev**
University of Library Studies and Information Technologies – Sofia, Bulgaria
Stamus Networks – Paris, France
E-mail: e.manev@unibit.bg