SECTOR

Accepted Submission

Title	Do We Really Need to Worry about Critical Infrastructure? Discussion about Cyber Operations in the Context of Leaked Vulkan Files
Session Type	Briefings
Speaker	Marina Krotofil (Cyber Security Professional)
Primary Track	Management
Secondary Track	Technical

Abstract

Provide a concise, yet detailed description of your presentation (300 words maximum). Accepted talk abstracts will be published on SecTor's website and in other materials.

In the past, the definition of hybrid war was frequently reduced to a composition of kinetic and cyber warfare to simplify the discussion. Lessened to just two components and in the absence of real-world examples of hybrid war, it was often argued that cyberwarfare, and especially attacks on various critical infrastructures, had the potential of having a critical role at times of significant conflicts with combat actions. However, the events in the Ukrainian war theater have shown that kinetic weapons were preferred at the time of tactical military operations. Ever wondered why this was the case?

This talk will consist of two parts. The first part will provide a short yet comprehensive summary of the recently leaked "Vulkan files", classified documentation which provides details about Russian hybrid warfare strategy and distributed software platforms to prepare and manage cyber- and information operations in a centralized manner. In the second part, we will analyze notable Russian cyber operations in the post-Stuxnet era (after 2010) and show how Russia gradually evolved and tested its cyber capabilities and hybrid warfare vision. Some of the operations will be discussed with technical details based on first- and second-hand experiences with such operations. By the end of this talk, the audience should get a better idea about a wide range of factors that impact the success of cyber operations and why cyber on critical infrastructures are more frequently opportunistic than strategic as well as may not always yield the desired impact. As the final conclusion, the talk will outline a type of cyber operations being conducted in war and peace times.

Presentation Outline

Show the progression of your presentation. Submissions that include detailed outlines score higher. (This field will display plain text only. Add line breaks as necessary, for easy reading by our Advisory Committee.)

- Setting up the stage through a short intro into history of industrial revolutions and where we are now (between Industry 4.0 and Industry 5.0) -> this will help the audience to understand why we have so many security and policy issues.
- Short intro into "Vulkan file" leak (more than 1000 documents) and my role in the file analysis
- General characteristics of the leaked/analyzed files
  - This will include the types of files and documents being leaked, characteristics of their content, challenges with the analysis, etc. The end user of the system are Russian Armed Forces (various units)
- Overview of three major distributed software platforms mentioned in leaked files (Amesit, Scan and Krystal)
  - Short overview of each platform, its purpose, scope and components
  - More detailed overview of the platforms on the example of the design diagrams

    - Examples of the graphical user interfaces for different types of users (analysts, commanders, etc.)
    - Examples of requirements/specs to both hybrid warfare capabilities and to the management platform capabilities (I picked some of the interesting ones out of numerous)
    - Coverage of the interesting points, topics and challenges covered in the documents (again, my own cherry picking)
    - Discussion about what capabilities discussed in Vulkan files are already being deployed and where (GRU and Military Academy of the General Staff of the Armed Forces of Russia) with some anecdotes about developers having remote access to those secret systems
- Definition of hybrid war and hybrid warfare and how Vulkan files confirm that Russia is executing its hybrid warfare vision with commendable persistence.
    - Short touch on impactful RU diplomacy efforts and Ru influence spread across international organizations with few examples
    - Explanation that despite a popular believe cyber play just one of the roles in hybrid warfare but not the leading role.
- Analysis of leaked files in the context of past RU cyber operations
    - A timeline of key Ru hybrid operations in post-Stuxnet era (after 2010) with short explanations how these operations relate to the information in the leaked files
    - On the examples of attacks in Ukraine in 2015-16 and Triton attack (I have first-hand experience with them) it will be shown what effort (time and human resources) it takes to conduct planned cyber operations and what factors suggested that these operations might have been planned by or for military command. This section will also explain to the audience why TARGETED cyber attacks/operations are, in general, not suitable for fast-pace tactical military operations (especially attacks on critical infrastructures).
- Analysis of cyber and kinetic attacks on critical infrastructure during RU invasion in Ukraine (with examples). Explanation why both countries resolved to physical sabotage (this part will refer to the previous section).
- In conclusion we will summarize the major limitation when using cyber warfare during military times and explain the preparations and testing of the strategic cyber capabilities is happening during peace times. The impact of cyber operations is perceived differently during peace and war times. Human costs of cyber operations may have been overestimated in the past (with the reference to previous study of Red Cross in which I participated as an expert).
-

Is this content 100% new, never before presented/published? - No

If no, explain what's new and what's already been presented and where.
I gave the proposed talk a couple of times to the invitation-based small communities of professionals in Norway, Germany and Singapore to test the waters. Specifically, to see how the storyline flows and to evaluate audience's interest. The feedback was overwhelmingly positive. For this reason, I would now like to present this material to a wider audience.

Will you be releasing a new tool? – No

Will you be releasing a white paper? - No

Prepared Materials/Published Papers/Previous Speaking Engagements
I spoke at BH USA, EU and Asia six times in total throught 2015-2021 as well as at most largest security conference around the world.
This is the link to the slides from BH EU 2021: https://i.blackhat.com/EU-21/Wednesday/EU-21-Krotofil-Greetings-from-the-90s-Exploiting-the-Design-of-Industrial-Controllers-in-Modern-Settings.pdf
And the video of the talk: https://www.youtube.com/watch?v=DIB_1q9WPfw

SECTOR

Accepted Submission

Title	The Future of Threat Intelligence with AI
Session Type	Briefings
Speaker	Susan Peediyakkal (Service Management Practice Lead for the Cybersecurity Services (CyS) Service Line, NASA)
Primary Track	Security Fundamentals
Secondary Track	Technical

Abstract

Provide a concise, yet detailed description of your presentation (300 words maximum). Accepted talk abstracts will be published on SecTor's website and in other materials.

As the world becomes increasingly reliant on technology, the threat landscape also continues to evolve, making it more important than ever to have effective threat intelligence programs in place. The development of artificial intelligence (AI) has the potential to revolutionize the way threat intelligence is gathered, analyzed, and acted upon.

AI can sift through vast amounts of data, identify patterns, and make predictions in ways that would be impossible for a human to do; meaning it can quickly identify emerging threats and provide actionable insights to help organizations stay ahead of potential attacks. Also, AI can automate certain tasks allowing analysts to focus on more complex tasks.

There are challenges associated with the use of AI in threat intelligence. One is ensuring that the AI algorithms are trained on high-quality data sets, as poor-quality data can lead to inaccurate predictions. Another challenge is the potential for AI to be hacked or manipulated by threat actors, which could lead to false alarms or missed threats.

By leveraging the power of AI, organizations can better protect themselves against a constantly evolving threat landscape. However, it is important to approach the use of AI in threat intelligence with caution and ensure that proper safeguards are in place to mitigate the risks.

Presentation Outline

Show the progression of your presentation. Submissions that include detailed outlines score higher. (This field will display plain text only. Add line breaks as necessary, for easy reading by our Advisory Committee.)

I. Introduction - Introduce myself (6 min)

A. Definition of threat intelligence

B. Importance of threat intelligence in today's digital world

C. Brief overview of the role of AI in threat intelligence

II. Benefits of AI in threat intelligence (10 min)

A. Ability to process vast amounts of data

B. Identification of patterns and predictions

C. Automation of certain tasks

D. Faster response times

III. Challenges associated with the use of AI in threat intelligence (10 min)

A. Quality of training data

B. Potential for AI to be hacked or manipulated

C. Ethical considerations

IV. Best practices for using AI in threat intelligence (10 min)

A. Ensuring the quality of training data

B. Implementing safeguards to prevent AI manipulation

C. Training personnel in the use of AI

V. Case studies (10min)

A. Successful implementations of AI in threat intelligence

B. Lessons learned from unsuccessful implementations

VI. Future developments in AI and threat intelligence (10 min)

A. Advances in machine learning

B. The role of AI in threat prevention

C. The ethics of AI in threat intelligence

VII. Conclusion (4 min)

A. Recap of the benefits and challenges of using AI in threat intelligence

B. Call to action for organizations to incorporate AI in their threat intelligence strategies

C. Future outlook on the role of AI in threat intelligence.

Is this content 100% new, never before presented/published? - Yes

Will you be releasing a new tool? - No

Will you be releasing a white paper? - No

Message for Advisory Committee

I have been in the Threat Intelligence space for over 10 years; I feel like I could bring direct experience with how the field has evolved already to where AI can be applied in the future. It's something to start a conversation and bring the topic to the forefront of peoples' minds.

SECTOR

Accepted Submission

Title	Aikido: Turning EDRs to Malicious Wipers Using 0-day Exploits
Session Type	Briefings
Speaker	Or Yair (Security Research Team Lead, SafeBreach Inc.)
Primary Track	Technical

Abstract

Provide a concise, yet detailed description of your presentation (300 words maximum). Accepted talk abstracts will be published on SecTor's website and in other materials.

Wipers are becoming the go-to tool for nation-state cyber warfare in the last decade since the Shamoon attack. Wipers have been used by Russia, Iran, North Korea, and other APTs to support offensive acts. One of the most famous recent attacks was launched during the Russian invasion of Ukraine.

We were curious if we could build a next-gen wiper. It would run with the permissions of an unprivileged user yet have the ability to delete any file on the system, even making the Windows OS unbootable. It would do all this without implementing code that actually deletes files by itself, making it undetectable. The wiper would also make sure that the deleted files would be unrestorable.

Using the wisdom of martial arts, we understood the importance of using the power of our opponents against them in order to defeat them. Thus, we aimed to use the deletion power of EDRs to our advantage, triggering it by faking a threat.

We checked the leading EDR products and attempted to confuse them between malicious files and standard files during threat mitigation processes. We managed to discover and exploit 0-day vulnerabilities in more than 50% of them, leading to the creation of our Aikido wiper, which could be effective against hundreds of millions of endpoints all around the world.

In this talk we'll start by explaining the background of wiper usage, and our research goals and assumptions. Then we'll explain how different EDR products work when they detect a threat, and how we exploited their insecure actions in our Aikido wiper. We'll go on to present four vulnerabilities we found in Microsoft Defender Antivirus, Microsoft Defender For Endpoint, SentinelOne's EDR, Trend Micro Apex One, Avast Antivirus and AVG Antivirus. Finally - using those vulnerabilities - we'll demonstrate the wiping of all user data, and making the operating system unbootable.

Presentation Outline

Show the progression of your presentation. Submissions that include detailed outlines score higher. (This field will display plain text only. Add line breaks as necessary, for easy reading by our Advisory Committee.)

1. Agenda - Creating the best wiper of them all
    - 1. a. Requirements for the best wiper
2. Speaker Intro
3. Research Goals
    - 3.a. Find a way to delete files without being detected
    - 3.b. Have the freedom to choose any path to delete
4. Background - Wipers
    - 4.a. What is a wiper, why are they used
    - 4.c. Past wiper attacks - tactics, techniques and procedures

5. The power of EDR products: Quarantine & delete
    5.a. Why and when malicious files are deleted
    5.b. Why this is the ultimate ability for a wiper
6. Aikido - Use the opponents' power against them
    6.a. How can we exploit the power of the opponent
    6.a.1. We can trigger a deletion
    6.a.2. We need to find a way to get a standard file to be identified as malicious
    6.b. Target Confusion
    6.b.1. What does target confusion mean
    6.b.2. How can it possibly be done - symlinks, junctions
    6.b.3. Symlinks VS junctions required permissions
7. Windows of opportunity
    7.a. When is the right moment to confuse the security control
    7.b. How to do that with junctions
    7.c. Failed attempts
    7.d. Forcing a restart: Creating another window of opportunity with a simple CreateFile() and no CloseHandle()
    7.e. FILE_SHARE_READ - Must be passed to CreateFile()
    7.f. Explaining Windows "mark for deletion" mechanism using PendingFileRenameOperations
    7.g. Why is PendingFileRenameOperations vulnerable
8. Zero Day Vulnerabilities
    8.a.Listing all vulnerabilities
    8.b.Windows Defender VS the rest of the security controls
    8.c. Windows Defender / MDE vulnerabilities - Making the machine unbootable
    8.c.1. Steps to reproduce
    8.c.2. Demo
    8.d. SentinelOne's EDR vulnerability - Aikido Wiper Deletes all administrators users folders
    8.d.1. Steps to reproduce
    8.d.2. Demo
    8.e. Windows Defender Controlled Folder Access security feature bypass using the exploit
9. Result summary of all tested security controls
10. Vendors' response
11. How Aikido makes sure that deleted files are unrestorable
12. Lessons learned
    12.a. A wiper is more dangerous if it uses an arbitrary deletion vulnerability as a proxy.
    12.b. Having security controls does not mean you are secure
    12.c. Security controls run with the highest permissions and so they might be a preferred target for attackers.
    12.d. Be prepared by simulating new techniques and approaches in your organization.
13. Aikido Wiper - the next gen wiper
    13.a. How was the agenda accomplished
    13.b. Making data unrestorable
    13.c. About the tool itself, usage, and implementation
14. GitHub

- The session is about the creation process of the next-gen fully undetectable wiper malware using 0-day vulnerabilities in EDRs.

- The presentation will start with the background of wiper usage. Then, focus on the EDRs' superpower which is the ability to delete any file on the system no matter the permissions. A kind of a superpower that wipers are after. We'll explain how different EDR products work when they detect a threat. We will show our original ideas for how we can use the power of EDRs against them in order to defeat them. Then, we'll see how we checked the leading EDR products and attempted to confuse them between malicious files and standard files during threat mitigation processes. We had some failed attempts that will be presented, but then we will talk about how we created another window of opportunity for finding a vulnerability by forcing EDRs to postpone the file deletion to after the next reboot. We will present the 0-day vulnerabilities we discovered in Microsoft Defender Antivirus & Defender For Endpoint, SentinelOne's XDR, Trend Micro Apex One, Avast AntiVirus, and AVG AntiVirus, leading to the creation of our Aikido wiper, which could be effective against hundreds of millions of endpoints all around the world. The Windows features that make some of these products vulnerable will be explained. The vulnerabilities can even bypass a Windows security feature that is called Controlled Folder Access, which we will talk about as well. We will present our Aikido wiper, see how it works, and see why it takes wipers to the next level. We will also share a link to its open-source repo. Lastly, we'll demonstrate the wiping of all user data, and making the operating system unbootable.

- Using the defenders' actions to actually achieve malicious goals is pretty innovative. We believe it can inspire the crowd to choose interesting problems to solve, just like "How to be a wiper without actually wiping?".

- Takeaways:
  - *A wiper is more dangerous if it uses an arbitrary deletion vulnerability as a proxy.
  - *Having security controls does not mean you are secure.
  - *Security controls run with the highest permissions and so they might be a preferred target for attackers.
  - Always assume permissions can be escalated

- All the vulnerabilities were reported and fixed. These are the CVEs:
  - Microsoft: CVE-2022-37971
  - TrendMicro: CVE-2022-45797
  - Avast & AVG: CVE-2022-4173
  - SentinelOne did fix the vulnerability but did not issue a CVE.

- We predict the usage of wipers by APTs will grow like the usage of ransomwares. This is the first public research that analyzes how could the next generation of wipers look like in the next future. We want to raise awareness to it so EDRs will be prepared for mitigating them. It demonstrates how powerful it could be since there are at least hundreds or millions of computers vulnerable to it.

Is this content 100% new, never before presented/published? NO

If this content is not new, explain what's new and what's already been presented and where.
If you have previously presented this research/any portion of this talk, what will you be presenting at SecTor that is new? If the information has been previously published/presented, provide the name (conference/publication), date and URL. Include a URL to any presentation materials or video of the talk as well.

- The presentation was presented at Black Hat Europe 2022, RSAC 2023, HackCon Online 2023, Security Fest 2023 and CONFidence 2023. The reviews were extremely positive. In fact, my Black Hat Europe session received an outstanding evaluation score of 4.7 out of 5, well above the average score of 4.07.
- On top of Black Hat's, HackCon's and RSAC's presentation, we added new content that talks about potential vulnerabilities that can be found as a result of the risks in using the MoveFileEx function with the flag MOVEFILE_DELAY_UNTIL_REBOOT (The PendingFileRenameOperations feature that is the cause for 3 of the the 4 vulnerabilities we found)

Prepared Materials/Published Papers/Previous Speaking Engagements
The presentation was presented at Black Hat Europe 2022, RSAC 2023, HackCon Online 2023, Security Fest 2023 and CONFidence 2023

SECTOR

Accepted Submission

Title	Going Undercover in the Underground - A Practical Guide on How to Safely Infiltrate and Engage
Session Type	Briefings
Speaker	Michael-Angelo Zummo (NA Intelligence Manager, Cybersixgill)
Primary Track	Technical
Secondary Track	Tools

Abstract

Provide a concise, yet detailed description of your presentation (300 words maximum). Accepted talk abstracts will be published on SecTor's website and in other materials.

The dark web is filled with threat actors planning nefarious crimes. Cybersecurity professionals know that threat hunting in these underground environments is necessary, but they don't know the most crucial step to beginning the process. 'How do you access the deep and dark web?' and 'How do you gain a threat actor's trust?' These are the most commonly asked questions of cybersecurity professionals preparing a proactive threat hunt.

Navigating the underground requires dedication to persona management and setting up a safe and secure environment to ensure one does not expose themselves to malicious actors. Senior Threat Intel Specialist at Cybersixgill, Michael-Angelo Zummo, will demonstrate how to set up a secure environment (dirty machine) using Tails, how to find sources in the dark web, best practices when creating your first persona, communicate with threat actors, and of course, how to seek out threats once you gain access to the sources where threat actors plan, play, and profit. All while using real examples that attendees can try for themselves.

From this session attendees will:

1) Gain practical knowledge on the tools threat actors use to remain anonymous and communicate

2) Identify popular sources where threat actors communicate and share malicious tools and sensitive data

3) Learn how to threat hunt once one has successfully infiltrated these underground sources

Presentation Outline

Show the progression of your presentation. Submissions that include detailed outlines score higher. (This field will display plain text only. Add line breaks as necessary, for easy reading by our Advisory Committee.)

- Introduction
- Why I'm presenting how to manage your underground personas
- What do I consider the "underground"
- Setting up your darkweb environment
- Access precautions
- Using Tails
- Finding Sources
- Different types of underground forums, markets, chat groups, and more
- Tips on finding sources
- Barriers of entry

- Registering to underground sources
- Language barriers and VIP sections
- Creating your first persona
- Minimum requirements
- Modeling after other hackers
- Communication methods
- Using Telegram, PMs, Jabber, PGP, and more
- Pros and cons of each communication method
- Demonstration of PGP
- Threat Hunting: How to security teams can find threats in the underground
- Real example of recent breach
- Finding initial access and ways into the organization network
- Stealer logs
- Bonus content : Openbullet2 demonstration
- Conclusion

Is this content 100% new, never before presented/published? NO

If this content is not new, explain what's new and what's already been presented and where.
If you have previously presented this research/any portion of this talk, what will you be presenting at SecTor that is new/never before presented (if anything)? If the information has been previously published/presented, provide the name (conference or publication), date and URL. Include a URL to any presentation materials or video of the talk as well.
A version of this session was presented at BSides Tampa, April 1, 2023. It was very well received from a packed room with standing room only.

Will you be releasing a new tool? NO

Will you be releasing a white paper? NO

Message for Advisory Committee
Detail any special considerations that apply to your talk (i.e. 0-day specifics, disclosure process, legalities, job change) including any assistance you may need preparing for the talk or on-site at the conference. This information will not be published and will only be seen by the Advisory Committee.
This is a new session. Last year, Zummo presented on Threat Hunting. This is a deeper dive into previous year's presentation answering the specific questions he was asked most often.