International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

ADVANCED THREAT DEFENSE (ATD) FOR MALWARE DETECTION IN SANDBOX ENVIRONMENTS

John Komarthi
San Jose, CA
john.komarthi@gmail.com

Abstract

Cyber security threats are getting more sophisticated daily, often slipping through traditional security. This paper takes a closer look at Advanced Threat Defense (ATD) using sandbox environments to detect and analyze the malware. Traditional security systems are signature-based and struggle to keep up with novel and targeted attacks, particularly in cases where stealth techniques such as polymorphism or fileless execution have been used. Sandboxing the malware provides a safe and controlled environment to run suspicious files and observe how they behave in real-time. Instead of relying on traditional signature-based threat detection systems, sandboxing focuses on the behavior, which helps to detect previously unknown or custom malware. The present study will explore the architecture of a sandbox-based ATD system, how it fits in security operations, and the impact on threat detection and response. Further, evasion techniques employed by attackers are examined, along with the methods used to detect and neutralize them. Our findings will highlight why sandboxing is an essential tool in today's cybersecurity landscape.

Keywords: Advanced Persistent Threat (APT); Advanced Threat Defense; Cybersecurity; Dynamic Analysis; Evasive Malware; Sandboxing; Threat Intelligence; Zero-Day Threat

I. INTRODUCTION

Modern-day organizations face a surge of sophisticated malware threats. According to the AV-TEST Institute, over 300,000 new malicious programs are discovered each day [1], which far exceeds the detection capabilities of any traditional signature-based antivirus solutions. Apart from the volume, attackers are using advanced evasion techniques such as polymorphism and fileless malware to bypass traditional defenses [2].

To bridge this gap, security strategies are shifting towards a more dynamic, behavior-based approach. Advanced Threat Defense (ATD) is one such approach. ATD is a collection of continuously evolving techniques that are designed to detect, observe, analyze, and respond to the threats that escape the standard scanning tools [3]. Sandboxing is a technique used in ATD where suspicious files or URLs are executed in an isolated virtual environment to observe their behavior. This dynamic analysis helps to understand the threats based on their actual behavior, such as registry change, memory usage, file system activity, or anomalous network traffic,

rather than based on known signatures [4].
Security teams are provided with Indicators Of Compromise (IOC's) through Sandbox-based ATD. IOCs make it possible to uncover previously unknown malware. Sandboxing has become a widely adopted method in modern threat detection and response workflows [5].

The effectiveness of sandboxing didn't go unnoticed by the attackers. Malware creators have developed evasion techniques that will enable their code to detect when it is being run in a sandbox and adjust its behavior further to avoid triggering alarms [6]. These evasion techniques present a significant challenge to the security team and require continual adaptation of sandboxing technologies and detection strategies. Therefore, the study aims to provide practical insights supported by real-world industry research and tools, referencing sources such as McAfee Labs, VMRay, and CrowdStrike.

II. NEED FOR ADVANCED THREAT DEFENSE

Traditional security solutions (antivirus & intrusion prevention) mainly rely on signatures or basic heuristics. These are becoming increasingly ineffective at detecting modern-day advanced threats. The attackers can quickly modify their malware binaries to generate polymorphic variants, hence they don't match existing signatures. Along with this, techniques like code mutation (metamorphism), payload packing, and encryption make it harder for static signature-based defense systems to keep up.
A large portion of the newly developed malware can bypass the tools that solely rely on known indicators. E.g., in 2023, more than 100 million new malware strains have been discovered, of which many were specifically designed to evade the traditional detection method [8]. Even a single undetected threat can often lead to serious data breaches, ransomware incidents, or undetected activity by attackers inside the enterprise environment.
This is where Advanced Threat Defense (ATD) comes in. The dynamic behavior-focused approach uses multiple detection techniques to analyze suspicious files or objects from multiple perspectives. A Typical ATD process looks like this:

1. Static analysis examines the file metadata, known malicious code patterns, and embedded scripts without executing them.
2. Dynamic analysis is also known as sandboxing. The file is executed in an isolated virtual environment to monitor the behavior in real-time.
3. Adaptive analytics, along with machine learning classifiers and threat intelligence feeds, assess the risk level of the threat.

By layering these techniques, ATD can detect threats that were never seen before, including zero-day exploits.
Targeted attacks and Advanced Persistent Threats (APTs) are also driving the adoption of ATD techniques. These kinds of attacks generally involve custom-built malware that is specifically tailored to a specific organization or specific objective, making it difficult for generic security

tools to detect. Even though traditional scanners overlook these threats, sandbox-based analysis exposes the true intentions of the malware. For example, if an unknown binary attempts to change the system settings, communicate with unfamiliar external servers, or disable endpoint protection, sandboxing provides visibility to analyze and detect those behaviors [9].

III. SANDBOX-BASED MALWARE DETECTION

A sandbox is an isolated, secure environment that mimics a real computer system. It has a complete operating system, network stack, file system, and memory. But sandbox is completely isolated from any live resources, allowing the execution of potentially dangerous malware without risk.

When a suspicious email attachment or a file enters an organization's network, an Advanced Threat Defense (ATD) can automatically route the file into the sandbox for analysis. The environment is isolated, and the file can act freely. Every action performed by the file is observed and recorded. This includes file system modifications, memory usage, registry changes, network communication, and process creation [10].

Dynamic analysis gives information that static scanning methods might miss. E.g., sandboxing can uncover a payload that identifies remote domains that the malware is trying to contact or only decrypts in memory. The resulting behaviour report is filled with indicators of compromise (IOCs), and the security team uses this to classify the threat and feed the IOCs to broader defenses.

As sandboxing focuses on the behaviour of the file during the runtime, it's effective at identifying complex hidden threats like fileless malware, multistage droppers, or logic bombs. These types of threats only reveal themselves during execution, and thus make sandboxing a critical line of defense.

Modern-day ATD platforms pair sandboxing techniques with hybrid analysis, combining static code inspection, memory analysis, and runtime behavior monitoring. This layered approach increases detection rates, for example, if the malware detects that it is being analyzed and suppresses its payload, ATD will still flag it based on partial execution traces or memory artifacts [11].

Advances in sandbox solutions have specially designed features to counter sandbox-aware attacks. CrowdStrike's Falcon Sandbox operates at the kernel level while using stealth techniques, making the sandbox environment nearly identical to a real machine. This allows it to catch evasive malware that might otherwise stay dormant [12][13].

This low-level monitoring enables CrowdStrike's system to capture comprehensive sets of behavioral indicators. It also detects subtle signs like memory injections, API calls, or unusual traffic patterns [14].

Sandbox-based ATD is not limited to analysing the executable. It can be configured to run scripts, open document files, or simulate user interaction like clicking a pop-up or moving the mouse. This enables the safe triggering of exploits embedded in PDFs, Excel macros, or browser-based malware. Instead of trying to identify threats, sandboxing allows the malware to

reveal itself through actions.

IV. MALWARE SANDBOX EVASION TECHNIQUES

Modern malware strains are equipped with sandbox evasion techniques, which are designed to detect when being analysed and hide their true behaviour. These evasion techniques are the same across both advanced persistent threats (APTs) [15] and everyday malware [16].
The objective is that if the malware suspects that it's being run in an artificial environment such as a VM (Virtual Machine) or sandbox, it will not exhibit any malicious behaviour to avoid detection. Some of the malware enter a dormant state while others may immediately terminate. Thus, the sandbox won't be able to sense any suspicious activity, and the sample can be misclassified as benign.
Below are some of the most common evasion methods observed:

1. Delaying Execution

This is the simplest evasion tactic to delay malicious activity. Early sandbox systems observed this kind of malware behaviour for only a short time window. Malware attackers started to exploit this by introducing delays using APIs like Sleep, NtDelayExecution, or API flooding, calling benign functions repeatedly to stall [17]. If no malicious activity is reported during the observation period in the sandbox, the sample may be marked clean.
Modern sandboxes have countermeasures like fast forwarding virtual clocks, detecting abnormal sleep behaviour, but some advanced malware delay payload decryption to outwait the analysis window.

2. Environment Artifact Checks

Malware scans for clues if it's running in a virtual or sandboxed environment. These environmental checks include:

- Scanning for virtualization tools (VMware Tools or VirtualBox services)
- Examining BIOS strings, MAC addresses, or CPU identifiers for signs of virtualization
- Checking RAM, CPU core counts, or disk sizes for unrealistic values [18]

In addition, malware may search system registry entries or file paths for keywords like "sandbox," "VMware," or "VirtualBox." If any of these indicators are found, the malware assumes it's under observation and disables its payload.

3. User Interaction Checks

Generally, sandbox environments run in full automation mode without human input. Malware authors take advantage of this by checking for user interaction, such as keyboard input or mouse movement, before executing the payload. They monitor GUI APIs (like GetForegroundWindow) or track mouse activity to know if a human is using the system [19]. For example, some ransomware variants only start encryption after detecting a mouse click.

International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

4. Multi-Stage Payloads and External Triggers

Some malware operates in multiple stages; the first stage may look benign and will only decrypt the real payload when a set of conditions are met, such as detecting extended system uptime or receiving a response from the command control server. Sandboxes with fresh boot times or limited internet access may not satisfy these conditions, causing the malware to delay payload [20][21].

5. Self-Termination on Sandbox Detection

If the malware detects the environment to be a sandbox or a virtual machine, it may simply terminate the process. Agent Tesla is a well-known Remote Access Trojan (RAT) that immediately shuts down when a sandbox is detected [22].

6. Other Evasion Tactics

- Timing attacks, where malware uses high-resolution timers to detect performance anomalies caused by emulation.
- Mutex or file collisions, where malware attempts to create system artifacts used by sandbox software.
- Conditional payloads, where behavior only activates on specific hostnames, keyboard layouts, or geographic regions.

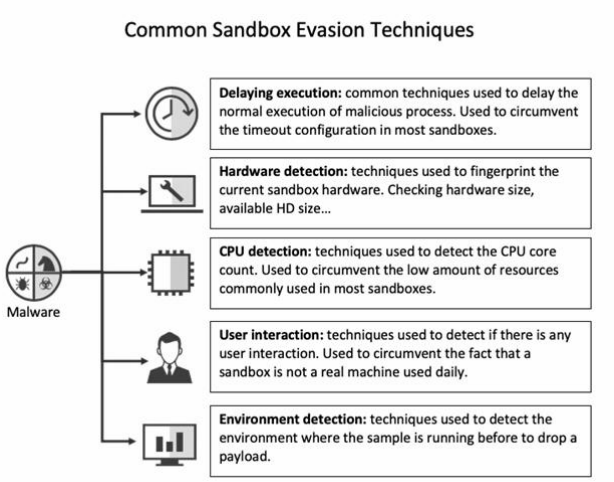

Figure 1: Common sandbox evasion techniques

V. OVERCOMING SANDBOX EVASION IN ATD SOLUTIONS

1. Extended and Adaptive Analysis

Time-based evasion is bypassed by extending the duration of analysis or by adapting to suspicious delays. If the malware stalls the execution using API loops or long Sleep calls, advanced sandboxes can fast-forward these delays [24]. Some systems can detect stalling

patterns like inactivity, repeated benign action, and extend the analysis window or use hooking to bypass stalling.

2. Deeper-Level Instrumentation
Sandbox environments have been made stealthier to prevent detection through virtualization artifacts. For example, CrowdStrike's Falcon Sandbox places the monitoring components at the kernel or hypervisor level [25]. By emulating real-world environments, using hooks, simulating hardware profiles, simulating recent document activity, and introducing fake user interaction to fool malware that it's running on a real machine [26].

3. Multi-Faceted Detection (Static + Dynamic + ML)
ATD solutions now combine static analysis, dynamic behavior monitoring, and machine learning (ML) to detect sophisticated threats. Even when the file doesn't behave visibly maliciously, its structure and metadata can raise red flags. McAfee Advanced Threat Defense uses machine learning to analyze the code structure, entropy, function imports, and more to identify malware even when it doesn't detonate in a sandbox [27]. McAfee has a Family Classification Engine (FCE) that examines the assembly-level code in memory. This allows detection even when the execution of malware is aborted. [28].

4. Memory Dump and Forensics
When the malware partially executes and halts, it will leave some traces behind in the memory. Modern sandboxes take memory snapshots during or after the execution and run forensic analysis on them. This can uncover unpacked payloads sitting in RAM, remnants of fileless malware, or shellcodes [29].

5. Diverse Sandbox Environments
ATD platforms run samples of malware on multiple sandbox configurations to counter malware that targets specific environments. Multiple configurations include different operating systems, e.g., Windows 10, Windows 7, language packs, or regional settings [30]. Bare metal sandboxes may be used for especially evasive malware. This is the case where malware performs advanced environment checks, even though this is slower and resource-intensive, bare metal analysis is the evolution in defeating sandbox evasion [31].

6. Layered Defense and Correlation
Sandboxing is most effective when it is part of a multiple-layered defense system. ATD solution shares findings with firewalls, threat intelligence platforms, and endpoint detection systems. Shared intelligence strengthens future detections [32].
As the attackers improve their sandbox evasion techniques, defenders find stealthier, smarter, and integrated detection technologies. The most effective ATD platforms today blend real-time behaviour monitoring, static analysis, memory forensics, and ML-based classification across different environments to expose malware. Vendors like CrowdStrike, FireEye, McAfee, and

VMray demonstrate high detection rates against previously unseen threats.

VI. COMPARATIVE ANALYSIS: SANDBOXING VS OTHER MALWARE DETECTION TECHNIQUES

Even though sandboxing plays an important role in Advanced Threat Defense (ATD), it is salient to understand how it fares against other security technologies. Traditional security tools like antivirus (AV) are signature-based; they are resource-efficient and fast, but they are only effective against previously known threats. They fall short against zero-day or polymorphic malware. Heuristic scanners, in the same way, try to find suspicious patterns, but are prone to false positives; they often fall short in catching multi-stage payloads or fileless malware.

Endpoint Detection and Response (EDR) platforms monitor system behaviors over time, which gives better visibility on the progression of the attack, but they rely on retrospective analysis and agents. So the attacks are detected only after they have started [47]. Network Intrusion Detection/Prevention Systems (NIDS/NIPS) focus on packet signatures and traffic analysis, but they may miss malware embedded in compressed or encrypted payloads.

Sandboxing gives real-time behavior analysis inside a controlled setting, unlike AV scans or static analysis, sandboxing allows malware to reveal itself by executing it. This helps to uncover memory injections, logic bombs, C2 communication, and more. However, sandboxing needs more resources and is less suited for high-throughput scanning when compared to NIDS or AV tools.

Every detection method has its pros and cons. While sandboxing excels in finding previously unseen and evasive malware, it gets more effective when combined with multiple layers like static scan for pre-filtration, EDR for post-detection. Modern ATD platforms integrate sandboxing along with these technologies to create a layered defense [48].

VII. CHALLENGES AND LIMITATIONS OF SANDBOXING

Sandboxing, with all its strengths, comes with its fair share of challenges. Performance overhead is the most common one, and sandboxes that are running full operating system VMs need significant computational resources to run at scale. High volume environments like cloud storage or email gateways can struggle to detonate every suspicious file in tight time constraints.

Handling of encrypted or obfuscated payloads is another limitation of sandboxing. Malware authors often encrypt the code in such a way that external triggers or user interaction are needed to decrypt and execute the file. If the set conditions are not met, the sandbox may give a false negative [49].

False positives will also occur, especially with legitimate software that behaves in a similar way to malware. E.g., launching scripts, modifying the registry, or accessing network resources. Employing machine learning classification and tuning the behavioral thresholds helps to reduce

the risk, but it can't eliminate it.

Executing potentially destructive code on the cloud can violate privacy regulations or data sovereignty in some regions, raising ethical and operational concerns. Organizations need to ensure that the sandbox environments are compliant and isolated, especially when handling sensitive documents or customer files [50].

Targeted malware is generally designed for specific application versions or operating systems, but if the sandbox does not replicate the intended environment, the malware won't execute. This limits the generic sandbox profiles and pushes the industry towards customizable or adaptable sandbox environments.

VIII. CASE STUDIES AND INDUSTRY ADOPTION

Many modern-day organizations have adapted to sandbox-based Advanced Threat Defense (ATD) to stay ahead of increasingly sophisticated and evasive threats. Over the past decade, vendors like FireEye (now part of Trellix) have led the charge. Their network and email security appliances, equipped with built-in sandboxing, have been widely deployed in enterprise and government networks to detect malware before it has a chance to spread [36]. FireEye exposed APT1, which is a sophisticated, state-sponsored threat group, by Mandiant in 2013 [37]. This investigation remains a landmark in threat intelligence history.

Paolo Alto Networks also played an important role in advancing ATC with their WildFire platform. WildFire automatically analyzes any suspicious files in the cloud, and it shares the results across its customer base. WildFire generates a new signature if a file is flagged as malicious within minutes, giving organizations real-time protection [38]. They also have the AutoFocus platform to understand the malware behavior [39].

CrowdStrike has a different approach by sandboxing its endpoint ecosystem. CrowdStrike integrated Hybrid Analysis technology into its Falcon X suite, which allows endpoint agents to automatically submit suspicious files for analysis [40].

Microsoft has also embraced sandboxing in its Defender suite. It has Safe Attachment in Microsoft Defender for Office 365, which automatically detonates email attachments and URLs before they are delivered to the end user [41]. Microsoft's sandboxing has become smarter and faster, leveraging Microsoft's vast cloud telemetry from Windows, Azure, and Office 365 services [42].

These solutions highlight how sandboxing evolved into a standard security layer. In sectors like government, healthcare, and finance, sandboxing has been integrated into endpoint agents, firewalls, and cloud email security to stop and analyze the attacks even before they cause any damage. Real-world deployments show that sandboxing is efficient in stopping ransomware before it spreads and catching sophisticated phishing payloads.

IX. INTEGRATION OF ATD WITH THREAT INTELLIGENCE PLATFORMS

Even though sandboxing itself is powerful on its own, it's even more effective when paired with

threat intelligence. Modern-day ATD platforms work hand-in-hand with external and internal intelligence feeds to deliver smarter and contextual alerts fast. For example, FireEye's Dynamic Threat Intelligence (DTI) platform collects malware samples from its global customer base and immediately shares the IOCs with other customers [43].

Palo Alto's WildFire continuously analyzes unknown files globally and keeps on pushing updates. STIX and TAXII standards allow the sandbox tools to push the findings into the organization's threat intelligence platform or SIEM [44].

CrowdStrike's Falcon X automatically maps the sandbox findings to known threats, tools, and threat actors. When a suspicious file matches a technique that is used by a known group, the sandbox report will include that attribute, which will help the analysts to understand better and respond with confidence [45].

The integration between ATDs and threat intelligence platforms creates a feedback loop. The sandbox contributes new intel, while the existing feeds will improve the sandbox judgment.

X. AUTOMATED RESPONSE AND SOAR INTEGRATION

Analysis and detection of threats is only part of the battle; the next step is to take action and ideally take action automatically based on the threat. That is the reason organizations are connecting their ATD tools with their Security, Orchestration, Automation, and Response (SOAR) platforms.

After a sandbox flags a file as malicious, the SOAR playbook can be triggered instantly. It can isolate the affected endpoint, block the responsible file hash across the organization, alert the SOC (Security Operations Center), and update the firewall rules almost instantly without manual intervention. This automation is key to containing fast-moving threats like ransomware.

CrowdStrike's Charlotte AI automates the triage (identifying, prioritizing, and managing security incidents) and response process. If Falcon sandbox detects any suspicious behavior, Charlotte can recommend and execute the appropriate responses automatically [46]. Microsoft Defender uses its sandbox insights to perform actions such as isolating infected devices in real time or quarantining emails [42].

This kind of integration helps eliminate the delay between detection and response, a delay that has affected many companies previously with serious data breaches. When sandboxing, threat intelligence, and automated responses work together, defenders can move as fast as attackers.

XI. CONCLUSION

The Advanced Threat Defense (ATD), enhanced with sandboxing, is a foundational part of modern cybersecurity. ATD focuses on analyzing the behavior and intent of the suspicious files in isolated environments, unlike traditional tools that rely on known signatures [4]. This allows the defenders to detect any threats that the traditional dense often miss, which include zero-day malware, fileless attacks, and custom-built payloads [9],[11].

Throughout this paper, we have examined how sandboxing enhances malware detection by observing the real-time behavior, such as injecting into memory, modifying files, or calling back to remote servers. We also observed how attackers are adapting to this by building sandbox-aware malware that can detect virtual environments, delay execution, or wait for user interaction and stay under the radar [15]-[22].

Modern ATD sandbox solutions are also continuously evolving, getting stealthier, operating at kernel or hypervisor level, blending static and dynamic analysis, incorporating machine learning, and extending observation timeframe to spot even subtle signs of malicious activity [24]-[29]. Traditional tools are faster and more lightweight, while sandboxing adds critical depth by exposing behavior that only occurs during execution, especially in highly targeted or polymorphic attacks [47], [48].

It is acknowledged that there are limitations to sandboxing. They can be resource-heavy, and cloud-based detonation raises valid concerns around data privacy and compliance. In some cases, generic sandbox environments may miss malware designed to activate only in specific conditions [49], [50].

However, it is clear now that sandboxing no longer works in a vacuum. Sandboxes are now integrated with threat intelligence platforms (TIPs), enriching the alerts with external context, mapping indicators of compromise (IOCs) to previously known attacks, and helping analysts connect the dots [43]–[45]. This feedback loop strengthens both the sandbox and the overall security posture.

Organizations are tying ATD into their SOAR platforms to automate responses. If a file is flagged as malicious during detonation, actions like isolating the affected endpoint, blocking associated IOCs, or alerting security teams can happen automatically, almost instantly [42],[46].
The industry's direction shows the importance of ATD; vendors like FireEye (Trellix), Palo Alto Networks, CrowdStrike, and Microsoft have built highly scalable, cloud-integrated solutions that protect large enterprises, governments, and critical infrastructure [36]-[42]. The widespread adoption rates reflect that in today's threat landscape, behavior-based detection is essential.
Sandboxing is set to evolve continuously, we are already seeing advances such as bare-metal analysis that eliminates virtualization artifacts, AI-driven behavior modeling for precision, and GPU acceleration to process large volumes of samples faster [31], [51]. Attackers keep on developing increasingly sophisticated evasion tactics, and defenders must respond with systems that are integrated, intelligent, automated, and adaptive.

In conclusion, Advanced Threat Defense for malware detection in sandbox environments is an essential component of any modern cybersecurity program. Organizations that embrace this are better equipped to disrupt targeted attacks, detect zero-day malware, and respond to threats before any damage is done. The attackers will always try to maintain their stealth, but with this

defense, the security team is armed with intelligent, layered detection systems and can stay a step ahead.

REFERENCES

1. AV-TEST Institute, "Malware Statistics & Trends," 2024. [Online]. Available: https://www.av-test.org/en/statistics/malware/
2. KnowBe4, "Polymorphic and Fileless Malware: What You Need to Know," 2023. [Online]. Available: https://blog.knowbe4.com
3. VMRay, "What is Advanced Threat Detection?" 2023. [Online]. Available: https://www.vmray.com/glossary/advanced-threat-detection/
4. VMRay, "Sandboxing 101: How Dynamic Malware Analysis Works," 2023. [Online]. Available: https://www.vmray.com/blog
5. VMRay, "VMRay Technology Whitepaper," 2023. [Online]. Available: https://www.vmray.com/resources/vmray-technology-whitepaper/
6. McAfee, "McAfee Defenders Blog: Reality Check for Your Defenses," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-reality-check-for-your-defenses/
7. McAfee, "Evolution of Malware Sandbox Evasion Tactics – A Retrospective Study," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
8. KnowBe4, "Malware Trends: Over 100 Million New Strains in 2023," 2023. [Online]. Available: https://blog.knowbe4.com
9. McAfee, "Using Sandboxing to Detect Advanced Persistent Threats," 2023. [Online]. Available: https://www.mcafee.com/blogs/enterprise/sandboxing-and-apts/
10. VMRay, "Sandboxing 101: How Dynamic Malware Analysis Works," 2023. [Online]. Available: https://www.vmray.com/blog
11. VMRay, "VMRay Technology Whitepaper," 2023. [Online]. Available: https://www.vmray.com/resources/vmray-technology-whitepaper/
12. CrowdStrike, "Falcon Sandbox Overview," 2023. [Online]. Available: https://www.crowdstrike.com
13. CrowdStrike, "Falcon Sandbox Datasheet," 2023. [Online]. Available: https://assets.crowdstrike.com
14. CrowdStrike, "Falcon Sandbox Product Page," 2023. [Online]. Available: https://www.crowdstrike.com/products/falcon-sandbox/
15. McAfee, "Sandbox Evasion Techniques: How Malware Avoids Detection," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sandbox-evasion-techniques/
16. McAfee, "Understanding Sandbox Evasion in Modern Malware," 2023. [Online]. Available: https://www.mcafee.com/blogs/enterprise/malware-evasion-overview/

17. McAfee, "Delaying Tactics: How Malware Outwaits Sandboxes," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malware-delay-tactics/
18. McAfee, "How Malware Detects Virtual Environments," 2023. [Online]. Available: https://www.mcafee.com/blogs/enterprise/anti-vm-checks/
19. McAfee, "Malware Detection Evasion via User Interaction Checks," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/user-interaction-malware/
20. McAfee, "Multi-Stage Malware: Bypassing Sandboxes in Layers," 2023. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/multi-stage-evasion/
21. McAfee, "External Triggers and Sandbox Limitations," 2023. [Online]. Available: https://www.mcafee.com/blogs/enterprise/external-triggers-in-advanced-malware/
22. Picus Security, "Agent Tesla: A Case Study in Sandbox Evasion," 2023. [Online]. Available: https://www.picussecurity.com/resource/blog/agent-tesla-sandbox-evasion
23. McAfee, "Common Malware Families Using Sandbox Evasion," 2023. [Online]. Available: https://www.mcafee.com/blogs/enterprise/sandbox-evasion-in-the-wild/
24. McAfee, "Malware Evasion Tactics: Delays and Time-Based Evasion," 2023. [Online]. Available: https://www.mcafee.com/blogs
25. CrowdStrike, "Falcon Sandbox Datasheet," 2023. [Online]. Available: https://assets.crowdstrike.com
26. CrowdStrike, "Falcon Sandbox Stealth Capabilities," 2023. [Online]. Available: https://www.crowdstrike.com/products/falcon-sandbox/
27. McAfee, "How Machine Learning Powers ATD," 2023. [Online]. Available: https://www.mcafee.com/blogs
28. McAfee, "Family Classification Engine in Advanced Threat Defense," 2023. [Online]. Available: https://www.mcafee.com
29. McAfee, "Memory Forensics in Sandbox Analysis," 2023. [Online]. Available: https://www.mcafee.com/blogs
30. VMRay, "Dynamic Analysis with Multi-Profile Sandbox Environments," 2023. [Online]. Available: https://www.vmray.com
31. McAfee, "Bare-Metal Sandboxing: The Next Frontier," 2023. [Online]. Available: https://www.mcafee.com/blogs
32. VMRay, "Defense-in-Depth with Integrated Threat Detection," 2023. [Online]. Available: https://www.vmray.com/resources
33. VMRay, "How ATD Defeats Modern Malware Evasion," 2023. [Online]. Available: https://www.vmray.com/blog
34. VMRay, "Defense-in-Depth: Why Layered Security is Essential," 2023. [Online]. Available: https://www.vmray.com/resources

35. McAfee, "The Future of Sandbox Technology: Bare Metal and Beyond," 2023. [Online]. Available: https://www.mcafee.com/blogs
36. Trellix, "What is FireEye?," Trellix Knowledge Base, 2023. [Online]. Available: https://www.trellix.com/en-us/about/newsroom/stories/what-is-fireeye.html
37. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant Intelligence Report, 2013. [Online]. Available: https://www.fireeye.com/current-threats/apt-groups/rpt-apt1.html
38. Palo Alto Networks, "WildFire Malware Prevention Service," 2023. [Online]. Available: https://www.paloaltonetworks.com/products/security-subscriptions/wildfire
39. Palo Alto Networks, "AutoFocus Threat Intelligence," 2023. [Online]. Available: https://www.paloaltonetworks.com/cortex/autofocus
40. CrowdStrike, "CrowdStrike Acquires Payload Security," Press Release, 2017. [Online]. Available: https://www.crowdstrike.com/blog/crowdstrike-acquires-payload-security/
41. Microsoft, "Microsoft Defender for Office 365: Safe Attachments," Microsoft Learn, 2024. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments
42. Microsoft, "Microsoft 365 Defender," 2024. [Online]. Available: https://www.microsoft.com/en-us/security/business/threat-protection/microsoft-365-defender
43. FireEye, "Dynamic Threat Intelligence," 2022. [Online]. Available: https://www.fireeye.com/solutions/dynamic-threat-intelligence.html
44. Palo Alto Networks, "Threat Intelligence Sharing Using STIX and TAXII," Palo Alto Networks Blog, 2023. [Online]. Available: https://www.paloaltonetworks.com/blog
45. CrowdStrike, "Falcon X: Intelligence-Driven Malware Analysis," 2023. [Online]. Available: https://www.crowdstrike.com/products/falcon-x/
46. CrowdStrike, "Charlotte AI: Meet Your AI Security Analyst," 2024. [Online]. Available: https://www.crowdstrike.com/blog/meet-charlotte-ai-your-ai-security-analyst/
47. MITRE, "A Guide to EDR Capabilities and Use Cases," 2023. [Online]. Available: https://attack.mitre.org/resources
48. Palo Alto Networks, "Combining Static and Dynamic Analysis in WildFire," 2023. [Online]. Available: https://www.paloaltonetworks.com
49. Kaspersky, "Challenges in Modern Sandbox Environments," 2023. [Online]. Available: https://www.kaspersky.com/blog/sandbox-evasion
50. SANS Institute, "Sandboxing: Ethical Considerations in Cloud Malware Analysis," 2022. [Online]. Available: https://www.sans.org/white-papers
51. Microsoft, "XDR and the Role of Behavioral Analytics," 2024. [Online]. Available: https://www.microsoft.com/security

Figure-1:

Network Solutions, "How Sandbox Security Helps Prevent Malware Attacks," Network Solutions Blog, 2023. [Online]. Available: https://www.networksolutions.com/blog/protect/cybersecurity/how-sandbox-security-helps-prevent-malware-attacks