×

Search

- Experienced a breach?
- Small Business
- CrowdStrike Marketplace
- Us
- Blog

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

undles
et started with CrowdStrike
ext-gen antivirus and USB device
otect your business.
ptimize your defense
ivirus and threat intelligence for greater
our environment. Automated threat
s accelerate alert, triage and response.
prise: never miss a threat
urity tools to provide a single source of truth:
ivirus, EDR, XDR, managed threat hunting
ed threat intelligence.
e: advanced breach prevention
Integrated endpoint and identity protection, the expanded
y of Falcon Insight XDR, unequaled threat-hunting and
ded protection of identity security to stop every breach.
Falcon Complete: superior prevention, detection & response
The full suite of managed endpoint threat and identity protection
with expert monitoring and remediation.

Platform categories
Cloud security
Stop cloud breaches with unified cloud security posture management and breach prevention.
Data protection
Stop data theft with policy enforcement that automatically follows content, not files.
Endpoint security & XDR
Supercharge protection, detection and response – for endpoint and beyond.
Exposure management
Reduce risk with complete attack surface visibility and AI-powered vulnerability management.
Identity protection
Stop breaches faster by protecting workforce identities everywhere.
Next-gen SIEM
Rapidly shut down threats with real-time detections, blazing-fast search, and cost-effective data retention.
Threat intelligence & hunting
Disrupt adversaries and their attacks. Know them. Find them. Stop them.
IT Automation
Ask, answer, and act on any question across the IT estate, as an extension of the CrowdStrike platform.
Application Security Posture Management
See and secure every application and API with Bionic, a CrowdStrike company.

Platform capabilities
About the CrowdStrike platform
Charlotte AI
Falcon Foundry
Falcon Fusion
AI & machine learning
Threat Graph
FAQs

**CrowdStrike Marketplace**

- Services

Main Menu

Prepare
Prepare and train your organization to defend against sophisticated threat actors using real-life simulation exercises.
Tabletop Exercise
Red Team / Blue Team Exercise
Adversary Emulation Exercise
Penetration Testing

Respond
Available under a Services Retainer, giving
you access to security consultants and

expertise to respond to a breach.
Incident Response
Compromise Assessment
Endpoint Recovery
Network Detection

**Experienced a breach?**

Enhance your cybersecurity practices and controls with actionable recommendations to improve your cybersecurity posture.
sessment
isk Assessment
ment
rity Assessment
urity Assessment
es
etection & Response
Falcon Complete and backed by CrowdStrike's Breach Prevention Warranty.
reat Hunting
Watch, as an extension of your team, hunting relentlessly to stop hidden threats.
es
rity Services
tection Services
cale Services
vices
ike?

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

Main Menu
Strike?
Considering Microsoft?

Ransomware protection
Learn what you can do to stop ransomware threats in their tracks.
Log4Shell mitigation
Get the latest information on this evolving vulnerability.
Observability & log management
Fills in the gaps, logs everything, and realizes real-time observability for your entire system.
Solutions by industry
Small business
ion security
sector
Healthcare
ervices
Definition
Types
Use Cases
Stages
Falcon Sandbox
es
Microsoft?
hat starts with Microsoft
rowdStrike
ty 101 glossary
s, examples and best practices
of cybersecurity topics.
eat landscape
adversaries targeting
y.
Threat Report
ead cybersecurity report of the year.
eat Hunting Report
CrowdStrike's threat hunting insights
uly 1, 2022 to June 30, 2023.
CrowdStrike blog


Discover how CrowdStrike protects you against the most advanced attacks.
From the front lines
Executive viewpoint
Counter Adversary Operations
Customer focused
Free trial guide
Customer support portal
CrowdStrike University
CrowdStrike Tech Center
Developer portal
Knowledge resources
Case studies
White papers

Webinars
Adversary Universe Podcast
Reports
Logging guides
Try interactive demo
All resources

- Company

Main Menu
ith us
Events
024
unter Hands-on Labs
s
tners and distributors
viders
chnology partners
e Marketplace
e a
er
eam
ectors
elations
Environmental, social & governance
Strike & F1 Racing

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

- Login
- English (US)
  - English (US)
  - Deutsch
  - English (AU)
  - English (UK)
  - Español
  - Français
  - Italiano
  - Português
  - LatAm
  - 繁體中文
  - 日本語
  - 한국어
  - عربى

View Bundles & Pricing →

- View bundles & pricing
- Platform
- Services
- Why CrowdStrike?
- Learn
- Company
- Contact Us
- EXPERIENCED A BREACH?
- Languages

Main Menu

Falcon platform bundles
Falcon Go: get started with CrowdStrike
Affordable next-gen antivirus and USB device control to protect your business.
Falcon Pro: optimize your defense
Next-gen antivirus and threat intelligence for greater insight into your environment. Automated threat investigations accelerate alert, triage and response.
Falcon Enterprise: never miss a threat

Unify all security tools to provide a single source of truth: next-gen antivirus, EDR, XDR, managed threat hunting and integrated threat intelligence.
Falcon Elite: advanced breach prevention
Integrated endpoint and identity protection, the expanded visibility of Falcon Insight XDR, unequaled threat-hunting and the added protection of identity security to stop every breach.
Falcon Complete: superior prevention, detection & response
uite of managed endpoint threat and identity protection
monitoring and remediation.

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

hes with unified cloud security posture management and breach prevention.

ith policy enforcement that automatically follows content, not files.
y & XDR
tection, detection and response – for endpoint and beyond.
ement
complete attack surface visibility and AI-powered vulnerability management.
on
ster by protecting workforce identities everywhere.

n threats with real-time detections, blazing-fast search, and cost-effective data retention.
ce & hunting
ies and their attacks. Know them. Find them. Stop them.

d act on any question across the IT estate, as an extension of the CrowdStrike platform.
Application Security Posture Management
ure every application and API with Bionic, a CrowdStrike company.

Platform capabilities
About the CrowdStrike platform
Charlotte AI
Falcon Foundry
Falcon Fusion
AI & machine learning
Threat Graph
FAQs

**CrowdStrike Marketplace**

‹ Main Menu

Prepare
Prepare and train your organization to defend against sophisticated threat actors using real-life simulation exercises.
Tabletop Exercise
Red Team / Blue Team Exercise
Adversary Emulation Exercise
Penetration Testing

Respond
Available under a Services Retainer, giving you access to security consultants and expertise to respond to a breach.
Incident Response
Compromise Assessment
Endpoint Recovery
Network Detection

**Experienced a breach?**

Fortify
Enhance your cybersecurity practices and controls with actionable recommendations to fortify your cybersecurity posture.
Maturity Assessment
Technical Risk Assessment
SOC Assessment
Cloud Security Assessment
Identity Security Assessment

Managed Services
Managed Detection & Response

Included in Falcon Complete and backed by CrowdStrike's Breach Prevention Warranty.
Managed Threat Hunting
Falcon OverWatch, as an extension of your team, hunting relentlessly to stop hidden threats.

Additional Services
Cloud Security Services
Identity Protection Services
Falcon LogScale Services
Partner Services

Main Menu

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

rosoft?


Compare CrowdStrike
See how we stack up against our competitors
Industry recognition
CrowdStrike is the recognized leader in endpoint protection solutions.
Customer stories
Don't take our word for it, hear what our customers have to say.

Solutions by topic
Zero Trust
Real-time breach protection on any endpoint, cloud workload or identity, wherever they are.
Cloud threat detection and response
Stop cloud breaches for multi-cloud and hybrid environments in a single platform.
Ransomware protection
Learn what you can do to stop ransomware threats in their tracks.
Log4Shell mitigation
Get the latest information on this evolving vulnerability.
Observability & log management
Fills in the gaps, logs everything, and realizes real-time observability for your entire system.

Solutions by industry
Small business
Election security
Public sector
Healthcare
Financial services
Retail

Main Menu

Featured resources
Considering Microsoft?
Cyber risk that starts with Microsoft ends with CrowdStrike
Cybersecurity 101 glossary
Explanations, examples and best practices on a variety of cybersecurity topics.
Get your threat landscape
the adversaries targeting
2024 Global Threat Report
cybersecurity report of the year.
ting Report
reat hunting insights
to June 30, 2023.

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox


Discover how CrowdStrike protects you against the most advanced attacks.
From the front lines
Executive viewpoint
Counter Adversary Operations

Customer focused
Free trial guide
Customer support portal
CrowdStrike University
CrowdStrike Tech Center
Developer portal

Knowledge resources
Case studies
White papers
Webinars
Adversary Universe Podcast
Reports
Logging guides
Try interactive demo
All resources

‹ Main Menu

Connect with us
Careers
Events
Fal.Con 2024

# MALWARE ANALYSIS

Kurt Baker - April 17, 2023

## What is Malware Analysis?

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat.

The key benefit of malware analysis is that it helps incident and security analysts:

- ragmatically triage incidents by level of severity
- ncover hidden indicators of compromise (IOCs) that hould be blocked
- nprove the efficacy of IOC alerts and notifications
- nrich context when threat hunting



# Types of Malware Analysis

The analysis may be conducted in a manner that is static, dynamic or a hybrid of the two.

## Static Analysis

Basic static analysis does not require that the code is actually run. Instead, **static analysis examines the file for signs of malicious intent**. It can be useful to identify malicious infrastructure, libraries or packed files.

Technical indicators are identified such as file names, hashes, strings such as IP addresses, domains, and file header data can be used to determine whether that file is malicious. In addition, tools like disassemblers and network analyzers can be used to observe the malware without actually running it in order to collect information on how the malware works.

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox




However, **since static analysis does not actually run the code, sophisticated malware can include malicious runtime behavior that can go undetected**. For example, if a file generates a string that then downloads a malicious file based upon the dynamic string, it could go undetected by a basic static analysis. Enterprises have turned to dynamic analysis for a more complete understanding of the behavior of the file.

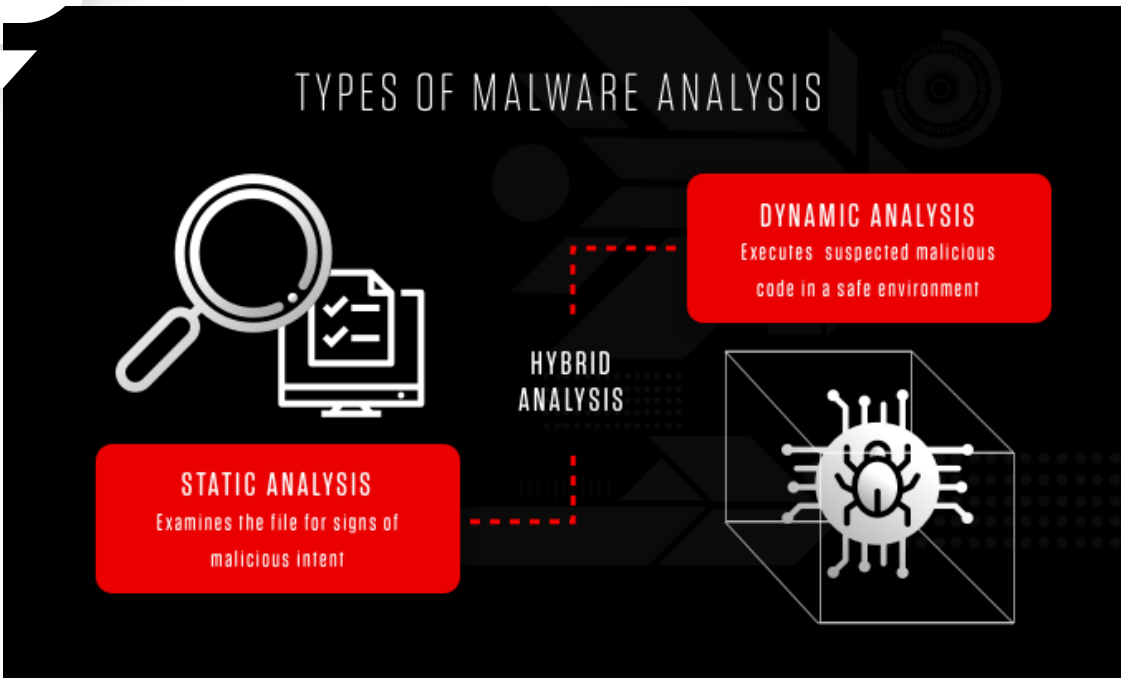
## Dynamic Analysis

**Dynamic malware analysis executes suspected malicious code in a safe environment called a *sandbox*.** This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

Dynamic analysis provides threat hunters and incident responders with deeper visibility, allowing them to uncover the true nature of a threat. As a secondary benefit, automated sandboxing eliminates the time it would take to reverse engineer a file to discover the malicious code.



...nge with dynamic analysis is that adversaries are smart, ...now sandboxes are out there, so they have become ...at detecting them. To deceive a sandbox, adversaries ...nside them that may remain dormant until certain ...are met. Only then does the code run.




## Hybrid Analysis (includes both of the techniques above)

Basic static analysis isn't a reliable way to detect sophisticated malicious code, and sophisticated malware can sometimes hide from the presence of sandbox technology. **By combining basic and dynamic analysis techniques, hybrid analysis provide security team the best of both approaches –**primarily

because it can detect malicious code that is trying to hide, and then can extract many more indicators of compromise (IOCs) by statically and previously unseen code. Hybrid analysis helps detect unknown threats, even those from the most sophisticated malware.



e, one of the things hybrid analysis does is apply static data generated by behavioral analysis – like when a alicious code runs and generates some changes in ynamic analysis would detect that, and analysts would to circle back and perform basic static analysis on that ump. As a result, more IOCs would be generated and zero-day exploits would be exposed.



# Malware Analysis Use Cases

## Malware Detection

Adversaries are employing more sophisticated techniques to avoid traditional detection mechanisms. By providing deep behavioral

analysis and by identifying shared code, malicious functionality or infrastructure, threats can be more effectively detected. In addition, an output of malware analysis is the extraction of IOCs. The IOCs may then be fed into SEIMs, threat intelligence platforms (TIPs) and security orchestration tools to aid in alerting teams to threats in the future.




## Threat Alerts and Triage

Malware analysis solutions provide higher-fidelity alerts earlier in the attack life cycle. Therefore, teams can save time by prioritizing the results of these alerts over other technologies.

## Incident Response

The goal of the incident response (IR) team is to provide root cause analysis, determine impact and succeed in remediation and recovery. The malware analysis process aids in the efficiency and effectiveness of this effort.

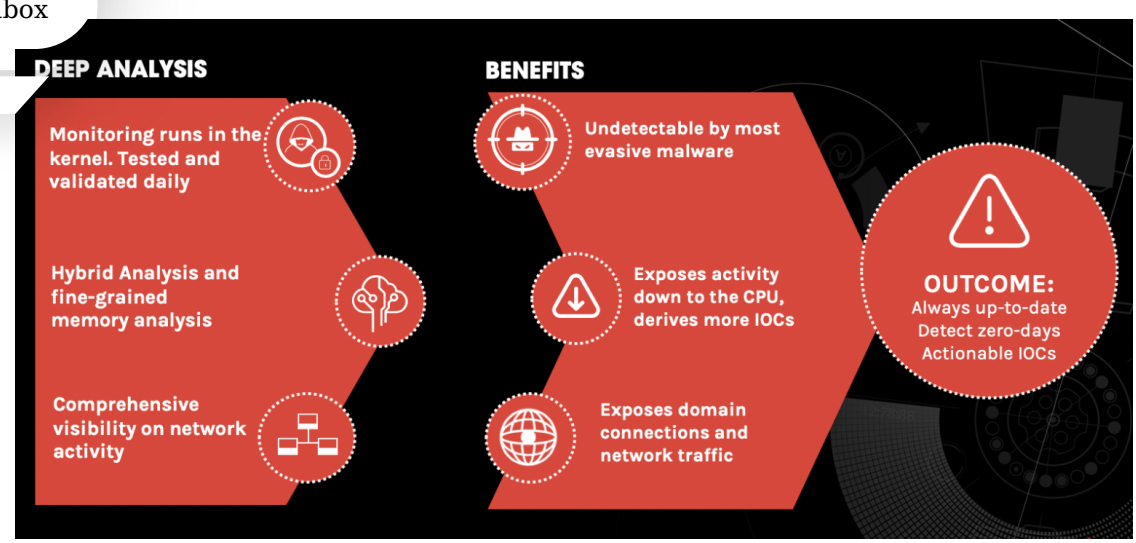
## Threat Hunting

Malware analysis can expose behavior and artifacts that threat hunters can use to find similar activity, such as access to a particular network connection, port or domain. By searching firewall and proxy logs or SIEM data, teams can use this data to find similar threats.



### Research

or industry malware researchers perform malware gain an understanding of the latest techniques, exploits sed by adversaries.




# Stages of Malware Analysis

## Static Properties Analysis

Static properties include strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc. This type of data may be all that is needed to create IOCs, and they can be acquired very quickly because there is no need to run the program in order to see them. Insights gathered during the static properties analysis can indicate whether a deeper investigation using more comprehensive techniques is necessary and determine

which steps should be taken next.

## Interactive Behavior Analysis

Behavioral analysis is used to observe and interact with a malware ...ning in a lab. Analysts seek to understand the sample's ...e system, process and network activities. They may also ...emory forensics to learn how the malware uses memory. ...sts suspect that the malware has a certain capability, ...et up a simulation to test their theory.


- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox


... analysis requires a creative analyst with advanced skills. The process is time-consuming and complicated and cannot be performed effectively without automated tools.

## Fully Automated Analysis

Fully automated analysis quickly and simply assesses suspicious files. The analysis can determine potential repercussions if the malware were to infiltrate the network and then produce an easy-to-read report that provides fast answers for security teams. Fully automated analysis is the best way to process malware at scale.

## Manual Code Reversing

In this stage, analysts reverse-engineer code using debuggers, disassemblers, compilers and specialized tools to decode encrypted data, determine the logic behind the malware algorithm  and understand any hidden capabilities that the malware has not yet exhibited. Code reversing is a rare skill, and executing code reversals takes a great deal of time. For these reasons, malware investigations often skip this step and therefore miss out on a lot of valuable insights into the nature of the

malware.


- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox


## EARN MORE

out the largest online malware analysis community
ld-tested by tens of thousands of users every day.

**ad: Falcon Sandbox Malware Analysis Data**

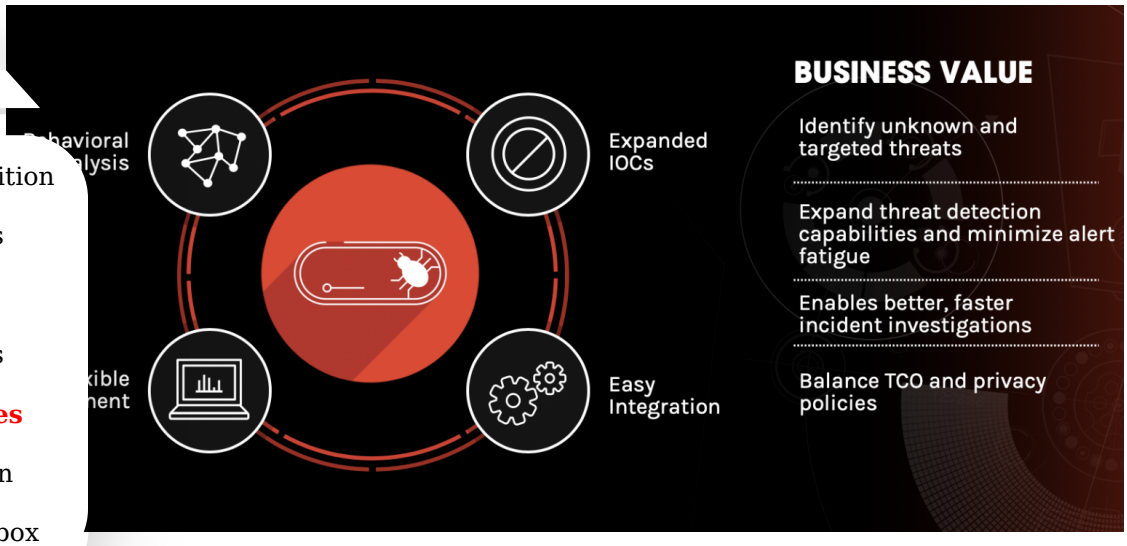
## The World's Most Powerful Malware Sandbox

Security teams can use the CrowdStrike Falcon® Sandbox to understand sophisticated malware attacks and strengthen their defenses. Falcon Sandbox™ performs deep analyses of evasive and unknown threats, and enriches the results with threat intelligence.

### Key Benefits Of Falcon Sandbox

- Provides in-depth insight into all file, network and memory activity
- Offers leading anti-sandbox detection technology
- Generates intuitive reports with forensic data available on demand
- Supports the MITRE ATT&CK® framework

→ Orchestrates workflows with an extensive application programming interface (API) and pre-built integrations






# LEARN MORE

**DID YOU KNOW?** Falcon Sandbox is also a critical component of CrowdStrike's CROWDSTRIKE FALCON® INTELLIGENCE threat intelligence solution? CrowdStrike Falcon® Intelligence enables you to automatically analyze high-impact malware taken directly from your endpoints that are protected by the CrowdStrike Falcon® platform. This analysis is presented as part of the detection details of a Falcon endpoint protection alert. Built into the Falcon Platform, it is operational in seconds.

**Watch a Demo >**

## Detect Unknown Threats

Falcon Sandbox extracts more IOCs than any other competing sandbox solution by using a unique hybrid analysis technology to detect unknown and zero-day exploits. All data extracted from the hybrid analysis engine is processed automatically and integrated into Falcon Sandbox reports.



dbox has anti-evasion technology that includes state-of-i-sandbox detection. File monitoring runs in the kernel be observed by user-mode applications. There is no can be easily identified by malware, and each release is ly tested to ensure Falcon Sandbox is nearly ble, even by malware using the most sophisticated sandbox detection techniques. The environment can be customized by date/time, environmental variables, user behaviors and more.

## Identify Related Threats

Know how to defend against an attack by understanding the adversary. Falcon Sandbox provides insights into who is behind a malware attack through the use of malware search a unique capability that determines whether a malware file is related to a larger campaign, malware family or threat actor. Falcon Sandbox will automatically search the largest malware search engine in the cybersecurity industry to find related samples and, within seconds, expand the analysis to include all files. This is important because it provides analysts with a deeper understanding of the attack and a larger set of IOCs that can be used to better protect the organization.

## Achieve Complete Visibility

Uncover the full attack life cycle with in-depth insight into all file, network, memory and process activity. Analysts at every level gain access to easy-to-read reports that make them more effective in their roles. The reports provide practical guidance for threat prioritization and response, so IR teams can hunt threats and ams can drill down into memory captures and stack deeper analysis. Falcon Sandbox analyzes over 40 e types that include a wide variety of executables, and image formats, and script and archive files, and it indows, Linux and Android.



## d Faster

Security teams are more effective and faster to respond thanks to Falcon Sandbox's easy-to-understand reports, actionable IOCs and seamless integration. Threat scoring and incident response summaries make immediate triage a reality, and reports enriched with information and IOCs from CrowdStrike Falcon® MalQuery™ and CrowdStrike Falcon® Intelligence™ provide the context needed to make faster, better decisions.

Falcon Sandbox integrates through an easy REST API, pre-built integrations, and support for indicator-sharing formats such as Structured Threat Information Expression™ (STIX), OpenIOC, Malware Attribute Enumeration and Characterization™ (MAEC), Malware Sharing Application Platform (MISP) and XML/JSON (Extensible Markup Language/JavaScript Object Notation). Results can be delivered with SIEMs, TIPs and orchestration systems.

Cloud or on-premises deployment is available. The cloud option provides immediate time-to-value and reduced infrastructure costs, while the on-premises option enables users to lock down

and process samples solely within their environment. Both options provide a secure and scalable sandbox environment.

## Automation



dbox uses a unique hybrid analysis technology that utomatic detection and analysis of unknown threats. All cted from the hybrid analysis engine is processed lly and integrated into the Falcon Sandbox reports. enables Falcon Sandbox to process up to 25,000 files and create larger-scale distribution using load- Users retain control through the ability to customize settings and determine how malware is detonated.

**Learn how CrowdStrike can help you get more out of malware analysis:**

Start Free Trial

# T TO KNOW THE AUTHOR

senior director of product marketing for Falcon Intelligence at CrowdStrike. He has over 25 years of nior leadership positions, specializing in emerging software companies. He has expertise in cyber threat urity analytics, security management and advanced threat protection. Prior to joining CrowdStrike, Baker cal roles at Tripwire and had co-founded startups in markets ranging from enterprise security solutions s. He holds a bachelor of arts degree from the University of Washington and is now based in Boston,

**Featured Articles**

# What is a Man in the Middle (MITM) Attack?




# Advanced Persistent Threat (APT)


# Incident Response Plan: Frameworks and Steps

New to CrowdStrike?
About the platform
Explore products
Services
Why choose CrowdStrike?

Company
About CrowdStrike
Newsroom

- Definition
- Types
- Use Cases
- **Stages**
- Falcon Sandbox

Your Privacy Choices
Accessibility