



NEXT GENERATION EDR EVASION:

# EvadeX

A PHANTOMSEC TOOL



# EXECUTIVE SUMMARY

As defensive tools for network security evolve, so do adversarial tactics. Traditional methods of penetration testing and threat emulation have become inadequate due to the widespread adoption of advanced endpoint detection and response (EDR) systems, such as Microsoft Defender. In this environment, modern red teams and penetration testers face significant challenges when attempting to bypass these security layers.

EvadeX offers a streamlined solution to this challenge. Our cloud-based platform enables security professionals to quickly generate evasive payloads that avoid EDR detection, allowing red teams to focus on testing and evaluation rather than spending resources on payload development. EvadeX empowers organizations to optimize their security testing efforts, making their teams more efficient, professional, and effective.

## Why EDR evasion is necessary for best-in-class penetration teams

In today's cybersecurity landscape, threat actors are continuously developing new techniques to bypass advanced security measures. Traditional tools and methods often fall short in simulating these sophisticated attacks, leaving gaps in defense strategies. Modern penetration testing requires tools that are not only innovative, but also adaptive to the rapidly changing threat environment. EvadeX meets this demand by providing a platform that keeps pace with the latest evasion techniques, ensuring that your testing capabilities remain cutting-edge.

Moreover, the need for customized payloads has never been greater. Off-the-shelf tools are more likely to be flagged by EDR systems, making bespoke payload generation essential for realistic threat emulation. EvadeX fills this gap by enabling operators to create tailored payloads that evade detection, mimicking the behavior of real-world adversaries.




## Using EvadeX to emulate threats

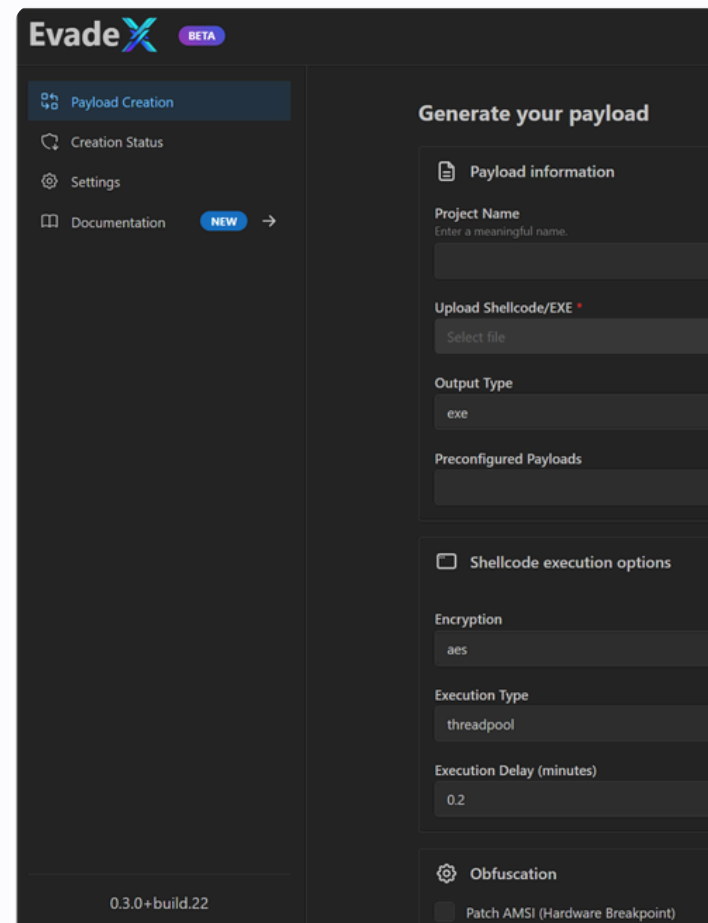
EvadeX is designed with the modern threat landscape in mind. With the ability to incorporate various execution techniques and evasion patches, the platform enables operators to simulate the tactics, techniques, and procedures (TTPs) used by today's most sophisticated threat actors. By leveraging EvadeX, your team can test defenses against the latest malware strains, advanced persistent threats (APTs), and custom exploits that are currently being deployed in the wild.

This emulation capability is crucial for understanding how your security infrastructure would hold up against real-world attacks. By using EvadeX, your testing team can identify vulnerabilities that might otherwise go unnoticed, allowing for more targeted and effective remediation efforts.

# Using EvadeX

With the increasing complexity of security defenses, traditional payload generation tools fall short of the capabilities required to evade detection by sophisticated security systems. EvadeX simplifies this process by providing operators with an intuitive, cloud-based platform that enables the creation of evasive and customizable payloads in just three steps.

-  **Upload Shellcode:** Operators can generate shellcode using popular tools such as Metasploit, Sliver, or Mythic, then upload it to the EvadeX portal.
-  **Customize Payload:** Operators select from a wide array of options, from basic application customization (e.g., icons and metadata) to advanced evasion techniques that help bypass detection by EDR systems.
-  **Generate & Deploy:** After selecting the desired options, the operator clicks “Generate” to create the customized payload. The payload is then ready for immediate download and deployment.



EvadeX significantly reduces the time and expertise needed for custom payload development, ensuring operators have more time to focus on executing comprehensive security assessments.



# EvadeX Saves Time and Money

## Eliminate in-house development costs

EvadeX automates the payload creation process, removing the need for dedicated development resources or team members taking time off operations to do development.

## Enable immediate payload creation

Generate payloads before the engagement begins, and start evading payloads on day 1.

## Adapt Immediately

Want to switch up your payload to avoid detection? Simply create a new payload. With our polymorphic generation each payload is unique.

## Reduce onboarding time

While other solutions may require in-depth technical knowledge or significant manual effort, EvadeX is designed to be accessible to a wide range of users. Its intuitive interface and automated processes enable operators to create sophisticated, evasive payloads with minimal training.

## Stay ahead of the curve

EvadeX ships continuous updates, incorporating the latest evasion techniques and threat intelligence into the platform along with our own novel research.

Our users always have access to cutting-edge tools for simulating the most advanced attacks, without spinning development wheels on adapting.

---

Hiring dedicated capability developers is expensive.

Save your team from resource drain by leaving payload generation to EvadeX.

---

EvadeX pricing is publicly available on our site. No need to get a quote or talk to a sales person!.



Book a demo  
[phantomsec.tools/book](https://phantomsec.tools/book)



Contact us  
[info@phantomsec.tools](mailto:info@phantomsec.tools)

## The Need for Advanced Tool Development

The modern threat landscape is more dynamic and dangerous than ever. Cyber attackers constantly develop new techniques to bypass even the most advanced security measures, often rendering traditional tools obsolete. As organizations rely on EDR systems to detect and respond to threats, red teams are tasked with creating custom payloads capable of bypassing these defenses to provide realistic assessments of security postures.

## Why Off-the-Shelf Solutions Fall Short

Off-the-shelf tools, such as generic payloads generated by common frameworks, are easily recognized by security systems. These predictable methods often lead to premature detection, limiting the effectiveness of penetration tests. EvadeX addresses this gap by providing tailored, evasive payloads that better emulate the techniques used by sophisticated adversaries. This results in more realistic threat simulations and, ultimately, stronger security defenses.

## Emulating Current Threats with EvadeX

EvadeX was developed with the latest cybersecurity threats in mind. It allows red teams to incorporate modern execution techniques, evasion tactics, and custom payload patches to simulate the tactics, techniques, and procedures (TTPs) used by today's most advanced adversaries.

## Realistic Threat Emulation

With EvadeX, operators can create payloads that mirror real-world threats, including advanced persistent threats (APTs), ransomware, and custom malware strains. These payloads are designed to bypass detection by EDR systems, making them invaluable for testing an organization's defenses under realistic conditions. By using EvadeX, security teams can better identify and address vulnerabilities before they can be exploited by malicious actors.

## Ready for a Demo?

EvadeX is ready to revolutionize the way your team conducts penetration testing and threat emulation. If you're interested in seeing how EvadeX can enhance your security testing capabilities, book a demo today.

We'll walk you through the platform's features and demonstrate how EvadeX will save you time, money, and resources while keeping your security assessments ahead of the curve.



Visit the site  
[evadex.io](https://evadex.io)



Book a demo  
[\*\*phantomsec.tools/book\*\*](https://phantomsec.tools/book)



Contact us  
[\*\*info@phantomsec.tools\*\*](mailto:info@phantomsec.tools)

### Grant Smith

#### President

A proven cybersecurity leader with experience at the DoD, ARCYBER, and The Walt Disney Company. Regular conference speaker, most recently at DEF CON.

Certifications: OSCP, GCIH, GSEC, Security+, eCPPTv2, eWPT, eJPT

### Justin Perez

#### CTO

A highly skilled software engineer with a strong focus in information security. Work experience includes Microsoft and the US Air Force.

Certifications: Security+, eJPT

### Jane Lawing

#### CEO

An experienced US Navy surface warfare officer with work experience around the globe. Holds a degree in neurotechnology.