Be a part of the next generation of ransomware defense

The CounterCraft Ransomware Public Beta Program

Introduction

Ransomware is one of the most common threats facing organizations globally across all sectors, and incidents of ransomware attacks continue to rise. Threat actors, meanwhile, are only becoming more and more sophisticated with their attack methods. The need to heighten ransomware protection for any business is clear.

CounterCraft's Ransomware Cloud Public Beta Program offers you the chance to deploy a cutting-edge ransomware defense campaign before anyone else. We've created a cyber deception campaign that is designed to detect even sophisticated ransomware attacks at various points on the kill chain, from reconnaissance to lateral movement.

Your organization now has the chance to build on the success of the Alpha phase of CounterCraft's ransomware cloud deception campaign. We are selecting 10 organizations to run a beta version of our sophisticated ransomware cyber deception campaign. Your company will test drive this campaign at no risk and no cost if selected to participate.

Take a step to improve your organization's cyber resilience to ransomware.

The Ransomware Cloud Deception Campaign

The CounterCraft Cloud™ ransomware campaign is deception as a service. Designed to be used as a subscription service, it was created to detect initial stages of targeted ransomware attacks.

A successful ransomware attack against your organization disrupts business operations resulting in lost revenue and stopping your production assets. It can also result in temporary or permanent loss of company data, together with the reputational damage that creates.

The Ransomware Cloud deception campaign is designed to:

- **Detect targeted ransomware activity early in the attackers' discovery and lateral movement stages.**
- **Collect threat intelligence on the techniques that are being used against you by the attackers.**
- **Proactively reconfigure your current security ecosystem to better defend against the attacks.**

How it Works

The goal of the Ransomware Cloud campaign is to detect ransomware activity in its early stages and deflect attacks away from the infrastructure of the organization by deploying a deception buffer zone.
The service will deliver real time intelligence that will be used to harden your infrastructure.

Deploy: CounterCraft deploys the assets associated with the service. This includes the creation of the attack vector discovery assets (breadcrumbs), any associated IT assets, and full configuration and deployment of the campaign.

Discover: The threat actors follow a prepared breadcrumb trail to discover and attack external-facing services, hosted on your behalf by CounterCraft.

Detect: CounterCraft will detect when threat actors are conducting reconnaissance externally and/or moving laterally internally; you will be alerted immediately.

Collect Intel: The platform continues to collect intel in real time on how the threat actors are trying to compromise internal and external Windows servers (Domain Controllers), and what techniques, tools and procedures they are using to attack.

Proactively Protect: make it actionable. Integrate the intelligence gathered with your security infrastructure: e.g. SIEM, SOAR, and TIPs.. SIEM, SOAR, and TIPs.

The Benefits for Your Organization

- **Mitigate the threat of ransomware** to your business operations and maintain the integrity of your network.
- **Minimal Internal Resource Use.** The CounterCraft Cloud Ransomware campaign is deployed and managed entirely by CounterCraft in our own cloud and internet, and it only needs the instrumentation of two Windows servers.
- **Assure business continuity** avoiding loss of data or reputational damage.
- **Cover the gaps left by security solutions.** Attackers use off-the-shelf tools available in your network in order to perform their attacks, making detection by standard security solutions almost impossible.
- **Obtain actionable threat intelligence** that is specific to your organization, and that enhances your corporate security strategy. Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

How to Participate

Click here to fill out a brief, four-question application to be considered for the public beta program. For the first round, CounterCraft will choose ten companies to try a ransomware campaign at no cost to them.

Eligibility

Any organization globally is eligible to apply. We do recommend that your organization have a cybersecurity department, team or head.

The Beta Process

If your organization is selected for the Public Beta Ransomware Program, you will be notified via the contact info given at the time of application. You will be assigned a threat intel expert from the CounterCraft team who will guide you and your security team through the process. The deployment can take anywhere from a couple hours to a few days, depending on the complexity of your organization. You will work hand in hand with our Customer Success Team, receiving credible notifications should any threat actors do recon on your organization or execute lateral movement during the testing.

You can opt out at any time, for any reason

Frequently Asked Questions

The CounterCraft Ransomware Cloud Public Beta Program

What is the CounterCraft Ransomware Cloud Public Beta Program?

The CounterCraft Ransomware Cloud Public Beta Program is designed to help in the development of a deception-powered ransomware detection program. As a member of the CounterCraft Ransomware Cloud Beta Program, you can adopt the most advanced deception technology at no cost to you. There are only 10 places available, so **sign up** by June 23 to be considered.

We are looking for the right type of companies to partner with and take our idea of next generation ransomware protection and response to the next level. This deception-as-a-service campaign is easy to deploy, and our team will work with yours to set up the three-month beta in no time. This is a great opportunity to try a novel security solution at no risk or cost to your organization. **Sign up today >>>**

How do I get the public beta?

Sign up for the selection process at **www.countercraftsec.com**. Interested organizations should fill out their contact information by June 23, 2021. CounterCraft will notify the selected businesses soon after.

How do I provide my feedback to CounterCraft?

In addition to ongoing dialogue, there will be a meeting between you and your CounterCraft rep at the end of the beta period in which you will be able to provide any final feedback.

Who can participate?

The CounterCraft Ransomware Cloud Public Beta Program is open to organizations across the globe who accept the terms and conditions during the sign-up process.

Do I have to pay a fee to join the program?

No, the beta program has no cost.

How long does it take to get the program started?

Install and deployment time can range from a few hours to up to two weeks, depending on your organization's complexity.

How long does the beta last?

From deployment, the beta program lasts three months.

What kind of compensation do I receive for testing?

This program is voluntary, and there is no compensation for your participation.

How does the CounterCraft Ransomware Cloud Public Beta Program contact me?

CounterCraft will contact you using the information you provide on the application form.

Will deploying the ransomware service from the CounterCraft Ransomware Cloud Public Beta Program require access to my network?

The program can be run with or without access to your network. Running the program with access improves its efficacy. This will be discussed in detail with the selected organizations.

Technical Description

We use social engineering techniques against the attackers on your external perimeter and in your internal network. Technical discovery information will be placed where it can be found by a threat actor searching for your organization's infrastructure online.

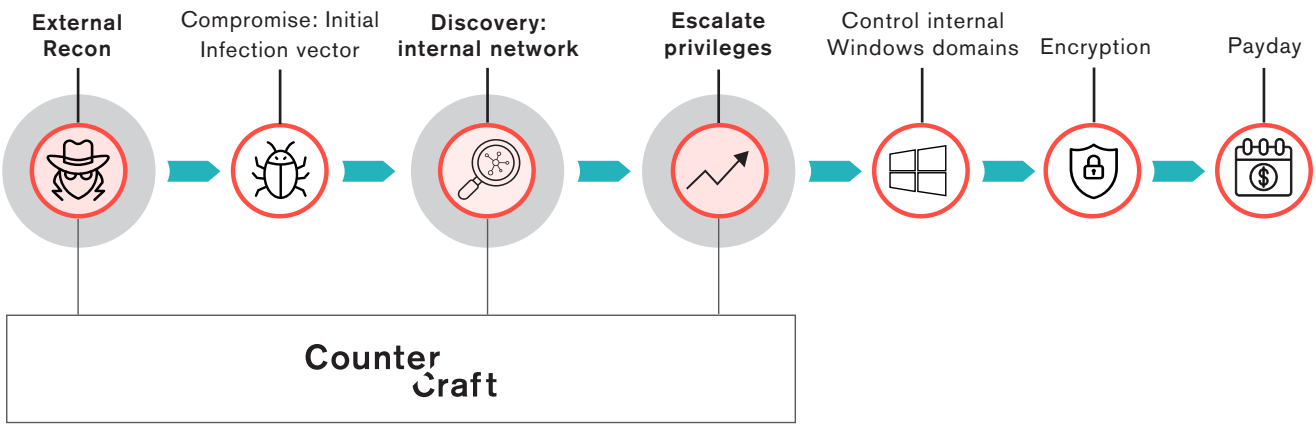
The external deception buffer zone infrastructure will be hosted on cloud infrastructure. In the deception buffer zone, external services will provide the attackers with a credible target: Windows servers with exposed RDP. If an attacker is searching any exposed Windows RDP server related to your organization, they will find our deception buffer zone.

The internal deception buffer zone will be using your own internal Windows Servers with a valid Domain Controller and some open shared folders. By using a number of internal breadcrumbs in the real Active Directory, attackers will be attracted to our servers.

When an attacker interacts with the deception buffer zone, an alert is immediately sent from our console and threat intelligence collection starts.

The deliverables are actionable threat intelligence data with enrichments in the form of TTPs (MITRE ATT&CK) and IoCs including IP addresses, and credentials used by threat actors. The threat intel data can be sent to external security tools such as MISP, a SIEM or SOAR platforms.

This deception campaign breaks the ransomware attack path in the early stages highlighted in the graph below:



About CounterCraft

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time.

Their award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload. Founded in 2015, CounterCraft is present in New York, London, and Madrid, with R&D in San Sebastian, Spain. Learn more at **www.countercraftsec.com**.

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com

The Beta Process

If your organization is selected for the Public Beta Ransomware Program, you will be notified via the contact info given at the time of application. You will be assigned a threat intel expert from the CounterCraft team who will guide you and your security team through the process. The deployment can take anywhere from a couple hours to a few days, depending on the complexity of your organization. You will work hand in hand with our Customer Success Team, receiving credible notifications should any threat actors do recon on your organization or execute lateral movement during the testing.

You can opt out at any time, for any reason

Frequently Asked Questions

The CounterCraft Ransomware Cloud Public Beta Program

What is the CounterCraft Ransomware Cloud Public Beta Program?

The CounterCraft Ransomware Cloud Public Beta Program is designed to help in the development of a deception-powered ransomware detection program. As a member of the CounterCraft Ransomware Cloud Beta Program, you can adopt the most advanced deception technology at no cost to you. There are only 10 places available, so **sign up** by June 23 to be considered.

We are looking for the right type of companies to partner with and take our idea of next generation ransomware protection and response to the next level. This deception-as-a-service campaign is easy to deploy, and our team will work with yours to set up the three-month beta in no time. This is a great opportunity to try a novel security solution at no risk or cost to your organization. Sign up today >

How do I get the public beta?

Sign up for the selection process at **www.countercraftsec.com**. Interested organizations should fill out their contact information by June 23, 2021. CounterCraft will notify the selected businesses soon after.

How do I provide my feedback to CounterCraft?

In addition to ongoing dialogue, there will be a meeting between you and your CounterCraft rep at the end of the beta period in which you will be able to provide any final feedback.

Who can participate?

The CounterCraft Ransomware Cloud Public Beta Program is open to organizations across the globe who accept the terms and conditions during the sign-up process.

Do I have to pay a fee to join the program?

No, the beta program has no cost.

How long does it take to get the program started?

Install and deployment time can range from a few hours to up to two weeks, depending on your organization's complexity.

How long does the beta last?

From deployment, the beta program lasts three months.

What kind of compensation do I receive for testing?

This program is voluntary, and there is no compensation for your participation.

How does the CounterCraft Ransomware Cloud Public Beta Program contact me?

CounterCraft will contact you using the information you provide on the application form.

Will deploying the ransomware service from the CounterCraft Ransomware Cloud Public Beta Program require access to my network?

The program can be run with or without access to your network. Running the program with access improves its efficacy. This will be discussed in detail with the selected organizations.

The Ransomware Cloud Deception Campaign

The CounterCraft Cloud™ ransomware campaign is deception as a service. Designed to be used as a subscription service, it was created to detect initial stages of targeted ransomware attacks.

A successful ransomware attack against your organization disrupts business operations resulting in lost revenue and stopping your production assets. It can also result in temporary or permanent loss of company data, together with the reputational damage that creates.

The Ransomware Cloud deception campaign is designed to:

- **Detect targeted ransomware activity early in the attackers' discovery and lateral movement stages.**
- **Collect threat intelligence on the techniques that are being used against you by the attackers.**
- **Proactively reconfigure your current security ecosystem to better defend against the attacks.**

How it Works

The goal of the Ransomware Threat Intelligence Service is to detect ransomware activity in its early stages and deflect attacks away from the infrastructure of the organization by deploying a deception buffer zone. The service will deliver real time intelligence that will be used to harden your infrastructure.

1. **Deploy:** CounterCraft deploys the assets associated with the service. This includes the creation of the attack vector discovery assets (breadcrumbs), any associated IT assets, and full configuration and deployment of the campaign.

2. **Discover:** The threat actors follow a prepared breadcrumb trail to discover and attack external-facing services, hosted on your behalf by CounterCraft.

3. **Detect:** CounterCraft will detect when threat actors are conducting reconnaissance externally and/or moving laterally internally; you will be alerted immediately.

4. **Collect Intel:** The platform continues to collect intel in real time on how the threat actors are trying to compromise internal and external Windows servers (Domain Controllers), and what techniques, tools and procedures they are using to attack.

5. **Proactively Protect:** Proactively Protect: make it actionable. Integrate the intelligence gathered with your security infrastructure: e.g. SIEM, SOAR, and TIPs.. SIEM, SOAR, and TIPs.

The Benefits for Your Organization

- **Mitigate the threat of ransomware** to your business operations and maintain the integrity of your network.
- **Minimal Internal Resource Use.** The Threat Intelligence Service for Ransomware Activity is deployed and managed entirely by CounterCraft in our own cloud and internet, and it only needs the instrumentation of two Windows servers.
- **Assure business continuity** avoiding loss of data or reputational damage.
- **Cover the gaps left by security solutions.** Attackers use off-the-shelf tools available in your network in order to perform their attacks, making detection by standard security solutions almost impossible.
- **Obtain actionable threat intelligence.** that is specific to your organization, and that enhances your corporate security strategy. Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

How to Participate

Click here (insert link) to fill out a brief, four-question application to be considered for the public beta program. For the first round, CounterCraft will choose ten companies to try a ransomware campaign at no cost to them.

Eligibility

Any organization globally is eligible to apply. We do recommend that
your organization have a cybersecurity department, team or head.

The Ransomware Cloud Deception Campaign

The CounterCraft Cloud™ ransomware campaign is deception as a service. Designed to be used as a subscription service, it was created to detect initial stages of targeted ransomware attacks.

A successful ransomware attack against your organization disrupts business operations resulting in lost revenue and stopping your production assets. It can also result in temporary or permanent loss of company data, together with the reputational damage that creates.

The Ransomware Cloud deception campaign is designed to:

- **Detect targeted ransomware activity early in the attackers' discovery and lateral movement stages.**
- **Collect threat intelligence on the techniques that are being used against you by the attackers.**
- **Proactively reconfigure your current security ecosystem to better defend against the attacks.**

How it Works

The goal of the Ransomware Threat Intelligence Service is to detect ransomware activity in its early stages and deflect attacks away from the infrastructure of the organization by deploying a deception buffer zone. The service will deliver real time intelligence that will be used to harden your infrastructure.

Deploy: CounterCraft deploys the assets associated with the service. This includes the creation of the attack vector discovery assets (breadcrumbs), any associated IT assets, and full configuration and deployment of the campaign.

Discover: The threat actors follow a prepared breadcrumb trail to discover and attack external-facing services, hosted on your behalf by CounterCraft.

Detect: CounterCraft will detect when threat actors are conducting reconnaissance externally and/or moving laterally internally; you will be alerted immediately.

Collect Intel: The platform continues to collect intel in real time on how the threat actors are trying to compromise internal and external Windows servers (Domain Controllers), and what techniques, tools and procedures they are using to attack.

Proactively Protect: Proactively Protect: make it actionable. Integrate the intelligence gathered with your security infrastructure: e.g. SIEM, SOAR, and TIPs.. SIEM, SOAR, and TIPs.

The Benefits for Your Organization

- **Mitigate the threat of ransomware** to your business operations and maintain the integrity of your network.
- **Minimal Internal Resource Use.** The Threat Intelligence Service for Ransomware Activity is deployed and managed entirely by CounterCraft in our own cloud and internet, and it only needs the instrumentation of two Windows servers.
- **Assure business continuity** avoiding loss of data or reputational damage.
- **Cover the gaps left by security solutions.** Attackers use off-the-shelf tools available in your network in order to perform their attacks, making detection by standard security solutions almost impossible.
- **Obtain actionable threat intelligence.** that is specific to your organization, and that enhances your corporate security strategy. Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

How to Participate

Click here (insert link) to fill out a brief, four-question application to be considered for the public beta program. For the first round, CounterCraft will choose ten companies to try a ransomware campaign at no cost to them.

Eligibility

Any organization globally is eligible to apply. We do recommend that your organization have a cybersecurity department, team or head.