CounterCraft **The Edge**™

Ransomware threat intelligence service

Detect initial stages of targeted ransomware attacks

Fighting Ransomware with Active Defense

Ransomware is one of the most intractable — and common — threats facing organizations globally across all sectors, and **incidents of ransomware attacks continue to rise**. In Q3 2020, Check Point Research saw a 50% increase in the daily average of ransomware attacks, compared to the first half of the year.

Meanwhile, ransomware threat actors are adjusting their attack model to adapt to the improvements that organizations are making to defend themselves from these attacks.

The extra challenges:

- Ransomware has evolved to become smarter and less noisy, infecting systems the attacker knows exists.
- The time from initial breach to exploitation of attacks has dropped significantly and is now measured in days, and sometimes hours.
- It is very difficult to gather accurate and actionable threat intelligence about the attack that is delivered in real time.
- All organizations face a lack of resources: no one has the time or money to make threat data into actionable intelligence.

Implications:

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 it creates.

Burning Questions For CISOs:

- How can you be more active in your security defenses against ransomware?
- Can you improve your organization's cyber resilience to ransomware?
- Can you do this without increasing your full-time employee requirements?
- Are you maximising the efficiency of your current security ecosystem with timely and accurate threat intel data?

CounterCraft's Key Service Outcomes:

Deploying our ransomware activity threat-intel campaign allows you 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.

Technical Solution

Threat Intelligence Service: Ransomware Intelligence

Technical Scope

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

Technical Description

We use social engineering techniques against the attackers in 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.

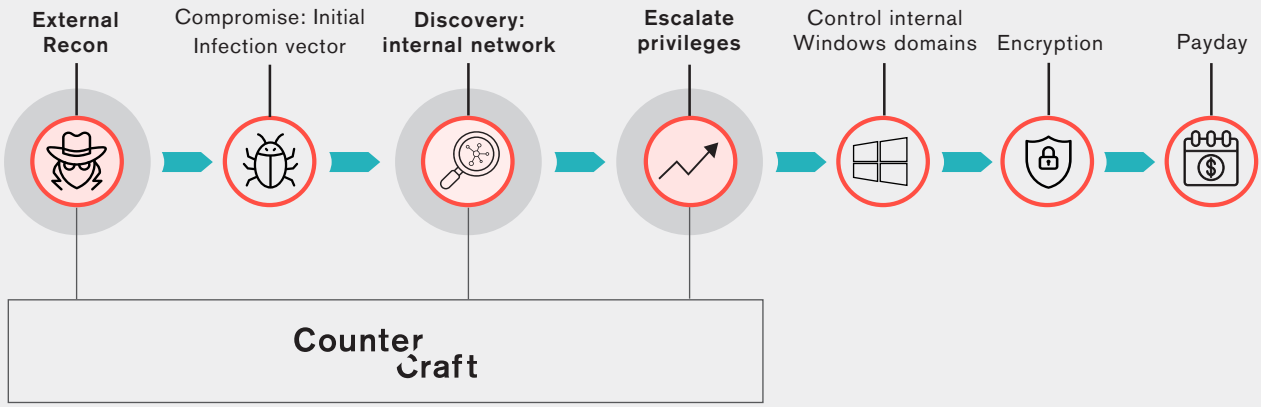
The external deception buffer zone infrastructure will be hosted on cloud infrastructure. In the deception buffer zone, external services will provide the attackers with a credible target: Windows servers with exposed RDP. If an attacker is searching any exposed Windows RDP server related to your organization,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

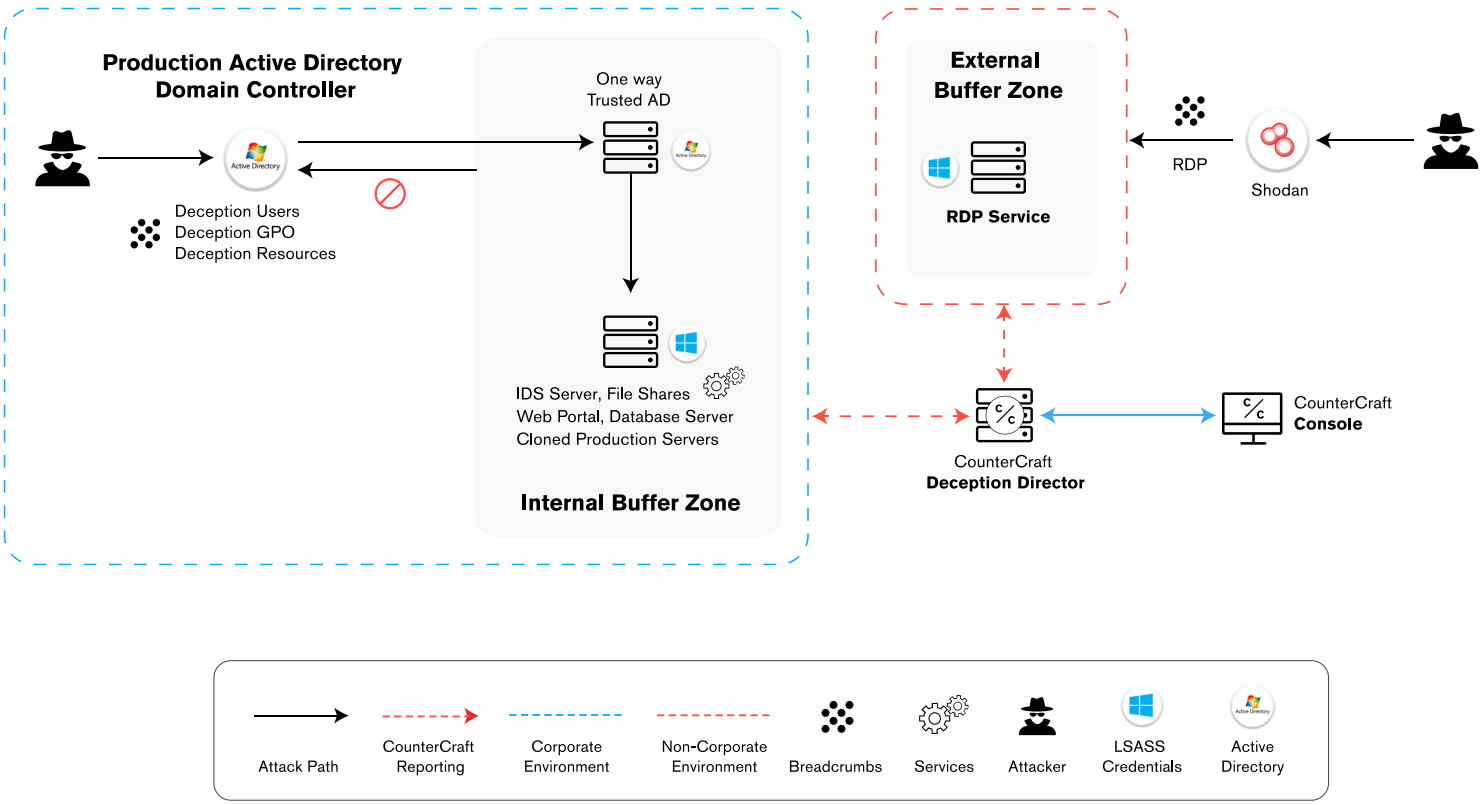
When an attacker interacts with the deception buffer zone, an alert is immediately sent from our console and threat intelligence collection starts.

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:



Technical Architecture



Business Benefits

- **Mitigate the threat of ransomware to your business** operations and maintain the integrity of your network thus defending and protecting your key revenue streams.

- **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.

Strategic Benefits

Cover the gaps left by security solutions. Attackers use off-the-shelf tools available in your network in order to perform their attacks, making the detection by standard security solutions almost impossible.

Obtain actionable threat intelligence that is specific to your organization, that enhances your corporate security strategy.

Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

Operational Benefits

Deploy

deception buffer zones with zero workload and effort to your threat intel team.

Detect Threats

detect ransomware attacks in its early discovery stages in real time.

Collect Threat Intelligence

collect real time, focused and actionable intel, with zero increase to analyst workload:

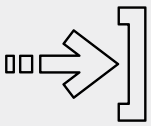
- Gain insight on the IOCs and MITRE ATT&CK TTPs actively being used when the threat actor is trying to compromise external Windows Servers and when they move laterally in your network.
- Catalogue the abilities of threat actors.
- Identify the most active Attack Vectors used to explore your infrastructure via analysis of the use of Technical Discovery Information.

Proactively Protect

- The service delivers organization-specific threat intelligence to achieve your operational goals:
  - Send machine-readable threat intel data (IOCs, TTPs and Logs to your SIEM or SOAR platform).
  - Send incident data to MISP or other Threat Intel Platforms.
- Investigate Incidents rapidly to discover Threat Actor modus operandi.
- Use the Threat Intelligence output to reconfigure enterprise systems: e.g. Firewalls, IPS, IDS and EDR in real time.

Buying the service

We have designed a low-friction journey for you to start enjoying the benefits of the service:



Access the full-service description and commercial offer by completing the form on the website.

Resolve any doubts with the sales team and return the signed commercial offer.

Enjoy the service! Attend the onboarding tutorial, meet your account manager and hold regular meetings with your client satisfaction team.

About CounterCraft

CounterCraft is a pioneering provider of full-spectrum cyber deception technology offering attack detection, threat intelligence collection and proactive defence to clients. Our award-winning solution combines powerful campaign automation with controlled synthetic environments to allow attackers to penetrate organizations without doing real damage.

CounterCraft is recognized worldwide for its radical contribution to the deception technology market and operates in more than 20 Fortune500 Index companies globally, including financial institutions, governments and Law Enforcement Agencies. Founded in 2015, CounterCraft is present in London, Madrid and Los Angeles, with R&D in San Sebastián (Spain).

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com