Threat Intelligence Service for Spear Phishing Intelligence Collection

CounterCraft

Mitigate the risk of spear phishing attacks penetrating your organization

Spear phishing is a targeted attack that, unlike general phishing attacks, does not rely on an easily detected spam campaign. Instead, the victims are carefully selected.

- In 2019 the Verizon data breach investigation report listed phishing as the leading cause of data breaches in that year.
- According to Cofense (formerly PhishMe Cofense.com) 91% of cyber-attacks begin with a spear phishing attack.
- 83% of information security professionals have experienced phishing attacks in 2018-Proofpoint, State of The Phish Report 2019.

How does the current operating environment for business make this threat even more virulent?

Many organizations have been forced to move rapidly to a remote working profile. This results in different security challenges for the individuals having to work from home. The most important one is that people now have to work in isolation from fellow team members. Add to this, that it is natural to relax more when working in an informal atmosphere —the risk of clicking on an email that appears to be from a legitimate source increases exponentially.

"Between March 1 and March 23, Barracuda Sentinel has detected 467,825 spear phishing email attacks, and 9,116 of those detections were related to COVID-19." - CIO & Leader Study (Mar 27, 2020).

It is clear from the data that no matter what security may be in place, **there is always the possibility that someone, somewhere in your organization will click on a link that will result in your corporate network being compromised.**

You could adopt the old approach of hoping you can block everything, despite evidence to the contrary. Or you could take a dynamic approach, to meet the new security landscape that you face.

The challenges for incident responders:

- Successfully investigating and mitigating a spear phishing attack involves analysing all the stages of the attack, from initial compromise of computers to exploitation. Gathering adequate intelligence on these stages is difficult and may put the organization at risk.
- Attackers use compromised mail accounts to cross-phish within organizations How can you identify when this is happening?
- It is very difficult to gather accurate and actionable spear phishing threat intelligence that is delivered in real-time.
- All organizations face a lack of resources: no one has the time or money to investigate or mitigate all the spear phishing attacks that a large organization faces.

CounterCraft's spear phishing Intel campaigns deliver on all four challenges

CISOs Burning questions:

- Are my security controls ready to stop targeted spear phishing attacks?
- Can I improve my organization's cyber resilience to spear phishing activity?
- Can I do this without increasing my full time employee requirements?

CounterCraft's Key Service Outcomes:

Turbocharge your response to Spearphishing attacks and use our threat intelligence service for Spearphishing to collect intel from the attack and proactively protect your organization from the current and future attacks. Deploying our spear phishing threat-intel campaign allows you to:

Detect and analyze targeted spear phishing activity.

Collect real-time intel on the techniques that are being used against you and understand the strategic drivers behind the spear phishing attack.

Proactively protect your organization by reconfiguring your current security ecosystem to better defend against a successful spear phishing attack.

Technical Solution

Threat Intelligence Service: Spear Phishing

Technical Scope

The goal of the Spear Phishing Intelligence Service is to deflect the spear phishing attack into a buffer zone to collect actionable and real-time threat intelligence about the attacker.

1 **Deploy:** CounterCraft deploys the assets associated with the service, these include: web based email service accounts and web based supporting infrastructure, for example servers. This is your deceptive buffer zone to fool the spear phishers.

2 **Discover:** Your SOC takes known Spear Phishing emails that are attempting account compromise, for example by offering a plausible website that requests a name and password, and then adds the credentials for the web based email service accounts, deployed above, to the Spear Phishers infrastructure.

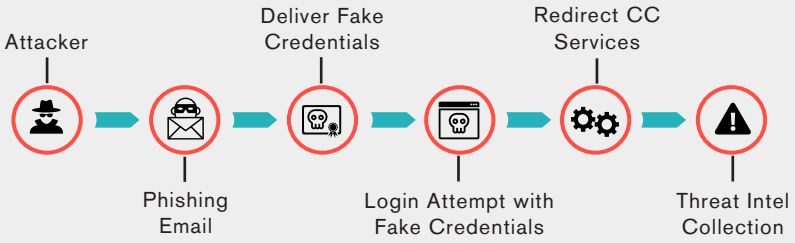
3 **Detect:** CounterCraft will detect when the threat actors are interacting with the deception buffer zone and you will be alerted immediately.

4 **Collect Intel:** The platform continues to collect intel in real-time on how the threat actors use the compromised account, and where they pivot to from the account. Various attractive targets will be offered to them in the buffer zone. CounterCraft will be collecting the techniques, tools and procedures (TTPs) they are using to attack. You will be able to access all this information through an easy-to-understand dashboard.

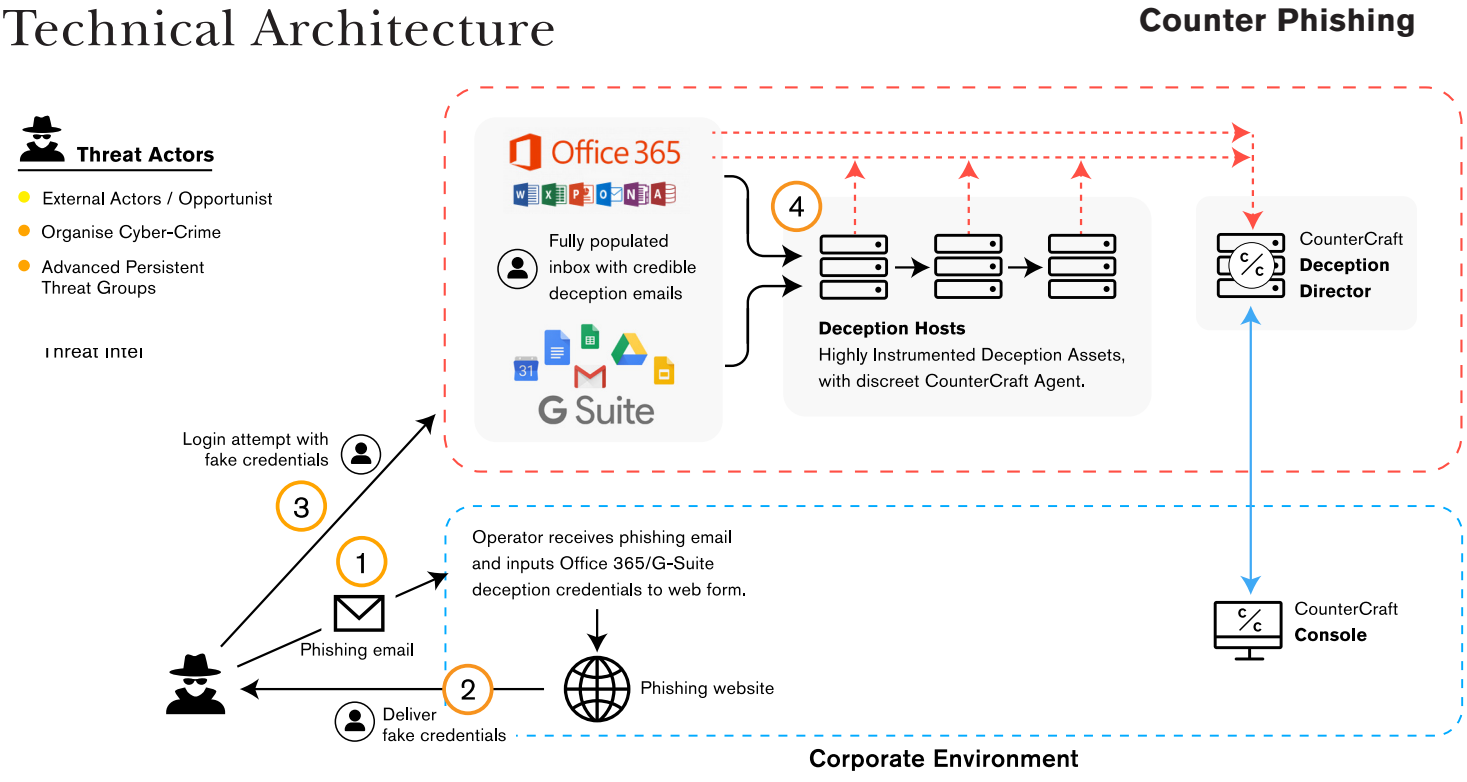
5 **Proactively Protect:** make it actionable. Integrate the intelligence gathered with your security infrastructure: e.g. SIEM, SOAR, and TIPs. Reconfigure your other security systems to detect and stop the TTPs you have discovered.

Technical Deliverables

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.



Technical Architecture



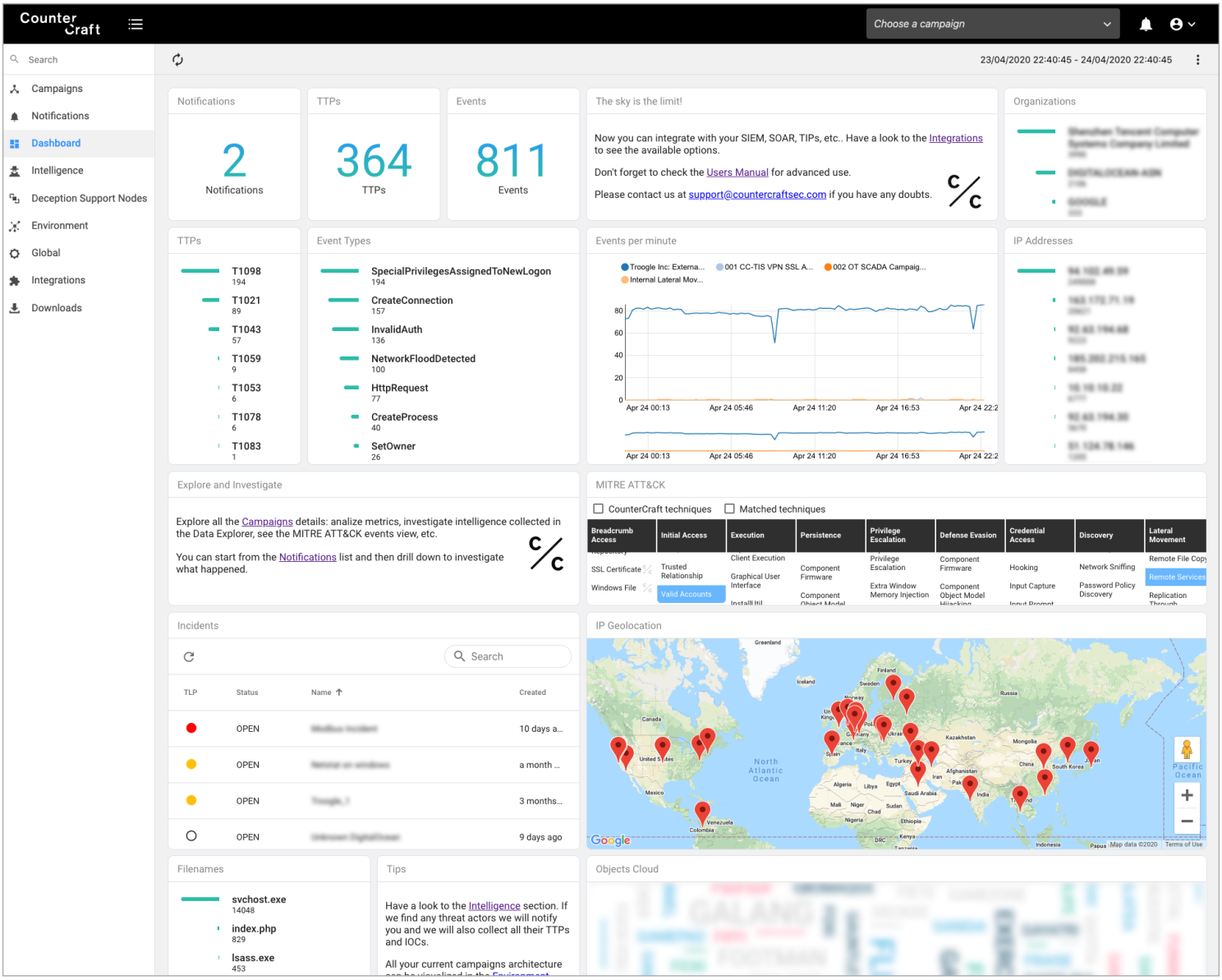
Business Benefits

Mitigate the risk of a spear phishing attack penetrating your organization by aligning your security real estate and ensuring that it is tuned to operate at its maximum efficiency and capacity.

Zero Internal Resource Use. The Threat Intelligence Service for Spear Phishing is a managed service that uses no internal resources. It is deployed and managed entirely by CounterCraft in our own cloud and the Internet.

Assure business continuity to ensure that key revenue generating operations are kept stable and online without disrupting either internal stakeholders or external customers.

Service Dashboard



Strategic Benefits

- Simplify communication with board members and key management about the strategic merit of threat intelligence - use hard evidence, and organisation specific intel to back up your messaging.
- Obtain actionable threat intelligence, that is specific to your organisation, that enhances the corporate security strategy.
- Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

Operational Benefits

Deploy

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

Collect Threat Intelligence

Collect real-time, focused and actionable intel about active Spear Phishing campaigns running against you, with zero increase to analyst workload:

- ☑ Gain insight on the IOCs and MITRE ATT&CK TTPs actively being used by Spear Phishers.
- ☑ Classify who is attacking you: understand if the attack is from known threat actors.
- ☑ Catalogue the abilities of threat actors.
- ☑ Identify the most active TTPs used by Spear Phishers against your organization.

Detect Threats

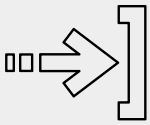
Detect activity by Spear Phishers making attacks on your external infrastructure in real-time.

Proactively Protect

- ☑ The service delivers organisation 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