Segasec – You have a Security Blind Spot as Wide as the Infinite Web. What's Keeping your Customers Safe?

> Segasec is the strongest solution for covering consumer phishing scams from end to end, a managed service for intelligence and response.
>
> With proactive insight into digital risk at the earliest possible stage and holistic defense that covers **block, take-down, and deception**, your customers are given iron-clad protection from the growing dangers originating in the hidden corners of the internet.

General

The vast majority of cyber-security solutions on the market today focus on attacks that threaten business's internal networks and data centers. And yet, 90% of data breaches come from phishing and social engineering attacks,[1] the kind that originate outside of a company's own perimeter. These could be hidden anywhere on the infinite web, and so solutions that focus on malware and threats to your own network are simply ineffectual.

This type of digital risk threatens your customers and your brand integrity, by fooling your consumers with websites that mimic your own. When successful, they trick users into providing personal and identifiable information that can be used for identity theft, fraud, or crime on the Dark Web. Reports of credential compromise **have risen by 280%, nearly tripling**, since 2016. This risk has a direct impact on a business's bottom line. Consumer phishing attacks **cost businesses more than $150 billion** in 2017, not just in stolen data and direct earnings, but in customer loyalty, brand damage and legal recourse.

Segasec has created the first all-in-one solution for these threats, a managed service that takes the whole problem off your hands, from initial intelligence to final response. Unlike its competitors, Segasec does not simply uncover threats, and neither does it focus on taking down a problem only once your users have brought it to your attention. It uncovers 99% of phishing schemes at the preparation stages, monitoring the threat while it evolves, protecting your customers before they are aware of a risk, and then removing it entirely to defend your brand without any harm being caused.

The Problem

Consumer phishing scams are increasingly common, with **83% of InfoSec respondents suffering from phishing attacks in 2018,** an increase from 76% in only one year, and growing.[2] In fact, in just Q3 of 2018, the amount of **unique phishing websites uncovered was 151,014**. While the online payment sector was the most targeted during this period, they were closely followed by SaaS companies and financial institutions, proving that no one is safe, employee training or security in-house simply cannot sufficiently reduce the threat, and consumer phishing scams can target any customer, anywhere.

On top of this, phishing schemes are becoming more complex. One example is the surge in phishing websites that utilize HTTPS encryption. Experts often suggest that users check the URL of the website they are visiting, to ensure that it has the HTTPS marker, and is secure. However, a secure website does not equal a safe one. As of Q3 of 2018, **nearly 50% of phishing sites now use encryption, making them seem safe** to an unsuspecting user. This is an increase of almost 900% since the end of 2016, and a 40% increase over Q2 of 2018.

In an attempt to manage this growing threat, competing digital risk solutions fall at a number of hurdles:

- **Intelligence alone:** Finding the threats is only stage one of a holistic solution. Many services provide you with some intelligence, and then leave you with a problem to solve, providing existing tools that are simply not on par with today's attackers. Your company will now need to fill the gaps in this intelligence, track and monitor the threat, and work out a way to mitigate it before your customers are affected.
- **Response-based:** In contrast, many solutions for managing phishing threats act only once an attack has been uncovered by your business, or more likely – uncovered by your customers. At this point, the damage has been done.
- **Domain/brand-related only:** While some phishing schemes will use a variant of your domain to launch a threat, others might try to avoid detection by relying on textual or visual similarities to your brand. Domain only is not enough to alert to content scraping or manipulation, as an attack can surface from a domain that is unrelated to your brand.
- **Complex integration:** In today's agile business landscape, solutions for evolving threats need to be easy to onboard and manage, with no lengthy installation or hardware to consider.

Solution

In response to these limitations, Segasec has created the strongest solution on the market, addressing consumer phishing scams head-on. With four unique elements, the entire problem is handled from end to end.

1. **Quadrillions of Scans 24/7**
   Machine Learning and Artificial Intelligence (patent pending) on data that shows historical attacks tells us where to look, **uncovering domain and sub-domain manipulation**. We shine a flashlight into the darkest corners of the internet, recognizing attack patterns and malicious behavior at the earliest possible stages, while the hackers are still preparing their threat. Segasec has **the largest capacity when it comes to scale**, covering billions of suspects and both known and unknown threats to your brand.
2. **Powerful Web Agent**
   Unlike the competition, Segasec does not stop at domain related threats. Our lightweight web agent (patent-pending) has no operational effect on your website, and **alerts us to content scraping or manipulation**, warning you of malicious behavior before it becomes a live attack. With our forensic approach, we have **vital data on the attackers** and where they are posting the stolen assets.

3. **Automated Block and Take-Down**
   Segasec monitors the threats at each stage, watching while they evolve from a suspect into a confirmed risk, taking the management off your hands for you. At this point, **we secure endpoints with a variety of defensive techniques**, actively protecting your customers from any risk. Our perfect track record has allowed us to build relationships with many hosting providers and registrars, providing **automated take-down of a malicious website**.

4. **Dynamic Deception**
   Smart deception technology is the 'next big thing' in incident response. Segasec allows you to **spread false data to the attackers**, from a global network of 20 million bots that mimic real victims. This dilutes the genuine information, ensuring that **criminals will not be able to use it in any way**. As each piece of data sent is marked, this enables faster incident response and identification of the attacker, leading them into traps without them suspecting they have been seen.

Conclusion

Phishing schemes are continually evolving, as attackers get smarter and launch more sophisticated phishing websites every year. Meanwhile, the cost to your business racks up, with brand damage resulting in a direct hit to your bottom line.

With zero onboarding, Segasec provides unbeatable intelligence that uncovers 99% of phishing schemes against your customers. Unlike any other, the solution covers both domain and non-domain threats. Scaling larger than any other, Segasec covers infinite detection variations 24/7, monitoring the evolution of billions of potential suspects in a proactive way.

When a risk is ready to launch, Segasec acts with lightning fast precision, securing endpoints, taking down the malicious website, and confusing and deceiving the attackers in order to make their data worthless. An entirely managed service, customer-facing online risk is no longer your problem.

Since its launch in 2017, Segasec has yet to uncover a single false positive.

References

Verizon Data Breach Investigations Report, 2017: Retrieved from,
https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report
Wombat Security State of the Phish Report, 2019: Retrieved from, https://www.wombatsecurity.com/state-of-the-phish

01 | https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report
02 | https://www.wombatsecurity.com/state-of-the-phish