# Disrupting the Phishing Supply Chain
## with Threat Intelligence

A Spire Research Report

Sponsored by Malcovery Security, LLC

# Executive Summary

It is obvious that the Internet is providing great value to all types of enterprises. It is a major contributor to overall economic benefits with its productivity enhancements. The Internet is estimated to contribute more than 3.4% to overall GDP - an amount greater than some major economic sectors.

Scalability is the vehicle that provides the benefits of the Internet. But scalability does not distinguish between good and bad. The same opportunities provided to the world's productivity-enhancing enterprises are also provided to attackers.

Email provides an excellent example of this dual-nature of scalability. Email use has undeniable benefits yet is dominated in volume by spam and malware-laden messages.

A more in-depth look at the phishing supply chain shows the economies of scale an attacker can gain. It mirrors the creation of websites and email messages, then leverages the most popular communication mechanism to distribute billions of messages every day. A single attacker can easily perpetrate an attack against millions of users, thousands of victim organizations, and hundreds of trusted brands.

Defenders today are stuck at the wrong end of the scalability equation. They have too many vulnerabilities and are attacked too many times to be 100% effective. A few email messages are bound to get through to their target. Ultimately, a defense that is strictly reactive to inbound emails cannot succeed.

Strategic defenders are leveraging their knowledge of the phishing supply chain to drive further towards the origin of any attack. They look to disrupt phishers at the website and email creation stage, prior to the execution of a campaign.

It takes a village with a strong collaborative defense to share intelligence in ways that leads to the strongest form of prevention - defeating the phishers themselves at a point before they can reap the benefits of scale.

## About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire's objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by Malcovery Security, LLC. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and risk management experience.

# DISRUPTING THE PHISHING SUPPLY CHAIN with Threat Intelligence

## Table of Contents

# Internet Value: The Benefits of Scale

The Internet has come a long way from the days www.whitehouse.gov served up pictures of the White House and www.whitehouse.com served up other sorts of pictures. Alongside its pictures of kittens and viral videos has come a profound change in the ways humans live their daily lives. From communications to commerce, through education and entertainment, and driving value within every industry, it is more difficult to come up with examples where it *hasn't* had an effect.

A recent McKinsey study of 13 countries estimated that the Internet accounts for 3.4% of their gross domestic product (GDP) on average. More importantly, its contribution to GDP growth averages 21% across those countries. If the Internet were a sector, it would be larger than the agriculture and energy sectors, and if it were a country it would have a larger GDP than Canada.[1]

The key characteristic of technology that drives the Internet's value is scalability - the opportunity for a system to replicate and grow its processes (outputs) at very low cost (inputs). Every benefit that is driven by technology is, at its core, a result of scalability.

# The Dark Underbelly: Scalability Risks

Scalability provides the functional value of the "technology tool." It drives up productivity, drives down costs, and provides new ways to think about business operations.

But scalability has no moral character. The attribute doesn't differentiate between conducting robotic telesurgery to save lives in developing countries and executing a salami attack to steal thousands of dollars by shaving fractions of pennies from millions of financial transactions.

Nowhere is this dual-nature of scalability more apparent than with email.

# The Two Faces of Email

We use email to communicate with individuals or groups of people in the office next door or on another continent. Its functional value - both from its breadth and depth - is on a level greater than any other form of communication. Whether it is communicating with doctor's about individual health, conducting daily business operations, or collaborating on a multi-million dollar project, email provides great benefits to people.

On the other hand, email provides the communication vehicle for various forms of fraud. Spam is the bane of many email recipients' existence as we are bombarded with unsolicited advice on losing weight, increasing energy, and living to be a hundred years old. We are constantly receiving fraudulent solicitations to purchase black-market medicine, fake designer goods, and other random paraphernalia. And, of course, we are regaled with opportunities of great fortune from deposed world

[1] Perspectives on Digital Business, McKinsey Center for Business Technology, McKinsey & Co.

leaders, princes, and other dignitaries with hidden financial reserves throughout the world. All to our detriment.

Perhaps the biggest challenge to enterprises in their pursuit of email-oriented value is distinguishing between legitimate messages with excellent benefits and those that contribute to fraudulent activity. We receive phishing emails that look exactly like our typical bank notices with account issues and contact requirements, with links to third party websites waiting to capture credential information and clean out bank accounts. We get malware-laden attachments to messages that appear to come from colleagues and containing pertinent information.

# The Phishing Supply Chain

Attackers can benefit significantly from scalability. Since they are constantly looking for ways to become more effective, they build out their own version of a supply chain. They amass the 'raw goods' of existing websites and phishing emails and 'manufacture' them into campaigns, distribute and process the phishing emails to their prospective 'customers' and ultimately lead some individuals to buy their products.

## Supply Chain Step-by-Step

A more detailed analysis of the phisher's supply chain shows those places where scale is used to their significant advantage. Consider the diagram in Exhibit 1.

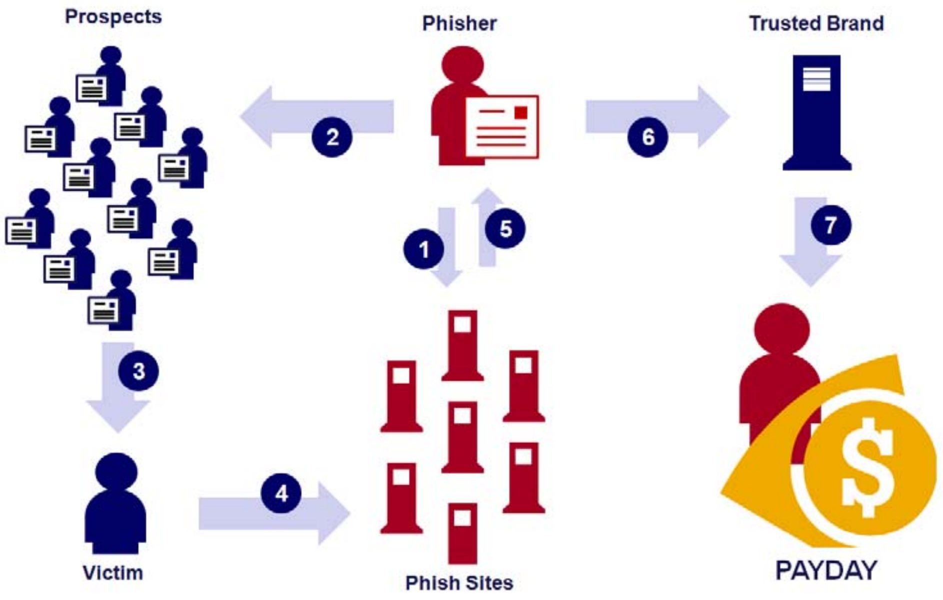

**Exhibit 1: The Phishing Supply Chain**

### 1. Phisher creates phishing websites that mimic trusted brand websites

As the attacker plans his attack, the first step is to create an applicable phishing site that will allow a target to input his credentials. The best way to create these sites is to scrape and copy the real site. Throughout the process, attackers find ways to scale by maintaining similar styles but swapping out logos, for example, or leveraging the same technical components. Attackers may also use this scalability by copying and creating many phishing sites, in preparation for the discovery and takedown of some portion of them.

### 2. Phisher creates an email template and generates the campaign mailing list

Leveraging the broadcast push capability of email, the phisher only needs to create one email in order to get billions of exact copies into the inboxes of people around the world. This capability is so obvious and powerful that it is ridiculous to even attempt a physical comparison incorporating letters being handwritten and mailed at similar volumes.

The universal availability of email addresses makes collecting them trivial - automated scripts can easily crawl websites and forums collecting publicly available email addresses; a loose configuration here or there can lead to leaked addresses; compromised email accounts lead to stolen address books. At this stage it doesn't matter, one must go to great lengths to protect an email address - often ultimately reducing its inherent value in the process.

### 3. Attacker sends billions of emails to millions of people - victims emerge

Phishers send out billions of emails every day. While some of the messages are obviously bogus, some will require more scrutiny. Attackers vary a few elements - just enough to evade most antispam solutions, and at this volume and speed many email messages will make it through the filters and reach their targets. Ultimately, discriminating users will ignore the malicious emails, but a few will be convinced to click and connect.

### 4. Victims connect to the phishing sites with their credentials

The phisher already has infrastructure in place to mimic the trusted brand. AT this stage, it is simply a matter of waiting for the victims. Because of the high benefits of technology, even being dormant is cost-effective - attackers can use the time to mount new campaigns with new phishing emails and websites.

### 5. The phisher collects credentials from the phishing websites

As the targets connect to phishing sites and present their credentials, the information can be stored locally for future disposition or it can be transmitted directly back to the attacker. This slow migration from a stored "batch" processing environment to real-time messaging highlights another benefit of scalability.

### 6. Phisher uses stolen credentials at the legitimate website

Finally, the phisher is faced with authenticating to a trusted brand site in the final phase of an attack campaign. At this point, the attacker must generally slow down. Since volume has finally been reduced through awareness and good defenses, and because defenses at trusted brands are heightened, the attacker needs to plot a careful path to complete the fraud.

### 7. Phisher reaps a payday

The phisher transfers funds or otherwise cashes in on his efforts.

## How Scalability Benefits the Attacker

The attacker supply chain reaps many benefits from the scalability of its systems.

Although the supply chain starts with its "raw goods" and ends with a "completed transaction," the process has been repeated so many times in previous campaigns that attackers can benefit from previous campaign experiences. Constantly building out their technical infrastructure, they can develop great efficiencies as they register domains, create websites, customize emails, and send them.

- High Volume - It is easy to generate hundreds of website and send billions of emails
- High Speed - by minimizing human interaction, campaigns can be executed within minutes and hours rather than weeks and months
- Low Cost - most importantly, the costs are minimal, if they even bother to pay them. Leveraging an existing, valuable mode of communication provides the conduit to targets.

# Disrupting the Phishing Supply Chain

The attackers have worked hard on their craft and have phishing and fraud down to a science. They are constantly developing new methods of attack that serve to reap current and future benefits. Most importantly - and concerning - is how well they have leveraged scalability to their significant advantage.

## Current State of Defense

In most enterprises, the first sign of a problem comes as an attack crosses the threshold, in real time, into the domain of the victim. That incursion, via email or web session or a handful of other communication mechanisms, is dealt with individually as it comes.

The defenders are constantly evaluating their enterprise attack surfaces. They perform vulnerability management scans identifying configuration weaknesses and known vulnerabilities throughout their environment. They review their custom developed software for software architecture weaknesses or security bugs. They monitor activity coming into the enterprise for signs of malicious behavior and that leaving the enterprise for signs of data leakage.

Today's IT environments are full of complexity and the chief information security officer must prioritize activities to manage risk. Therein lay the problem. There are so many options that prioritization can be difficult.

Within the email realm, emails are being delivered by the billions every day - about 100-200 messages to every user every day - and of those, upwards of 75-85% are fraudulent. Luckily, we have solutions constantly evaluating email for spam and fraud. And they can be very successful. However, even a small amount of success can lead to significant fraud against victims that is very lucrative for attackers.

The problem is simple - the attackers are winning the numbers game. Even with their low success rate, the defender is stretched thin across an entire enterprise attack surface and the solutions in place can filter out many fraudulent emails, but not all of them. There is no way to be 100% effective, and the fallout in terms of losses is still significant.

## Disrupting the Supply Chain

The technology risk management field is angling to change those attacker odds. Rather than playing a passive defensive role, the strategic thinker can plan defenses and quickly react to threat information. More importantly, the defender using threat intelligence can be proactive in disrupting the phishers supply chain.

In the military, commanders are constantly looking for force multipliers - ways to increase the effectiveness of their armies - to help them overpower an enemy to win battles and even wars. These force multipliers may relate to weaponry, tactics, and other methods that contribute to success.

The force multiplier for phishing is its economies of scale in the supply chain. Given this state, it only stands to reason that the way to defeat the phisher is to disrupt the supply chain closer to its starting point, rather than waiting for the attack cycle to begin.

## Intelligence-Led Options

Looking back at the phishing supply chain, the defender can develop strategies to use the attackers' scaling techniques against them.

### Disrupt the Phishing Websites

Because the websites follow templates, there are similar characteristics and attributes across websites and across phishing campaigns. Organizations can identify and takedown those websites so that any clickthroughs that occur will be unable to connect to the phishing site. This option will lead to the disruption of a phishing campaign.

### Disrupt the Email Creation

In a similar vein, finding patterns in emails can lead to a stronger understanding of the source of a phishing campaign. At this point, perhaps one or a few campaigns can be disrupted with the knowledge gained.

### Disrupt the Phisher

The weakest link in any phishing supply chain is the phisher himself. While he can easily create many campaigns that target many victims across many trusted brands due to economies of scale, the one thing he can't do is replicate himself. Catching the phisher leads to the best opportunity for turning the benefits of scalability back to the defender.

## Spire ViewPoint: It takes a Village... of Defenders

We know how these phishers operate. It is clear that they take full advantage of the Internet scalability as they attack their victims in volume. As we push further towards the origin of phishing - towards the phishers themselves - we can take back our email communication channel and fully realize its value.

The best option for defenders to beat the attackers at their game is to turn it against them. If we can get to them prior to the scaling points, we can make a significant dent in the volume of attacks.

The unique aspect of phishing as an attack vector is that two parties continue to be victimized - the users themselves and the trusted brands. It is crucial that these defenders join forces by sharing their threat intelligence to cross-fertilize defenses. Building out a village of defenders provides the best opportunity for success.

## Malcovery's Seven Phases of a Phishing Investigation

Malcovery leverages big data techniques to combat phishing and phishers. It has developed a "seven phase process" to evaluate all aspects of a set of campaigns and identify the phishers behind them.

Malcovery's Seven Phases of a Phishing Investigation:

1. Spam Analysis - The first step is to review the actual email messages for similarities - URLs, email addresses, etc.

2. Site Analysis - Second, Malcovery reviews individual websites to pull out elements that can be catalogued and associated with specific phishers.

3. Kit Analysis - Phishers often use the same "kit" of tools as they create new campaigns. Malcovery reviews the components of the tools and use and identifies similar pieces across campaigns.

4. Cluster Analysis - As the information develops, Malcovery evaluates the bigger picture, looking for campaign similarities and tying them back to individuals.

5. Log Analysis - as more information becomes available on the site itself, Malcovery factors in log information from all available sources, including hacked servers, victim log files, etc., to build out the complete picture.

6. Search Warrant Analysis - Malcovery assists with the search warrant process as investigations about individual phishers develop, preparing affidavits and, on law enforcement request, processing results data.

7. Open Source Intelligence - All pertinent information that is publicly available is gathered to provide support for investigations and further legal action.

The Malcovery approach provides a complete cross-campaign analytical process to drive investigations to the phishers themselves. This effectively eliminates the economies of scale that usually benefit the phishers.

## Contact Spire Security

To provide feedback on this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was commissioned by Malcovery Security, LLC. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.