



BCNET
CONNECT
HIGHER ED & RESEARCH TECH SUMMIT

GoPHiSH Yourself!!

Running a Self-Phishing Program

Max Opushnyev – UBC - Vulnerability Management Security Specialist

Matthew Ellis – UBC – Manager, Cybersecurity Incident Management



The Threat of Phishing

The Threat of Phishing

- Phishing activity has spiked since the start of COVID-19.
- Email-based attacks increased by 7.3% between May and Aug 2021 alone.
- Phishing accounts for around 90% of data breaches.
- Of all phishing attacks, 96% arrive by email.

The Threat of Phishing





BCNET
CONNECT

Why Self-Phishing

Why Self-Phishing

- Education
- Practice
- Just-in-Time Training
- Threat Insight
- Proactive Threat Management
- Postmortem Analysis



Where To Start!?

Gathering Requirements

- Target the user, not the technology
- Control access to the collected data
- Protect the end-user
- Ease of operation
- Ability to quickly adapt to current threats
- Maintain end-user experience
- Integrate with existing systems and workflows



Benefits Analysis

- **Paid Service**

- Customer support
- Existing infrastructure
- Selection of email templates

- **Open-Source**

- Ability to customize tools
- More agile system
- Better control of your data
- Price

Comparing Drawbacks

Paid Service

- Control of your data
- Ease of integration with other systems
- Price

Open-Source

- No Customer Support
- More time to deploy



Gophish

AN OPEN-SOURCE PHISHING TOOLKIT

Why GoPhish

- Designed for self-phishing drills, not PenTesting exercises
- Very easy to deploy and start phishing
- Well designed Graphical User Interface
- Potential to diversify test styles
- Python API client available



Building the system

User Experience

SA Service Now Sys Admin

goPhish script completed on [REDACTED] for INC [REDACTED]

RESULT: This ticket is not associated with self-phishing

- User receives identical experience as if it were a real phish
- Tickets get automatically cleaned up
- GoPhish gets updated automatically

SA Service Now Sys Admin

report sent to http [REDACTED] report?rid=thk0dk7

goPhish script completed on undefined

GoPhish Gotcha's

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Guide

API Documentation

Landing Pages

+ New Page

Show 10 entries

Search:

Name	Last Modified Date	
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>
		<div></div> <div></div> <div></div>

Showing 1 to 10 of 13 entries

Previous

1

2

Next

User content is not shared between users in the original implementation

GoPhish Gotcha's

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

Landing Pages

+ New Page

Show 10 entries

Search:

Name	Last Modified Date	Modified By	
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>
			<div></div> <div></div> <div></div>

Showing 1 to 9 of 9 entries

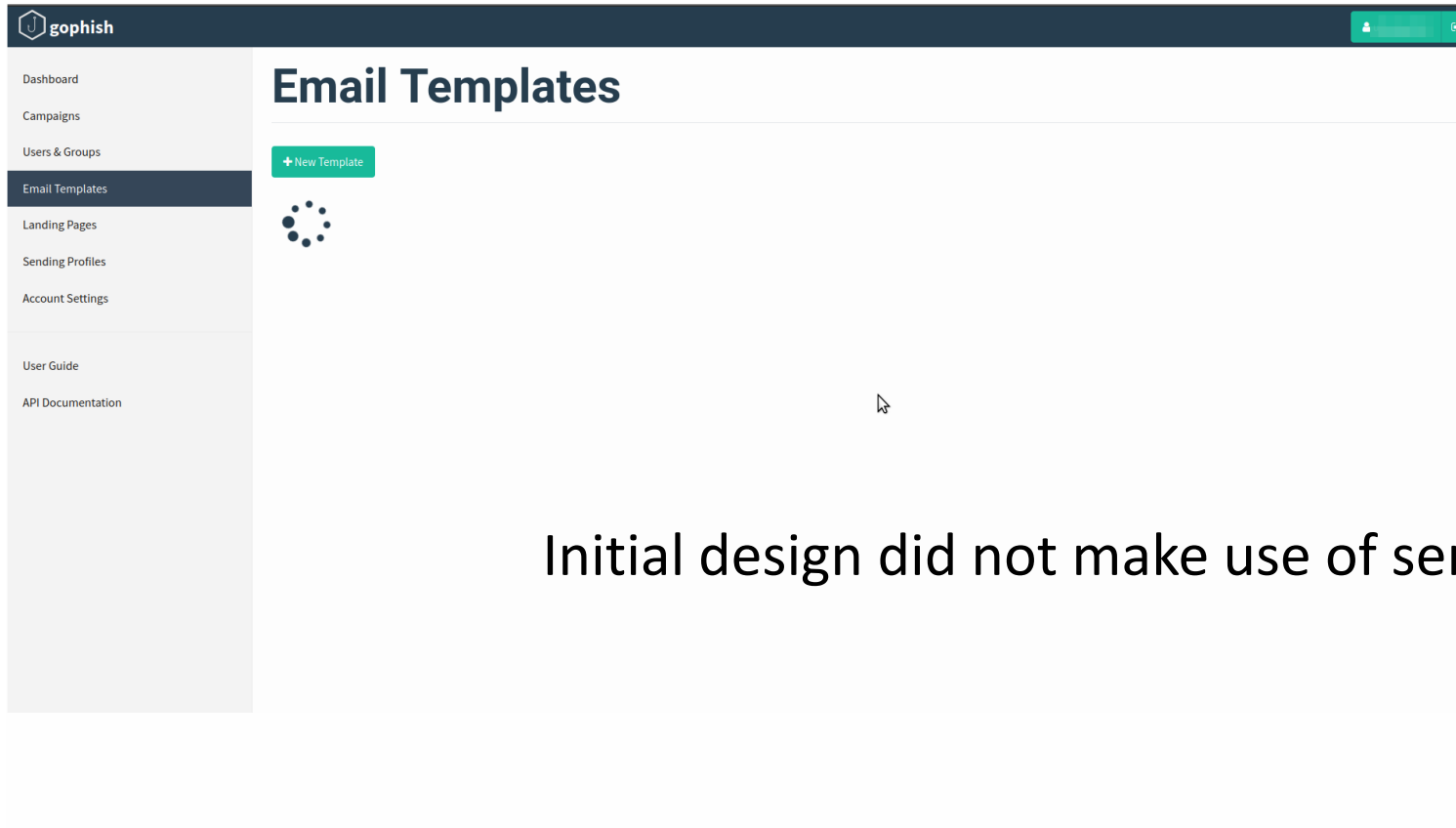
Previous

1

Next

Add content sharing and accounting features

GoPhish Gotcha's



Initial design did not make use of server-side pagination

GoPhish Gotcha's

```
ajax: function ( data, callback, settings ) {  
    api.campaigns.summary(data.length, data.start, 'active', getCampaignsSortOrder(data.order), data.search.value)  
    .done(function( data, textStatus, jqxhr ){  
        if(data.total == 0){  
            $("#campaignTable_wrapper").hide()  
            $("#emptyMessage").show()  
            $('#complete_button')[0].disabled = true;  
        }else{  
            $("#campaignTable_wrapper").show()  
            $("#campaignTable").show()  
            $("#emptyMessage").hide()  
            $('#complete_button')[0].disabled = false;  
        }  
        callback({  
            data: formatCampaignSummaryData(data),  
            recordsTotal: data.total,  
        })  
    })  
}
```

Add server-side pagination and server-side search capability

```
// GetCampaignSummaries gets the summary objects for all the campaigns  
// owned by the current user  
func GetCampaignSummaries(uid int64, limit int, offset int, complete_status string, sort string, search string) (CampaignSummaryOverview, []CampaignSummary, int64) {  
    overview := CampaignSummaryOverview{}  
    cs := []CampaignSummary{}  
    var total int64
```

GoPhish Gotcha's

New Group

Name:

+ Bulk Import Users

Download CSV Template

First Nam

Last Nam

Email

Position

+ Add

Show entries

Search:

First Name

Last Name

Email

Position

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Close

Save changes

Application lacks options for bulk target import
– CSV only

GoPhish Gotcha's


Not well suited for complex phishing schemes

New Landing Page

Name:

Import Site

HTML



```
<html><head>
  <title></title>
</head>
<body>
<h1>UBC PHISHING DRILL...</h1>

<form id="myForm" method="post" action="">
<p><input type="submit" style="visibility:hidden;" name="btnSignIn" value="Sign In">
...</p>
</body>
</html>
```

☒ Capture Submitted Data ?

☐ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: ?

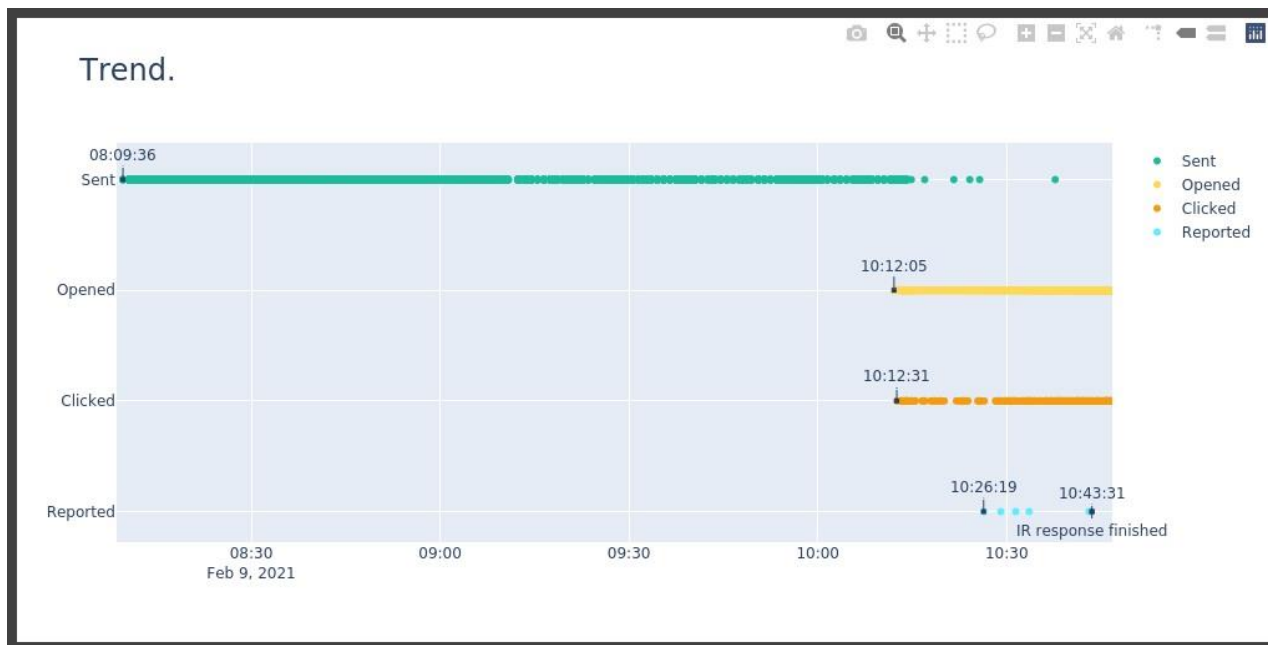
Cancel

Save Page



Discoveries

Timing is Everything



- **Sample size: ~25000**

Before email was first seen as reported:

People Clicked Link: 49
People Submitted Data: N/A

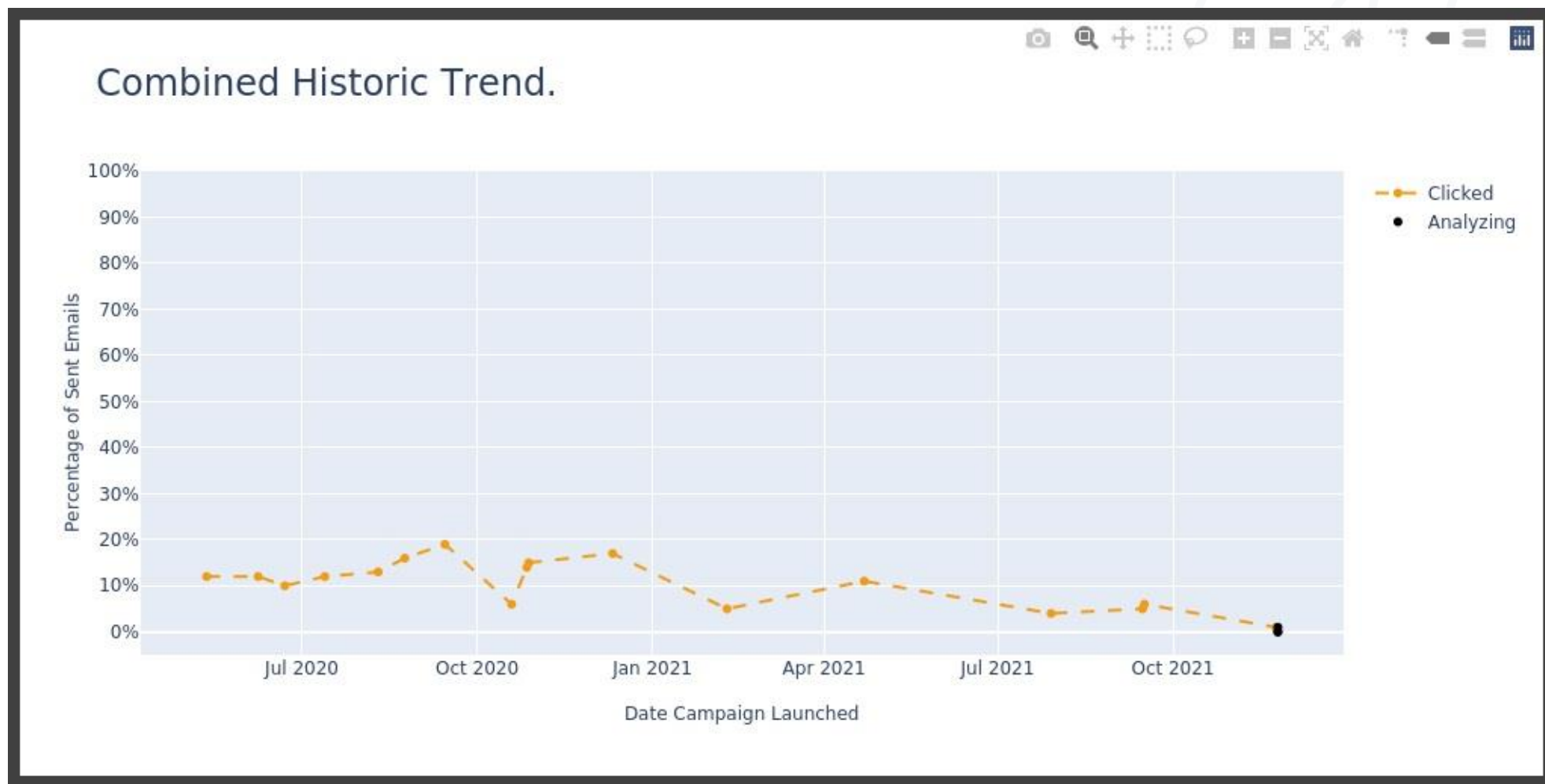
By the time IR Team responded:

Note: (Mean response time set to 0:17:12)

People Clicked Link: 186
People Submitted Data: N/A

- First click 25 seconds into the campaign
- Incident Response team sees first report after 14 minutes

Promising Results



Community Response

This is a good one., almost had me there for a second.

Cheers,

This was a good one guys! No clickly click though....

Hi there,

The wording is very close to actual [REDACTED] notification emails. I almost got tricked by this.

Thank you,

Hi – thank you for this and reminder – I was not concentrating and I got phished. V. much appreciate the training exercise.

Thank you and well done

Future Goals

- Migrate to a more robust reporting structure
- Implement missing pieces in GoPhish
- Analyze statistics for other interesting trends



BCNET
CONNECT

DEMO

Demo



BCNET
CONNECT

QUESTIONS?
COMMENTS?

References

<https://www.tessian.com/blog/phishing-statistics-2020/>

<https://getgophish.com/>