

# Splunking around the Phishmas Tree

SEC1494  
Technical Session



# Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at [www.investors.splunk.com](http://www.investors.splunk.com) or the SEC's website at [www.sec.gov](http://www.sec.gov). The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

---

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.



# Why am I here?



# Splunking around the Phishmas Tree

**Steve  
Behm**

Solutions Engineer | Security Researcher  
DomainTools  
[LinkedIn](#)



# How can this story help you?

**1**

Stay ahead of  
emerging threats


**2**

Reduce risk exposure


**3**

Improve team efficiency


# Learning Objectives



Pivot on data  
points to  
expand visibility



Create a search  
to find the  
threat actor's  
domains



Automate the  
search to run  
regularly

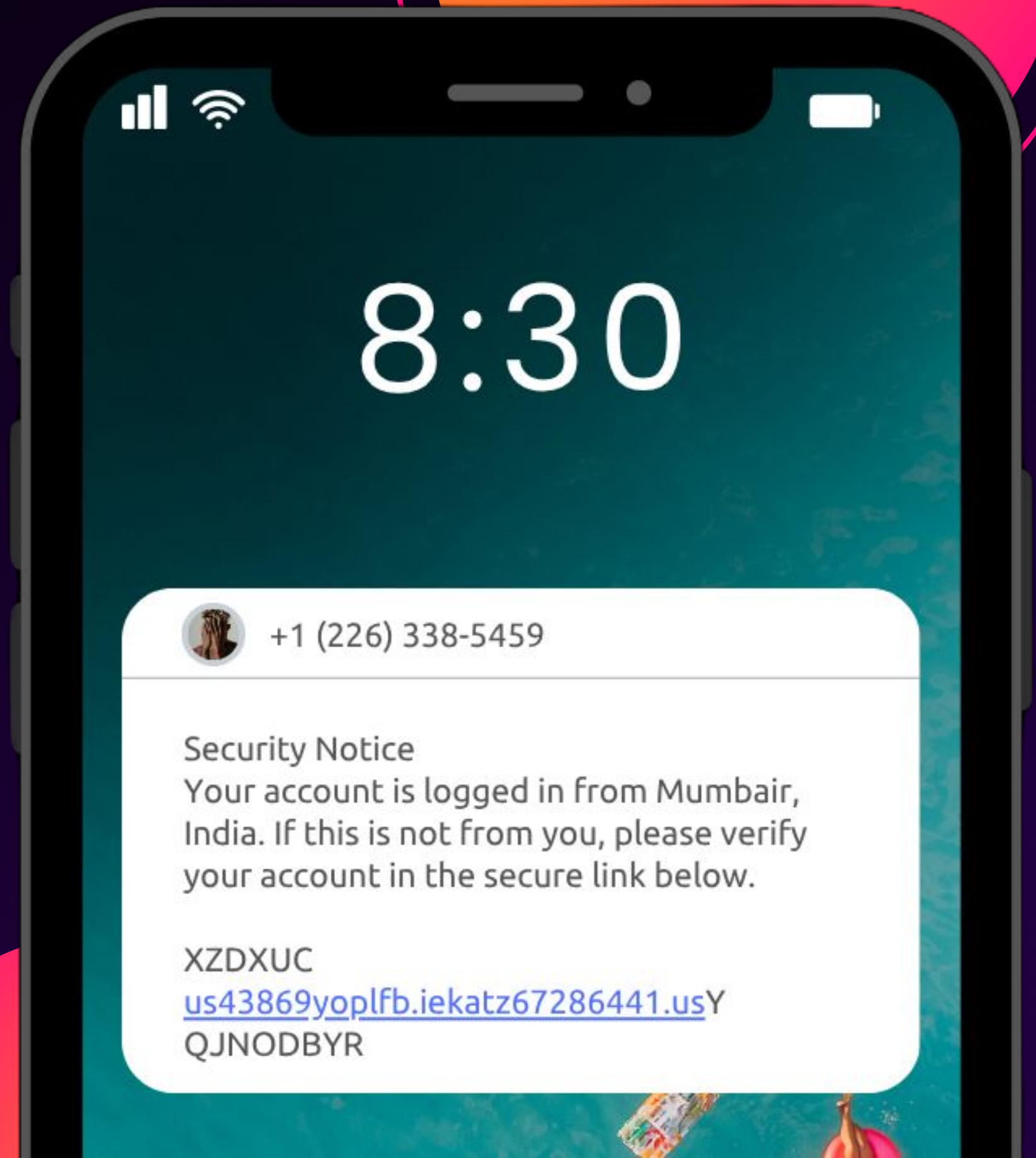


Explore last mile  
possibilities

# Attack Overview

# Initial Contact

- iPhone 14
- SW Ontario, CA area code
- Security notice for possible unexpected login attempt
- Subdomain
- Attributed to a TA named Chenlun/Sinkinto01





# Domain Profile

splunk>enterpriseAppsSPLUNK-FOR-INDUSTRIAL-IOT

Iris EnrichIris InvestigateFarsight DNSDBIris DetectEnrichment ExplorerWhois HistoryDomain RDAPDT SettingsSearchHelpFeedback

DomainToolsFor Splunk

Domain

iekatz67286441.us

SLD,TLD format. Press Return to search

Add To Monitoring List

Add To Allowlist

Open in Iris Investigate

Farsight pDNS Standard Search

Recent Events Search

Risk Score

100

Domain

iekatz67286441.us

Age (Days)

29 Days

Domain Status

Active

Threat Profile Scoring

Phishing

99

Malware

28

Spam

98

Proximity

100

Threat Profile Reason

phishing, spam

Threat Evidence

registrant, domain name, name server

charles SCHWAB

Log in to Schwab

Login ID

Password

Remember Login ID

Start Page

Accounts Summary

Log In

Forgot Login ID or Password?

New User?

English

- Domain is relatively young
- Shows high Domain Risk Score
- Charles Schwab login

# Domain Profile

Contact Information			
Admin Contact Information		Technical Contact Information	
Field ↕	Value ↕	Field ↕	Value ↕
email	domain1@csmslink.com ⚙	email	Number of Connected Domains: 75
name	mate kika ⚙	name	Pivot
org		org	
street	7622 17th Avenue ⚙	street	7622 17th Avenue ⚙
city	brooklyn ⚙	city	brooklyn ⚙
state	NY ⚙	state	NY ⚙
postal	11214 ⚙	postal	11214 ⚙
Billing Contact Information		Registrant Contact Information	
Field ↕	Value ↕	Field ↕	Value ↕
name		email	domain1@csmslink.com ⚙
org		name	mate kika ⚙
street		org	
city		street	7622 17th Avenue ⚙
state		city	brooklyn ⚙
postal		state	NY ⚙
country		postal	11214 ⚙

## Guided Pivots:

- Alias tied to 75 other domains
- Email address
- Street address

# DNS Activity

- Original subdomain seen 5/30/25
- Youngest subdomain seen 6/9/25
- Many other recently active subdomains

splunk>enterpriseAppsSPLUNK-FOR-INDUSTRIAL-IOT

Iris EnrichIris InvestigateFarsight DNSDBIris DetectEnrichment ExplorerWhois HistoryDomain RDAPDT SettingsSearchHelpFe

pDNS Standard Search

Farsight DNSDB Documentation

Time Range

Resource Record Type (RRType) ⓘ

OR Add Custom RRTYPE

IP, Domain Name, FQDN or Subnet ⓘ

All time

A

X

A

\*.iekatz67286441.us

Submit

Hide Filters

DNSDB RDATA Results

DNSDB RRSET Results

Time First ↕	Time Last ↕	RRName ↕	RRType ↕	bailiwick ↕	RData ↕
06/02/25 21:50:39	06/09/25 10:05:28	<a href="#">iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
06/06/25 01:19:40	06/08/25 09:52:19	<a href="#">us46871hhguyez.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
06/06/25 13:52:42	06/08/25 02:18:26	<a href="#">www.us46871hhguyez.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
06/05/25 04:09:02	06/05/25 04:09:02	<a href="#">us43869xrr.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
06/02/25 22:58:41	06/04/25 03:53:53	<a href="#">www.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
06/02/25 22:07:42	06/03/25 14:21:24	<a href="#">us46871rctfy.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">75.2.115.196</a>
05/30/25 10:22:41	06/02/25 11:01:49	<a href="#">iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">104.21.16.69</a> <a href="#">172.67.166.226</a>

05/30/25 18:51:01	05/30/25 18:51:01	<a href="#">us43869yoplfb.iekatz67286441.us.</a>	A	iekatz67286441.us.	<a href="#">104.21.16.69</a> <a href="#">172.67.166.226</a>
-------------------	-------------------	--	---	--------------------	--

# Related Domains



# Pivoting on alias

19 other domains with same alias seen in the last month

Two patterns emerge. One at apex-level and another at the subdomain level

Domain ↕	Risk Score ↕
ajvsgx72941760.us	100
ccdwet22559668.us	100
ccrizv77518814.us	100
eyjveg50956366.us	100
iciqfv25486908.us	100
iekatz67286441.us	100
ieymob32761302.us	100
irbsoo67934556.us	100
ivecqk13344821.us	100
kiuddi95581479.us	100
kwmqpk84060386.us	100
nkqogc11466552.us	100
nqgopi95040498.us	100
renivj45317060.us	100
utnazq92814937.us	100
wjtvcn35599165.us	100
wpmcal14629035.us	100

Original domain has 5 subdomains

rrname ↕
us43869xrr.iekatz67286441.us.
us43869fjjr.iekatz67286441.us.
us46871rctfy.iekatz67286441.us.
us43869bdgyfxl.iekatz67286441.us.
us46871hhguyez.iekatz67286441.us.

# DGA Pattern

# Example DGAs

randomstring20250718[.]com (date-based)

randomstring1752868754341[.]com (time-based)

abc12345[.]xyz (alphanumeric combo)

cityjulydish[.]net (word-based)

# pDNS Flexible Search

[Flexible Search Documentation](#)

Select a time range

Query ⓘ

Query type ⓘ

All time ▼

^us[[:digit:]]{5}.\.[[:alpha:]]{6}[[:dig

RRName (Left-Hand) ▼

rrname ⚡
us49951cxh.ajvs gx72941760.us.
us49951dvp.ajvs gx72941760.us.
us49951wzy.ajvs gx72941760.us.
us49951abej.ajvs gx72941760.us.
us49951dlqj.ajvs gx72941760.us.
us49951chfpf.ajvs gx72941760.us.
us49951wfeoq.ajvs gx72941760.us.
us49951lvmwrjm.ajvs gx72941760.us.
us43338cwa.ccdwet22559668.us.
us43338qkq.ccdwet22559668.us.

# Regex Query Results

274 unique subdomains

```
^us[[:digit:]]{5}.\.[[:alpha:]]{6}[[:digit:]]{8}\.us\.$
```



# Automating in Splunk

# Demo

# SPL Report

```
| dtdnsdbflex query_type=rrnames match_type=regex query="^us[[:digit:]]{5}.\.[[:alpha:]]{6}[[:digit:]]{8}\.us\.$"  
    time_last_after=`toEpoch("-24h@h")` time_first_before=`toEpoch("now")` rrtype="A"  
| eval domain=lower(rrname)  
| search NOT [ search index=chenlun_domains | stats values(domain) AS domain | table domain ]  
| collect index=chenlun_domains marker="new_dns_entry"  
| fields rrname rrtype
```

- Detect subdomains matching DGA pattern.
- Filter out domains already seen in past searches.
- Save the new subdomains for reference and analysis.
- Output the list of new, potentially malicious domains.

# Demo



# Scheduling the Report

- Set to run every 8hrs
- Priority can be raised depending on level of risk
- No schedule window for consistent execution

## Edit Schedule

Report	Chenlun_Domain_Discovery
Schedule Report	<input checked="" type="checkbox"/> <a href="#">Learn More</a>
Schedule	Run on Cron Schedule ▼
Cron Expression	0 */8 * * *
Time Range	Last 24 hours ►
Schedule Priority ?	Default ▼
Schedule Window ?	No window ▼

# Trigger Actions

# Demo

# Trigger Actions

Automate an action after your report runs to:

- Email your SOC team
- Execute a custom script
- Trigger a Webhook
- Create a Notable Event
- Send results to Splunk SOAR

## Trigger Actions

+ Add Actions ▼

Forwards search results from Splunk Enterprise to UBA



Send email

Send an email notification to specified recipients



Send to SOAR

Send search results to SOAR.



Send to Splunk Mobile

Send a notification to Splunk Mobile recipients



Stream Capture

Creates stream capture



Webhook

Generic HTTP POST to a specified URL



# Last Mile Options

# Email SOC Members

Send the latest results of the search via email:

- Can include CSV of results
- Can link to the reports or results for easy access
- Adjust priority easily

When triggered



Action icon Send email

To

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

[Show CC and BCC](#)

Priority

Normal ▼

Subject

Splunk Report: \$name\$

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

The scheduled report '\$name\$' has run.

Include



Link to Report



Link to Results



Search String



Inline

Table ▼



Attach CSV



Attach PDF



Allow Empty Attachment

Type

HTML & Plain Text

Plain Text

# Splunk SOAR

If you are a Splunk SOAR user,  
there are two handy options:

- Send to SOAR
- Run Playbook in SOAR

## Trigger Actions

+ Add Actions ▼

When triggered



Send to SOAR

SOAR  
Instance

Select...



Forward results to this Server/Asset.

Sensitivity



\*Sensitivity level for these events.

Severity



\*Severity of these events.

Label

Label for these events.

Worker Set

Select...



Select adaptive response relay worker set.  
Use "local" for non-adaptive response relay  
server.

Alert Action  
Account

Select...



Search produced no results.  
Select Account from SOAR Alert Action  
Configuration. Use blank for non-adaptive  
response relay server.

# External SOAR

If you don't use Splunk SOAR  
you can still use a trigger action  
to connect to your SOAR via:

- Webhook
- Custom Script

## Trigger Actions

+ Add Actions ▼

When triggered



Webhook

URL

https://your.server.com/foo/bar

Specified URL to send JSON payload via  
HTTP POST (ex.,  
https://your.server.com/api/v1/webhook).

[Learn More](#)

# Sinkhole via DNS

If you know the results of your report are bad news and want to take immediate action by sinkholing at the DNS level.

```
1 $TTL 2h
2 @          IN      SOA    localhost. root.localhost. (
3              2025063001 ; serial
4              1h        ; refresh
5              15m       ; retry
6              30d       ; expire
7              2h )      ; minimum TTL
8
9              IN      NS    localhost.
10
11 ; Block specific domains by returning NXDOMAIN
12 bad-domain.com.      CNAME  .
13 malicious-site.net.  CNAME  .
14
15 ; Redirect to a sinkhole IP
16 phishing-site.org.   A       192.0.2.1
17
18 ; Wildcard block all subdomains
19 *.tracking-domain.com. CNAME  .
20
```



# Review



# Why do this?

**1**

Stay ahead of  
emerging threats

**2**

Reduce risk exposure

**3**

Improve team efficiency

# Questions?



# Thank You!

**Steve  
Behm**

Solutions Engineer | Security Researcher  
DomainTools

[LinkedIn](#) | email: [sbehm@domaintools.com](mailto:sbehm@domaintools.com)

