USER GUIDE V1.0.0

SlashNext Threat Intelligence Integration Guide ThreatConnect TIP

TABLE OF CONTENTS

1	INTRODUCTION	2
2		2
	Requirements)
	App Installation)
	Attributes Configuration	3
	ThreatConnect Job Configuration5	;
3		}
4	LIST SPECIFIC IOCS	,
	Filter Feed Types	,
	Filter Attributes1	10

1 | INTRODUCTION

This document outlines the process to integrate SlashNext Threat Intelligence feeds into the ThreatConnect platform and provides details on how to efficiently use the integrated Threat Intelligence to get a specific list of Indicators of Compromise (IoCs).

SlashNext Threat Intelligence provides three types of feeds as per the corresponding type of IoCs which are listed below:

- 1. SlashNext Intel Phishing IPs as the name indicates contains IPv4 IoCs and are represented in ThreatConnect under Address type of Indicators.
- 2. SlashNext Intel Phishing FQDNs as the name indicates contains domain IoCs and are represented under **Host** type of Indicators.
- 3. SlashNext Intel Phishing Wildcard URLs as the name indicates contains wildcard URL IoCs and are also represented under URL type of Indicators.

All the IoCs within SlashNext threat feeds have four attributes which are also updated in the ThreatConnect Platform to facilitate the filtering of feed to get a list of more desired IoCs as per threat nature or as per usage which are as follows:

- 1. SlashNext Threat Type as the name indicates contains the broad threat nature posed by the loC.
- 2. SlashNext Threat Name as the name indicates contains the exact threat name posed by the IoC.
- 3. First Seen as the name indicates contains the timestamp when the IoC was first observed to be active threat.
- 4. Last Seen as the name indicates contains the timestamp when the IoC was last observed to be active threat.

2 | CONFIGURATION

The following section provides details on how to configure **SlashNext Phishing Threat Intelligence** app developed for the ThreatConnect Platform, as a job to download and ingest IoCs from SlashNext threat feeds into the platform.

2.1 | REQUIREMENT

The above requirements must be met to ingest SlashNext feeds into the ThreatConnect Platform:

- 1. Access to ThreatConnect instance
- 2. At least one ThreatConnect API user (See Creating User Accounts)
- 3. SlashNext API Key provisioned by SlashNext to authenticate requests to SlashNext cloud
- 4. SlashNext Phishing Threat Intelligence app installed in ThreatConnect Instance. (See App Installation section)
- 5. SlashNext Threat feed attributes properly configured in your ThreatConnect instance (See Attributes Configuration section)

2.2 | APP INSTALLATION

SlashNext Phishing Threat Intelligence app for ThreatConnect is available on Github at: Github Link. Download the app package with tcx extension and install it in your instance. To install the app in your ThreatConnect instance, refer to the ThreatConnect System Administration Guide (Install an App and Feed Deployer) for more information or contact your ThreatConnect Customer Success Engineer.

Also, download the **attributes.json** file in the Github repository which is required for attributes configuration step (See **Attributes Configuration**)

2.3 | ATTRIBUTES CONFIGURATION

Note

This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

As mentioned above, indicators ingested in the ThreatConnect Platform have four types of attributes to represent different characteristics of the threat posed by it. All of these attribute types must be available in your ThreatConnect instance to be able to display and update them accordingly. By default, in any ThreatConnect instance, only First Seen and Last Seen attribute types are present and the rest (**SlashNext Threat Type** and **SlashNext Threat Name**) have to be imported by the users themselves. In order to import these attributes in your instance, follow the steps below:

1. Login to your ThreatConnect instance and hover your mouse cursor over the gear icon on the top menu-bar. From the drop-down menu, Click on **Org Config** (highlighted by the red rectangle below) to go to your Organization Configuration page.

🔀 ThreatConnect			Dashboard 🗸 Posts Playbooks 🗸 Browse 🗸 Spaces 🗸 Create 🗸 Import	v 🕐 🏟 🌲 Q
MY INTEL SOURCES (1)		My Dashboard	My Pro	ile :
➢ 625499093915589-dot-ifile-do SlashNext 10-11-2019	incident		Org Set	tings
	Email		Org Cor	fig
FC06F0A7B0F833B04B880FB VXVault 10-08-2019	Adversary	SlashNext	Help	2
DE E1B9B89096AB6365E01ACD1 VXVault 10-08-2019	Signature Document		Logout	
Эт вк5740E40AD18E7A7DDB505 VXV/ault 10-08-2019	Campaign			

2. Click on Attribute Types tab on the Organization Config page, which is selected by default. Also, click on the Upload button and the Upload Attributes dialog box will appear.

🔀 ThreatConnect	Dashboard 🗸	Posts	Playbooks 🗸	Browse 🗸	Spaces 🗸	Create 🗸	Import 🗸 🥐 🕯	🛊 🏚 ९
SlashNext - Organization Config								
Attribute Types Attribute Validation Rules Default Attributes Indicator Exclusions Security Labels Deprecation Rules								
include System Types + NEW UPLOAD							Attribute Ty	e 🗸

3. On the **Upload Attributes** dialog box, click on + **SELECT FILE** button shown below and upload the file **attributes.json** (present in the Github Repository), that contains the configuration metadata of the required attributes.

Up	load Attributes	×
	+ SELECT FILE	
Up	load any text file in the format:	
	Name, Description, Error Message, Length, Applicable Types	
For	r example:	
	Penort ID My Penort ID Invalid report ID 50 Incident/HostIIIr/IAddress	
	Report Type, My Report Type, Invalid Report Type, 100, Incident Document	
No	Report Type,My Report Type,Invalid Report Type,100,Incident/IDocument ste that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	
No	Report Type,My Report Type,Invalid Report Type,100,Incident[Document te that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	ANCEL
No	Report Type,My Report Type,Invalid Report Type,100,Incident/Fostpon/Rodiess Report Type,My Report Type,Invalid Report Type,100,Incident/Document ote that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	ANCEL
No	Report Type,My Report Type,Invalid Report Type,100,Incident[Document stet that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	ANCEL
No	Report Type,My Report Type,Invalid Report Type,100,Incident[Document ste that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	ANCEL
No	Report Type,My Report Type,Invalid Report Type,100,Incident[Document ote that ',' is used as a column delimiter, but ' ' is used to deliminate applicable types.	ANCEL

4. The dialog box will then show you the attributes to be uploaded and ask for confirmation. Click on Save button to confirm.

Save attributes for 'SlashNext'?		
Name	Action	
SlashNext Threat Name	Create	
SlashNext Threat Type	Create	
	CAN	ICEL SAVE

5. Once the file is uploaded, the attributes along with their corresponding metadata will start appearing in your instance as shown below. The attributes configuration step is completed at this stage.

🔀 ThreatConnect			Dashboard 🗸 Po:	sts Playbooks 🗸 Browse 🗸 Spaces 🗸	Create 🗸 imp	iort 🗸 🕐 🏟	<u>ه</u> ۹
SlashNext - Organization	n Config						
Attribute Types Attribute Validation Rules E	Default Attributes Indicator Exclusions Securit	y Labels Deprecation Rules					
Include System Types + NEW	UPLOAD					Attribute Type	~
Name	Description	Max Length	Турез	Error Message		Options	
SlashNext Threat Name	The name of the Threat detected by SlashNext Threat Intelligence in this indicator.	100 characters	Address Host Url	Max length of SlashNext Threat Name attribute is 100 characters.	/ 🗇		
SlashNext Threat Type	The type of the Threat detected by SlashNext Threat Intelligence in this indicator.	100 characters	Address Host Url	Max length of SlashNext Threat Type attribute is 100 characters.	/ 🗇		

2.4 | THREATCONNECT JOB CONFIGURATION

Note

This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

The ThreatConnect Platform provides the ability for customers to schedule applications as jobs, specifically known as Job apps, that can be run at configured intervals. SlashNext, Inc has developed a Job app for ThreatConnect customers by the name of **SlashNext Phishing Threat Intelligence** that handles the complete process of downloading and ingesting the threat feed into the ThreatConnect Platform. In order to configure the SlashNext threat feed ingestion job app, follow the steps mentioned below:

1. Hover your mouse cursor over the gear icon present on the top menu-bar. From the drop-down menu, Click on **Org Settings** to go to your Organization Settings page.

🔀 ThreatConnect			Dashboard 🗸 Posts	Playbooks 🗸	Spaces 🗸	Create 🗸	Import 🗸 🥐 🌣	્ર વ
MY INTEL SOURCES (1)		My Dashboard					My Profile	÷
3 My Recent History	Intelligence Breakdown	Source Composition					Org Config	
Summary Owner Viewed	Threat						Help 🛛 🖓	
³ ≥ 625499093915589-dot-file-do SlashNext 10-11-2019	Incident Email						Logout	

2. Click on the **Apps** tab to configure **Jobs**. Also, click on the small + button (shown in the image below) to show the **Add Job** panel.

Dashboard 🗸	Posts	Playbooks 🗸	Browse 🗸	Spaces 🗸	Create 🗸	Import 🗸	?	<u>م</u> م
								1
Q Clear							G	o ±
	Dashboard 🗸	Dashboard V Posts	Dathbard V Posts Playbooks V	Daihbaard • Posts Playbooks • Browse •	Daibhbaard • Posts Playbooks • Browse • Spaces • Q	Daihbaard • Posts Playbooks • Browse • Spaces • Create •	Dathboard • Posts Playbooks • Browse • Spaces • Create • Import •	Dashboard v Posts Playbooks v Browse v Spaces v Create v Import v 🕐 🗱 .

3. In the Add Job panel, choose a suitable name for your Job in the Job Name option. Also select SlashNext Phishing Threat Intelligence from the Run Program drop-down list.

Add Job			
Program	2 Parameters	3 Schedule	Output
Job Name *			
SNX Job Test			
Run Program			
SlashNext Phishing Threat Intelligence			*
RSA NetWitness Packets and Logs Recorded Future Risk List			
SlashNext Phishing Threat Intelligence			
Symantec DeepSight			
TC - ACTRA v1.0			

Note

If you cannot see **SlashNext Phishing Threat Intelligence** in the drop-down list, please follow the **App Installation** step above or contact your Customer Success Engineer.

4. Click Next to configure the parameters of the Job app then select a suitable Api User configured in your instance. For the SlashNext API Key parameter, insert the 32 character API key provided to you by SlashNext or contact at support@slashnext.com if you do not have a valid API key. Under the Feed Type parameter, select the type of feeds from the multi-choice drop-down menu, that you want to ingest in your instance. Optionally, you can also set the Confidence Rating and Threat Rating parameter values for all the indicators ingested from SlashNext feeds other than the default values. Select the appropriate Log Level and finally, choose an owner for the ingested feed from the ThreatConnect Owner drop-down menu.

1 Program	2 Parameters	3 Schedule	4 Output
Api User *			
SNX App			*
SlashNext API key *			
Feed Type *			
IPs,Domains,Wildcard URLs			•
Confidence Rating *			
100			
100			
Threat Rating *			
5 (Critical)			*
Log Level *			
warning			*
ThreatConnect Owner *			

Click Next button to configure the schedule of running the job app, at which the feed will be ingested in your instance.
 Select the suitable period from the Schedule drop-down menu.

Note

SlashNext recommends that the job is executed after every two hour interval daily, as set in the figure below, for best syncing with the latest feed.

Add Jo	b					
	1 Program		2 Parameters	 3 Schedule	4 Output	
i) Schedule	neduled job timezo Daily 🔹	ne "Asia/Karachi"		 		
i scl Schedule	Daily -	ne "Asia/Karachi"		 		

6. Finally, click Next to setup the Output of the job app. Optionally, you can check the Enable Notifications checkbox to enable email notifications upon completion of the Job and provide the receiving Email Address. Under the Notify on Job Result option, check all the required scenarios at which email notifications are desired to be received. Also, click on Include Log Files checkbox under the Attachments option to receive job execution logs as attachments in the email notifications.

Add Job			
1 Program	2 Parameters	3 Schedule	4 Output
 Enable Notifications 			
Enable Notifications Email Address			
Enable Notifications Email Address your_email@yourcompany.com			
Enable Notifications Email Address your_email@yourcompany.com Notify on Job Result			
Enable Notifications Email Address your.email@yourcompany.com Notify on Job Result Success			

7. Click on **Save** button to save the job configuration. At this point, the job app is configured but is currently not active for execution. Click on the toggle button under **Active** as shown below to activate the job for running. The job configuration step is now complete.

🔀 ThreatConnect		Dashboard 🗸	Posts Playbooks 🗸 Browse 🗸 S	Spaces 🗸 Create 🗸 Import	v 🕐 🏟 🌲 Q
SlashNext - Organization Settings					
Membership Communities/Sources Invitations Variables Metrics Settings Email	Apps Styling				
Jobs					:
Search		Q, Clear			c o 1
Job Name	Start Time	Last Execution	Next Execution	Active	Options
SNX Job Test	N/A	N/A	10-22-2019 21:00 PKT	-	⊙ 🖌 i
					25 👻

3 | INDICATOR DEPRECATION CONFIGURATION

From time to time, SlashNext retires indicators in its threat feed that it estimates are, no longer malicious and pose any significant threat. These indicators previously ingested into the ThreatConnect Platform should also be deleted accordingly to avoid false-positives. ThreatConnect provides the ability for users to configure an indicator deprecation policy to allow ThreatConnect indicators to drop in confidence rating if their confidence rating is not being maintained and updated. Once the indicator rating reaches a minimum value (i.e. 0%), it can either be set to inactive or delete. To configure an indicator deprecation policy depending upon the type of your ThreatConnect instance, please refer to the detailed knowledge-base article from ThreatConnect: CONFIGURING INDICATOR CONFIDENCE DEPRECATION (See sections **Configuring Indicator Confidence Deprecation for an Organization** and **Configuring Indicator Confidence Deprecation for a Community or Source**)

The recommended indicator deprecation rule settings for SlashNext threat feed are as follows:

- Action at Minimum selected to be Delete so that indicators are deleted as soon as they reach minimum confidence
- **Percentage** checkbox checked which means that indicator confidence will be dropped as a percent of its previous value
- Confidence amount set to 100 so that 100% of an indicator's confidence is dropped
- Interval value set to 1 day which is the period after which the confidence will be dropped
- Recurring checkbox also selected so that deprecation is performed on a recurring basis

In simple words the recommended deprecation rule can be stated as, "After every day, drop the confidence of each indicator by 100% of its previous value and when any indicator's confidence reaches the minimum value, delete it from ThreatConnect".

4 | LIST SPECIFIC IOCS

ThreatConnect provides the ability to filter and display indicators from a number of sources. We can filter different types of indicators from the feed by applying a filter on either indicator tags or attributes.

4.1 | FILTER FEED TYPES

In order to filter indicators by their types, we can apply a filter on indicator tags. SlashNext threat feed indicators can have three types of tags:

FEED TYPE	INDICATORS TYPE	TAG
SlashNext Intel – Phishing IPs	Address	"Phishing-IPs"
SlashNext Intel – Phishing FQDNs	Host	"Phishing-FQDNs"
SlashNext Intel – Phishing Wildcard URLs	URL	"Phishing-Wildcard-URLs"

To filter all the indicators with one of these tags, follow the steps below:

1. Click on Browse from the top menu-bar to go to the ThreatConnect Browse page that displays indicators from all the sources.

🔀 ThreatC	onne	cť						Dashboard 🗸	Posts Playbooks 🗸	Browse 🗸 Spaces 🗸	Create 🗸 Impor	॰ 🕐 🏟 🌲 Q
MY INTEL SOURCES (1)	•	FILTERS -	Contains Text		Clear All							Advanced I
Indicators	(%)	Type 🗢	Summary ¢		Owner 🖨	Threat Rating 🖨	ThreatAssess 🗢	Obs 🗢	F/P ≎	Tags	Added \$	Modified \$
Address E-mail Address File	* * *	Address	192.185.93.105	=	SlashNext		356	-	-	Phishing IPs	10-31-2019	10-31-2019
Host URL	2	Address	142.93.59.165		SlashNext		503			Phishing IPs	10-31-2019	10-31-2019

 Click on FILTERS button shown in the figure below to expand the Filters panel. In the Tags textbox, write phishing and a drop-down auto completion list will appear with all SlashNext tags. Select the required tag according to the table given above. Let's filter all the indicators which have a tag of "Phishing-IPs" representing Phishing IPs in SlashNext feed.

🔀 ThreatCon	inect	ť		Dashboard 🗸 Posts	Playbooks 🗸 🛛 Browse	✓ Spaces ✓	Create 🗸	Import 🗸 🕐 🗄	💠 🌲 ९
MY INTEL SOURCES (1)		FILTERS A Contains Text	Q Clear All	1					Advanced :
Address E-mail Address) • •	Tags phishing ips ×		Attributes (up to 5) Select an attribute		Owner	Value		•
File Host URL		Created After	Created Before	No attributes selected					
ASN Bitcoin CB Alert		Indicator Status	Not Active						
CB Watchlist CIDR CVE	· · ·	Observed Since	TATALAN.						- 1
Filename Hashtag		Threat Rating							- 1
Mutex Registry Key testtest		Any							- 1
User Agent Groups	_	Observations Eales Pretitives							- 1
Campaign Document E-mail									APPLY

3. The Browse page will then start showing all the indicators with "Phishing-IPs" tag as shown in the figure below:

🔀 Threat	Conne	ect						Dashboard 🗸	Posts Playbooks 🗸	Browse 🗸 Spaces 🗸	🖌 Create 🗸	Import 🗸 🕐 🏟 🛕 🔍
MY INTEL SOURCES (1) 🔻	FILTERS -	Contains Text		Clear All							Advanced
Indicators		Tags: phishing i	ps 🗙									
Address E-mail Address	1	Tana A		Cummun A	Current &	Threat Daling	ThreatAnnan	Che e	F/D A	Tour	a ddad	1-10 of 436 Results
File Host	<i>.</i>	Address	185.178.211.162	Summary ÷	SlashNext	eeeee	503	-	F/F -	Phishing IPs	10-29-2019	10-29-2019
URL 2File Name ASN	~ ~ ~	Address	159.203.46.12		SlashNext		195	-	_	(Phishing IPs)	10-29-2019	10-29-2019
Bitcoin CB Alert	~	Address	167.99.65.140		SlashNext		503	-	-	Phishing IPs	10-29-2019	10-29-2019
CIDR CVE	ž	Address	106.15.32.77		SlashNext	****	503	-	-	Phishing IPs	10-29-2019	10-29-2019
Email Subject Filename	~	Address	23.23.46.58		SlashNext	*****	503	-	-	Phishing IPs	10-29-2019	10-29-2019
IPPort Mutex	2	Address	68.183.230.134		SlashNext		503	-	-	Phishing IPs	10-29-2019	10-29-2019
Registry Key testtest	~	Address	157.230.253.61		SlashNext	*****	833	-	-	Phishing IPs	10-29-2019	10-29-2019
Groups	-	Address	67.207.68.88		SlashNext	*****	333	-		Phishing IPs	10-29-2019	10-29-2019
Adversary Campaign		Address	186.75.130.46		SlashNext	*****	366	-		Phishing IPs	10-29-2019	10-29-2019
E-mail Event		Address	209.97.132.113		SlashNext	*****	281	-		Phishing IPs	10-29-2019	10-29-2019
Incident Intrusion Set							>					10 👻
Report Signature		EXPORT	DELETE									

4.2 | FILTER ATTRIBUTES

Each indicator in the SlashNext feeds has the following four attributes:

- 1. SlashNext Threat Type
- 2. SlashNext Threat Name
- 3. First Seen (First Seen time)
- 4. Last Seen (Last Seen time)

SlashNext Threat Type attribute has one of the following values:

- 1. Phishing & Social Engineering
- 2. Malware & Exploit
- 3. Callback/C2s

SlashNext Threat Name attribute can have the following values:

- 1. Fake Login Page
- 2. Scareware
- 3. Rogue Software
- 4. Internet Scam
- 5. Exploit:Win32/MSDocs
- 6. BadObject:Multi/RogueBinary
- 7. BadObject:Win32/InstallCore
- 8. Trojan:OSX/SearchJack
- 9. Trojan:Win32/Hijacker
- 10. Trojan:Multi/RogueExtension
- 11. Trojan:Win32/Spigot
- 12. BankingTrojan:Win32/Zbot

Indicators in the ingested SlashNext threat feed can be filtered by any specific value of the above indicators. Let us demonstrate how to filter all the indicators with **SlashNext Threat Type** of **Phishing & Social Engineering**:

1. Click on Browse from the top menu-bar to go to the ThreatConnect Browse page that displays indicators from all the sources.

🔀 ThreatC	onne	cť						Dashboard 🗸	Posts F	Playbooks 🗸	Browse 🗸	Spaces 🗸	Create 🗸	Import 🗸 🕐 🏟 🛕 🔍
MY INTEL SOURCES (1) 👻	FILTERS 🛩	Contains Text	٩,	Clear All									Advanced :
Indicators	di di													1-10 of 446 Results
Indicators	(1)	Type ≑				Threat Rating 🖨								
Address	 * 											_		
E-mail Address	 Image: A second s	Address	192.185.93.105	=	SlashNext	****	356	-		-	Phishing IP	s	10-31-2019	10-31-2019
File	 Image: A second s													
Host	 Image: A second s										(
URL	 Image: A second s	Address	142.93.59.165		SlashNext	***	503	-		-	Phishing IP	s	10-31-2019	10-31-2019

2. Click on **FILTERS** button shown in the figure below to expand the Filters panel. From the **Attributes** drop-down list select **SlashNext Threat Type** and it will appear below. Next to it, write the value in the **Value** textbox, against which you want to filter the indicators as shown below in the highlighted section:

Threat	Connec	:ť		Dashboard 🗸 Posts Playbooks 🗸	Browse 🗸 Spaces 🗸 Create 🗸 Import 🗸 🕐 🍁 🌲
MY INTEL SOURCES	(16) 👻	FILTERS A Contains Text	Clear All		Advance
ndicators	(*)	Tags		Attributes (up to 5)	
Address	~			Select an attribute	
E-mail Address	 Image: A second s				
ile	 Image: A second s	Created After	Created Before	Name	Owner Value
lost	 Image: A second s			SlashNext Threat Type	SlashNext Phishing & Social Engineering
RL	 Image: A second s				
ile Name	 Image: A set of the set of the	Indicators			
SN	 Image: A second s	mulcatora			
tcoin	× .	Indicator Status			
Alert	 Image: A set of the set of the	Lotion .	Nat Setion		
8 Watchlist	× .		1997 Partic		
DR	×	Observed Since			
/E	× .				
nail Subject	× .	Threat Ration			
ename	× .	> • Omene Unknown			
shtag	×.	000000			
Port	×.	Confidence Rating			
tex		> - Any			
gistry key					
strest		ThreatAssess Score			
ser agent					
ups		Observations			
lversary		False Positives			
mpaign		-			
cument					
mail					CLOSE

3. All the indicators in the threat feed with **SlashNext Threat Type** attribute equal to **Phishing and Social Engineering** will now appear on the Browse page:

🔀 ThreatC	onne	ect					Dashboard	✓ Posts Pla	aybooks 🗸 🛛 🖪	owse 🗸 Spaces 🗸 Create 🗸	Import 🗸 🥐	💠 🌲 ९
MY INTEL SOURCES (1) 👻	FILTERS -	Contains Text Q	Clear All				∑ http://ww	w34.safecu	reappleweb.brsignin.co	m/*	≡ ×
Indicators	(«	Attributes: Slas	hNext Threat Type = Phishing & Social Engineering 🛛 🗙					J status set by	•			
Address	×						т	ype	Owner	Added	Last Mod	ified
E-mail Address	× .	Turno 🔺	Summanı 🔺	Owner +	Threat Pation + Thre	uatheenee 🔺	Obe -	IRL	SlashNex	t 10-31-2019	10-31-20)19
File	~	Type 👻	Summary 🗸	Owner 🗸	Theat Nating 👻 Thin	au455655 🗸	005 4	hrant Dating		Confidence Dation		
Host	× .	URL	http://www34.safecureappleweb.brsignin.com/*					nieat Kating	inal	Confidence Rating		
URL	×.						•	중중중중중 Curr	ICal	Confirm	ned	
2File Name	Č.	URL	https://apple.com.info-location.todav/*	SlashNext		-	-					
Bitcoin	- U						1	ags				
CB Alert	÷.	LIDI	https://pakreizaue.com/t	Clockblost				Phishing Wildcard	URLs			
CB Watchlist	~	ORL	https://pakielicus.com/~	arabilivext	*****							
CIDR	× .		the second states	-				Atributes				
CVE	× .	URL	https://www.thenorth.info/*	SlashNext	****	-	- 4	Attributes	Local Mandaland			
Email Subject	× .							ype	Last Modified	value		
Filename	× .	URL	https://referenc3ser1vice-ca.com/*	SlashNext		-	- L	ast Seen	10-31-2019	2019-10-25T07:47:05Z		
Hashtag	×.						F	irst Seen	10-31-2019	2019-10-24T04·12·117		
IPPOR	Č.	URL	http://proxyspare4.open.tips/*	SlashNext	****	-		lashblash Theore	10 01 2010	Dhishing & Ossial Facilities		
Mutex Registry Key	Č.						T	lashNext Inreat	10-31-2019	Phisning & Social Engineer	ing	
testest	- U	URL	https://www.acceso24.banorte.com.bxi69.com/*	SlashNext		-		and the second sec				
User Agent							5	lashNext I hreat	10-31-2019	Fake Login Page		
		LIRI	http://annle.annleid.helpdask terms check inclinies.46chz8 dvpv	SlashNext		_		ame				
Groups		OIL	http://appreappretonelpueak.terma.creok.jpoiloiea=400020.uym	JIBBIIINEAL	00000			Al II Incidate				
Adversary								AL Insights				CAL
Campaign		UKL	nttps://login.septicmaxx.com/*	SlashNext	****	-	- [() Thursdown		An electric transmitter and an electric fee date		
Document								administrator	or learn more about	e whatytics cayer) is not enabled for this t upgrading.	account. To activate, p	rease contact your
E-mail		URL	https://d-jackets.net/*	SlashNext		-	-					
Event												
Intrusion Set						>	1	nvestigation Linl	(S			Open All 🗷
Report							-	Archive.org 🕑		DomainTools 🗷	Google 🗷	
Signature		EXPORT	DELETE					IRM Y-Force Excha	inge 12	NetCroft 12	StonBadware 17	
Task								IDWINT OFCE EXCITE	inge o	Notoran E	oropoutware is	