Test suspicious URL

#4286

Summary Report

July 28th 2017, 3:11:48 am

Generated by: Guy Rinat (guy@demisto.com)

Breach Type
Ransomware

Severity
Medium

Occurred
28th Jul 2017

Closure
28th Jul 2017

Time to resolve
9d 12h 37m

Reason for closing
Incident resolved

Earliest Evidence
28th Jul 2017

Most recent Evidence
28th Jul 2017

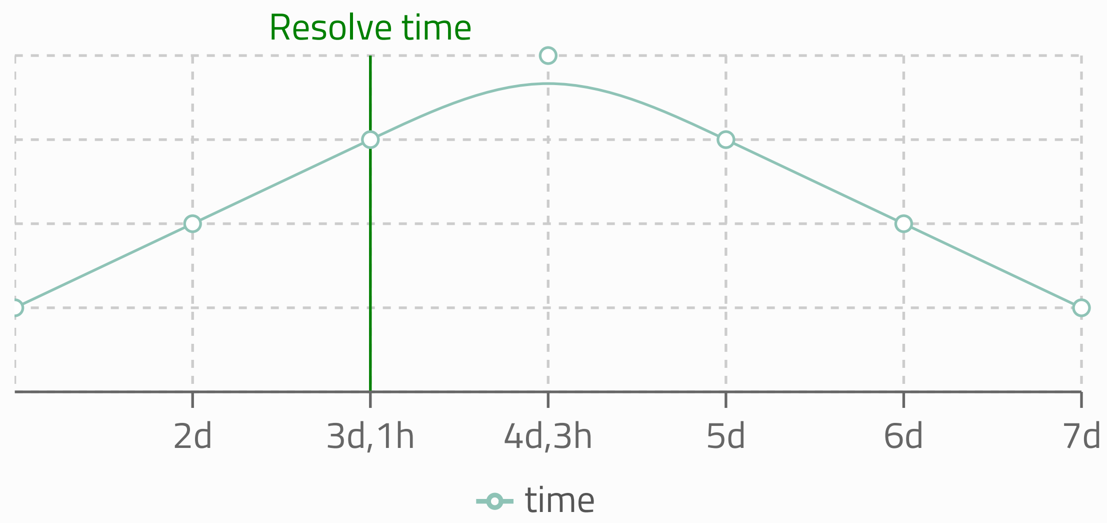
Owner

Doron Sharon (dorsha@demisto.com)

Playbook Used

Ransomware Playbook - Manual

Actual vs Mean time to resolve


Resolve time
2d
3d,1h
4d,3h
5d
6d
7d
time

Custom Data

Field	Data
boolean	true
date	Tue, 13 Dec 2016 15:35:29 IST
longtext	sdasdfjkasdlfj sdasdfjkasdlfj sdasdfjkasdlfj sdasdfjkasdlfj sdasdfjkasdlfj
multiselect	world, hello
shorttext	world, hello

Executive Summary

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Close Notes

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem

Ipsum.

Investigation Timeline

28 July 2017

Event	04 Dec 16, 2:00 pm	DBot

Another Close Reason !!!!!!!!!!!!!!!!!!!!!	Yeah!!!!
b	I think we solve this... lets pray...
Duration	6m40s

Task #7	04 Dec 16, 2:32 pm	ronda

Notify management chain #2
Notify appropriate people inside the organization.

```
console.log('hello')
```

Event	04 Dec 16, 3:11 pm	john

Field	Data
Another Close Reason	Yeah!!!
Incident Field #2	BONUS: $ 50 Macy’s Gift Card Opportunity sd asd ad
Some Incident Field	BONUS: $ 50 Macy’s Gift Card Opportunity

Event	04 Dec 16, 3:17 pm	john

```
▼ root: {} 1 item
  ▼ hello: {} 1 item
    ▼ how: {} 1 item
      are: you?
```

Evidence Timeline

Showing all Evidence as of start of investigation

Occurred	Description	Evidence ID
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1
8/1/16 02:25:13	Luluuu	#1

Detailed Evidence

#1 13 Sep 2016 12:15:13 PM

Computer requested IP address from the DHCP server; obtained a lease on 192.18.5.28

Occurred	Fetched	Marked as Evidence	By
13 Sep 2016 12:15:13 PM	13 Sep 2016 12:15:13 PM	13 Sep 2016 12:15:13 PM	dorsha

Field	Data
Phaze	Identification, Analysis
ACME code	ECajd-365-k33

Skipped Tasks

Generate IOC for malicious URL from SIEM Threat Feed #30 (skipped)

1. Get the list of flagged URLs/hashes from the Investigation Step
2. Check the URL against threat feed (virustotal, IBM Xforce).
3. Check your SIEM for threat feeds and see if there are IOC related to the URLs
4. Subscribe to the feed in SIEM. This will install the relevant IoCs into our SIEM automatically.
5. If none of the IoCs are on the TI feed, you need to generate IoCs manually in next step

Generate IOC for malicious URL manually #31 (skipped)

1. Go to the proxy logs again
2. Find 2-3 properties associated with the flagged URL, such as:
   The request is POST
   The User-Agent field is dodgy (Java, Python, IE6 etc.)
   URL contains more than 128 random characters
   URL contains .php
   URL contains lots of slashes (/)
   URL contains WordPress related things (wp-content)
   URL contains dodgy TLDs (for instance .tk, .ru)

3. Test your assumption on the proxy logs in the SIEM. Use your pattern and check how many false positives and true positives it produces.
4. If the pattern is good enough, append your results to the investigation.

Generate IOC from phishing emails #32 (skipped)

If you find in previous steps that source was phishing email -
1. Find all the URLs in the email and go through the URL IOC generation steps.

Team

	Name	Email	Phone Number
	John Barton	john@comany.com	+650-254-6491
	Shanny Semell	shanny@company.com	+650-254-6492
	Ronda Belisa	ronda@company.com	+650-254-6493
	Gregg Salkovitch	gregg@othercomapny.com	+650-254-6494
	Omer Lennon	omer@othercomapny.com	+650-254-6495