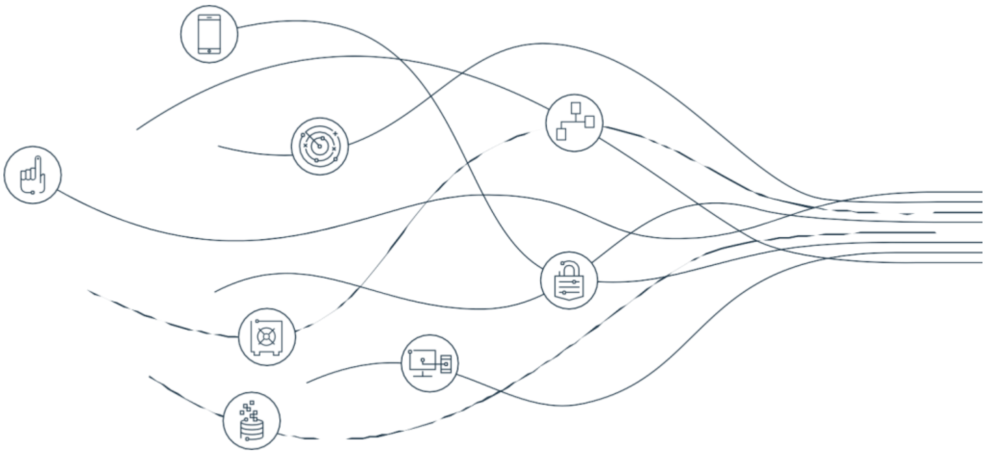
Monitoring Global Security Incidents

Lab 1

Version: 2021.02.08



IBM®

The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Contents

Preface

Overview

Over the course of this lab, we will dig deeper into cybercrimes, specifically WannaCry. Using interactive charts and free to use programs we will visualize all of the data collected from WannaCry around the world. We will then take a look at how we can keep tabs on security incidents happening around the world right now.

Estimated Time to Complete: 45 mins

Dependency

This lab leverages concepts imparted in the *Cybersecurity Landscape* lecture.

Objectives

There is one Milestones you must complete:

1. Monitor Global Attacks in Real Time with X-Force Exchange

Tools

X-Force Exchange

IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.

Flow

USER
X-Force Exchange

1. The User will access X-Force Exchange through their internet browser.

Milestone 1: X-Force Exchange

Milestone Overview

This lab requires the completion of one Milestones:

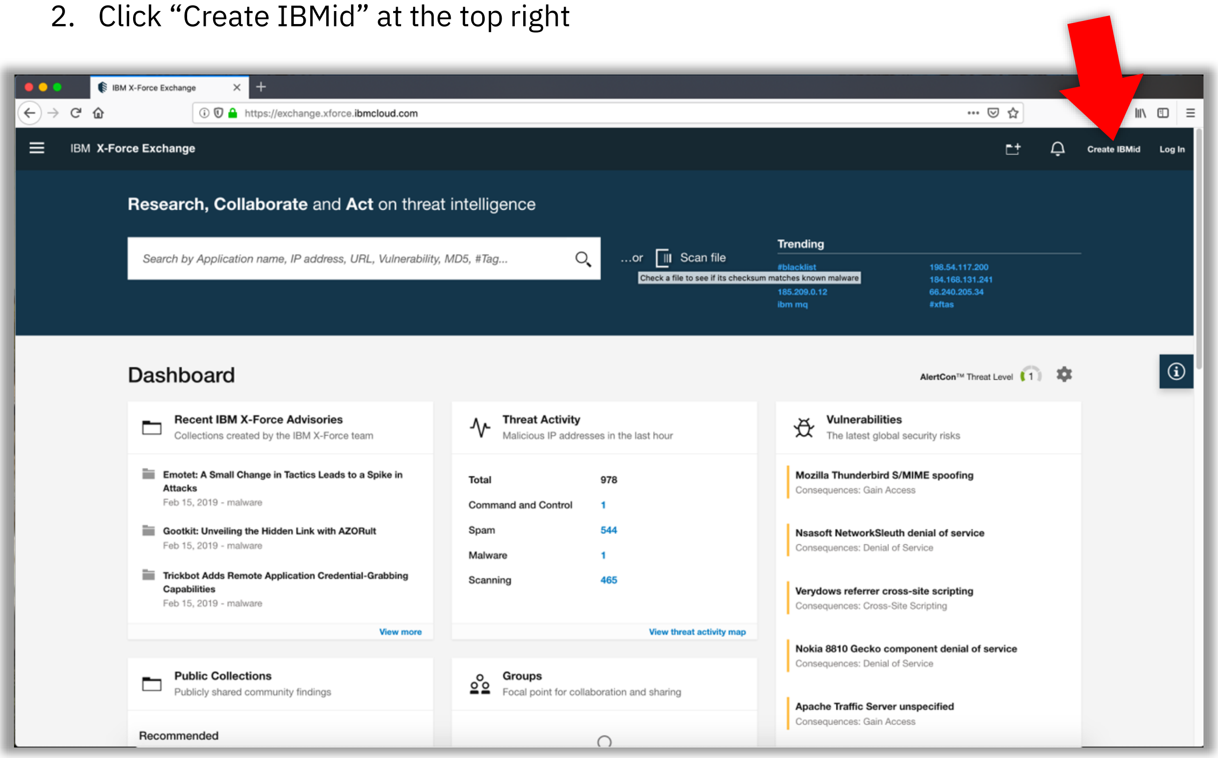
1. **X-Force Exchange**

In this Milestone, we will dive into the Cyber Landscape by using X-Force Exchange to witness attacks in real time and follow known vulnerabilities.

Create an Account

In order a better visual and more data on what happened during these attacks we are going to use IBM's X-Force Exchange. This is a completely free service, but you will need to create an account.

1. Navigate to https://exchange. xforce.ibmcloud.com/
2. Click "Create IBMid" at the top right


IBM X-Force Exchange
https://exchange.xforce.ibmcloud.com
IBM X-Force Exchange
Create IBMid
Log In
Research, Collaborate and Act on threat intelligence
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
...or Scan file
Check a file to see if its checksum matches known malware
Trending
#blacklist
185.209.0.12
ibm mq
198.54.117.200
184.168.131.241
66.240.205.34
#xftas
Dashboard
AlertCon™ Threat Level 1
Recent IBM X-Force Advisories
Collections created by the IBM X-Force team
Emotet: A Small Change in Tactics Leads to a Spike in Attacks
Feb 15, 2019 - malware
Gootkit: Unveiling the Hidden Link with AZORult
Feb 15, 2019 - malware
Trickbot Adds Remote Application Credential-Grabbing Capabilities
Feb 15, 2019 - malware
View more
Threat Activity
Malicious IP addresses in the last hour
View threat activity map
Vulnerabilities
The latest global security risks
Mozilla Thunderbird S/MIME spoofing
Consequences: Gain Access
Nsasoft NetworkSleuth denial of service
Consequences: Denial of Service
Verydows referrer cross-site scripting
Consequences: Cross-Site Scripting
Nokia 8810 Gecko component denial of service
Consequences: Denial of Service
Apache Traffic Server unspecified
Consequences: Gain Access
Public Collections
Publicly shared community findings
Recommended
Groups
Focal point for collaboration and sharing

Total	978
Command and Control	1
Spam	544
Malware	1
Scanning	465

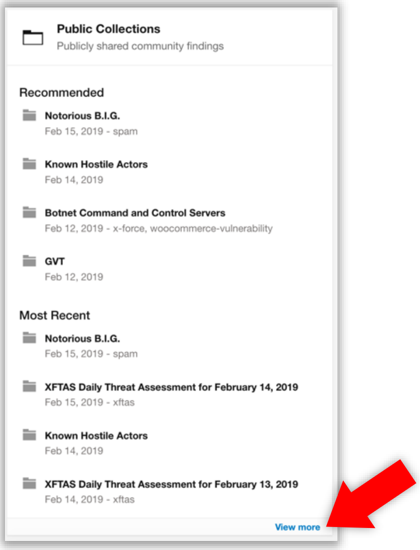
Figure 2-1 **X-Force Exchange - Dashboard**

3. Fill in the required information and continue.
4. Upon creation of your new account return to the homepage and login.

Deep Dive

Let’s continue our investigation of WannaCry.

1. Click “View More” at the bottom of *Public Collections.*



Public Collections
Publicly shared community findings

Recommended

Notorious B.I.G.
Feb 15, 2019 - spam

Known Hostile Actors
Feb 14, 2019

Botnet Command and Control Servers
Feb 12, 2019 - x-force, woocommerce-vulnerability

GVT
Feb 12, 2019

Most Recent

Notorious B.I.G.
Feb 15, 2019 - spam

XFTAS Daily Threat Assessment for February 14, 2019
Feb 15, 2019 - xftas

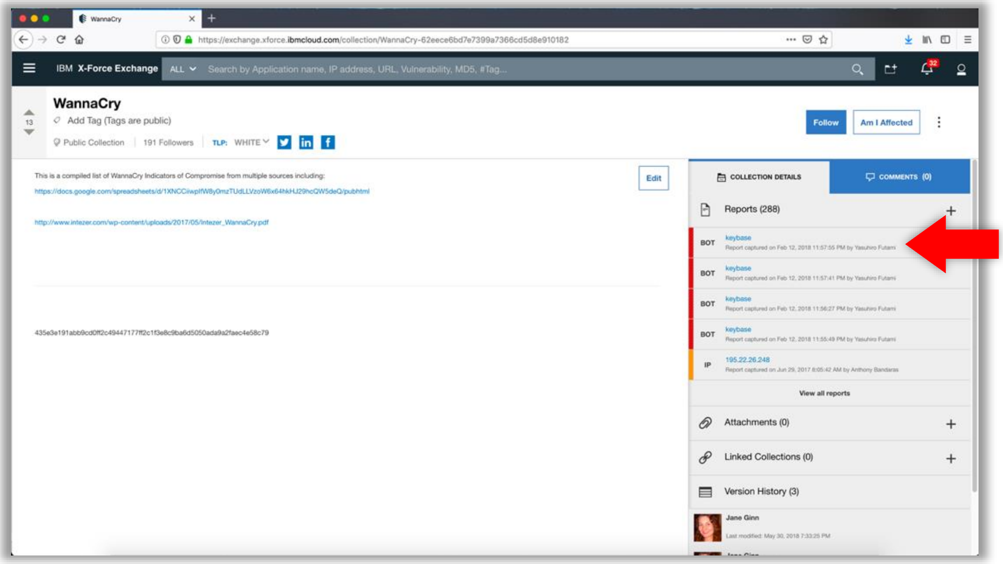
Known Hostile Actors
Feb 14, 2019

XFTAS Daily Threat Assessment for February 13, 2019
Feb 14, 2019 - xftas

Figure 2-2 **Public Collections**

2. In the search bar type in “WannaCry”.
3. Select the WannaCry collections folder.

The Collections folder contains over 280 reports on the activities of the WannaCry ransomware. What we are interested in for this lab is the most recent Botnet report. This will give an excellent visual on where the ransomware was last active.



WannaCry
https://exchange.xforce.ibmcloud.com/collection/WannaCry-62eece6bd7e7399a7366cd5d8e910182
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
32
13
Follow
Am I Affected
Edit
COLLECTION DETAILS
COMMENTS (0)

WannaCry
Add Tag (Tags are public)
Public Collection | 191 Followers | TLP: WHITE

This is a compiled list of WannaCry Indicators of Compromise from multiple sources including:
https://docs.google.com/spreadsheets/d/1XNCCiwplfW8y0mzTUdLLVzoW6x64hkHJ29hcQW5deQ/pubhtml

http://www.intezer.com/wp-content/uploads/2017/05/Intezer_WannaCry.pdf

435e3e191abb9cd0ff2c49447177ff2c1f3e8c9ba6d5050ada9a2faec4e58c79

Reports (288)

BOT keybase
Report captured on Feb 12, 2018 11:57:55 PM by Yasuhiro Futami

BOT keybase
Report captured on Feb 12, 2018 11:57:41 PM by Yasuhiro Futami

BOT keybase
Report captured on Feb 12, 2018 11:56:27 PM by Yasuhiro Futami

BOT keybase
Report captured on Feb 12, 2018 11:55:49 PM by Yasuhiro Futami

IP 195.22.26.248
Report captured on Jun 29, 2017 6:05:42 AM by Anthony Bandaras

View all reports

Attachments (0)

Linked Collections (0)

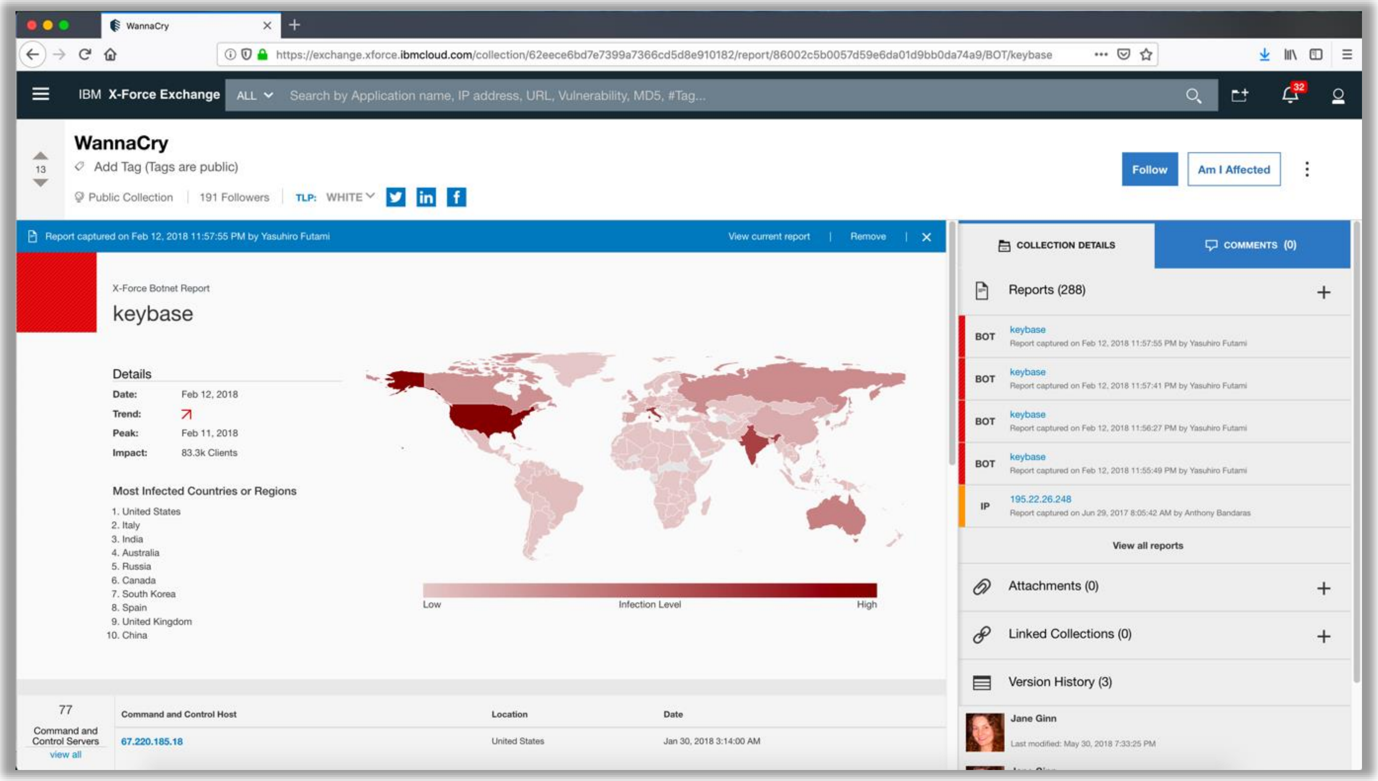
Version History (3)

Jane Ginn
Last modified: May 30, 2018 7:33:25 PM

Figure 2-3 **WannaCry Folder**

4. Click the most recent Botnet report on the right side.

The Botnet report (*Figure 2-4*) contains when the attack was last captured, if the attack has more or less botnet clients than previous attacks, when the attack was at its strongest, how many people were affected, as well as a list of the countries affected and a map which displays the severity in each country.


WannaCry
https://exchange.xforce.ibmcloud.com/collection/62eece6bd7e7399a7366cd5d8e910182/report/86002c5b0057d59e6da01d9bb0da74a9/BOT/keybase
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
32
13
Add Tag (Tags are public)
Public Collection
191 Followers
TLP: WHITE
Follow
Am I Affected
View current report
Remove
COLLECTION DETAILS
COMMENTS (0)
Low
Infection Level
High

WannaCry

Report captured on Feb 12, 2018 11:57:55 PM by Yasuhiro Futami

X-Force Botnet Report

keybase

Details

Date:	Feb 12, 2018
Trend:	↗
Peak:	Feb 11, 2018
Impact:	83.3k Clients

Most Infected Countries or Regions

1. United States
2. Italy
3. India
4. Australia
5. Russia
6. Canada
7. South Korea
8. Spain
9. United Kingdom
10. China

77 Command and Control Servers view all

Command and Control Host	Location	Date
67.220.185.18	United States	Jan 30, 2018 3:14:00 AM

Reports (288)

BOT	keybase Report captured on Feb 12, 2018 11:57:55 PM by Yasuhiro Futami
BOT	keybase Report captured on Feb 12, 2018 11:57:41 PM by Yasuhiro Futami
BOT	keybase Report captured on Feb 12, 2018 11:56:27 PM by Yasuhiro Futami
BOT	keybase Report captured on Feb 12, 2018 11:55:49 PM by Yasuhiro Futami
IP	195.22.26.248 Report captured on Jun 29, 2017 8:05:42 AM by Anthony Bandaras

View all reports

Attachments (0)

Linked Collections (0)

Version History (3)

Jane Ginn

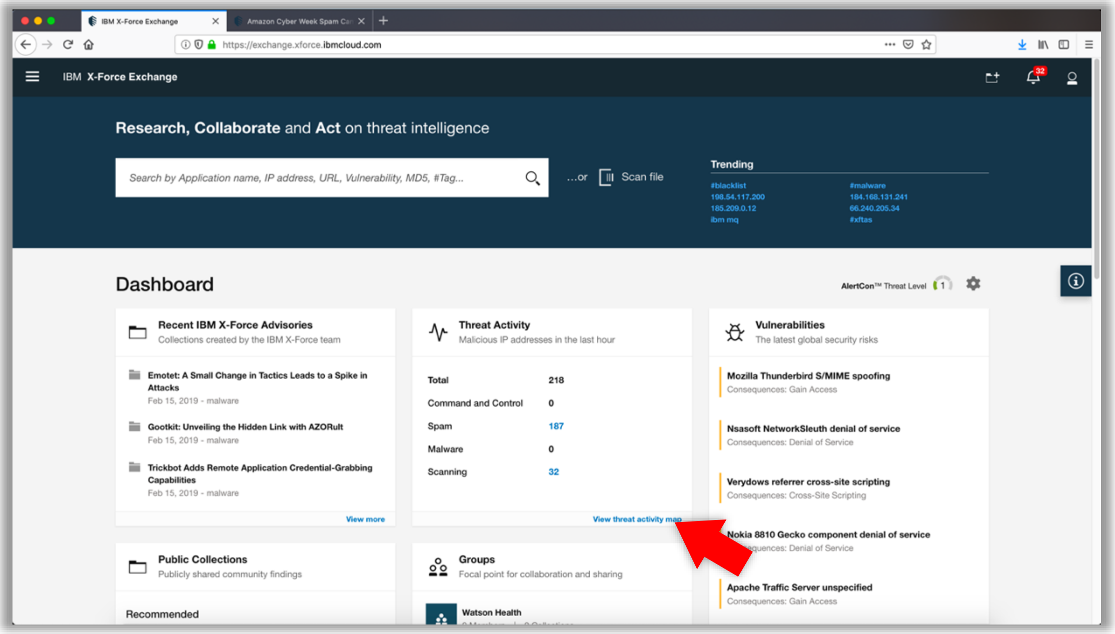
Last modified: May 30, 2018 7:33:25 PM

Figure 2-4 **WannaCry Botnet Report**

Taking a Look at Threats Today

X-Force Exchange offers a plethora of information on past cyberattacks, but what we need to know, as security experts, is “What is plaguing the world right now?” X-Force Exchange can help us out with this as well.

1. Navigate back to the X-Force homepage.
2. Click on “View threat activity map” under *Threat Activity.*


IBM X-Force Exchange
Amazon Cyber Week Spam Ca
https://exchange.xforce.ibmcloud.com
IBM X-Force Exchange
32
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
...or
Scan file
View more
View threat activity map

Research, Collaborate and **Act** on threat intelligence

Trending

#blacklist	#malware
198.54.117.200	184.168.131.241
185.209.0.12	66.240.205.34
ibm mq	#xftas

Dashboard

AlertCon™ Threat Level 1

Recent IBM X-Force Advisories
Collections created by the IBM X-Force team

- **Emotet: A Small Change in Tactics Leads to a Spike in Attacks**
  Feb 15, 2019 - malware
- **Gootkit: Unveiling the Hidden Link with AZORult**
  Feb 15, 2019 - malware
- **Trickbot Adds Remote Application Credential-Grabbing Capabilities**
  Feb 15, 2019 - malware

Threat Activity
Malicious IP addresses in the last hour

Total	218
Command and Control	0
Spam	187
Malware	0
Scanning	32

Vulnerabilities
The latest global security risks

- **Mozilla Thunderbird S/MIME spoofing**
  Consequences: Gain Access
- **Nsasoft NetworkSleuth denial of service**
  Consequences: Denial of Service
- **Verydows referrer cross-site scripting**
  Consequences: Cross-Site Scripting
- **Nokia 8810 Gecko component denial of service**
  Consequences: Denial of Service
- **Apache Traffic Server unspecified**
  Consequences: Gain Access

Public Collections
Publicly shared community findings

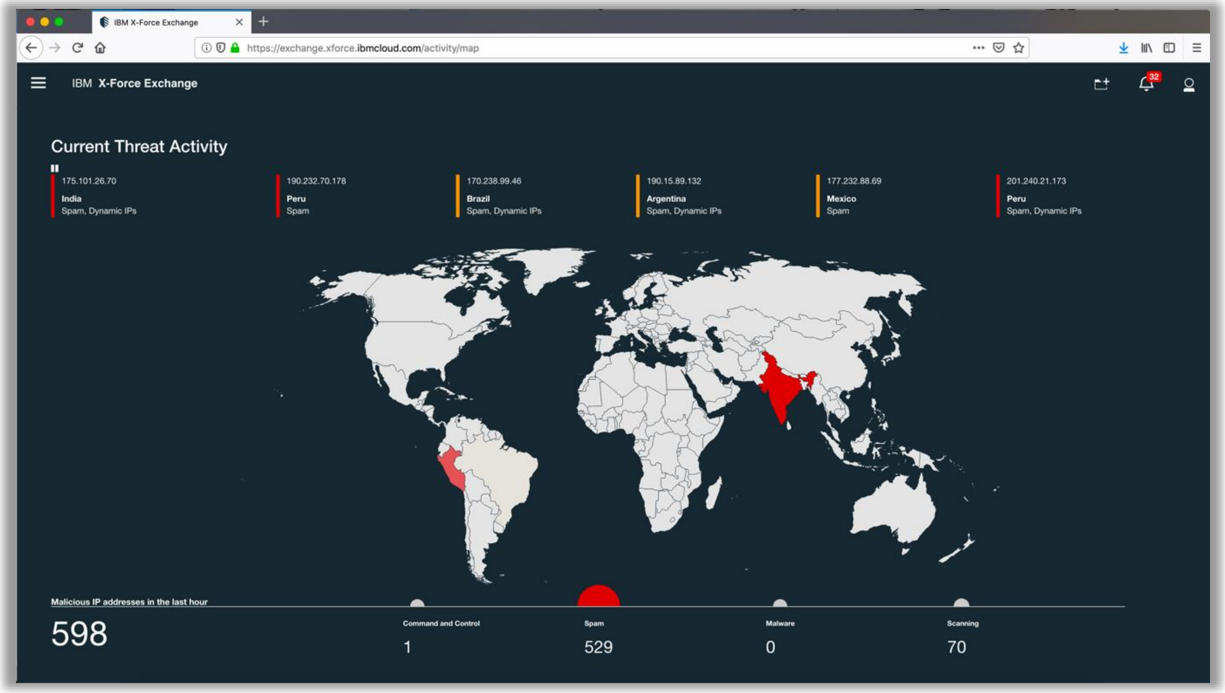
Recommended

Groups
Focal point for collaboration and sharing

Watson Health

Figure 2-5 **X-Force Exchange - Dashboard**

X-Force Exchange scans the globe and sends reports of current threat activity in real time (*Figure 2-6*). Scrolling over a report will halt more reports coming in and highlight the country affected by that attack.



Current Threat Activity

175.101.26.70
India
Spam, Dynamic IPs

190.232.70.178
Peru
Spam

170.238.99.46
Brazil
Spam, Dynamic IPs

190.15.89.132
Argentina
Spam, Dynamic IPs

177.232.88.69
Mexico
Spam

201.240.21.173
Peru
Spam, Dynamic IPs

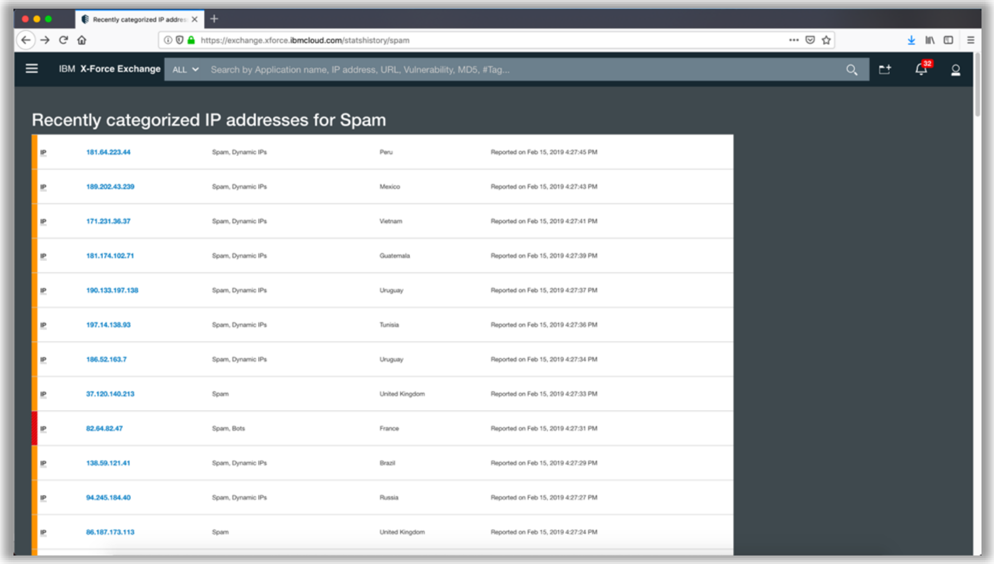
Malicious IP addresses in the last hour

598

Command and Control	Spam	Malware	Scanning
1	529	0	70

Figure 2-6 Current Threat Activity

3. Click on "Spam" at the bottom of the page.
4. A list of categorized IP addresses will appear that have all been connected to recent spam attacks.



Recently categorized IP addre...
https://exchange.xforce.ibmcloud.com/statshistory/spam
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
32

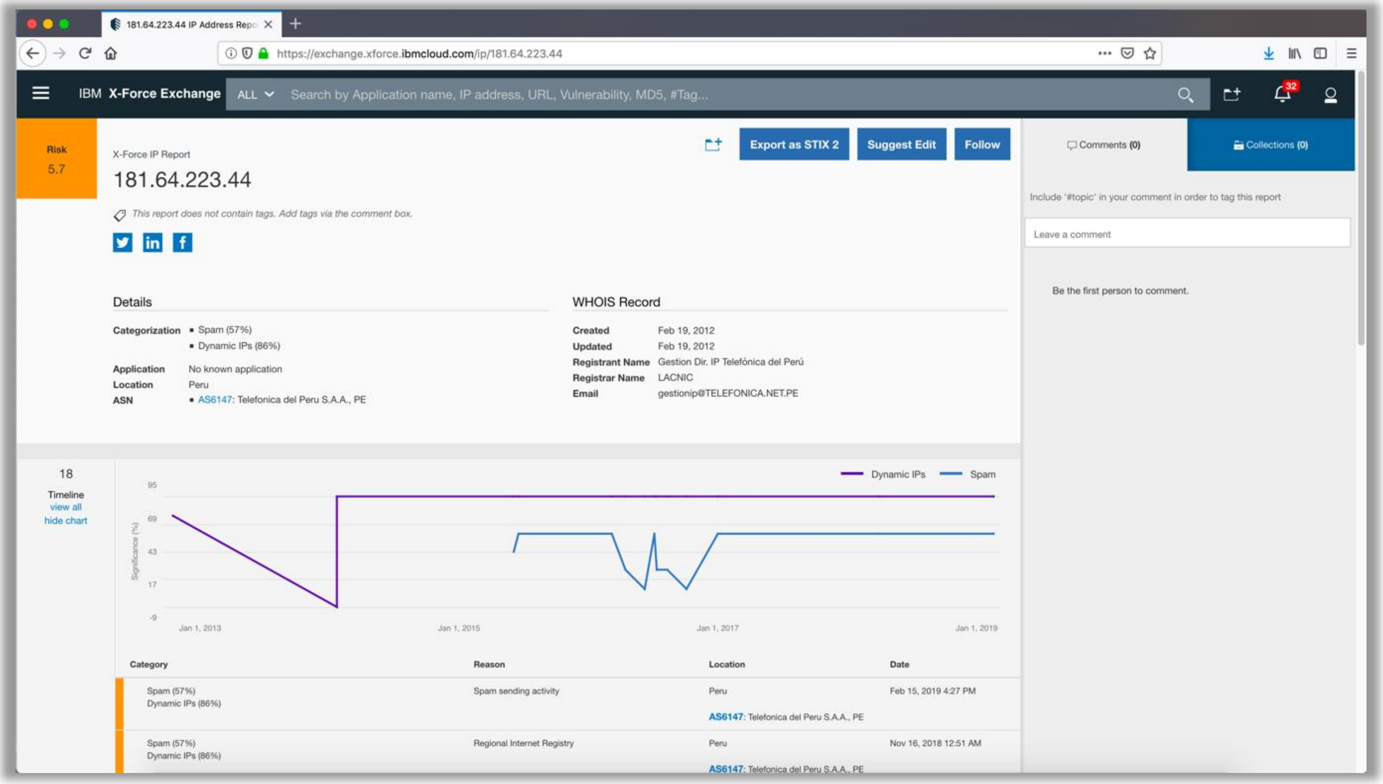
Recently categorized IP addresses for Spam

IP	181.64.223.44	Spam, Dynamic IPs	Peru	Reported on Feb 15, 2019 4:27:45 PM
IP	189.202.43.239	Spam, Dynamic IPs	Mexico	Reported on Feb 15, 2019 4:27:43 PM
IP	171.231.36.37	Spam, Dynamic IPs	Vietnam	Reported on Feb 15, 2019 4:27:41 PM
IP	181.174.102.71	Spam, Dynamic IPs	Guatemala	Reported on Feb 15, 2019 4:27:39 PM
IP	190.133.197.138	Spam, Dynamic IPs	Uruguay	Reported on Feb 15, 2019 4:27:37 PM
IP	197.14.138.93	Spam, Dynamic IPs	Tunisia	Reported on Feb 15, 2019 4:27:36 PM
IP	186.52.163.7	Spam, Dynamic IPs	Uruguay	Reported on Feb 15, 2019 4:27:34 PM
IP	37.120.140.213	Spam	United Kingdom	Reported on Feb 15, 2019 4:27:33 PM
IP	82.64.82.47	Spam, Bots	France	Reported on Feb 15, 2019 4:27:31 PM
IP	138.59.121.41	Spam, Dynamic IPs	Brazil	Reported on Feb 15, 2019 4:27:29 PM
IP	94.245.184.40	Spam, Dynamic IPs	Russia	Reported on Feb 15, 2019 4:27:27 PM
IP	86.187.173.113	Spam	United Kingdom	Reported on Feb 15, 2019 4:27:24 PM

Figure 2-7 IP addresses for Spam

5. Click on one of the captured IP Addresses.

This Threat Report (*Figure 2-8*) contains a risk score, from 1-10, that gives a general impression of how credible the threat from this IP is. It also provides us with further data that can be used by a team of security analysts to help pinpoint where the attack took place, who was attacked, and not only the date, but the exact timeframe of when the attack was active.



Risk
5.7

X-Force IP Report

181.64.223.44

This report does not contain tags. Add tags via the comment box.

Include '#topic' in your comment in order to tag this report

Be the first person to comment.

Details

Categorization	▪ Spam (57%) ▪ Dynamic IPs (86%)
Application	No known application
Location	Peru
ASN	▪ AS6147: Telefonica del Peru S.A.A., PE

WHOIS Record

Created	Feb 19, 2012
Updated	Feb 19, 2012
Registrant Name	Gestion Dir. IP Telefónica del Perú
Registrar Name	LACNIC
Email	gestionip@TELEFONICA.NET.PE

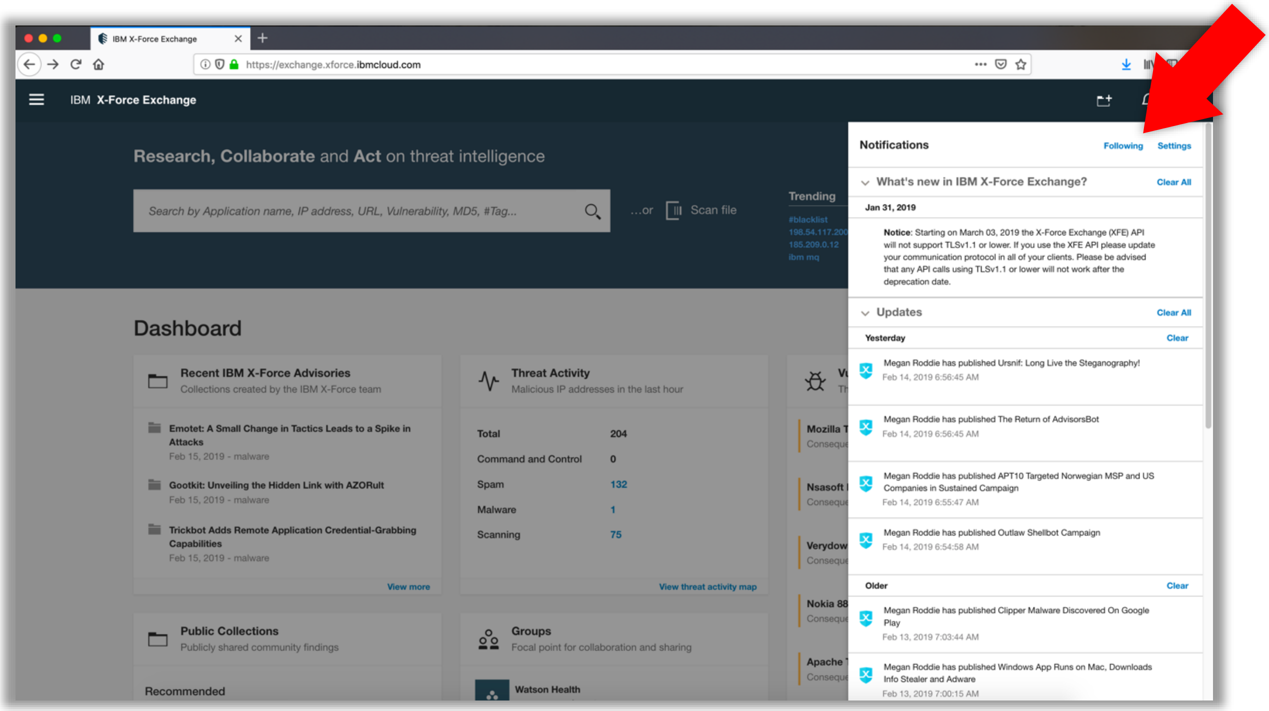
18
Timeline

Category	Reason	Location	Date
Spam (57%) Dynamic IPs (86%)	Spam sending activity	Peru **AS6147**: Telefonica del Peru S.A.A., PE	Feb 15, 2019 4:27 PM
Spam (57%) Dynamic IPs (86%)	Regional Internet Registry	Peru **AS6147**: Telefonica del Peru S.A.A., PE	Nov 16, 2018 12:51 AM

Figure 2-8 **Captured IP Address Threat Report**

6. Follow the incident by clicking the “Follow” button at the top right of the report. This will send you a notification if there are any new instances or changes to the report, so you do not need to keep checking in manually.

7. Return to the homepage, open up the notification tab on the top right, and click on the “following” link to see a list of what you are currently following.


IBM X-Force Exchange
https://exchange.xforce.ibmcloud.com
IBM X-Force Exchange
Research, Collaborate and Act on threat intelligence
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
...or
Scan file
Trending
#blacklist
198.54.117.200
185.209.0.12
ibm mq
Dashboard
Recent IBM X-Force Advisories
Collections created by the IBM X-Force team
View more
Threat Activity
Malicious IP addresses in the last hour
View threat activity map
Public Collections
Publicly shared community findings
Recommended
Groups
Focal point for collaboration and sharing
Watson Health
Mozilla T
Nsasoft
Verydow
Nokia 88
Apache
Notifications
Following
Settings
Clear All
Clear

Emotet: A Small Change in Tactics Leads to a Spike in Attacks
Feb 15, 2019 - malware

Gootkit: Unveiling the Hidden Link with AZORult
Feb 15, 2019 - malware

Trickbot Adds Remote Application Credential-Grabbing Capabilities
Feb 15, 2019 - malware

Total	204
Command and Control	0
Spam	132
Malware	1
Scanning	75

What's new in IBM X-Force Exchange?

Jan 31, 2019

Notice: Starting on March 03, 2019 the X-Force Exchange (XFE) API will not support TLSv1.1 or lower. If you use the XFE API please update your communication protocol in all of your clients. Please be advised that any API calls using TLSv1.1 or lower will not work after the deprecation date.

Updates

Yesterday

Megan Roddie has published Ursnif: Long Live the Steganography!
Feb 14, 2019 6:56:45 AM

Megan Roddie has published The Return of AdvisorsBot
Feb 14, 2019 6:56:45 AM

Megan Roddie has published APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign
Feb 14, 2019 6:55:47 AM

Megan Roddie has published Outlaw Shellbot Campaign
Feb 14, 2019 6:54:58 AM

Older

Megan Roddie has published Clipper Malware Discovered On Google Play
Feb 13, 2019 7:03:44 AM

Megan Roddie has published Windows App Runs on Mac, Downloads Info Stealer and Adware
Feb 13, 2019 7:00:15 AM

Figure 2-9 **X-Force Exchange - Notifications**

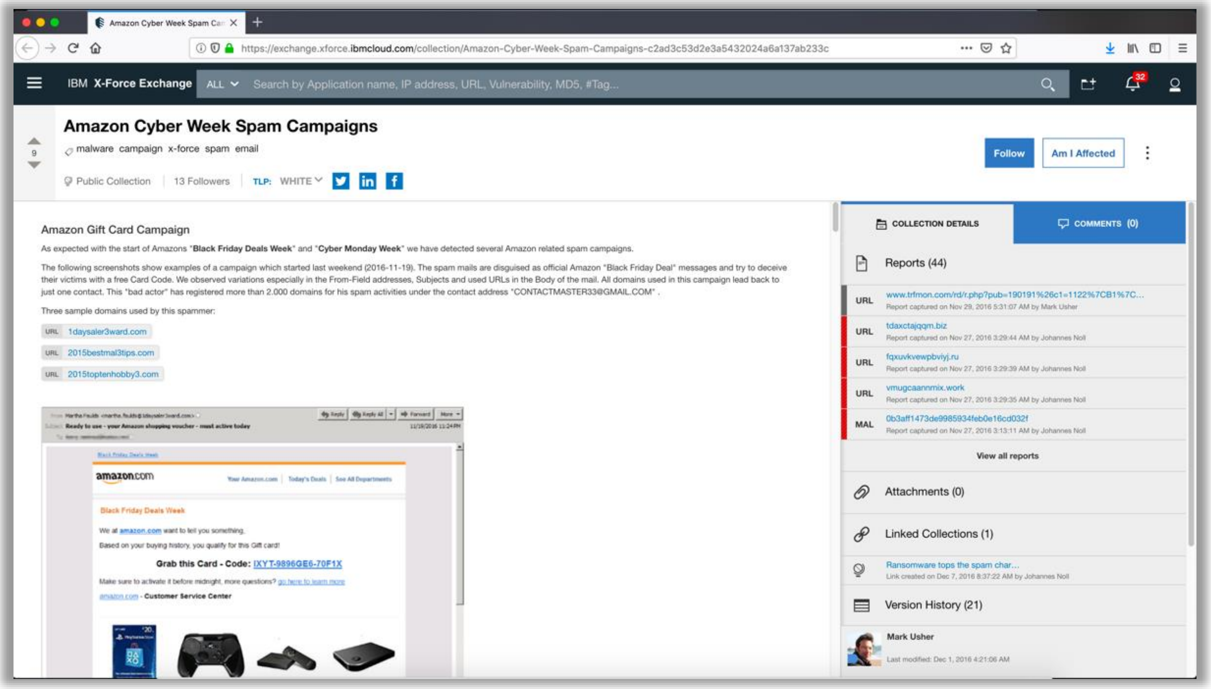
Milestone Summary

X-Force Exchange can be crucial for Cybersecurity and cyber awareness. With X-Force Exchange, we can monitor the online environment, in real-time, and actively follow known security issues. Security concerns can be investigated to not only tell us where the problem originated, but who has been affected and what type of systems are under threat.

More Examples

If you would like to explore more with X-Force Exchange, the *Amazon Cyber Week Spam Campaign* collection is a great example and contains a lot of information on how hackers scammed millions out of consumers by impersonating Amazon support and utilizing spam.

https://exchange.xforce.ibmcloud.com/collection/Amazon-Cyber-Week-Spam-Campaigns-c2ad3c53d2e3a5432024a6a137ab233c


Amazon Cyber Week Spam Ca
https://exchange.xforce.ibmcloud.com/collection/Amazon-Cyber-Week-Spam-Campaigns-c2ad3c53d2e3a5432024a6a137ab233c
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
32
9
Follow
Am I Affected
COLLECTION DETAILS
COMMENTS (0)

Amazon Cyber Week Spam Campaigns

malware campaign x-force spam email

Public Collection | 13 Followers | TLP: WHITE

Amazon Gift Card Campaign

As expected with the start of Amazons "**Black Friday Deals Week**" and "**Cyber Monday Week**" we have detected several Amazon related spam campaigns.

The following screenshots show examples of a campaign which started last weekend (2016-11-19). The spam mails are disguised as official Amazon "Black Friday Deal" messages and try to deceive their victims with a free Card Code. We observed variations especially in the From-Field addresses, Subjects and used URLs in the Body of the mail. All domains used in this campaign lead back to just one contact. This "bad actor" has registered more than 2.000 domains for his spam activities under the contact address "CONTACTMASTER33@GMAIL.COM" .

Three sample domains used by this spammer:

URL 1daysaler3ward.com

URL 2015bestmal3tips.com

URL 2015toptenhobby3.com

Ready to use - your Amazon shopping voucher - must active today

11/19/2016 11:24 PM

amazon.com | Your Amazon.com | Today's Deals | See All Departments

Black Friday Deals Week

We at amazon.com want to tell you something.

Based on your buying history, you qualify for this Gift card!

Grab this Card - Code: IXYT-9896GE6-70F1X

Make sure to activate it before midnight, more questions? go here to learn more

amazon.com - **Customer Service Center**

Reports (44)

URL	www.trfmon.com/rd/r.php?pub=190191%26c1=1122%7CB1%7C... Report captured on Nov 29, 2016 5:31:07 AM by Mark Usher
URL	tdaxctajqqm.biz Report captured on Nov 27, 2016 3:29:44 AM by Johannes Noll
URL	fqxuvkvewpbviyj.ru Report captured on Nov 27, 2016 3:29:39 AM by Johannes Noll
URL	vmugcaannmix.work Report captured on Nov 27, 2016 3:29:35 AM by Johannes Noll
MAL	0b3aff1473de9985934feb0e16cd032f Report captured on Nov 27, 2016 3:13:11 AM by Johannes Noll

View all reports

Attachments (0)

Linked Collections (1)

Ransomware tops the spam char...
Link created on Dec 7, 2016 8:37:22 AM by Johannes Noll

Version History (21)

Mark Usher
Last modified: Dec 1, 2016 4:21:06 AM

Figure 2-10 **Amazon Cyber Week Spam Campaign**