

**STANDARD OPERATING PROCEDURE**

**BOTNET**

January 22, 2018



© 2016 - 2018 IFF. All rights reserved.

No part of this technical document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, electronic, photocopying, recording, or otherwise, without prior written permission from IFF. The IFF logo is a trademark of IFF, registered in the U.S. and other countries.

|  |  |
| --- | --- |
| IFF Global Headquarters  521 West 57th Street  New York, NY 10019  United States  212-765-5500 | IFF Infrastructure Services  1515 State Highway #36  Union Beach, New Jersey 07735  732-264-4500 |

[www.iff.com](http://www.iff.com/)

|  |  |
| --- | --- |
| **Document Contributors and Approvers** | |
| The individuals listed below were involved in the creation, review and approval of this document. This section is for reference only. | |
| Name | Role |
| Sathyanarayanan N | Document Author |
| Senthil Kumar | Document Co-Author |
| George Griesler | Approver |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Control** | | |  |
| Details regarding the version control of this document can be found below. | | |  |
| Date Created | Effective Date | Expiration / Review Date | Modified Date |
| Jan 22, 2018 |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Modified By: |  | Version: |  | Revision: |  |

**Table of Contents**

[What is Botnet 4](#_Toc14418)

[Overview of the SOP 4](#_Toc14419)

[Tools Used for Analysis 5](#_Toc14420)

[Botnet Workflow 9](#_Toc14421)

[Procedure for Botnet 9](#_Toc14422)

[Steps by Security Support Team 10](#_Toc14423)

[Final Report 18](#_Toc14424)

# What is Botnet

The word Botnet is formed from the words ‘robot’ and ‘network’. Cybercriminals use special Trojan viruses to breach the security of several users’ computers, take control of each computer and organize all of the infected machines into a network of ‘bots’ that the criminal can remotely manage. A botnet may also be known as a zombie army.

Originally, botnets were created as a tool with valid purposes in Internet relay chat (IRC) channels. Eventually, hackers exploited the vulnerabilities in IRC networks and developed bots to perform malicious activities such as password theft, keystroke logging, etc.

An attacker will often target computers not safeguarded with firewalls and/or antivirus software.

Bots are designed to operate without users’ knowledge. However, there are some common signs that a computer may be infected with a botnet virus (listed below)

* IRC traffic (botnets and bot masters use IRC for communications)
* Multiple machines on a network making identical DNS requests
* High outgoing SMTP traffic (as a result of sending spam)
* Unexpected popups (as a result of click fraud activity)
* Slow computing/high CPU usage
* Outbound messages (email, social media, instant messages, etc) that weren’t sent by the user
* Problems with Internet access

# Overview of the SOP

Standard operating procedure for Security Support to carry out the Botnet Alerts.

1. ZScaler (Cloud-based Firewall) notifies the Security Team of the Bot Alerts.

1. An incident will be created and assigned to Security Support for further analysis / investigation.

# Tools Used for Analysis

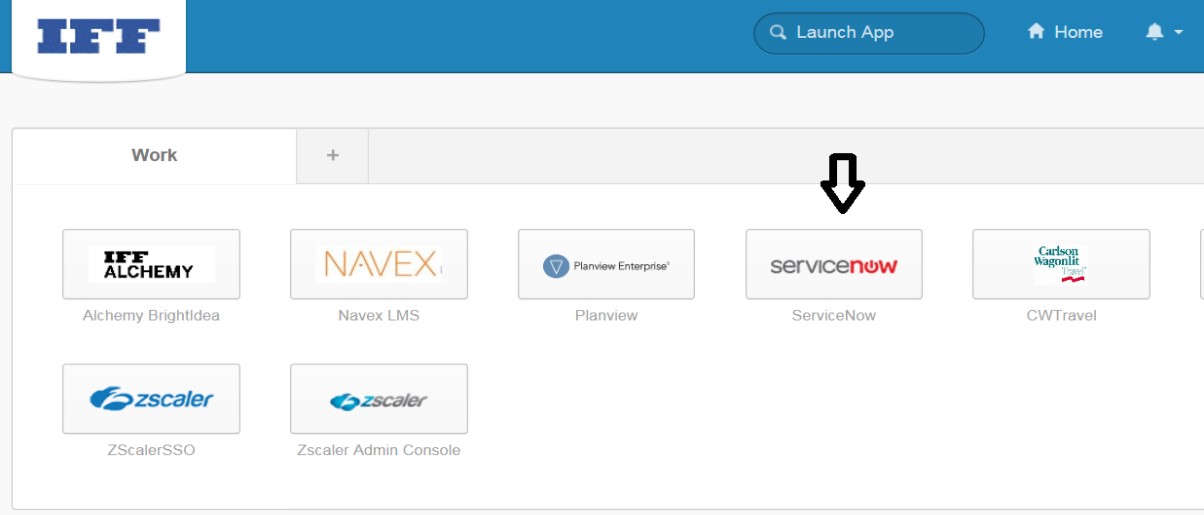
1. Servicenow
2. ZScaler Admin Console
3. Altiris
4. Solarwinds
5. Malwarebytes
6. Bluesocket
7. Aruba \*

\*Will be added once Aruba is live with our Team

## I. Service now

Servicenow is an ITSM tool that we use to create incidents for Botnet alerts.

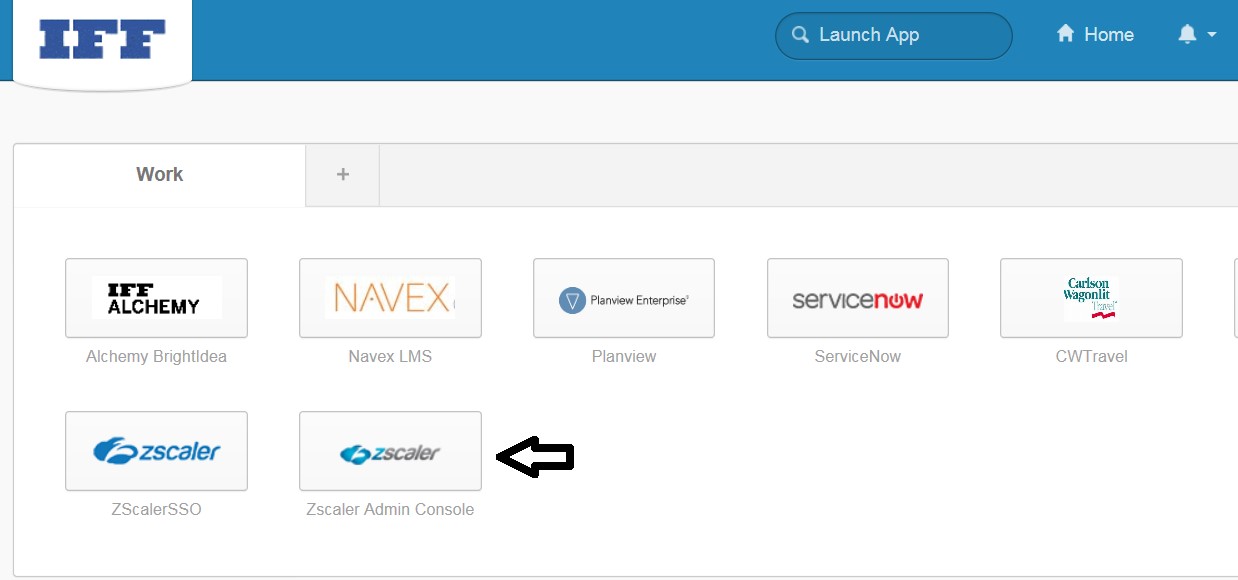
Link : SSO - Authenticated via OKTA [https://iff.okta.com/app/UserHome#](https://iff.okta.com/app/UserHome)



## II. ZScaler Admin Console

ZScaler is a cloud based firewall that monitors for Malicious traffic. Security Support Team is given access to ZScaler Admin console to view / analyze different types of logs including Spyware, Botnet, Phishing etc. from various dates.

Link : [https://admin.zscalertwo.net](https://admin.zscalertwo.net/) (Authenticated via OKTA)

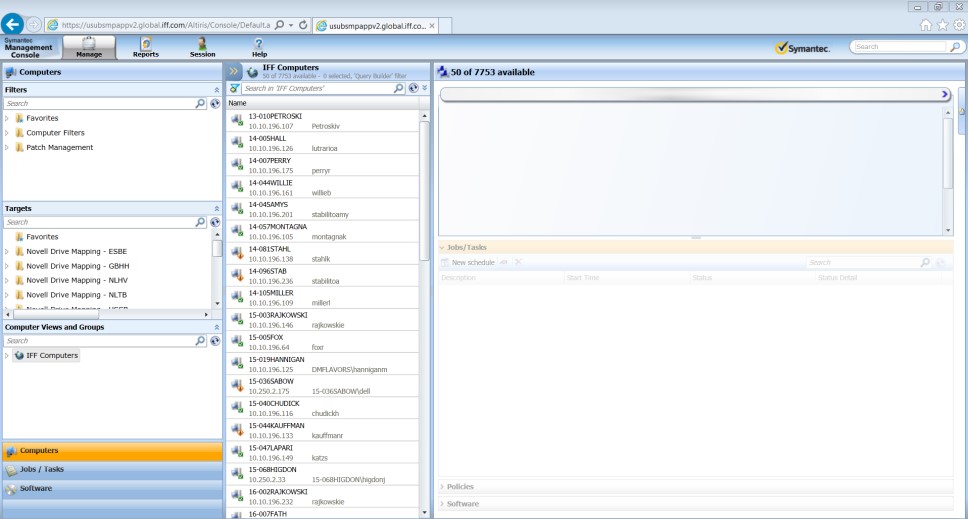


## III. Altiris

Altiris is an application distribution and asset management tool from Symantec, that is used to manage assets and ensure compliance. Altiris is used to capture Machine name using IP, User IDs, Server information, Policies, Software deployed on machines etc.

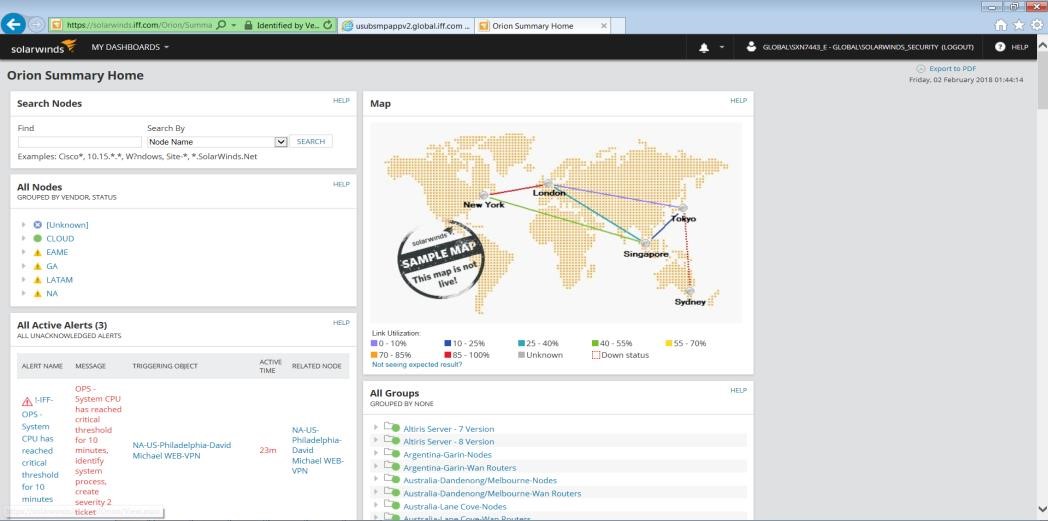
Note: End User machines must be configured with Altiris agent inorder for their machines to be displayed in the Altiris admin console.

Link :<https://usubsmpappv2.global.iff.com/Altiris/Console/Default.aspx>Credentials : E\_Account



## IV. Solarwinds

SolarWinds is a network & server monitoring software that enables to quickly detect, diagnose, and resolve network performance problems and outages.We use Solarwinds to find the Subnet information.



Link: <https://solarwinds.iff.com/Orion/SummaryView.aspx?>

Credentials : E\_Account

## V. Malwarebytes

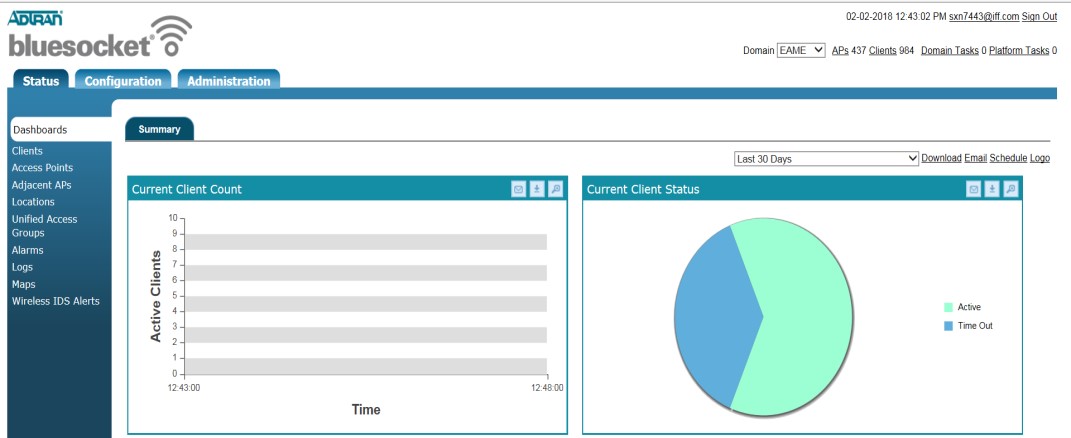


Link: <https://10.29.68.126/active/client/publish.htm>

Credential : E\_Account

## VI. Bluesocket

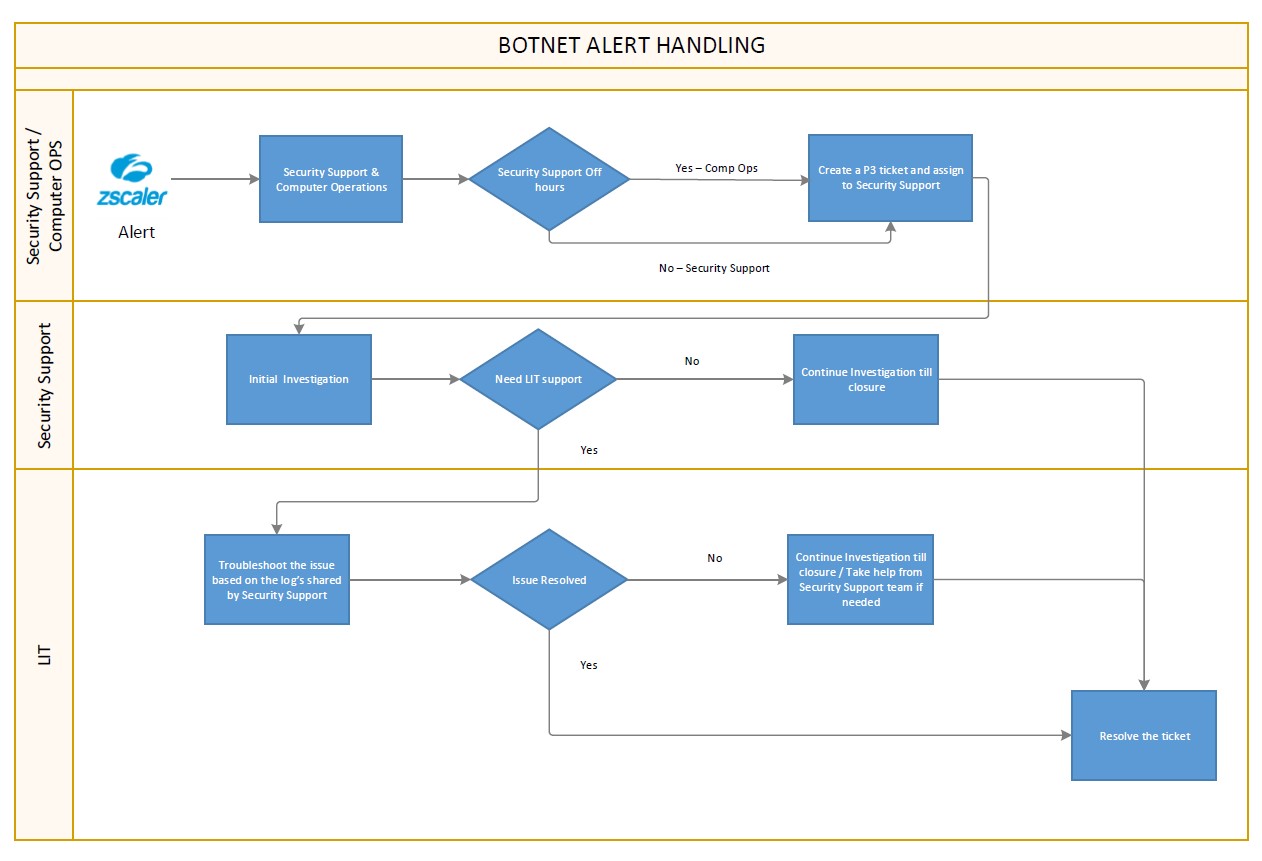
Bluesocket Adtran console helps to monitor and capture logs across WLAN.



Link:<https://ussbbsc01.global.iff.com:3000/platform/administrators/27> https://usubbsc02.global.iff.com:3000/platform/administrators

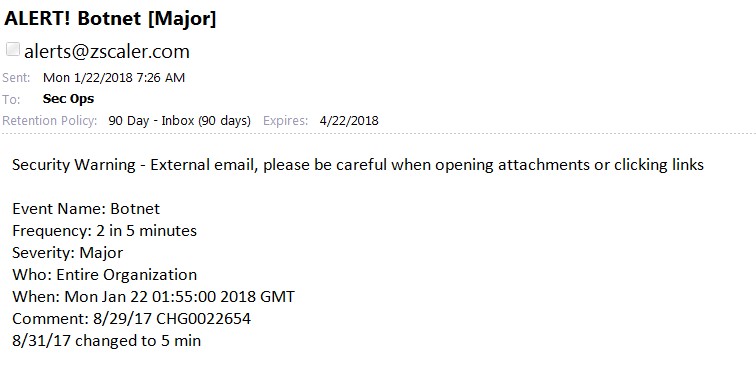
Credential : Global@iff.com / Password

# Botnet Workflow



# Procedure for Botnet

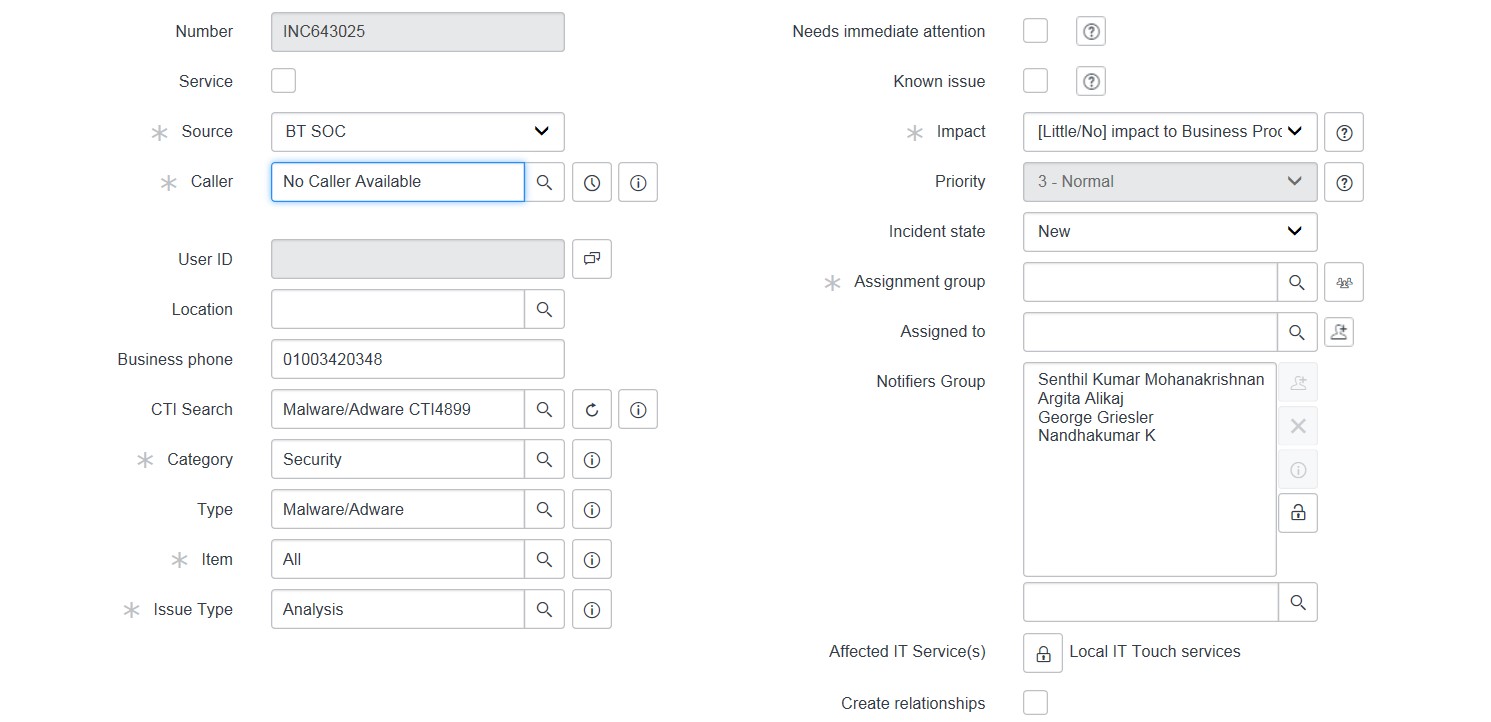
When a Bot alert is triggered by ZScaler Firewall, both Security Operations and Computer Operations Teams get an email notification as below.



1. Check if a ticket is in place if not create an internal ticket (P3).

1. Create an internal ticket, Sev 3 and Follow the CTI, notify group as given below screenshot.

Note: *Computer Operations create incidents on alerts outside Security team support hours.*

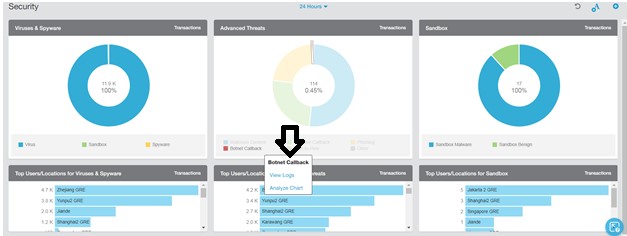


# Steps by Security Support Team

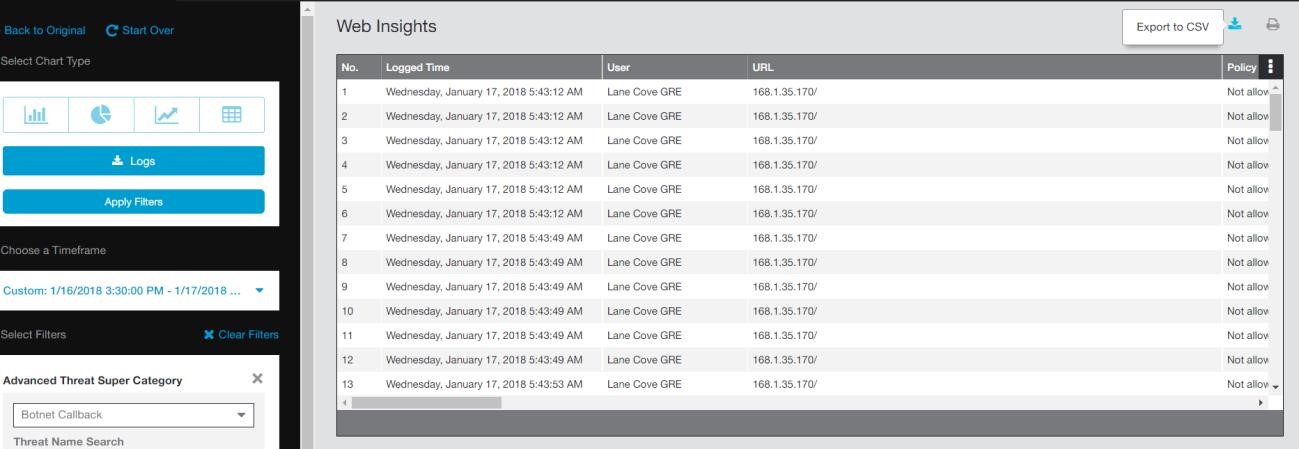
Bot activities can be monitored, detected, and prevented via ZScaler Admin Console.

1. Logon to Zscaler Admin

1. In the Dashboard, from the Advanced Threats, navigate to Botnet Callback > View logs (as below)



On clicking View logs, the below screen appears. Then, Export the log to the local machine in CSV format for analysis.



Below is the sample CSV log that is imported from ZScaler Admin console.



2018-01-11T04-50-22

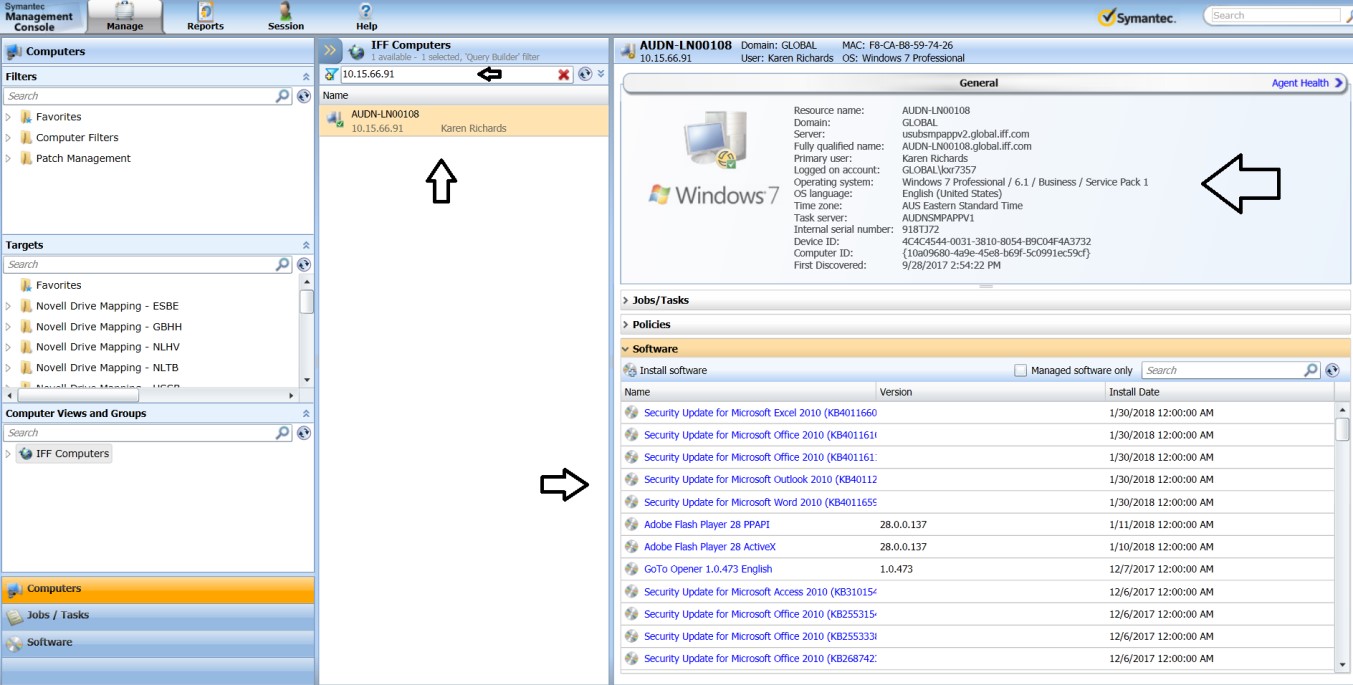
\_UTC\_web\_transaction

From the log, investigate the below categories.

* Event Time – When the event has occurred
* URL – The URL of the target
* Policy Action – Whether the traffic is allowed / not-allowed  Threat Nature – Whether it is a Trojan or Backdoor etc.
* Client IP – Source IP address
* Server IP - Destination IP address
* Response – Verify if the SIP has received response from the target

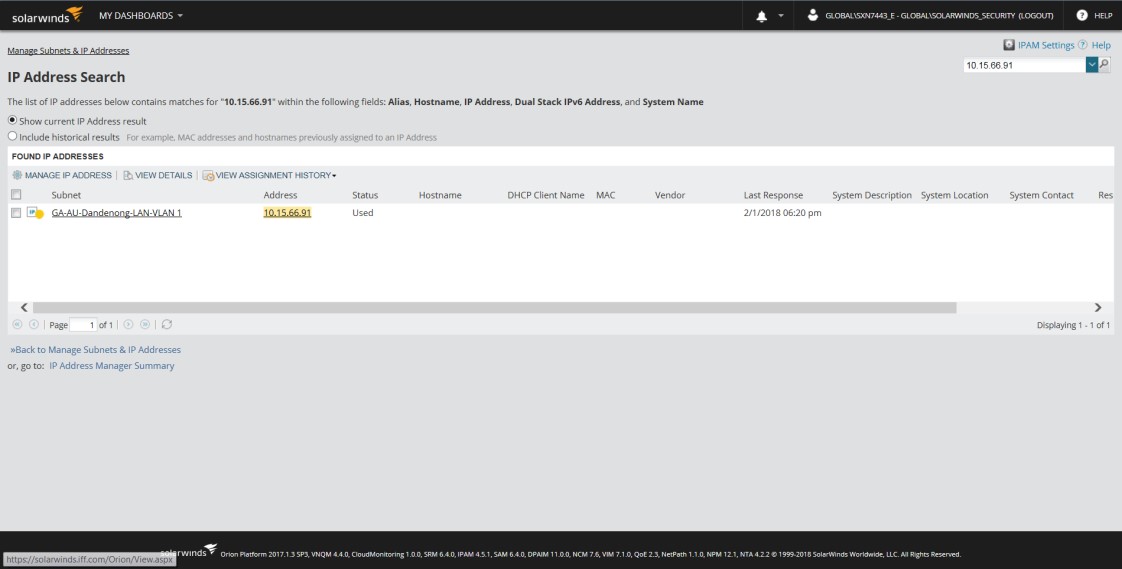
## Source IP Investiagation

1. With the Source IP (SIP), Search for the Machine name via Altiris

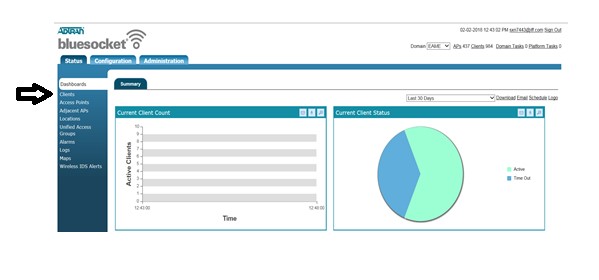


|  |  |  |
| --- | --- | --- |
|  | 1. With the Machine name, the User id, Location can be found as above 2. Check for any non-standard applications in the machine. If yes, document the same. 3. If the SIP is not found in Alteris, logon to Solarwinds to ch Subtnet where the IP is leased (as below).     Note: *Non-Standard applications, Browser addattackers to communicate with the target.*       1. Navigate to IP Addresses > IPAM Summary. | eck to see for the  *ons can also be used by* |
| 12 of 16 | IFF CONFIDENTIAL | LAST UPDATED: February 13, 2018 |

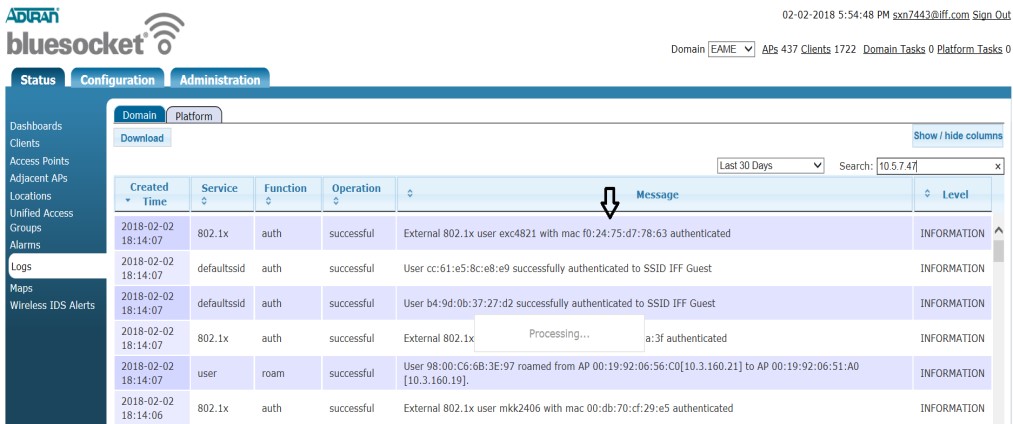
1. Enter the SIP and hit Search as above.



1. The Subnet information is available as above.
2. If the SIP belongs to WLAN / Guest Wireless Segment, the MAC Address that might have used the SIP can be found via Bluesocket or Aruba.
3. Logon to Bluesocket and navigate to Client as below



|  |  |
| --- | --- |
|  | 1. Now enter the SIP to find the MAC address that might have used the SIP.      1. Click on the drop down near domain to search for MAC address in other regions as well.            1. If no records are displayed for the SIP, Navigate to Logs in the same pane and enter the SIP. 2. Now, the MAC address of the SIP that belongs to WLAN can be found |
| 14 of 16 | IFF CONFIDENTIAL LAST UPDATED: February 13, 2018 |



1. To identify the MAC vendors using the MAC address, Use <https://macvendors.com/>

1. Refer to the below Mobile device management Inventory Excel sheet that has the list of devices and MAC addresses.

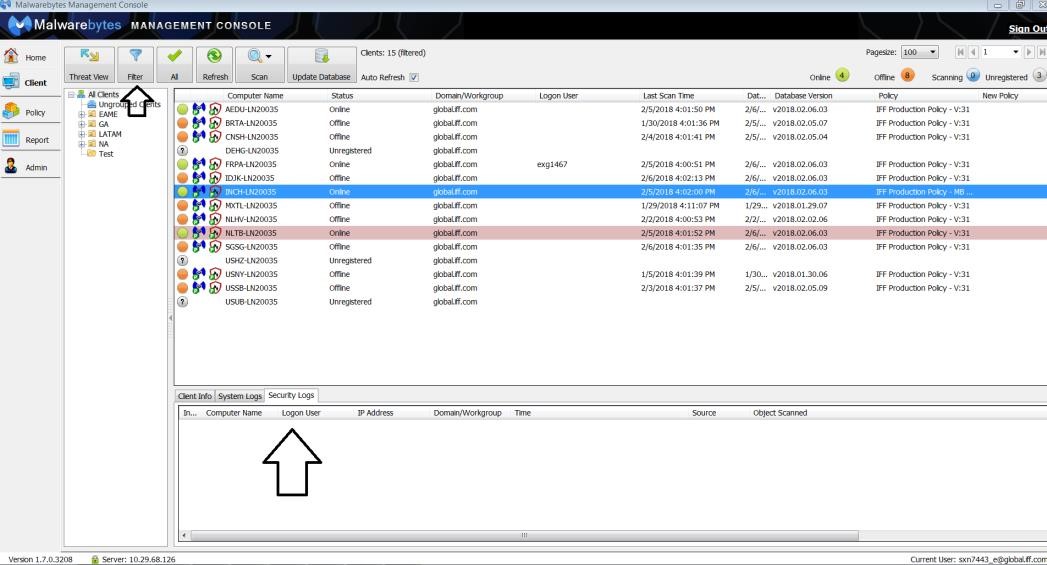


DevicesSearchResultmdm.iff.com-2017-12-

1. If the SIP was used as a WLAN / Guest Wireless, it can also be found in the DHCP logs. *Please reach out to Computer Operations for the DHCP Logs.*

*Note: Please check with respective teams for updated inventory sheets*

1. Once the IP is found, also check in the Malwarebytes for any Security Logs by Navigateing to Client > Client View > Filter >Search using machine name



*Note: If any security issues found, document the same while transferring the incident to Local IT Teams*

## Destination IP Investigation

1. Use the below resources to check to see if the DIP is blacklisted, Malicious.

1. <http://www.ipvoid.com/ip-blacklist-check/>- to check if the URL is blacklisted

1. <https://zulu.zscaler.com/>- to identify if the URL is malicious

1. [https://myip.ms/](https://myip.ms/info/whois/) - to find the rating / credibility of the URL

1. [https://www.virustotal.com](https://www.virustotal.com/) – to scan a URL for malicious detections

1. Other open source foot printing sites may also be used for analysis based on the scenarios.

1. Once the DIP is diagnosed to be Malicious and blocked by firewall (per the report), Document all the steps and information gathered using the SIP and DIP in the Incident and transfer the same to respective Local IT Teams with the Incident State as Assigned, for further investigation.

# Final Report

## Action by: Security Support

Once all the tasks above have been completed, update the Incident with all the findings and the actions taken for the Incident, and work with respective Local IT Teams if required until it is resolved.

16 of 16 IFF CONFIDENTIAL LAST UPDATED: February 13, 2018