Prepared by: EventTracker Control Center for Contoso Inc.

Report Created Date/Time: Aug 6, 2017 12:00:00 PM

From: Aug 6, 2017 12:00:00 AM
To: Aug 7, 2017 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 / Alert-EventTracker	Comments	Details
CRITICAL	Threats		Palo Alto detected network traffic which indicates a threat "ANGLER Exploit Kit Detection (38897)". Successful communication observed between system xacorp50 (by user Smith) and IP address XXX.170.76.85 (Ukraine) on port 80 (TCP)	**ACTION**: 1. Perform antivirus scan on the internal host to find and clean any possible infection. 2. If the given network traffic and the destination IP address is not legitimate, please block it at firewall level.	Link
			Outbound traffic was observed between internal IP address XXX.6.228.19 (unable to resolve) and XXX.226.11.139 (China). This traffic has been classified as Malware/Ransomware by snort	**ACTION**: 1. Revoke all admin privileges of the user associated with this system and revoke network drive/FTP access originating from the system. 2. Perform antivirus scan on the internal host to find and clean any possible infection.	
			The Palo Alto Firewall XXX.18.2.148 detected a potential malware threat delivery from multiple bad reputed public IPs to XXX.140.103.11 via email port 25 (SMTP). The Email was sent from multiple e-mail addresses to multiple recipients of testunion.org.	**ACTION**: Name of the attachment **scan.docm**. This file will download and run various Trojans and password stealers especially **banking Trojans like Dridex or Dyreza and ransomware** like Locky, Cryptolocker or Teslacrypt of Ransomware. To know more about this, visit link-1 and link-2. Educate users not to download files from unknown and suspicious contacts. Run periodic phishing test campaigns to learn and remain users about security.	
SERIOUS	Privileged User Monitoring		38,049 logon failures for account administrator".	**ACTION:** administrator" is invalid. Possible Brute Force attack.	Link
			A new application PAT FinSol has been installed (Event ID: 3208) by the user IDFireAcc (Event ID: 21) on the system TSACC2 by a remote interactive logon.	**ACTION:** If PAT FinSol is an approved application, it will be added to the whitelist, if it is not an approved application, recommended to uninstall the same from system TSACC2	
MEDIUM	Changes to Identity and Access Policies		A member added to security enabled local group	**INFO**: XTUCadmin" added to domain MENSA06. Please review	Link

Risk	Monitoring Activity	RSC	Incident / Alert-EventTracker	Comments	Details
SERIOUS	Identity/Role Context in User Activity		453 logon failures for User mlacamia" from source XXX.12.21.53. Logon Type 3.	ACTION: Network logon attempted and failed. Indicative that logon was attempted from a mobile device. Check with user	Link
			208 logon failures on system 'ETVAS8" from remote host 'XXX.3.202.103" (China) for user "root".	ACTION: This is indicative of a brute force attack. IP Address 183.3.202.103 is listed in the CBL. This IP address has been detected attempting to break into other sites using brute force password guessing attacks to an SSH-based login	
HIGH	Data Access Monitoring		DHCP service encountered error while backing up the database on the systems FOD-DC2, FOD-DC1 and SRVR-DC3. DHCP service encountered error while backing up the database on these systems	ACTION: If the DHCP server database becomes corrupted or is lost, recovery is possible by replacing the server database file (Dhcp.mdb). Also, it looks like DHCP has been configured on Domain Controllers. This is not a recommended configuration.	Link
HIGH	Identify Resource Access Exceptions		Configuration change by user SecAdmn" on Cisco Firewall - COLHAL-SYSLOG	INFO: Was change authorized?	Link
			Audit log was cleared by SS0DC5 on system TBLVM005	INFO: Was this activity authorized?	
HIGH	Application Activity Monitoring		McAfee McShield service terminated unexpectedly on multiple systems.	ACTION: Turn off Global Updating in ePO, under Configuration, Server Settings. Set Update through Automation, Server Tasks.	Link
HIGH	System Resource Monitoring		Low disk space on system SQLSVR	ACTION: Free disk space is down to 4% of total disk size - 120 GB. Free up disk space or change threshold (fixed size / %age).	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 of with Widespread Business Impact * Magnitude of The Event * Threat Vector * Limited Supporting Evidence (Event Logs)
HIGH	Asset of with High Business Impact * Magnitude of The Event * Threat Vector * Informational (Event Logs)
MEDIUM	Asset of with Nominal Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)
LOW	Asset of with Low Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)

Logbook Entries

Log Book Creation Time	Log Book Entry ID	Comment	Action Required	Status
08/09/2017 8:43:05 AM	10002	Possible **dictionary attack** was observed on the system **ETCMCLOUD02** from a bad reputed external IP address XXX.56.82.14 (**Netherlands**).	**ACTION**: If this is not legitimate, kindly investigate further and block this IP address.	Pending
07/25/2017 7:53:47 AM	10001	Potentially unwanted process **apnmcp.exe** has established network connection to the external IP address 199.36.100.106 (**Mindspark Interactive Network**) on the system **PNPL-5-SIEM (XXX.148.1.51).**	**ACTION**: 1. Uninstall the process apnmcp.exe. 2. Remove unwanted extensions from all the browsers. 3. Boot into safe-mode and perform antivirus scan.	Pending

Summary of Events

Summary	Nov 26	Nov 27	Nov 28	Nov 29	Nov 30	Dec 01	Dec 02
Log Volume	22,451,375	21,823,419	23,514,375	24,908,528	20,473,346	24,486,149	25,358,941
Alerts Triggered	16,779	16,728	14,229	16,737	16,779	16,728	14,229
Alerts High	16,489	16,457	13,408	16,189	16,489	16,457	13,408
Alerts Serious	12	21	17	11	13	12	11
Alerts Critical	2	4	3	1	0	2	1
New Activities	12	325	2	132	154	903	76

Behavior Analysis and Threat Intelligence for SIEM (Threats)

Back to Summary

- ECC observed Palo Alto detected network traffic which indicates a threat “ANGLER Exploit Kit Detection (38897)”. Successful communication observed between system **xacorp50** (user **smith**) and IP address **XXX.170.76.85** (Ukraine) on port 80 (TCP)

Log Time	Event ID	Event Type	Log Type	Computer	Event Source	Event Description	Category ID
08/06/2017 11:34:54 AM	8	Error	Application	Wt-ap3020-01-syslog	SYSLOG user	Aug 06 11:34:54 wt-ap3020-01 Dec 02 11:34:54 WT-AP3020-01..local 1, 2017/08/06 11:34:53, 001801006314, THREAT, vulnerability, 1, 2016/08/06 11:34:53, XXX.170.47.85, XXX.3.99.194, XXX.170.47.85, XXX.11.51.32, Allow Inside to All,, \smith, web browsing, vsys1, outside, inside, ethernet1/1,ethernet1/11,SyslogServer,2017/08/03 11:34:53, 230563, 1, 80, 62881, 80, 45568, 0x404000,tcp,alert,"",ANGLER Exploit Kit Detection(38897),not-resolved, critical, server-to- client, 28257,0x0,RU, 10.0.0.0-10.255.255.255,0,,0,,,1,,,,,0,0,0,0,0,,Palo Alto-01	2

Explanation: This signature detects attempts to download exploits from a malicious toolkit which may compromise a computer through various vendor vulnerabilities. For more information, please go through this link here

Affected Targets: Various Browsers

ACTION:

1. Perform antivirus scan on the internal host to find and clean any possible infection.
2. If the given network traffic and the destination IP address is not legitimate, please block it at firewall level.

- ECC observed outbound traffic was observed between internal IP address 10.6.228.19 (unable to resolve) and 101.226.11.139 (China). This traffic has been classified as Malware/Ransomware by snort

Log Time	Event ID	Computer	Event Description
08/06/2017 4:41:42 PM	8	ccids02	Aug 06 16:41:42 ccids02 [1:31299:5] MALWARE-CNC Win.Trojan.Necurs or Win.Trojan.Locky variant outbound detection [Classification: A Network Trojan was detected] [Priority: 1]: {TCP} XXX.61.28.19:50726 -> XXX.216.11.139:80
08/06/2017 4:41:41 PM	8	ccids02	Aug 06 16:41:41 ccids02 [1:31299:5] MALWARE-CNC Win.Trojan.Necurs or Win.Trojan.Locky variant outbound detection [Classification: A Network Trojan was detected] [Priority: 1]: {TCP} XXX.61.28.19:50722 -> XXX.216.11.139:80
08/06/2017 4:41:41 PM	8	ccids02	Aug 06 16:41:41 ccids02 [1:31299:5] MALWARE-CNC Win.Trojan.Necurs or Win.Trojan.Locky variant outbound detection [Classification: A Network Trojan was detected] [Priority: 1]: {TCP} XXX.61.28.19:50720 -> XXX.216.11.139:80

ACTION:

1. Revoke all admin privileges of the user associated with this system and revoke network drive/FTP access originating from the identified system.
2. Perform antivirus scan on the internal host to find and clean, any possible infection.
3. If the given network traffic and the destination IP address is not legitimate, block this IP at firewall level.

   For more details, check here

- ECC observed Palo Alto Firewall **XXX.18.2.148** detected a potential **malware** threat from multiple bad reputed public IP's to **XXX.140.103.11** via email port **25** (SMTP). The Email was sent from multiple e-mail addresses to multiple recipients of **testunion.org**. Details are attached as (TestUnion potential malware threat _05-09-16.xlsx).

ACTION: Name of attachment **scan.dcom**. This file will download and run various Trojans and password stealers especially **banking Trojans like Dridex or Dyreza and ransomware** like Locky, cryptolocker or Teslacrypt of Ransomware. To know more about this, visit the link-1 and link-2.

Privileged User Monitoring

Back to Summary

- ECC observed 38,049 logon failures for the account" administrator" on multiple systems from the source address XXX.168.220.236 due to "Unknown username or bad password". Below are the sample events: -

Log Time	Computer	User Name	User Domain	Logon Type	Reason	Workstation Name	Source Network Address
08/06/2017 5:50:10 AM	VEMPX701	administrator	MONITORAV	3	Unknown user name or bad password	MONITORAV	XXX.168.220.36
08/06/2017 5:50:41 AM	VEMPX701	administrator	MONITORAV	3	Unknown user name or bad password	MONITORAV	XXX.168.220.36

- ECC observed a new application **PAT FinSol** has been installed (Event ID: 3208) by the user **IDFireAcc** (Event ID: 21) on system T**SACC2** by a remote interactive logon (Event ID: 4624). Below are the correlated events.
  ACTION: Logbook entry ID 92344 - Incident # 201611014287.

Log Time	Event ID	Event User	Source Machine	Destination Machine	Event Description
08/06/2017 12:20:08 PM	3208	SYSTEM	-	TSACC2	Detected software <PAT FinSol> has been installed on this system.
08/06/2017 12:18:23 PM	21	SYSTEM	XXX.30.4.45	TSACC2-DLA	Remote Desktop Services: Session logon succeeded: User: IDFireAcc Source Network Address: XXX.30.4.45
08/06/2017 12:18:21 PM	4624	FireIDAcc	XXX.30.4.45	TSACC2	An account was successfully logged on. Security ID: S-1-5-18 Account Name: TSACC2$ Logon ID: 0x3E7 Logon Type: 10 Impersonation Level: Impersonation Security ID: S-1-5-21-2293766350-1974185745-1060264347-9638 Account Name: IDFireAcc Account Domain: TSA-PHOENIX Logon ID: 0x652B9 Logon GUID: {00000000-0000-0000-0000-000000000000}

Monitoring for Changes to Identity and Access Policies

Back to Summary

- ECC observed a member added to security enabled local group. Below are the event details: -

Log Time	Event ID	Site/Computer	Event Type	Event Source	Event Description
08/06/2017 8:38:16 AM	4732	SIEM / MENSA06	Audit Success	Microsoft-Windows-Security-Auditing	A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-3513740509-849566563-856728493-1000 Account Name: XTUCadmin Account Domain: MENSA06 Logon ID: 0x4bfbce9 Member: Security ID: S-1-5-21-494488399-1453150449-142223018-512 Account Name: - Security ID: S-1-5-32-544 Group Name: Administrators Group Domain: Builtin Additional Information:

Identity/Role Context in User Activity Monitoring Report

Back to Summary

- ECC observed 453 logon failures for user "mlacamia" from Source XXX.12.21.53. Failure Reason: *The specified account's password has expired.* Below is the reference event:

Log Time	Logo Type	User Name	Failure Reason	Workstation Name	Source Network Address
08/06/2017 9:15:38 PM	3	maclamia	The specified account's password has expired.	3SALESC	XXX.12.21.53

- ECC Observed 208 logon failures on system ‘ETVAS8” from the remote host ‘XXX.3.202.103” (China) for the user “root”. This could be a brute force attack. IP Address XXX.3.202.103 is listed in the CBL. This IP address has been detected attempting to break into other sites using brute force password guessing attacks to an SSH-based login. Below are the event details:

Log Time	Computer	Remote Host	Login Type
08/06/2017 12:38:19 AM	HQ\ETVAS8	XXX.3.202.103	ssh
08/06/2017 12:38:28 AM	HQ\ETVAS8	XXX.3.202.103	ssh

Data Access Monitoring

Back to Summary

- DHCP service encountered error while backing up the database on the systems FOD-DC2, FOD-DC1 and SRVR-DC3. DHCP service encountered error while backing up the database on these systems

Log Time	Event ID	Computer	Event Description
08/06/2017 4:14:56 AM	1016	FOD-DC2	The DHCP service encountered the following error when backing up the database: An error occurred while accessing the DHCP database. Look at the DHCP server event log for more information on this error.
08/06/2017 3:57:28 AM	1016	FOD-DC1	The DHCP service encountered the following error when backing up the database: An error occurred while accessing the DHCP database. Look at the DHCP server event log for more information on this error.
08/06/2017 3:47:05 AM	1016	SRVR-DC3	The DHCP service encountered the following error when backing up the database: An error occurred while accessing the DHCP database. Look at the DHCP server event log for more information on this error.

ACTION: If the DHCP server database becomes corrupted or is lost, recovery is possible by replacing the server database file (Dhcp.mdb), located in **%SystemRoot%\System32\Dhcp** folder, with a backup copy of the same file. If DHCP Manager was used previously to perform a backup, you can obtain the backup copy of the server database file located in the **%SystemRoot%\System32\Dhcp\Backup**folder. You can also restore the Dhcp.mdb file from a tape backup or other backup media.

Change Management Reports to Identify Resource Access Exceptions

Back to Summary

- Configuration change made by user "SecAdmn" on Cisco Firewall - COLHAL-SYSLOG.
- ECC observed Audit log was cleared by SS0DC5 on the system TBLVM005.

Log Time	Event ID	Computer	Event Type	Event Description
08/06/2017 8:32:24 AM	1102	TBLVM005	Audit Success	The audit log was cleared. Security ID: S-1-5-21-73586283-1606980848-682003330-77212 Account Name: SS0DC5 Domain Name: LABTOS Logon ID: 0x489be338

Application Activity Monitoring

Back to Summary

- McAfee McShield service terminated unexpectedly on multiple systems.

  ACTION: Logbook entry ID 93246 - Incident # 201511014274. Recommended action - Turn Off Global Updating in ePO, under Configuration, Server Settings. Set Update through - Automation, Server Tasks.

System Resource Monitoring

Back to Summary

- EventTracker incident number: 201511014274. Low disk space on the system "SQLSVR05". Below are the event details.

  ACTION: Logbook entry ID 93247 - Incident # 201509162237. Free disk space is down to 4% of total disk size. Free up disk space or change threshold (fixed size against percentage or change threshold percentage)

Log Time	Incident No.	Site/Computer	Drive	Free Space	Total Size
08/06/2017 2:57:30 PM	201509162237	HQDC1-APP-EVENT/SQLSVR	C	4910 MB	122910 MB