

### Prepared by: EventTracker Control Center for Contoso Inc.

Report Created Date/Time: Apr 21, 2018 05:45:00 AM EST

Period: Previous 1 Day

From: Apr 20, 2018 12:00:00 AM

To: Apr 21, 2018 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	Threats		<b>Malware Attack</b>  <a href="#">IR Playbook - Malware Attack</a>	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)	<b>ACTION:</b> <ol style="list-style-type: none"> <li>Perform antivirus scan on the internal host to find and clean any possible infection.</li> <li>If the given network traffic and the destination IP address is not legitimate, please block it at firewall level.</li> </ol>	<a href="#">Link</a>
			<b>Unauthorized Usage</b>  <a href="#">IR Playbook- Unauthorized Usage</a>	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	<b>ACTION:</b> <ol style="list-style-type: none"> <li>Revoke all admin privileges of the user associated with this system and revoke network drive/FTP access originating from the system.</li> <li>Perform antivirus scan on the internal host to find and clean any possible infection.</li> <li>If the network traffic and the destination IP address is not legitimate, please block this IP at firewall level.</li> </ol>	
			<b>Malware Attack</b>  <a href="#">IR Playbook - Malware Attack</a>	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.	<b>ACTION:</b> <p>Name of the attachment <a href="#">scan.docm</a>. This file will download and run various Trojans and password stealers especially <b>banking Trojans like Dridex or Dyreza and ransomware</b> like Locky, Cryptolocker or Teslacrypt of Ransomware. To know more about this, visit <a href="#">link-1</a> and <a href="#">link-2</a>.</p> <p>Educate users not to download files from unknown and suspicious contacts. Run periodic phishing test campaigns to learn and remain users about security. Log book entry: 10008.</p>	


		<p><b>Unauthorized Usage</b></p> <p><a href="#">IR Playbook- Unauthorized Usage</a></p>	<ul style="list-style-type: none"> <li>Numerous denied Port scan activities</li> <li>Successful Port scan and compromise</li> </ul>	<p><b>ACTION:</b></p> <ul style="list-style-type: none"> <li>Recommend blocking the IP addresses in firewall.</li> <li>Confirm if it was authorized penetration testing activity (ECC recommends to flag this in advance to avoid treat it as a red flag)</li> </ul> <p><b>ACTION:</b></p> <ul style="list-style-type: none"> <li>Isolate System/s from network</li> <li>Perform AV/Anti-malware scan</li> <li>Scan for open ports on the system in question</li> <li>Close ports not required for business reasons</li> <li>Harden the server/system in question</li> <li>SIEMphonics Team will also advice on if there are more systems in question where compromise was evident to take similar actions.</li> </ul>	
		<p><b>Malware Attack</b></p> <p><a href="#">IR Playbook - Malware Attack</a></p>	Vulnerabilities with CVSS score of 7.5 and above	<p><b>ACTION:</b></p> <p>Update the system with the recommended fix</p> <p>Advise SIEMphonics team once the patch updates are in place to perform re-scan</p>	
		<p><b>Unauthorized Usage</b></p> <p><a href="#">IR Playbook- Unauthorized Usage</a></p>	Possible Policy Violation (Web Content, Software Install/Uninstall etc.)	<p><b>ACTION:</b></p> <p>Verify if the user is authorized to perform the given action</p> <p>Re-validate group policy settings and proxy/firewall/content filter settings</p>	
<b>SERIOUS</b>	Privileged User Monitoring	<p><b>Unauthorized Usage</b></p> <p><a href="#">IR Playbook- Unauthorized Usage</a></p>	38,049 logon failures for account administrator".	<p><b>ACTION:</b></p> <p>administrator" is invalid. Possible Brute Force attack.</p>	<a href="#">Link</a>
		<p><b>Unauthorized Usage</b></p> <p><a href="#">IR Playbook- Unauthorized Usage</a></p>	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.	<p><b>ACTION:</b></p> <p>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</p>	

<b>MEDIUM</b>	Changes to Identity and Access Policies	<b>Improper Usage</b> <a href="#">IR Playbook-Improper Usage</a>	A member added to security enabled local group	<b>ACTION:</b> XTUCadmin" added to domain MENSA06. Please review	<a href="#">Link</a>
<b>SERIOUS</b>	Identity/Role Context in User Activity	<b>Improper Usage</b>	453 logon failures for User mlacamia" from source XXX.12.21.53. Logon Type 3.	<b>ACTION:</b> Network logon attempted and failed. Indicative that logon was attempted from a mobile device. Check with user	<a href="#">Link</a>
			208 logon failures on system 'ETVAS8" from remote host 'XXX.3.202.103" (China) for user "root".	<b>ACTION:</b> This is indicative of a brute force attack. IP Address 183.3.202.103 is listed in the <a href="#">CBL</a> . This IP address has been detected attempting to break into other sites using brute force password guessing attacks to an SSH-based login	
<b>HIGH</b>	Data Access Monitoring	<a href="#">IR Playbook-Improper Usage</a>	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	<b>ACTION:</b> 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.	<a href="#">Link</a>
<b>HIGH</b>		<b>Unauthorized Usage</b>  <a href="#">IR Playbook-Unauthorized Usage</a>	USB Data Copied, Modified, Deleted  Drop Box, One drive activities, large file movements	<b>ACTION:</b> Please verify if the user is authorized to move/copy data If not please verify your security policy  <b>ACTION:</b> Please verify if these are authorized activities If not please verify security policy	
<b>HIGH</b>	Identify Resource Access Exceptions	<b>Improper Usage</b> <a href="#">IR Playbook-Improper Usage</a>	Audit log was cleared by SS0DC5 on system TBLVM005	<b>ACTION:</b> Please verify if this is a legitimate/approved activity	<a href="#">Link</a>
<b>HIGH</b>	Application Activity Monitoring	<b>Others</b>	McAfee McShield service terminated unexpectedly on multiple systems.	<b>ACTION:</b> Turn off Global Updating in ePO, under Configuration, Server Settings. Set Update through Automation, Server Tasks.	<a href="#">Link</a>
<b>HIGH</b>	System Resource Monitoring		Low disk space on system SQLSVR	<b>ACTION:</b> Free disk space is down to 4% of total disk size - 120 GB. Free up disk space or change threshold (fixed size / %age).	<a href="#">Link</a>

\*(RSC) 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-SIEMphonics Team's Analysis Baseline	
<b>CRITICAL</b>	Asset Value with Substantial Business Impact * Magnitude of The Event * Threat Vector* Intact Supporting Evidence (Event Logs)
<b>SERIOUS</b>	Asset of with Widespread Business Impact * Magnitude of The Event * Threat Vector * Limited Supporting Evidence (Event Logs)
<b>HIGH</b>	Asset of with High Business Impact * Magnitude of The Event * Threat Vector * Informational (Event Logs)
<b>MEDIUM</b>	Asset of with Nominal Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)
<b>LOW</b>	Asset of with Low Business Impact * Magnitude of The Event * Threat Vector * Informational (Applicable Logs)

### Summary of Events

	Summary	Apr 15	Apr 16	Apr 17	Apr 18	Apr 19	Apr 20	Apr 21
	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
04/20/2018 11:34:54 AM	8	Error	Application	Wt-ap3020-01-syslog	SYSLOG user	May 01 11:34:54 wt-ap3020-01 Dec 02 11:34:54 WT-AP3020-01..local 1,2018/04/01 11:34:53, 001801006314, THREAT, vulnerability, 1, 2018/04/01 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,2018/03/24 11:34:53,	2

[Terms of Service](#)

[Terms of use for Third Party Services](#)

These sample report documents are property of EventTracker and Netsurion. No content may be copied, distributed, published or used in any way.

						230563, 1, 80, 62881, 80, 45568, 0x404000,tcp,alert,"", <b>ANGLER Exploit Kit Detection</b> (38897),not-resolved, critical, server-to- client, 28257,0x0,RU, 10.0.0.0-10.255.255.255,0,,1,,,,,0,0,0,0,,Palo Alto-01	
--	--	--	--	--	--	---	--

**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
04/20/2018 4:41:42 PM	8	ccids02	May 1 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
04/20/2018 4:41:41 PM	8	ccids02	May 1 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
04/20/2018 4:41:41 PM	8	ccids02	May 1 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
04/20/2018 5:50:10 AM	VEMPX701	administrator	MONITORAV	3	Unknown user name or bad password	MONITORAV	XXX.168.220.36
04/20/2018 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 **TSACC2** by a remote interactive logon (Event ID: 4624). Below are the correlated events.

**ACTION:** Logbook entry ID 92344 - Incident # 201811014287.

Log Time	Event ID	Event User	Source Machine	Destination Machine	Event Description
04/20/2018 12:20:08 PM	3208	SYSTEM	-	TSACC2	Detected software <PAT FinSol> has been installed on this system.
04/20/2018 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
04/20/2018 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
04/20/2018 8:38:16 AM	4732	SIEM / MENSA06	Audit Success	Microsoft-Windows-Security-Auditing	<p>A member was added to a security-enabled local group.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-3513740509-849566563-856728493-1000</p> <p>Account Name: XTUAdmin</p> <p>Account Domain: MENSA06</p> <p>Logon ID: 0x4bfbc9</p> <p>Member:</p> <p>Security ID: S-1-5-21-494488399-1453150449-142223018-512</p> <p>Account Name: -</p> <p>Security ID: S-1-5-32-544</p> <p>Group Name: Administrators</p> <p>Group Domain: Builtin</p> <p>Additional Information:</p>

### 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
04/20/2018 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
04/20/2018 12:38:19 AM	HQ\ETVAS8	XXX.3.202.103	ssh
04/20/2018 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
04/20/2018 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.
04/20/2018 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.
04/20/2018 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.

For more details, please refer [here](#).

**ACTION:** It looks like the DHCP has been configured on a Domain Controller. This is not a recommended configuration.

### Change Management Reports to Identify Resource Access Exceptions

[Back to Summary](#)

- ECC observed Audit log was cleared by SS0DC5 on the system TBLVM005.

Log Time	Event ID	Computer	Event Type	Event Description
04/20/2018 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
04/20/2018 2:57:30 PM	201509162237	HQDC1-APP-EVENT/SQLSVR	C	4910 MB	122910 MB

*The information provided in this report is intended solely for the use of designated employees or agents of Contoso Inc. 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.*