דו"ח מעבדה - תרחיש מס' 2

פרטים:

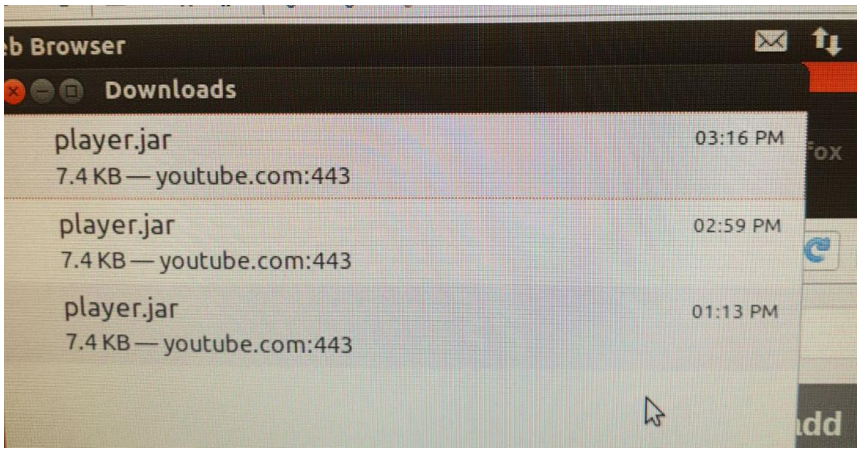
מגיש: דביר ברזילי

תאריך: 22.4.2018

שם התרחיש: חדירה לחברה מתחנת קצה

תהליך ההתקפה:

עובד בחברה הוריד לתחנת הקצה שלו קובץ player.jar מתוך האתר youtube. הקובץ הכיל נוזקה שהפילה את שרתי החברה. בנוסף, ע"מ להקשות עלינו באיתור הנוזקה בתחנת הקצה התוקף שיבש תאריכים ובכך גרם לנו לסווג קבצים כלא רלוונטים לתחקיר.



הורדו קבצים חשודים לתחנת הקצה

תהליך הזיהוי:

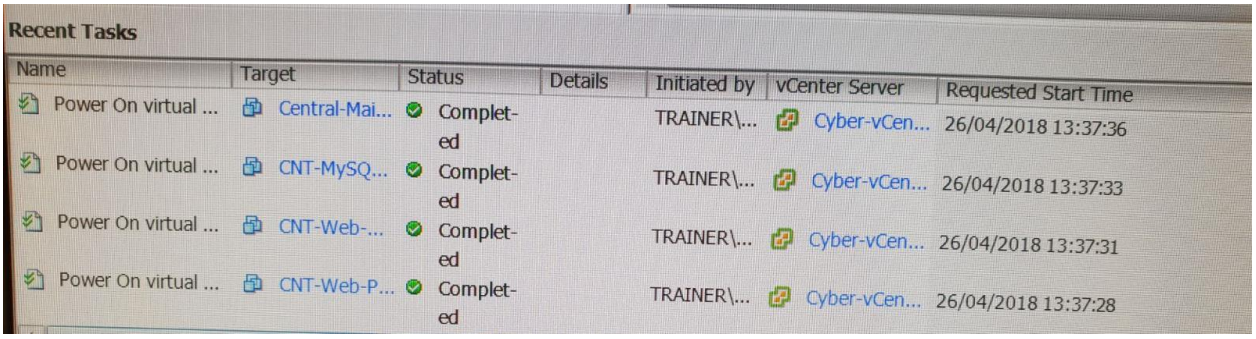
שמנו לב ששרת ה-Zenoss נפל. השתמשנו בכלי VMware כדי להרים את השרת חזרה, ומייד ראינו בו שיש עוד הרבה שרתים שנפלו. התחלנו לחקור את התחנות ומצאנו ב-SmartView Tracker שתחנת קצה מבצעת תקשורת חשודה עם השרתים וכנראה היא זו שגורמת לנפילת השרתים. חיפשנו בתחנת הקצה את הנוזקה שמפילה את השרתים. מצאנו בדפדפן שהמשתמש הוריד קובץ player.jar מיוטיוב שהכילה תקייה עם שמות של קבצים חשודים (כמו metasploit). אכן התברר שזו הייתה הנוזקה.

No.	Date	Ti...	Origin	Service	Source	Src. User Na...	Destination	R...	Curr. Rul...	Rule ...	Source Port	User	Src. Machine Na...	I
139...	6Jan20...	15:20:...	cnt-fw	ssh	192.168.110.102		CNT-Zenoss-N...	23	21-Standard	VPN_Acc...	38664			serv
278...	26Apr2...	13:15:...	cnt-fw	ssh	WS-Ubuntu-CNT1		CNT-Zenoss-N...	10	10-Standard	UsersToS...	35714			serv
279...	26Apr2...	13:20:...	cnt-fw	ssh	192.168.110.113		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51861			serv
279...	26Apr2...	13:20:...	cnt-fw	ssh	192.168.110.117		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51772			serv
279...	26Apr2...	13:20:...	cnt-fw	ssh	192.168.110.119		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49433			serv
279...	26Apr2...	13:20:...	cnt-fw	ssh	192.168.110.113		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51874			serv
279...	26Apr2...	13:21:...	cnt-fw	ssh	192.168.110.116		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50760			serv
280...	26Apr2...	13:24:...	cnt-fw	ssh	192.168.110.113		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51891			serv
280...	26Apr2...	13:25:...	cnt-fw	ssh	192.168.110.116		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50802			serv
280...	26Apr2...	13:26:...	cnt-fw	ssh	192.168.110.117		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51839			serv
280...	26Apr2...	13:27:...	cnt-fw	ssh	192.168.110.117		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51841			serv
280...	26Apr2...	13:27:...	cnt-fw	ssh	192.168.110.119		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49592			serv
280...	26Apr2...	13:27:...	cnt-fw	ssh	192.168.110.113		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51903			serv
280...	26Apr2...	13:28:...	cnt-fw	ssh	192.168.110.116		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50827			serv
280...	26Apr2...	13:28:...	cnt-fw	ssh	192.168.110.119		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49597			serv
280...	26Apr2...	13:28:...	cnt-fw	ssh	192.168.110.117		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51845			serv
280...	26Apr2...	13:29:...	cnt-fw	ssh	WS-Ubuntu-CNT1		CNT-Zenoss-N...	10	10-Standard	UsersToS...	35824			serv
282...	26Apr2...	13:37:...	cnt-fw	ssh	WS-Ubuntu-CNT1		CNT-Zenoss-N...	10	10-Standard	UsersToS...	35900			serv
282...	26Apr2...	13:39:...	cnt-fw	ssh	192.168.110.119		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49837			serv
282...	26Apr2...	13:40:...	cnt-fw	ssh	192.168.110.119		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49852			serv
282...	26Apr2...	13:40:...	cnt-fw	ssh	192.168.110.116		CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50968			serv

תחנת הקצה מתקשרת עם השרתים ברשת

תהליך הגנה:

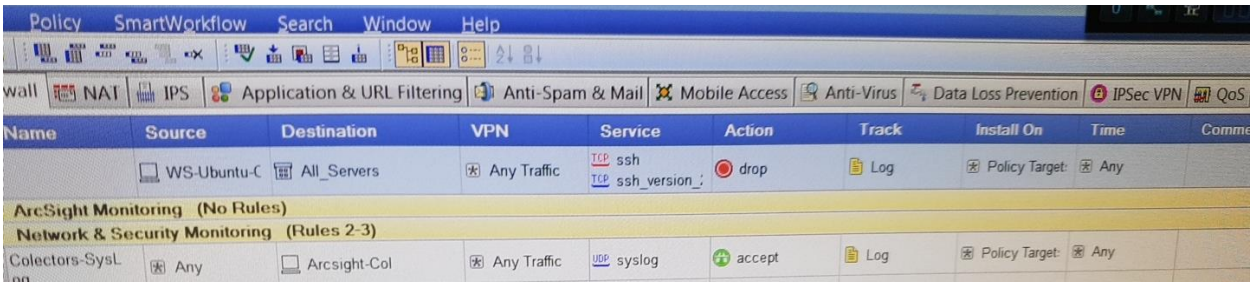
לאחר שזיהינו שהשרתים נפלו ניסינו להרים אותם חזרה, אולם הם נפלו כל פעם מחדש. כשהבנו בעזרת המעקב על התקשורת ברשת דרך ה-FireWall שתחנת הקצה היא זו שמפילה את השרתים חסמנו את התקשורת של התחנה עם הרשת. השרתים הפסיקו ליפול וכך אושר לנו שאכן זו הייתה התחנה הבעייתית. כך יכלנו לתחקר את תחנת הקצה ולבדוק אותה offline. בנוסף שינינו את הסיסמאות לשרתים להגנה נוספת.



Recent Tasks

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time
Power On virtual ...	Central-Mai...	Complet-ed		TRAINER\...	Cyber-vCen...	26/04/2018 13:37:36
Power On virtual ...	CNT-MySQ...	Complet-ed		TRAINER\...	Cyber-vCen...	26/04/2018 13:37:33
Power On virtual ...	CNT-Web-...	Complet-ed		TRAINER\...	Cyber-vCen...	26/04/2018 13:37:31
Power On virtual ...	CNT-Web-P...	Complet-ed		TRAINER\...	Cyber-vCen...	26/04/2018 13:37:28

מרימים את השרתים



Policy SmartWorkflow Search Window Help

wall | NAT | IPS | Application & URL Filtering | Anti-Spam & Mail | Mobile Access | Anti-Virus | Data Loss Prevention | IPSec VPN | QoS

Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comme
	WS-Ubuntu-C	All_Servers	Any Traffic	ssh ssh_version_	drop	Log	Policy Target:	Any	
ArcSight Monitoring (No Rules)									
Network & Security Monitoring (Rules 2-3)									
Colectors-SysL	Any	Arcsight-Col	Any Traffic	syslog	accept	Log	Policy Target:	Any	

חוסמים תקשורת של תחנת הקצה עם מחשבי הרשת

תהליך הגנה מונעת:

- שינוי סיסמאות לשרתים לסיסמאות חזקות יותר.
- סגירת פורט 20.
- ניהול חוקים ב-FireWall כך שתחנות קצה לא יוכלו לגשת חופשי לשרתים.
- התקנת תוכנת אנטי וירוס על המחשבים.

הפרצות באבטחת הארגון

סיסמאות חלשות. גישה לשרתי הארגון דרך תחנות קצה ללא צורך.
המחשבים לא מוגנים ע"י תוכנות אנטי וירוס ולכן חשופים לתקיפות סייבר.

אופן עבודת הצוות

תחילה חילקנו ביננו משימות ע"מ להיות יעילים ולהשגיח על החברה דרך הכלים השונים. כשהתחיל התרחיש היה מי שאחראי על הרמת השרתים והיה מי שאחראי לנסות לזהות את הבעייה. כשהיה חשד לבעייה כלשהי ניסינו לנטרל את המשך פעילותה. לאחר שחסמנו את התקשורת של תחנת הקצה עם הרשת נרתמנו כולנו לאיתור הנוזקה בתחנת הקצה.

חוסרים/קשיים

היה קושי באיתור הנוזקה במחשב הקצה. איתור הנוזקה דרש זמן רב של חיפוש ועיון בקבצים השונים של משתמשים שונים בתחנת הקצה.