

# דו"ח מעבדה- תרחיש מס' 2

פרטים:

מגיש: מירב בויס 206489155

תאריך: 30.4.2018

שם התרחיש:

תהליך ההתקפה:

עובד בחברה הוריד קובץ מיוטיוב player.jar



בקובץ זה הייתה נוזקה שלא הצלחנו לזהות מה היה בה כי הקובץ מחק את עצמו (קובץ זמני). הנוזקה הפילה לחברה מספר שרתים.



בנוסף גם zenoss נפל

בנוסף על מנת לבלבל אותנו התוקף שינה את התאריכים של קבצים רלוונטים לתחקיר כדי שלא נסתכל עליהם כחשודים.

תהליך הזיהוי:

ראינו שה zenoss נפל. הלכנו לכלי vmware כדי להרים אותו, הרמנו אותו ואז ראינו ב zenoss שנפלו לנו עוד שרתים.

Central-Mail1	/Status/Ping	192.168.200.3 is DOWN!
CNT-Web-Pro...	/Status/Ping	192.168.213.3 is DOWN!
CNT-Web-Apa...	/Status/Ping	192.168.213.4 is DOWN!

הרמנו את השרתים ואז התחלנו לחקור את התחנות שנפלו.

חיפשנו חיבורים חשודים לתחנות ב tracker וגילינו שיש מחשב בחברה שמחובר דרך SSH לשרתים שנפלו.

280..	26Apr2..	13:27...	cnt-fw	ssh	192.168.110.117	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51841	servi
280..	26Apr2..	13:27...	cnt-fw	ssh	192.168.110.119	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49592	servi
280..	26Apr2..	13:27...	cnt-fw	ssh	192.168.110.113	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51903	servi
280..	26Apr2..	13:28...	cnt-fw	ssh	192.168.110.116	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50827	servi
280..	26Apr2..	13:28...	cnt-fw	ssh	192.168.110.119	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49597	servi
280..	26Apr2..	13:28...	cnt-fw	ssh	192.168.110.117	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	51845	servi
280..	26Apr2..	13:29...	cnt-fw	ssh	WS-Ubuntu-CNT1	CNT-Zenoss-N...	10	10-Standard	UsersToS...	35824	servi
282..	26Apr2..	13:37...	cnt-fw	ssh	WS-Ubuntu-CNT1	CNT-Zenoss-N...	10	10-Standard	UsersToS...	35900	servi
282..	26Apr2..	13:39...	cnt-fw	ssh	192.168.110.119	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49837	servi
282..	26Apr2..	13:40...	cnt-fw	ssh	192.168.110.119	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	49852	servi
282..	26Apr2..	13:40...	cnt-fw	ssh	192.168.110.116	CNT-Zenoss-N...	21	21-Standard	VPN_Acc...	50968	servi

נכנסו למחשב זה דרך ה vmware והתחלנו לחקור אותו. זיהינו שהוא הוריד תיקיה לאחרונה, חקרנו את התיקיה וגילינו שהיא מכילה קבצים חשודים כמו metasploit



תהליך הגנה:

לאחר זיהוי נפילת השרתים הרמנו אותם.

Recent Tasks				
Name	Target	Status	Details	Initiated by
Power On virtual ...	Central-Mail1_C	Completed		TRAINER\...
Power On virtual ...	CNT-MySQL_C	Completed		TRAINER\...
Power On virtual ...	CNT-Web-Apache_C	Completed		TRAINER\...
Power On virtual ...	CNT-Web-ProFTPd_C	Completed		TRAINER\...

לאחר הזיהוי של המחשב שגרם לנפילת השרתים חסמנו אותו ב firewall

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)									

נכנסנו לשרתים שנפלו ושינינו בהם סיסמאות

תהליך הגנה מונעת:

ניהול מדיניות סיסמאות

לא לתת הרשאות למחשבי קצה להתחבר ב SSH לשרתים שאינם אמורים לגשת אליהם.

התקנת אנטי וירוס ובדיקת קבצים במחשבי קצה.

## הפרצות באבטחת הארגון

---

SSH פתוח

מחשבי קצה לא מוגנים

תקשורת חופשית בתוך הארגון ללא מידור

## כלים שפיתחנו

---

לא פיתחנו

## אופן עבודת הצוות

---

מישהו אחד ניהל את האירוע וכתב דברים על הלוח, מישהו היה אחראי לכתוב את

החוקים ב firewall .

שאר הזמן כל אחד עשה מה שהיה צריך לעשות כגון בדיקת שרת מסויים שהיה צריך לבדוק או תחנה מסויימת, הרמת השרתים וכו.

## חוסרים/קשיים

---

זיהוי איך עבד הקוד הזדוני