„DETEKCIA ÚNIKU INFORMÁCII CEZ DNS“

9.12.2020

Marek Kľoc

www.lynx.sk

$:Definovanie problému

DNS je široko používaný protokol pre preklad doménových mien/IP a je ťažké rozlíšiť preklad od prenášania dát.

DNS tunelovanie je niekedy používane aj bežným sofvérom.

„Problémom detekcie úniku dát cez DNS službu je nájsť takú techniku, ktorá deteguje únik informácií v čase, v ktorom sa predmetný únik deje“

$: Popis techniky uniku dát cez DNS
časť I.

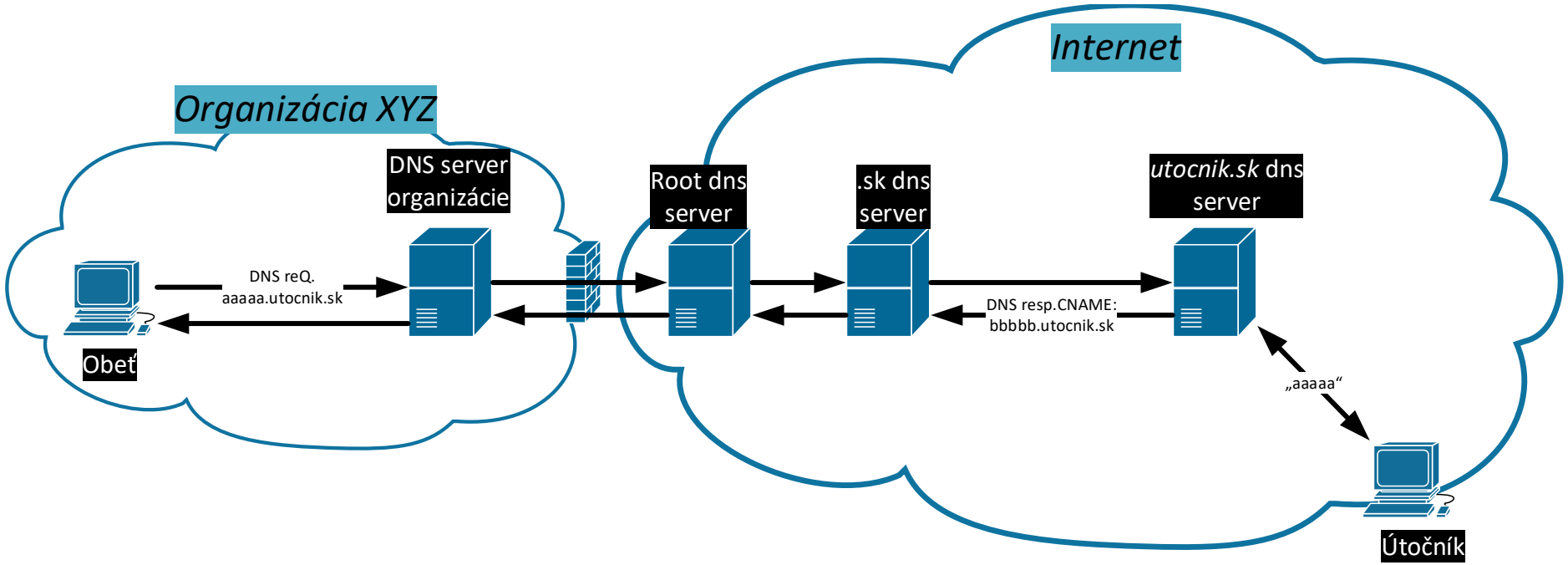
Únik informácií sa vykonáva tzv. tunelovaním DNS komunikácie, tzn. dáta sú *zakódované** do DNS dotazov a potvrdzovanie je kódované do odpovedí.

Podmienkou je, že útočník musí mať pod plnou kontrolou DNS server a možnosť prekladu verejných adries z vnútra infraštruktúry.

```
    10.1.139.70.64116 > 10.99.1.209.53: [udp sum ok] 51276+% [1au] CNAME? paeabvsq.mkloc.local.
r: . OPT UDPsize=4000 DO (49)
20:29:10.609272 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 88)
    10.99.1.209.53 > 10.1.139.70.62671: [bad udp cksum 0xa1d0 -> 0xf984!] 49217*- q: CNAME? paea
vsi.mkloc.local. 1/0/0 paeabvsi.mkloc.local. [0s] CNAME hsaaa.mk. (60)
20:29:13.505935 IP (tos 0x0, ttl 127, id 20555, offset 0, flags [none], proto UDP (17), length (
)
    10.1.139.70.64258 > 10.99.1.209.53: [udp sum ok] 51582+ CNAME? paeabvsy.mkloc.local. (38)
20:29:13.506086 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 88)
    10.99.1.209.53 > 10.1.139.70.64116: [bad udp cksum 0xa1d0 -> 0xdcd1!] 51276*- q: CNAME? paea
vsq.mkloc.local. 1/0/0 paeabvsq.mkloc.local. [0s] CNAME hsaaa.pr. (60)
```

$: Popis techniky uniku dát cez DNS

časť II: Ako funguje DNS tunnel



$: použitie DNS tunelovania malvérom

Ismdoor Malware Continues to Make use of DNS Tunneling
Black Lotus Labs
Posted On **September 5, 2019**

Though DNS tunneling is by no means a new threat, we've recently observed a rise in actors **using DNS to conduct such attacks, such as the information-stealing malware Nutshell/Ismdoor**, which was first identified in 2017.
https://blog.centurylink.com/ismdoor-malware-continues-to-make-use-of-dns-tunneling/

$: použitie DNS tunelovania malvérom

DNS Tunneling in the Wild: Overview of OilRig's DNS Tunneling
April 16, 2019 at 9:00 AM

On March 15, Unit 42 published a blog providing an overview of DNS tunneling and how malware can use DNS queries and answers to act as a command and control channel. To supplement this blog, we have decided to describe a collection of tools that rely on DNS tunneling used by an adversary known as **OilRig**.

This blog will dive deep into the **DNS tunneling protocols used by**https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/

$: použitie DNS tunelovania malvérom

- **OilRig’s a ISMAgent**
- **ALMACommunicator**
- **BONDUPDATER**
- **QUADAGENT**

Každý z uvedených „malvér nástrojov“ používa DNS tunnel

$: Vytvorenie DNS tunelu

```
Enter password:
Opened dns0
r mkloc.local to 10.1.139.70
y type (use -T to override).
eries
Version ok, both using protocol v 0x00000502. You are user #0
```

```
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=3.90 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=3.96 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=64 time=3.62 ms
```

```
5: dns0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1130 qdisc fq_codel state
fault qlen 500
    link/none
    inet 172.16.0.2/27 scope global dns0
       valid_lft forever preferred_lft forever
```

```
21: dns0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1130 qdisc pfifo_fast state
 default qlen 500
    link/none
    inet 172.16.0.1/27 scope global dns0
       valid_lft forever preferred_lft forever
```

$: Možnosti detegovania DNS tunnelu

- **Detegovanie neobvyklej dĺžky doménového mena (pravidlo)**
- **Detegovanie počtu dns dotazov za časové obdobie (štatistika)**
- **Detegovanie počtu rozdielnych dns mien per entita (pokročilá štatistika)**
- **Detegovanie s pomocou analýzy reťazca dns domény (strojové učenie)**

$: Typy detekcie

Detegovanie neobvyklej dĺžky doménového mena (pravidlo)

Výhody: rýchla implementácia

Nevýhody: DNS s tunelovanie s krátkymi DNS dotazmi nie sú detekovateľné

0iabbEnPJyobGCgvGujU6Y3hbGDhL4XObbIyGzUrGEhYhGzobKygrIzMfLy1DG.XmaRYGhaG.mkloc.local	72
blobcollector.events.data.trafficmanager.net	25
www.tm.a.prd.aadg.akadns.net	17
watson.telemetry.microsoft.com	16
0.debian.pool.ntp.org	13
paazvxtq.mkloc.local	8
paazvxty.mkloc.local	8
paazvxua.mkloc.local	8
login.microsoft.com	5
login.microsoftonline.com	5
au.download.windowsupdate.com.edgesuite.net	25

$: Detegovanie počtu dns dotazov za časové obdobie (štatistika)

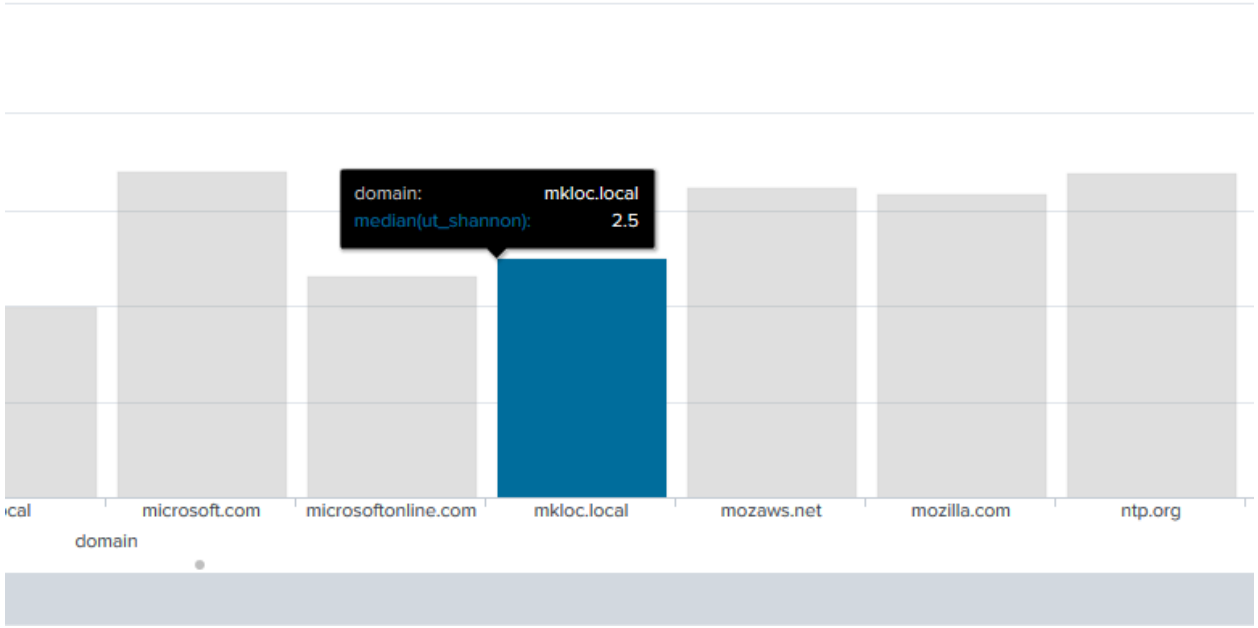
Výhody: **rýchla implementácia**

Nevýhody: **Občasne posielané pakety nie je možné detegovať**

src_ip	akadns.net	cloudapp.net	gmail.com	in-addr.arpa	microsoft.com	microsoftonline.com	mkloc.local	msidentity.com	trafficmanager.net	windows.net
10.99.3.149	0	0	1041	0	8521	7946	0	0	0	8462
10.1.131.204	0	0	0	15252	0	0	0	0	0	0
10.1.131.202	0	0	0	15238	0	0	0	0	0	0
10.1.136.22	2192	2051	287	289	964	295	0	1598	2076	457
10.1.139.60	1252	570	321	38	685	344	0	1607	1011	517
10.1.160.102	0	0	0	0	2706	0	0	0	0	0
10.99.1.7	0	0	0	0	0	0	2526	0	0	0
10.99.1.209	0	0	0	0	0	0	2526	0	0	0
10.99.3.193	0	0	0	0	891	0	0	0	0	0

$:Detegovanie s pomocou analýzy reťazca dns domény (strojové učenie)

Výpočet „entrópie“ reťazca



$:Detegovanie s pomocou analýzy reťazca dns domény (strojové učenie)

TFIDF a ML

Frekvenčná analýza znakov a inverzná frekvenčná analýza znakov v reťazci DNS doménového mena: (napríklad)

- Pomer samohlások voči dĺžke reťazca
- Pomer spoluhlások voči dĺžke reťazca
- Pomer samohlások voči spoluhláskam
- Pomer číslic k počtu znakov a ich poradie

$:Detegovanie s pomocou analýzy reťazca dns domény (strojové učenie) :: živá ukážka::

ut_subdomain_length	ut_meaning_ratio	digits	vowels	ut_subdomain_digit_ratio	ut_subdomain_vowe	ut_domain	ok	tunnel
6	0.166666					gmail.com	10	0
						gstatic.com	4	0
7	0.142857					microsoft.com	75	0
						microsoftonline.com	42	0
7	0.142857					mkloc.local	248	4
5						msidentity.com	18	0
						oit.local	2	0
						skypedataprdcoleus16.cloudapp.net	4	0
						ubuntu.com	9	0

$:Záver

Lx overenie jednotlivých metód

- Technika detekcie, ktorá používa dĺžku reťazca dns domény v dns dotaze, neodhalí DNS tunel, ak útočník definuje maximálnu dĺžku doménového mena v malých hodnotách
- Rovnako technika detekcie s pomocou celkového počtu dns dotazov je menej efektívna, pretože ak útočník ovplyvní počet generovaných dns dotazov v čase na malé hodnoty, algoritmus to nezachytí
- Vysoko efektívna je technika detekcie s pomocou počtu rôznych DNS dotazov v čase v porovnaní s populáciou. Táto technika je zároveň najrýchlejšia. Nevýhodou je, že detekcia je možná až po uskutočnení úniku.
- Vysoko efektívna je technika detekcie s pomocou analýzy reťazca doménového mena DNS dotazu. Technika deteguje DNS tunel v čase vytvorenia (*realtime*), nevýhodou je značná výpočtová náročnosť

Ďakujem za pozornosť

LYNX - spoločnosť s ručením obmedzeným Košice

www.lynx.sk