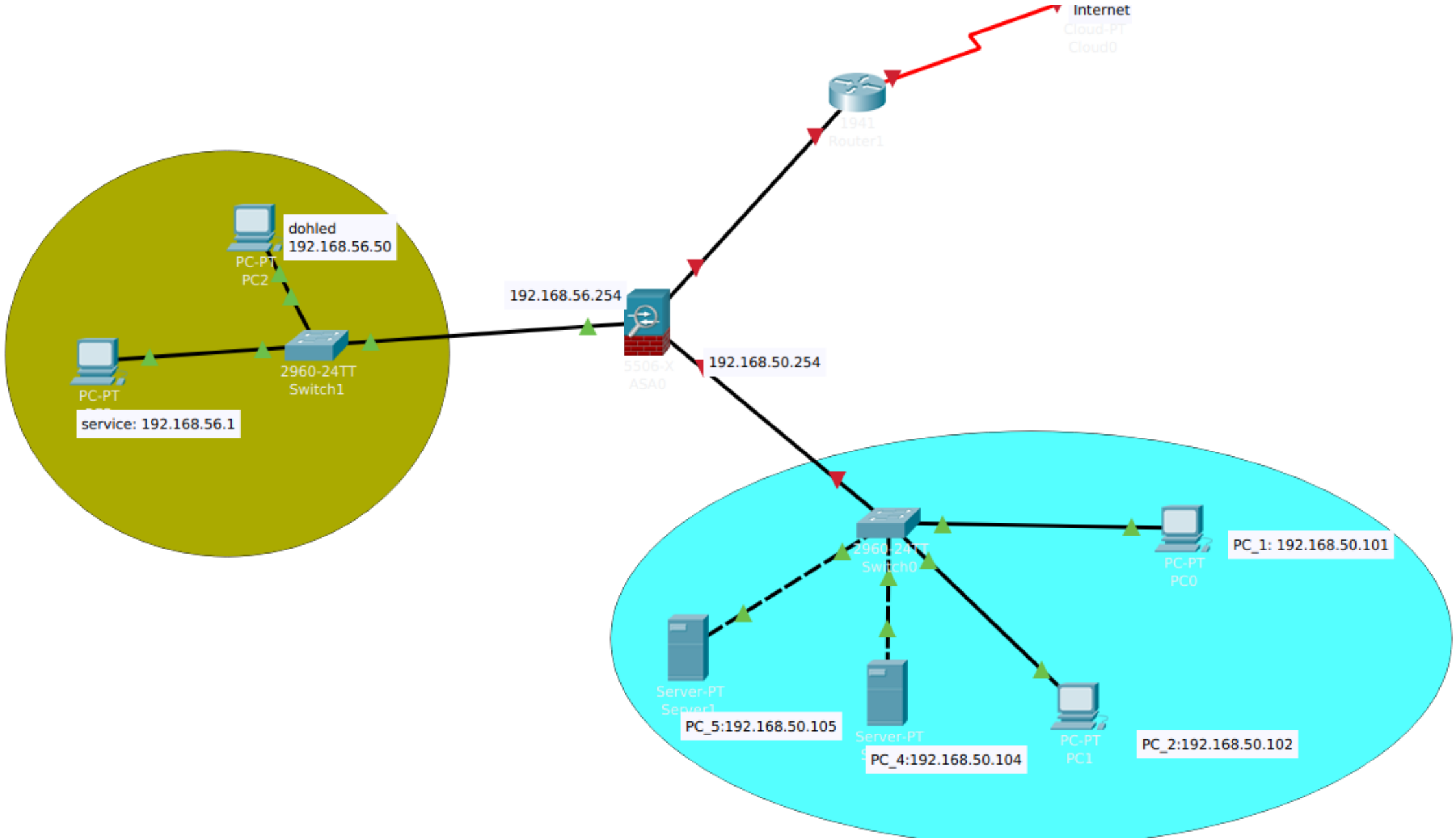
Big Data analysis

UnIT extended 19 – 2. tým

Andrej Tomči, Ádám Ruman,

Adam Ivora, Hana Pospíšilová


Internet
Cloud-PT
Cloud0
1941
Router1
dohled
192.168.56.50
PC-PT
PC2
192.168.56.254
PC-PT
2960-24TT
Switch1
service: 192.168.56.1
5506-X
ASA0
192.168.50.254
2960-24TT
Switch0
PC-PT
PC0
PC_1: 192.168.50.101
Server-PT
Server1
PC_5:192.168.50.105
Server-PT
PC_4:192.168.50.104
PC-PT
PC1
PC_2:192.168.50.102

Timeline - 25.3.

- 25.3 - 18:25:XX – disk Z: súbory pokusicek.pdf pokusicek.doc …. priečinok HACK_LAB
- 25.3 - 18:30:18 – myClearLogs.bat -> clear logov, PC1_sysmon
- 25.3 - 18:30:21,22 – clear logov PC2_system, PC2_security, PC2_sysmon
- 25.3 - 18:30:XX – clear, PC5 a PC6
- 25.3 - 18:38:19 – Virtual machine (10.0.2.15) z "dohled" -> Canonical
- 25.3 - 18:40:04 – PC1 -> bar.love.mail.ru (momentálne sa odtiaľ stahuje súbor)
- 25.3 - 18:53:51 – PC2 -> 10.32.128.68
- 25.3 - 18:56:36 – PC1 -> "Amazon" (inštancia AWS, predpokladaná route C2)
- 25.3 - 19:31:12 – PC5 -> "China" (123.103.93.214)
- 25.3 - 23:51:24 – packet z "Amazon" -> Virtual machine

Timeline – 26.3.

- 26.3-00:40:24 to 00:42:24 – "dohled" -> PC5 (veľa valid RDP loginov)
- 26.3-00:40:13 to 00:42:28 – "dohled" - scan (náhodných) portov na subnet 192.168.50.0/24
- 26.3-08:15:35 – reboot PC1 (system log)
- 26.3-08:15:29 – reboot PC2 (system log)
- 26.3-08:15:06 – reboot PC6 (system log)
- 26.3-10:17:27 – PC5 -> "Korea" (175.45.176.50)
- 26.3-12:53:45 – packet z 10.0.2.2 -> 10.0.2.15
- 26.3-13:46:20 – PC1 – CV_template.docm otvorený (viac v malware 1)

Timeline - 26.3.

- 26.3-13:59:52 - packet z "China" -> "Virtual machine"
- 26.3-20:41:43 - reboot PC1 (system log)
- 26.3-20:41:51 - reboot PC2 (system log)
- 26.3-20:42:00 - reboot PC5 (system log)
- 26.3-21:58:52 - PC6 -> "Korea" (firewall už nemá log)
- 26.3-22:07:34 - PC2 - putty_x64 -> "Škoda" (193.108.106.50), port 443
- 26.3-22:09:22 - PC2 - putty_x64 -> vbs script
- 26.3-22:09:24 - PC2 - malware2 -> "Škoda" (viac malware 2)
- 26.3-22:14:42 - PC2 "putty" -> cmd -> PowerShell -> bin?
- 26.3-22:31:40 - reboot PC5 (system log)
- 26.3-22:31:45 - reboot PC6 (system log)

In [5]:

```
x <- table(cut(fw_data$time, breaks="min"))
plot(x, type = "l")


head(fw_data)
```

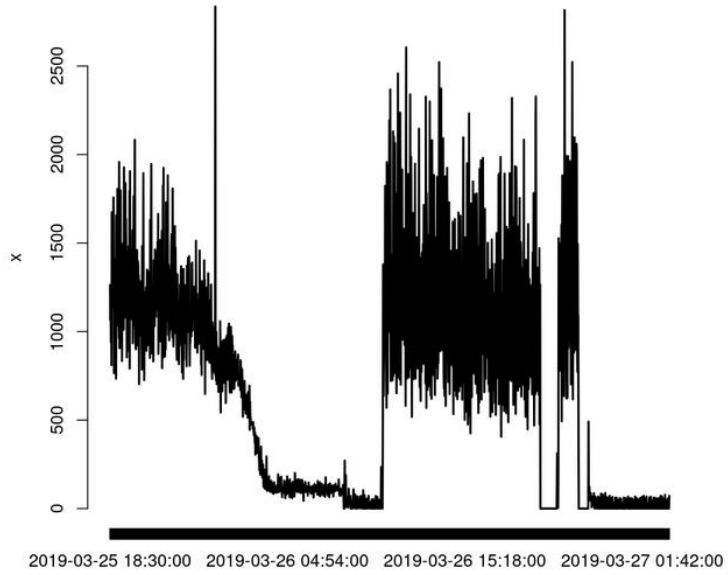
time	SRC	DST	PROTO	SPT	DPT
2019-03-25 18:30:29	192.168.50.102	216.58.201.99	UDP	57789	443
2019-03-25 18:30:29	192.168.50.102	8.8.8.8	UDP	58125	53
2019-03-25 18:30:30	192.168.50.102	172.217.23.234	TCP	51602	443
2019-03-25 18:30:30	192.168.50.102	216.58.201.110	UDP	57791	443
2019-03-25 18:30:30	192.168.50.102	216.58.201.110	TCP	51603	443
2019-03-25 18:30:30	192.168.50.106	216.58.201.99	TCP	50377	443

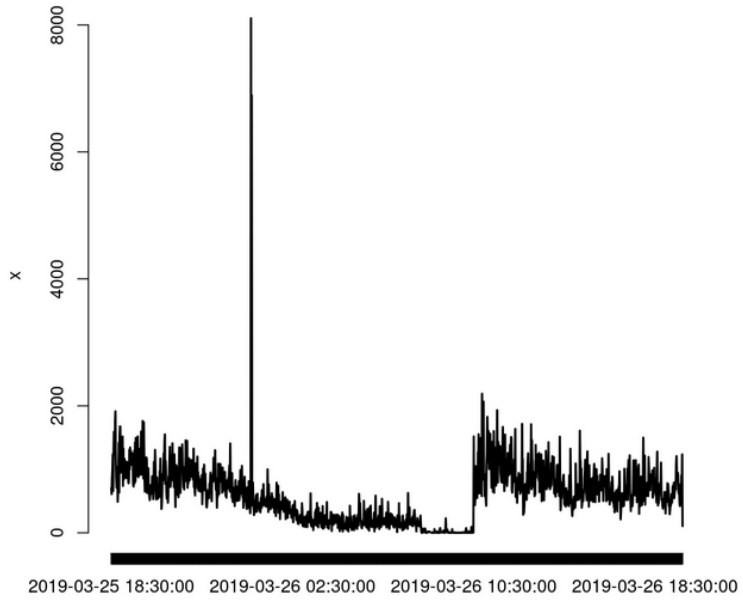
In [32]:

```
myplot <- function(x) {
    dates <- as.POSIXct(x$TimeCreated, format="%d.%m.%Y %H:%M:%S")

    x <- table(cut(dates, breaks="min"))
    plot(x, type = "l")
}

myplot(pc1_sec)
myplot(pc1_app)
myplot(pc1_sysmon)
myplot(pc1_system)
```





PC1 malware infection

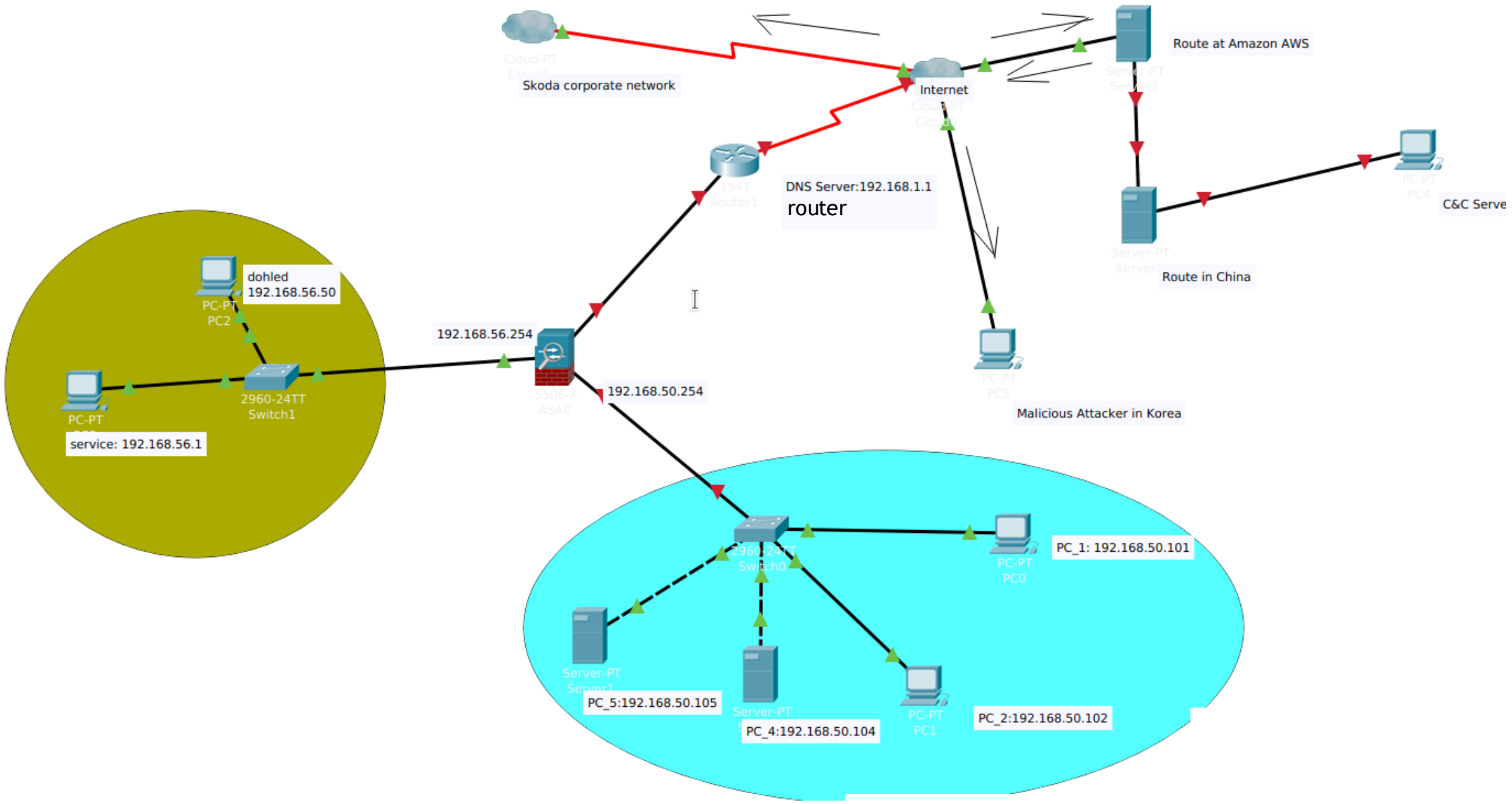
- explorer.exe otvára z plochy winword.exe súbor CV_template.docm
- winword.exe spúšťa cscript ""c:\users\.....\temp\MDnVBlZT.vbs
- V rovnakom čase PC1 spustený qmdmqrbg.exe -> "Korea"
- 26.3.-21:57:40 faulting application name: qmDmqRGb.exe (21:57:41 power off)

PC2 malware infection

- 26-22:07:04 otvorené putty_x64
- 26-22:09:22 putty_x64 spúšťa FWIsNAt.vbs
- 26-22:09:24 \user\AppData\local\temp\FWIsNAt.vbs spúšťa jvmzrcbznhdudp.exe (ten posiela requesty do "Skoda")
- 26-22:07:34 network connection putty_x64.exe do Skoda:443
- 26-22:14:42 putty otvára cmd -> hidden powershell pravdepodobne base64 encoded binárku

Útočníci

- Amazon + Čína – C2 server v pozadí (vedia o "Virtual machine" na 10.0.2.15)
- Korea ? (možno spolu s nimi)


Skoda corporate network
Internet
Route at Amazon AWS
DNS Server:192.168.1.1
router
Route in China
C&C Serve
dohled
192.168.56.50
PC-PT
PC2
PC-PT
service: 192.168.56.1
2960-24TT
Switch1
192.168.56.254
192.168.50.254
PC-PT
PC5
Malicious Attacker in Korea
PC_1: 192.168.50.101
PC-PT
PC0
Server-PT
PC_5:192.168.50.105
PC_4:192.168.50.104
PC-PT
PC1
PC_2:192.168.50.102

Ďalšie možné anomálie

- PC_6 chrome –gpu-preference= KAAAAA... -- možný overflow exploit
- chrome.exe "users local group membership enumerated"
- chrome.exe pokus o prihlásenie na "user"
- Empty.txt v temp adresári pod RDRBCC2.tmp, spustený pod chrome.exe

- Podozrivé adresy – porty – vyhľadali sme v CVE databáze, známe Trojany/backdoors, "Netbios" requesty mimo lokálnu sieť (do "Amazon")
- Aktivita v netradičný čas - mimo pracovnú dobu, v noci ...

- Po prvotnom prieniku do siete útočník pravdepodobne zmazal logy

Implementačná časť

- Azure BI + MSSQL vs grep + vim
  - Vyhral opensource :)
- Dokumentácia v githube