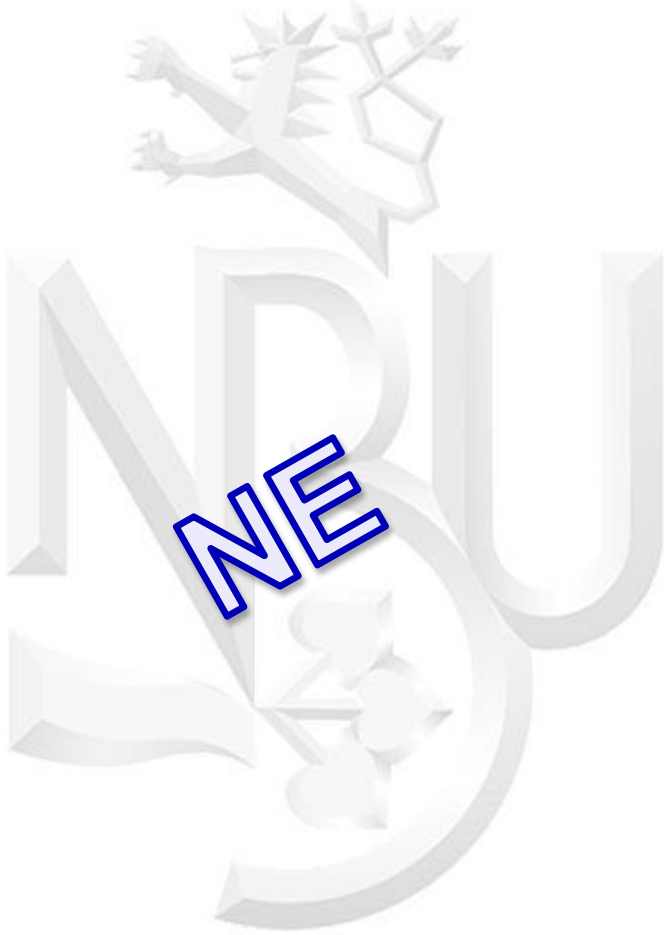

NBU

NBA a síťová bezpečnost ve státní správě

Mgr. Vladimír Rohel
pověřen řízením ICT
Národní bezpečnostní Úřad

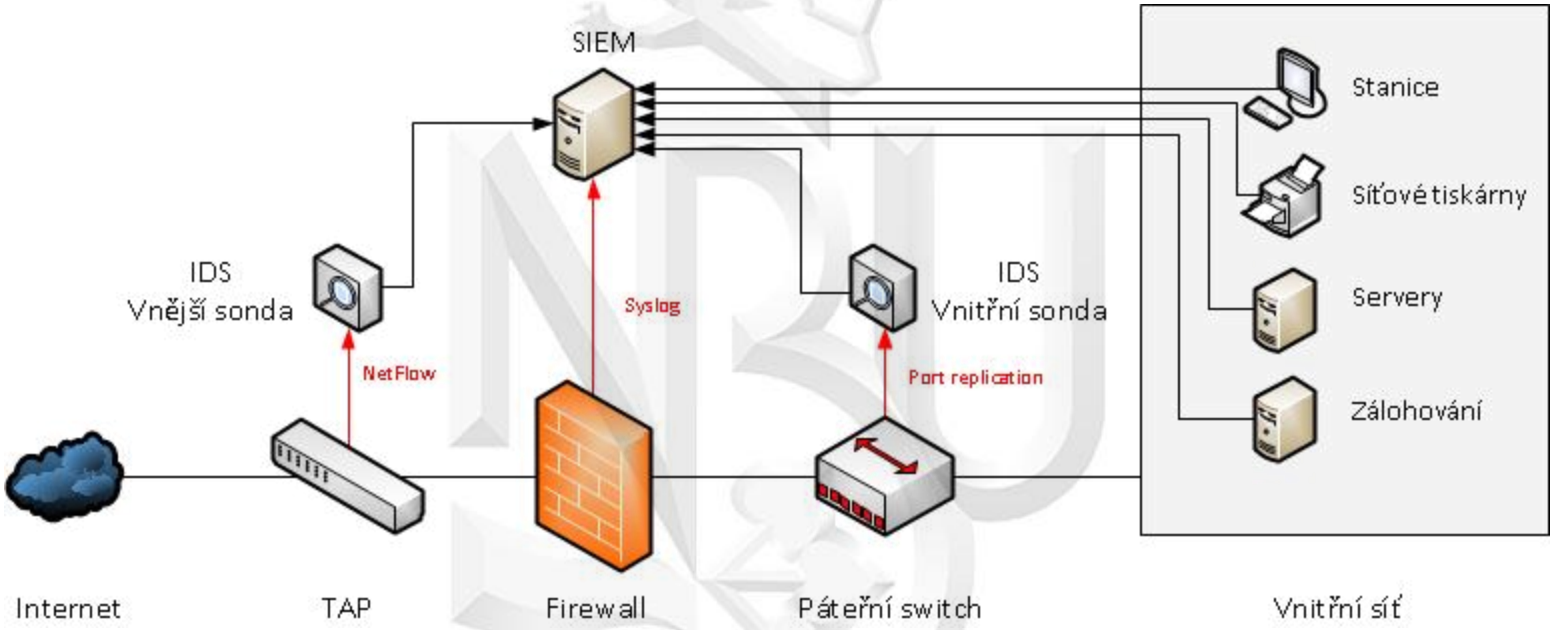
Přál jsem si NBA?

Znělo zadání pořídit behaviorální analýzu?



Co jsme tedy chtěli?

Naše řešení


SIEM
IDS
Vnější sonda
NetFlow
Syslog
IDS
Vnitřní sonda
Port replication
Stanice
Síťové tiskárny
Servery
Zálohování
Internet
TAP
Firewall
Páteřní switch
Vnitřní síť

Reporting I.


NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
ČESKÁ REPUBLIKA
NBÚ
Network Security Risk Report
Based on Network Behavior Analysis
Using Cognitive Analyst
August, 2012
support@cognitive-security.com
COSE
COGNITIVESECURITY

Reporting II.

Discovered activities, ordered by highest priority first

Activity 1: Objemný datový přenos – Low risk
Activity 2: Pokus o navázání pojení do Číny – For information only
Activity 3: Pokus o komunikaci se stanicemi ze světa – For information only
Activity 4: Multicastová komunikace v celé podsíti – Low risk
Activity 5: Zvýšení zátěže DNS serveru – Low risk
Activity 6: Uživatel ebay.com přistupuje k neznámé službě na port 82 – For information only
Activity 7: FTP přenos bez možnosti identifikace na vnitřní sondě – For infromation only
Activity 8: Přesměrování na neznámou službu na portu 1003 – For information only
Activity 9: Přesměrování na port 4051 pro nesouvisející adresy – For information only
Activity 10: Přesměrování na porty 8080, 8081 a 21 – For information only

Reporting III.

Activity 2: Pokus o navázání pojení do Číny – For information only

IP address:	192.168.4.128 I No reverse DNS
Asset identification:	192.168.4.0/24 – Windows stations subnet
Time span:	20.8.2012 11:41:17 – 20.8.2012 11:41:47 (29 seconds)
Business Impact:	Únik dat
Bookmark:	Link to the activity

Facts

1. Uživatelská stanice s IP 192.168.4.128 se pokusila navázat spojení na port 7024 se stanicemi ze světa, např:
   117.79.92.41 I No reverse DNS I China – Beijing
   117.79.92.44 I No reverse DNS I China – Beijing
   130.117.190.216 I No reverse DNS I United States – Washington
   202.177.216.233 I 233.193-254.216.177.202.in-addr.arpa I Australia – Sydney
   38.113.165.86 I No reverse DNS I United States – Bronx
   79.141.216.17 I ksn-msk-fe-1.kaspersky-labs.com I Russian Federation – Moscow
   79.141.216.19 I ksn-msk-fe-2.kaspersky-labs.com I Russian Federation – Moscow
2. V době kdy došlo k pokusu o spojení sloužila stanice dle informací jako pokusná stanice. Komunikace byla zastavena na úrovni firewall, jedná se proto pouze o pokus o komunikaci.

Interpretation

1. Symptomy komunikace ukazují na pokus aktivity nežádoucího softwaru typu malware. Došlo o pokus o komunikaci se vzdálenými stanicemi umístěnými Číně. U této komunikace existuje vysoké riziko potencionálního nebezpečí zneužití dat.
2. Aktivita může být důsledkem vědomé aktivity administrátora, protože stanice sloužila jako pokusná.

Recommendations

1. Ověřit účel a aktivity prováděné na stanici v době výskytu anomální komunikace tak, aby byla vyloučena možná kompromitace stanice nežádoucím sw.
2. V případě, že se jedná o vědomou aktivitu, doporučujeme ověřit, že je pokusná stanice dostatečně izolovaná od zbytku sítě.

COSE
COGNITIVESECURITY

Reporting IV.

Výstup ověření aktivity

Po ověření aktivity administrátorem bylo zjištěno vědomé použití testovacího notebooku s live CD Kasperski. Doporučujeme izolovat podobné pokusné aktivity od zbytku sítě. Riziko aktivity bylo po ověření sníženo z High risk na For information only.

Illustration: Activity overview

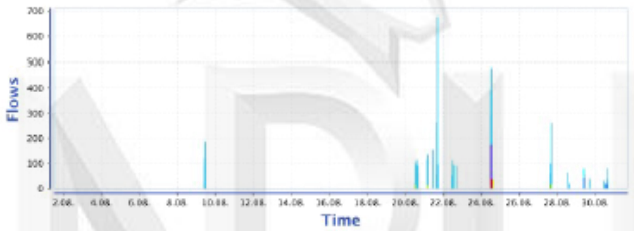


Illustration: Activity context

S	Type	First Incident	Last Incident	Activities	Flows	Bytes
9	port scan (horizontal, tcp)	24.8.2012 12:14:10	24.8.2012 12:14:29	1	38	9 920
	Source → Target	Start Time	End Time	Events	Flows	Bytes
	192.168.4.128:* → *:443	24.8.2012 12:14:10	24.8.2012 12:14:29	1	38	9 920
S	Type	First Incident	Last Incident	Activities	Flows	Bytes
5	unclassified behavior	20.8.2012 11:41:17	27.8.2012 15:38:09	3	131	65 109
	Source → Target	Start Time	End Time	Events	Flows	Bytes
	192.168.4.128:* → *:*	24.8.2012 11:58:55	24.8.2012 14:16:14	3	84	57 898
	192.168.4.128:* → 224.0.0.252:5355	27.8.2012 03:00:20	27.8.2012 15:38:09	2	31	6 440
	192.168.4.128:* → *:7324	20.8.2012 11:41:17	20.8.2012 11:41:47	1	16	902
S	Type	First Incident	Last Incident	Activities	Flows	Bytes
4	data transfer (tcp)	9.8.2012 10:00:16	9.8.2012 10:26:09	2	2	2 751 676
	Source → Target	Start Time	End Time	Events	Flows	Bytes
	192.168.4.128:49305 → 15.240.238.52:43629	9.8.2012 10:00:16	9.8.2012 10:05:19	1	1	1 320 452
	192.168.4.128:49474 → 15.240.238.56:44745	9.8.2012 10:21:05	9.8.2012 10:26:09	1	1	1 431 224
S	Type	First Incident	Last Incident	Activities	Flows	Bytes
4	scan-like behavior (horizontal, tcp)	24.8.2012 11:18:14	24.8.2012 11:23:54	1	173	77 838
	Source → Target	Start Time	End Time	Events	Flows	Bytes
	192.168.4.128:* → *:80	24.8.2012 11:18:14	24.8.2012 11:23:54	1	173	77 838

COSE
COGNITIVESECURITY

Reporting V.

Povinné vypořádání každého incidentu

Activity 2: Pokus o navazani pojeni do Činy – High Risk

V době výskytu události se jednalo o testovací notebook. Podle vyjádření administrátora bylo testováno live CD kaspesrsky.

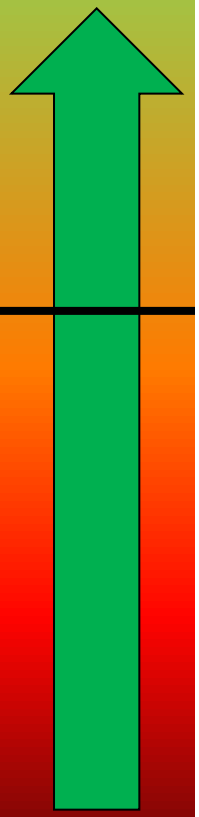
Z pohledu bezpečnosti se nejedná o bezpečnostní riziko. Tato událost by se z dané stanice již neměla opakovat.

Co dál?

- Jsme schopni „zajatce“ podrobit analýze:
  - Vlastními silami
  - Vládním CERTem
- Jsme schopni brát „zajatce“ (automaticky)

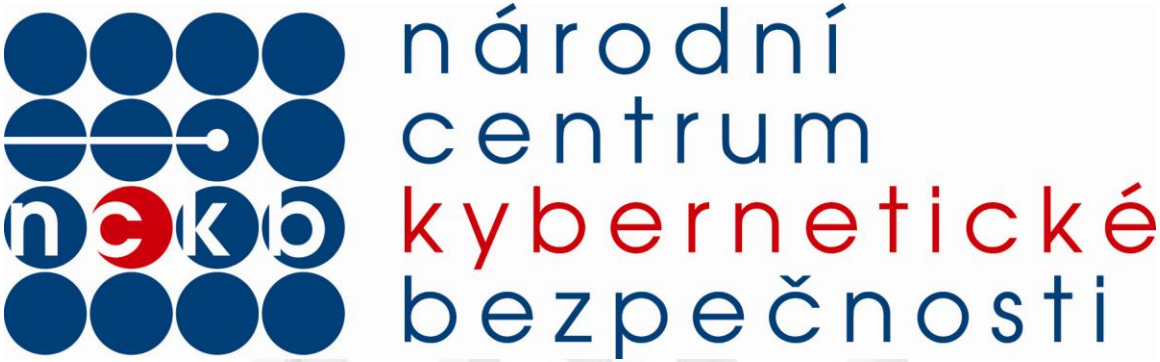
- Jsme schopni útok odlišit od normálního provozu (automaticky a v reálném čase)

- Útok nemá vliv na provoz a práci uživatelů
- Jsme schopni odolávat většině útoků
- Je vystavena robustní ochrana



Proč tedy sledovat svou síť, porovnávat a vyhodnocovat?

- detailní přehled o dění v síti
- z toho plyne optimalizace provozu, struktury sítě, konfigurací serverů i stanic, instalací,...
- lepší detekce incidentů v síti
- posílení sledování anomálií - možnost vysledovat i sofistikovanější útok ukrytý do běžného provozu
- pro státní správu a KII bude v budoucnu povinnost hlásit kybernetické incidenty vládnímu CERTu (součást NBÚ) - připravovaný zákon



Mgr. Vladimír Rohel

ředitel

Národní centrum kybernetické bezpečnosti

v.rohel@nbu.cz

http://www.govcert.cz/