Flowmon
Networks

Anatomy of Ransomware Attack

AFCEA: Kybernetická bezpečnost VIII.

Pavel Minarik, Chief Technology Officer

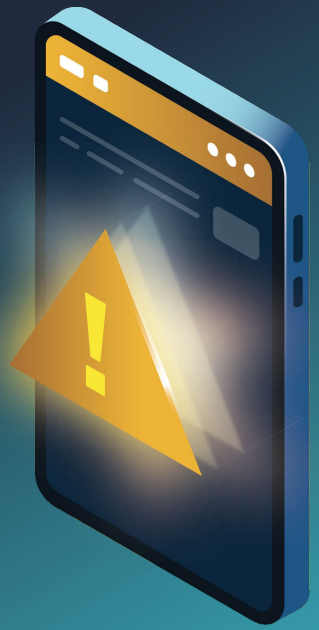
Prevention consumes 90% of budget

Firewall protects perimeter, but what if it's bypassed?

Endpoint protection can be evaded

On average it takes 197 days to identify a breach

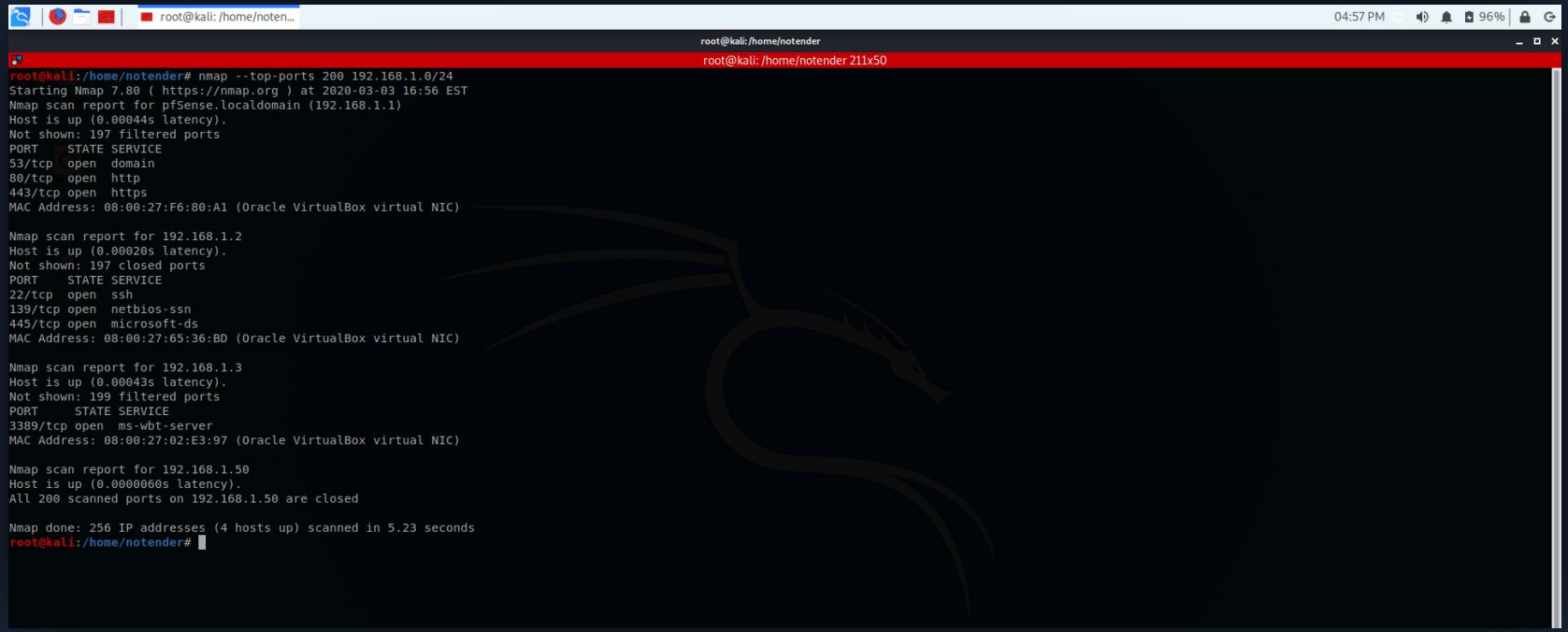
Source: Cost of a Data Breach Study, Ponemon Institute



Attacker activity starts now

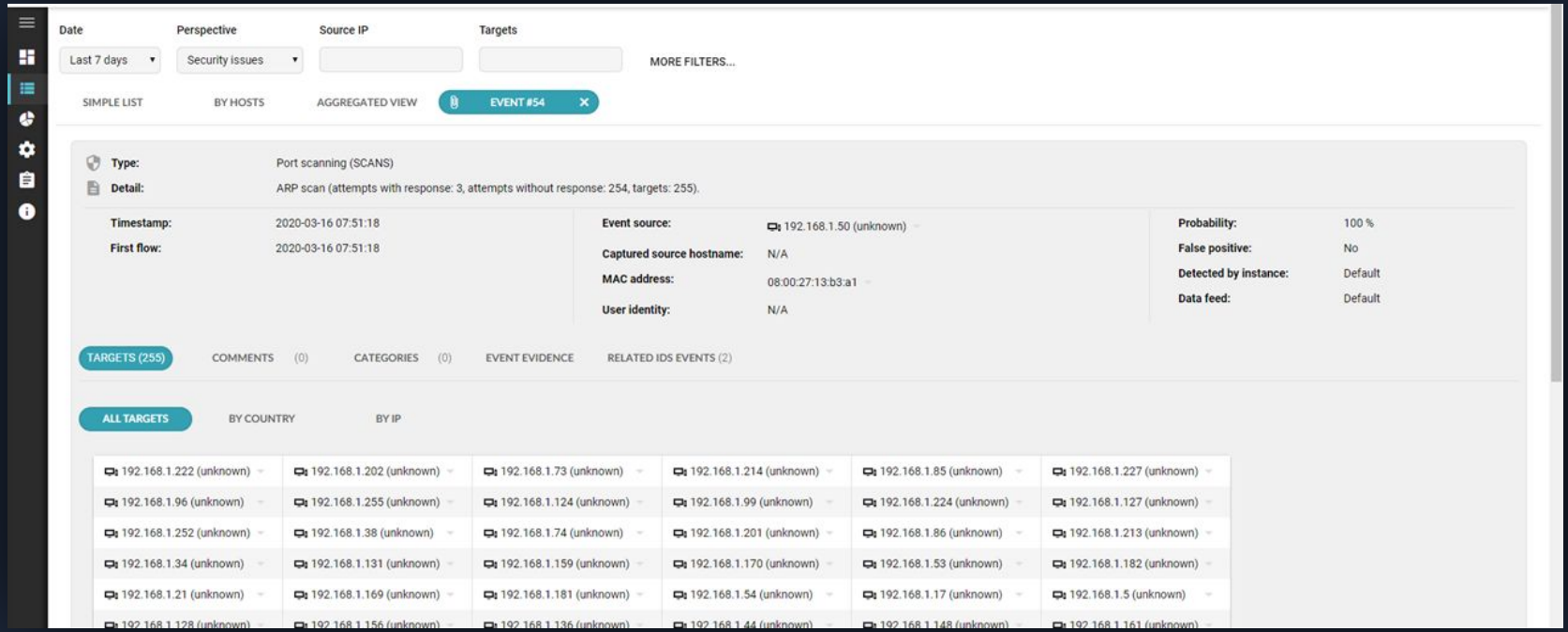
Discovery

Attacker seeking critical systems.



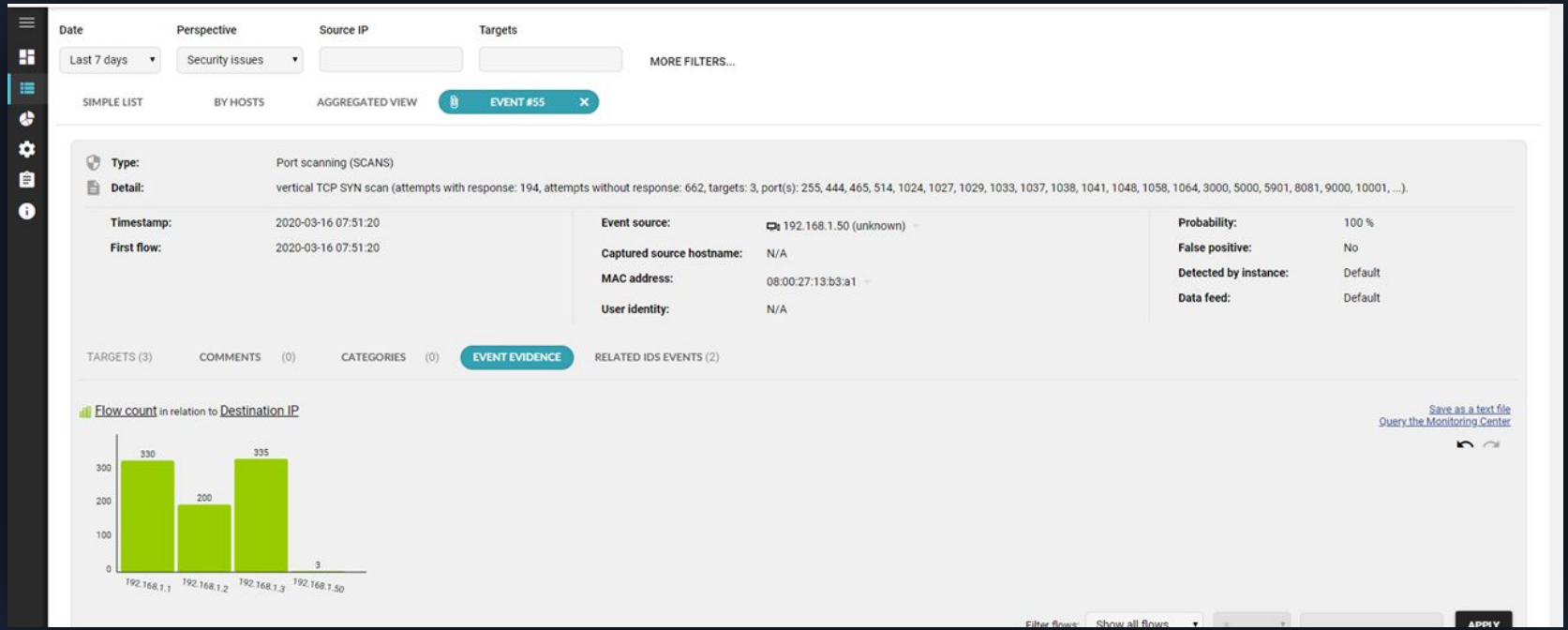
ARP Scan

Source 192.168.1.50, enumeration of active neighbor hosts on the network.



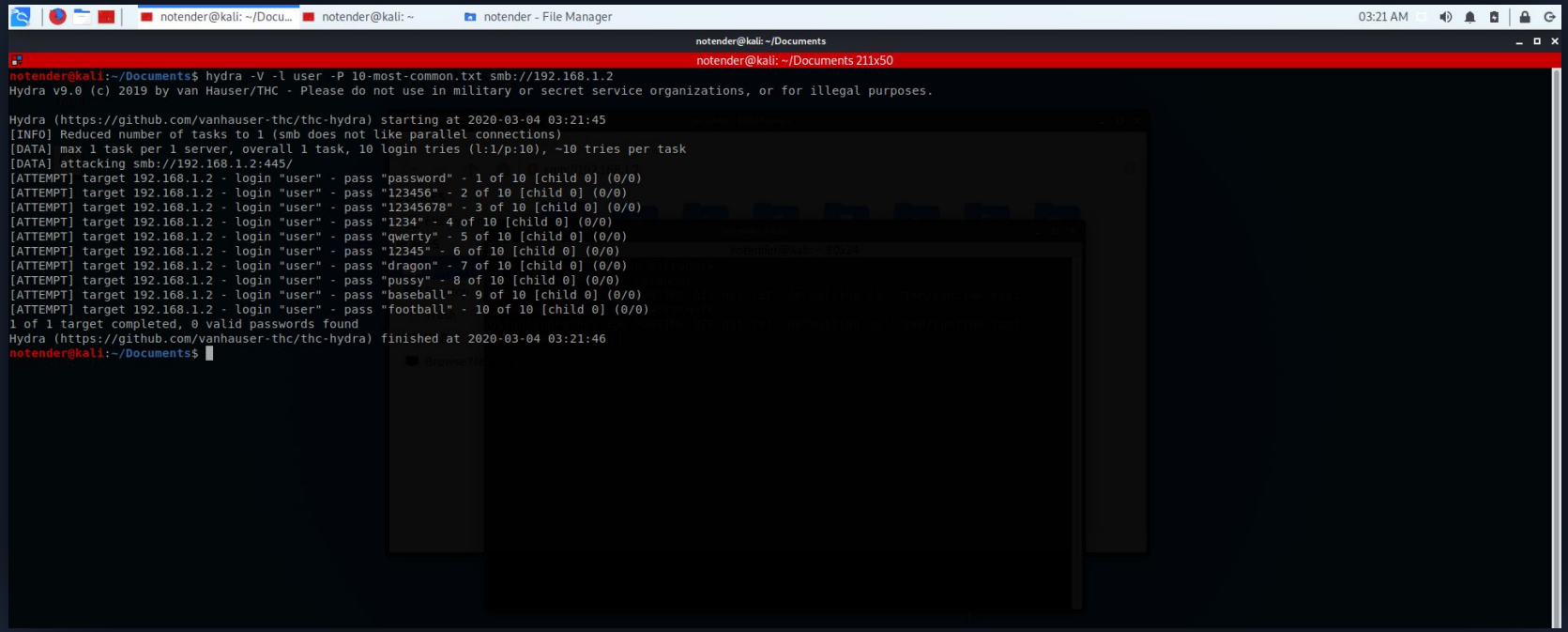
Vertical TCP SYN

Scan against 3 targets previously discovered to find potentially vulnerable services.



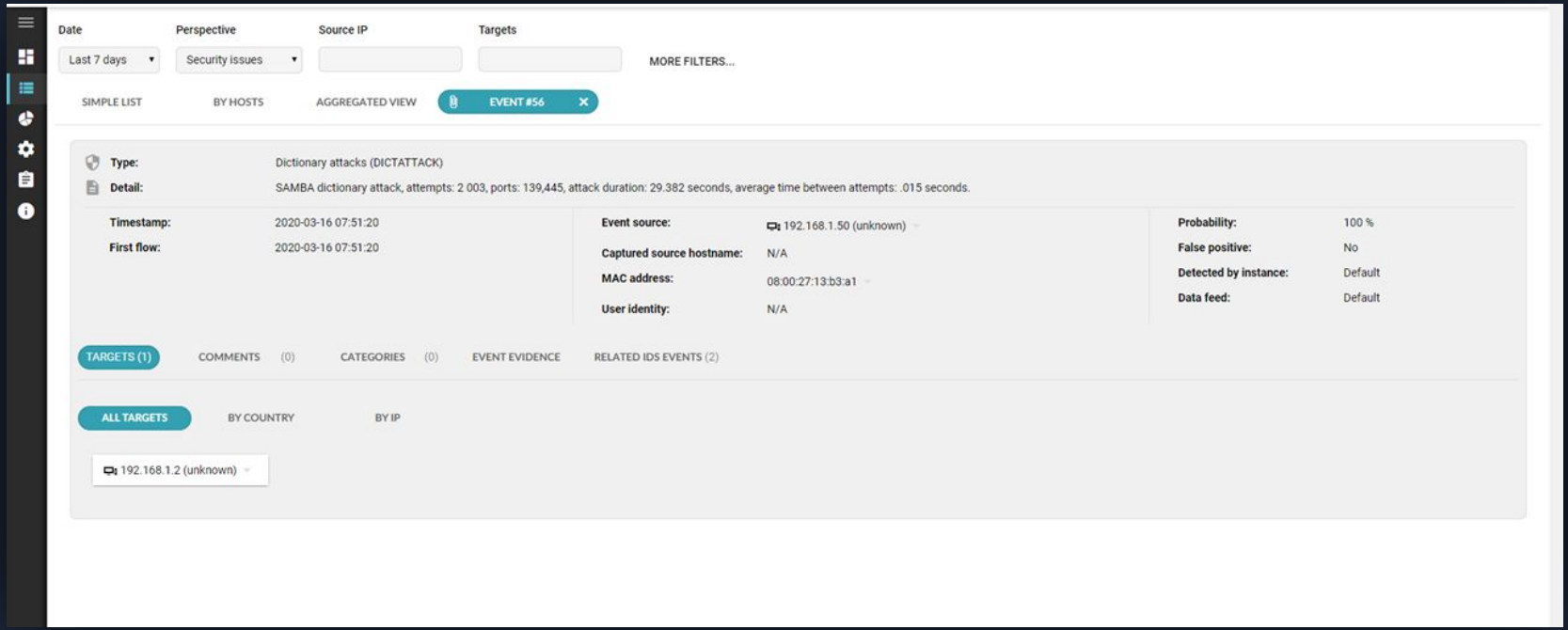
Credential Access

Password spraying against Samba server.



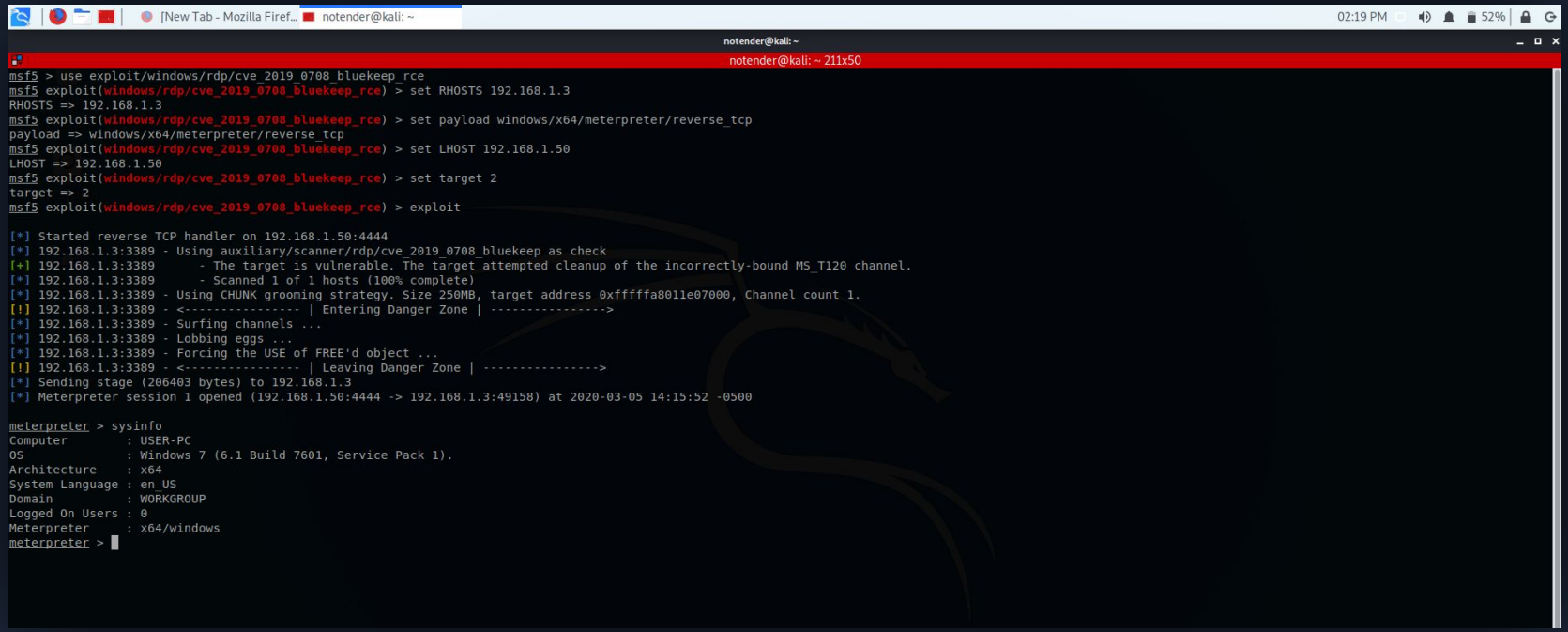
Samba Brute Force Attack

Source 192.168.1.50, target 192.168.1.2, brute force on user credentials.



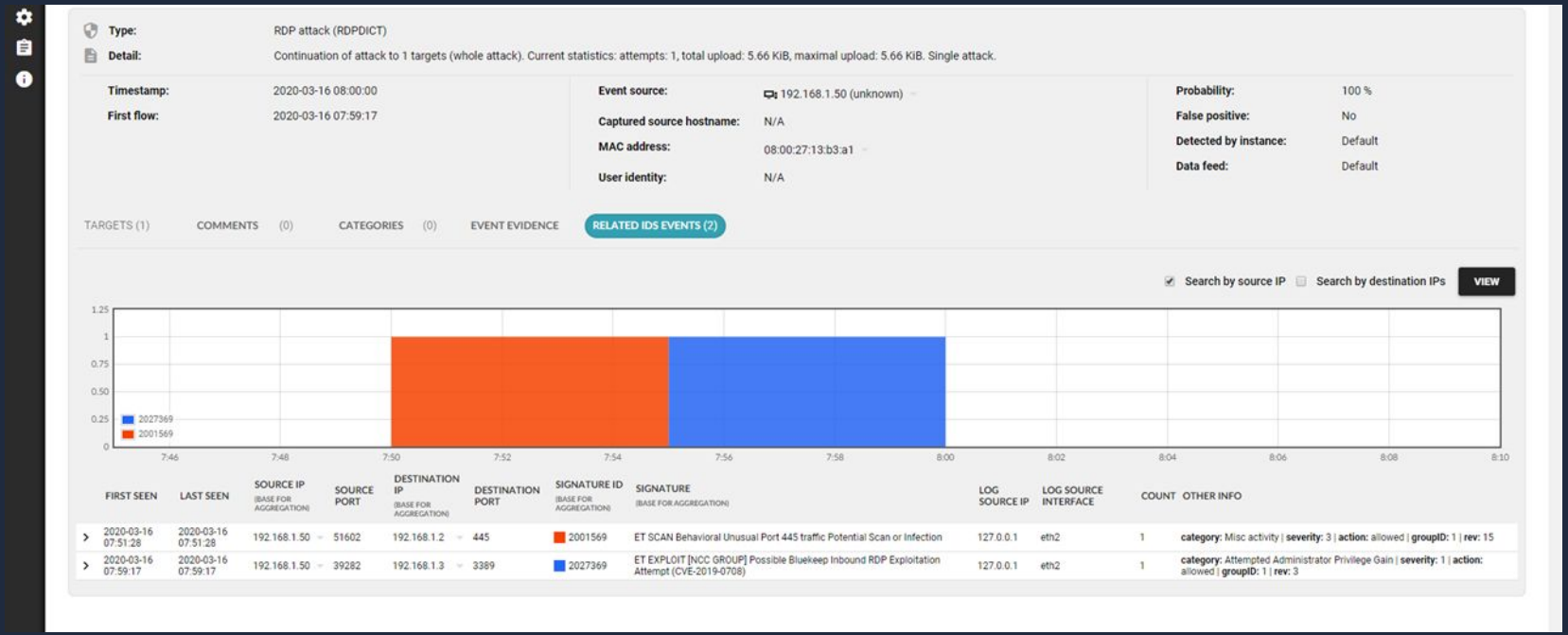
Lateral Movement

Attacker exploited Bluekeep vulnerability of RDP protocol.



RDP Attack

Attack against RDP using **Bluekeep vulnerability** (CVE-2019-0708).

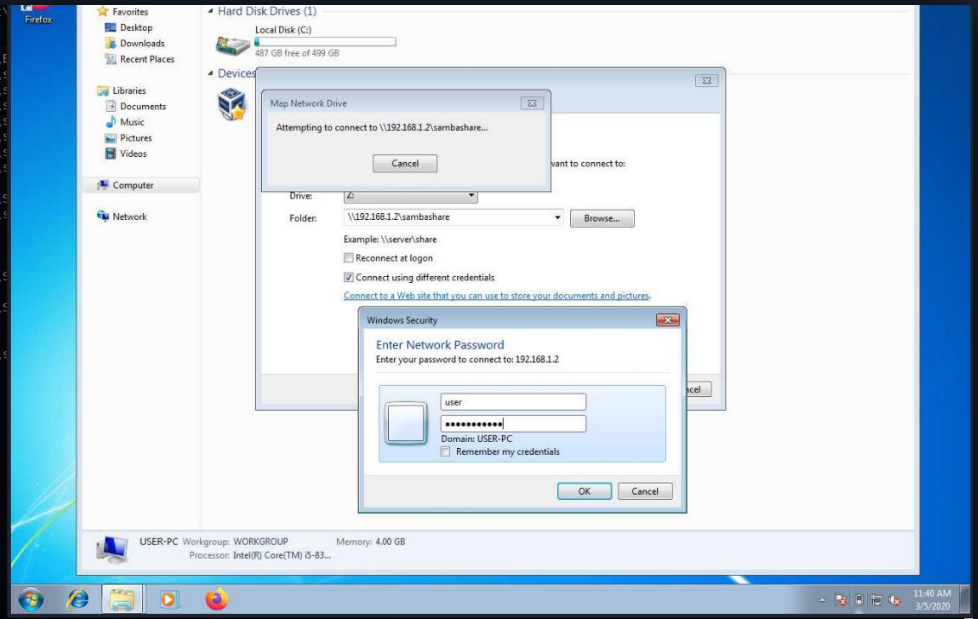


Input Capture

Attacker installed keylogger on the Windows device to collect credentials.

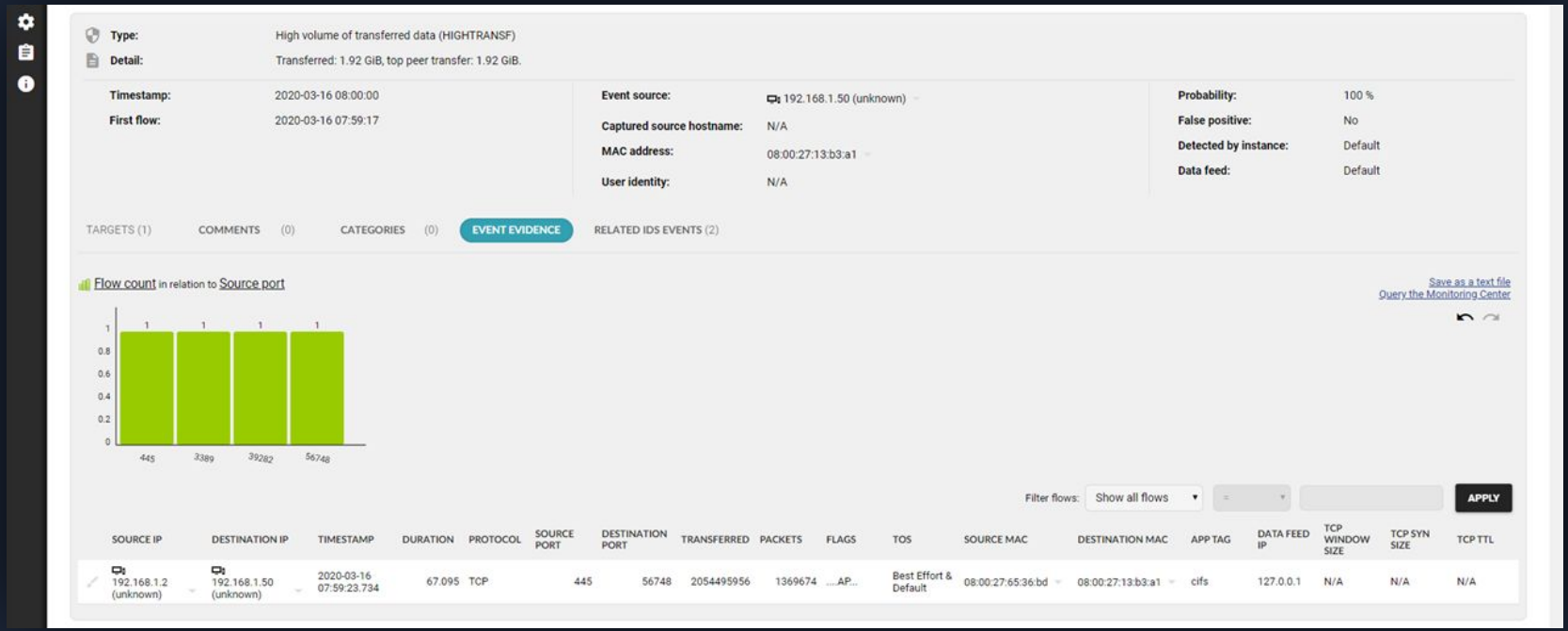
```
 268   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\
 300   480   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 320   480   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 324   1912  explorer.exe      x64   1        user-PC\user                  C:\Windows\E
 352   344   csrss.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 404   344   wininit.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 416   396   csrss.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\S
 480   404   services.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 496   404   lsass.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 504   404   lsm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 512   396   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Windows\S
 632   480   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 696   480   VBoxService.exe   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 708   888   dwm.exe           x64   1        user-PC\user                  C:\Windows\S
 752   480   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 804   480   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 888   480   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 932   480   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\S
 972   480   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
1112   324   VBoxTray.exe      x64   1        user-PC\user                  C:\Windows\S
1144   480   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
1340   480   SearchIndexer.exe x64   0        NT AUTHORITY\SYSTEM
1572   480   taskhost.exe      x64   1        user-PC\user                  C:\Windows\S
1740   480   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
1856   480   wmpnetwk.exe      x64   0        NT AUTHORITY\NETWORK SERVICE
1964   480   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
1996   480   sppsvc.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
2032   480   svchost.exe       x64   0        NT AUTHORITY\SYSTEM

meterpreter > migrate 324
[*] Migrating from 932 to 324...
[*] Migration completed successfully.
meterpreter > keyscan start
[-] Unknown command: keyscan.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > screenshot
Screenshot saved to: /home/notender/EMAosZtD.jpeg
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Left Windows>computer<CR>
\\192.168.1.2\sambashareuser<Tab>password123
```



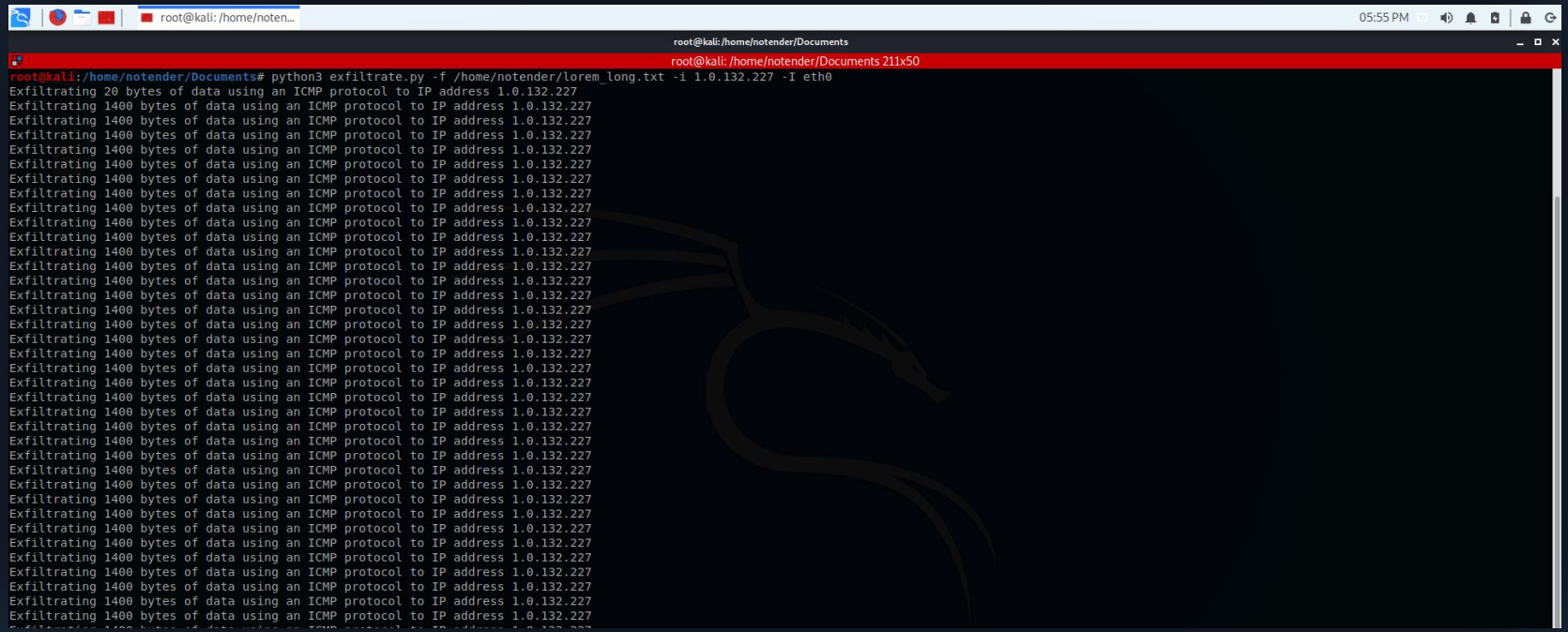
High Data Transfer

Attacker is hoarding company sensitive data from 192.168.1.2 server.



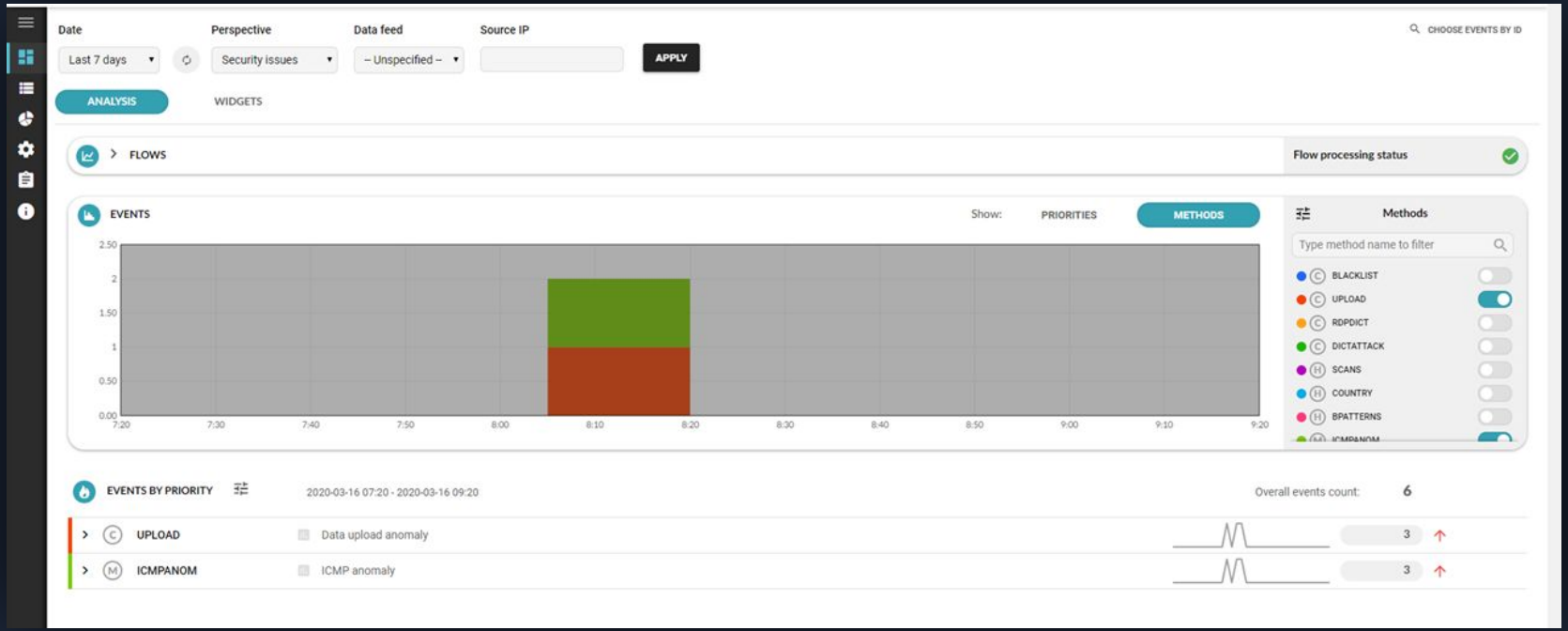
Exfiltration

Attacker splits data in chunks and exfiltrate it via ICMP (ping).



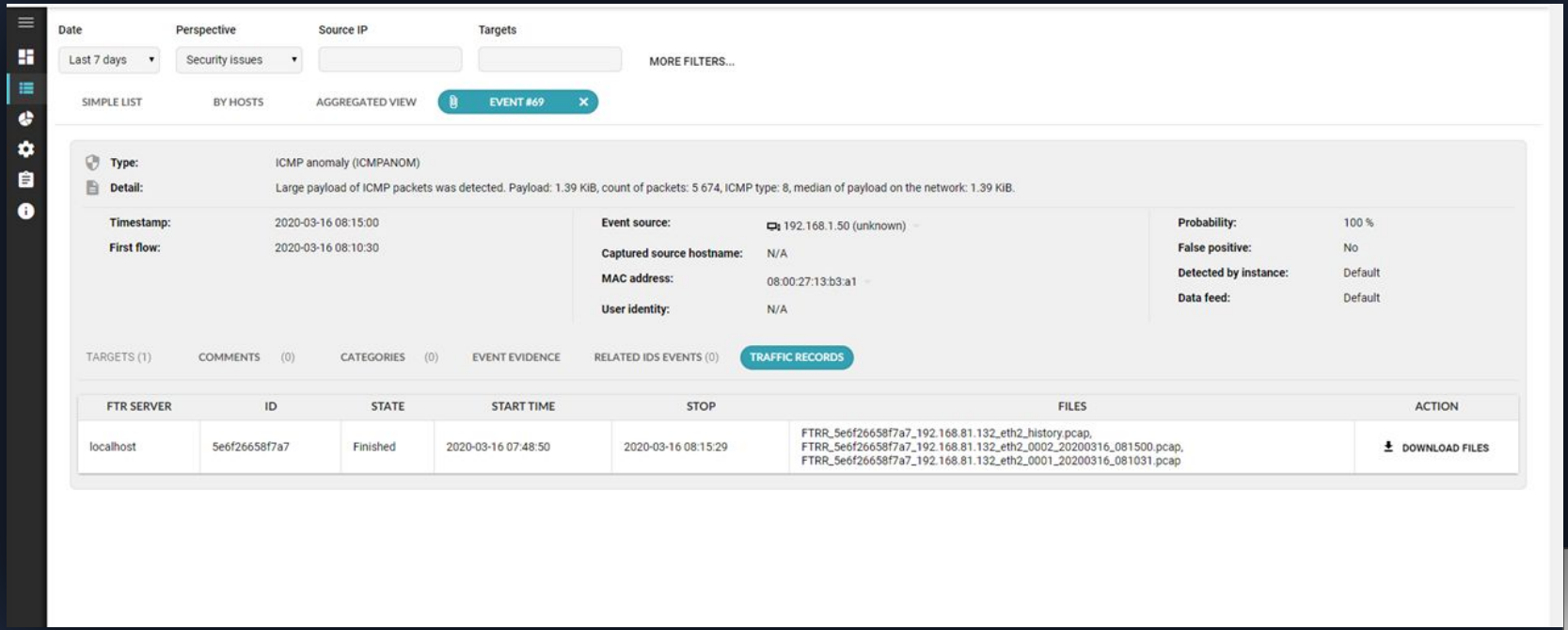
Exfiltration Over Alternative Protocol

Detection based on adaptive baselining.



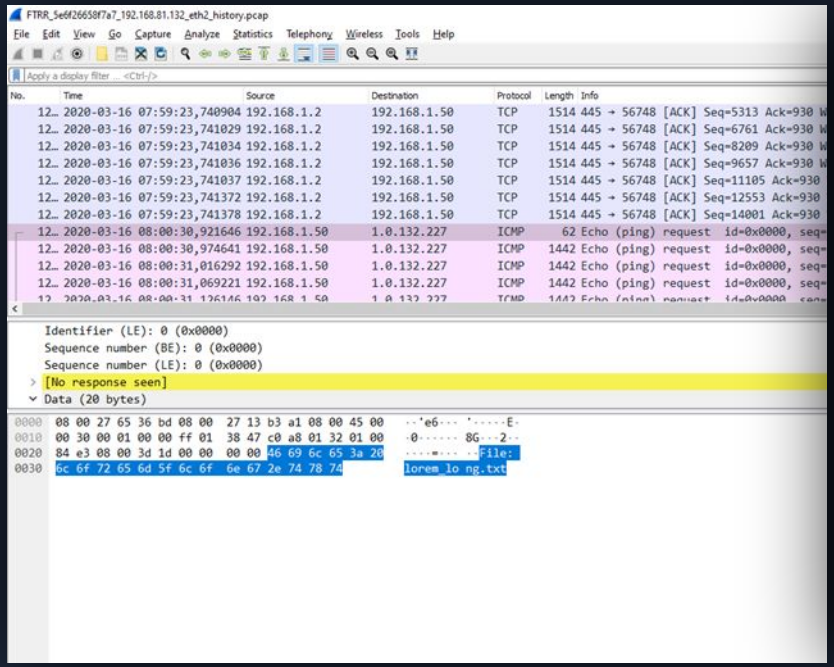
Suspicious Payload

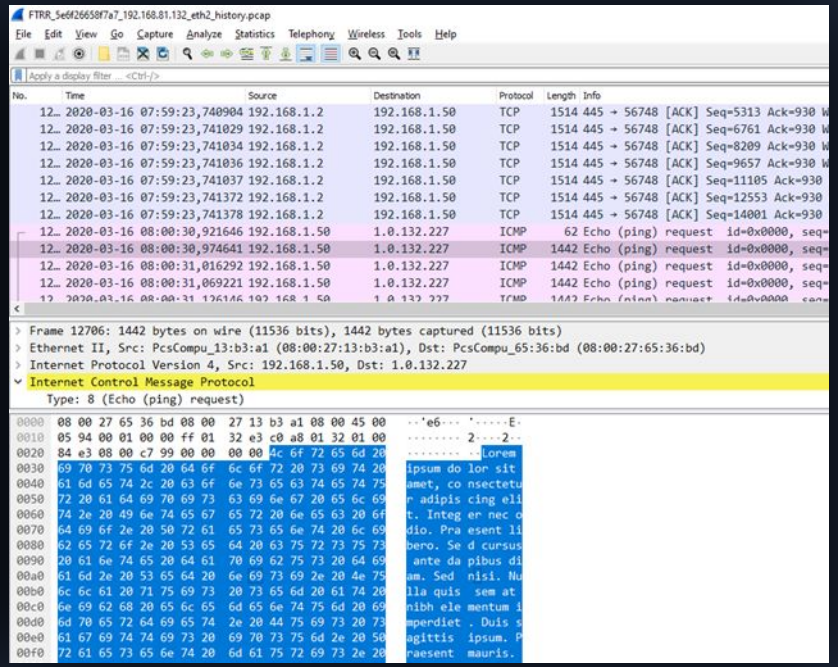
ICMP packets with suspicious payload detected. Capture triggered to provide full packet traces.



Exfiltrated File Detail

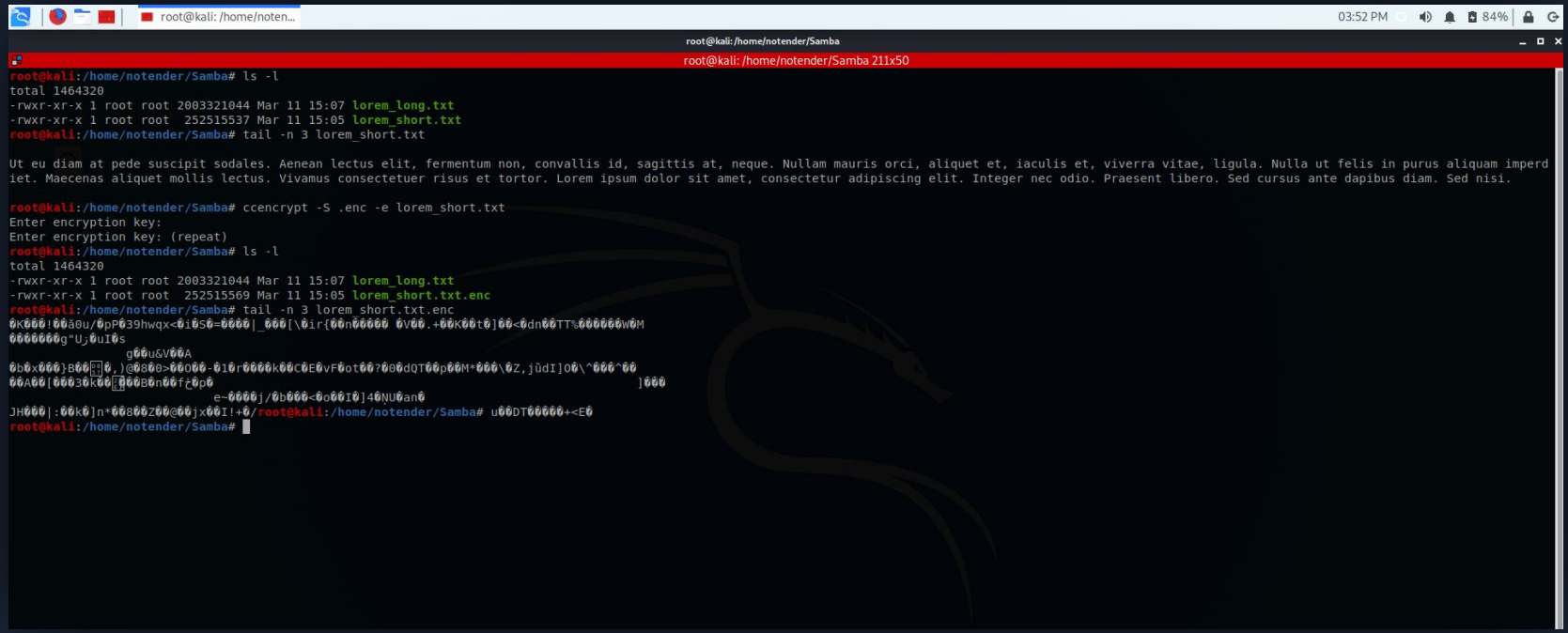
Full packet trace in Wireshark showing the **exfiltrated file** name and content.





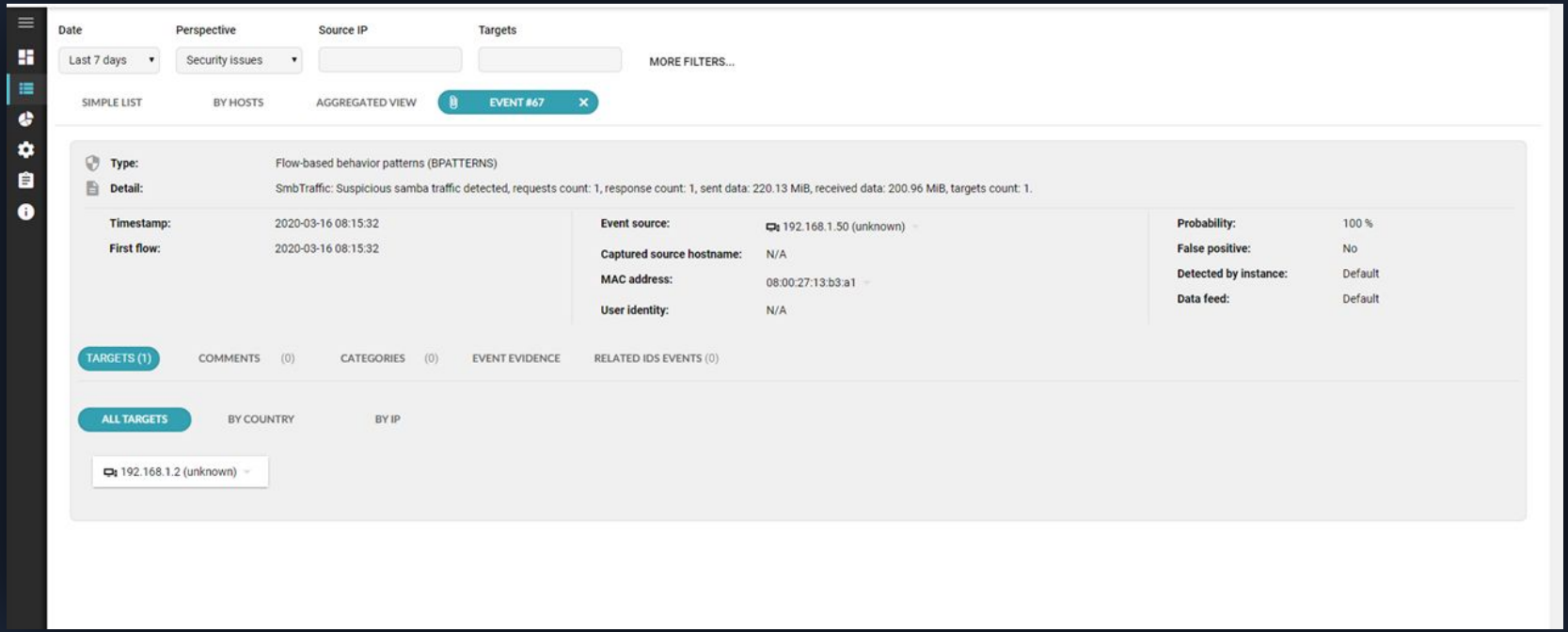
Impact

Data encrypted on network share. Destructive action taken.



Suspicious Samba Traffic

Detected on network share, this indicates data encryption.



Dear business owner,

you either pay 2.5 bitcoin for recovering the data we have encrypted or 2.5 bitcoin for not publishing your confidential data (see sample attached) on the internet. Please select the option of your preference.

YOUR ATTACKER

Incident detection summary

Input data

Network telemetry (flow data), reputation feeds, IDS signatures, full packet data.

Detection algorithms

Machine learning, adaptive baselining, behavior analysis, heuristics, reputation-based and signature-based.

Provided evidence

Events, network telemetry, packet capture.

Questions