HOW TO USE THE NETWORK: CYBERSECURITY'S SECRET WEAPON

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 Exfil[1]

INDUSTRY AVERAGE

6 Days

To Remediate

SEC ADOPTED RULE

4 Days

To Disclose Material Cybersecurity Incident[2]

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.

EXTRAHOP

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.
- Targetting reconnaisance, *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	• 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.	• 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.	• 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.	• 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
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.	**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.
	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.
	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.
	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.
	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.
	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.

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:** $625,000\ \text{MB/s} \times 60\ \text{s/min} \times 60\ \text{min/hr} \times 24\ \text{hr}$.

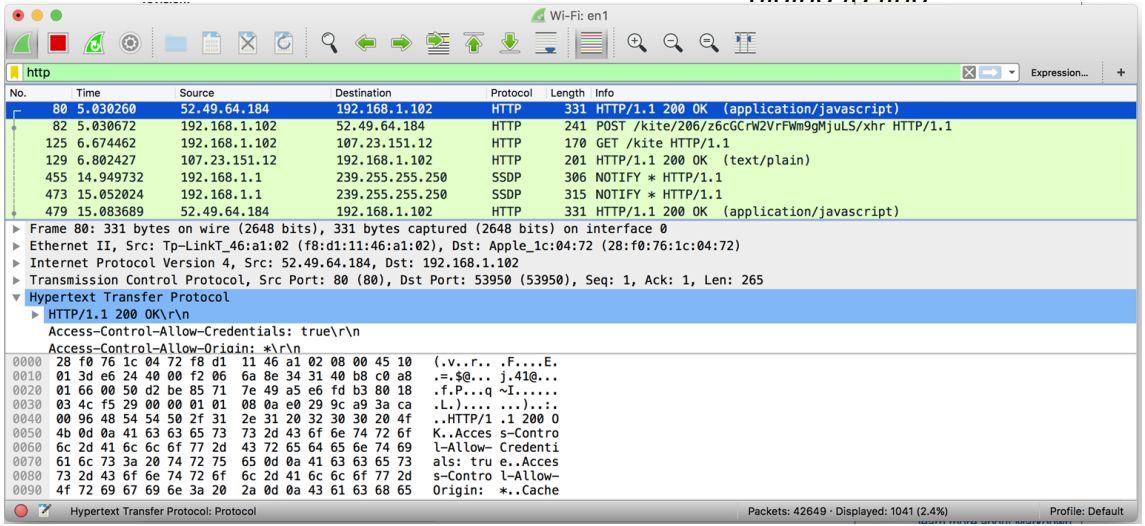
Let's compute this to get the total data volume in a more readable unit, like terabytes (TB).

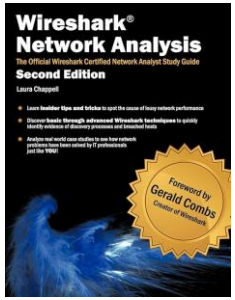
Under the assumption of 5% average utilization of their 1 Gb/s capacity, a network of 100,000 devices would typically generate about **54,000 terabytes** (TB) of traffic over a 24-hour period. This estimate serves as a rough indication and the actual traffic could vary significantly based on actual network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

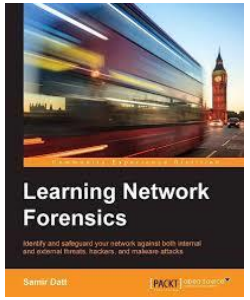
Hunting in packets

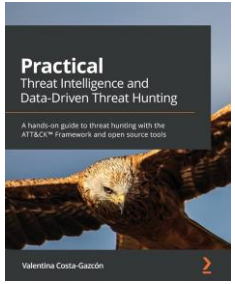
What do the tools look like?

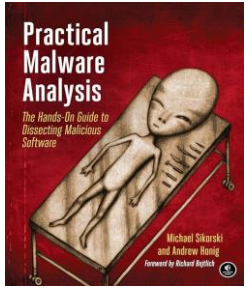
“Threat hunting in the network is like playing hide and seek – but you don’t know for certain there is even someone hiding to find”











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

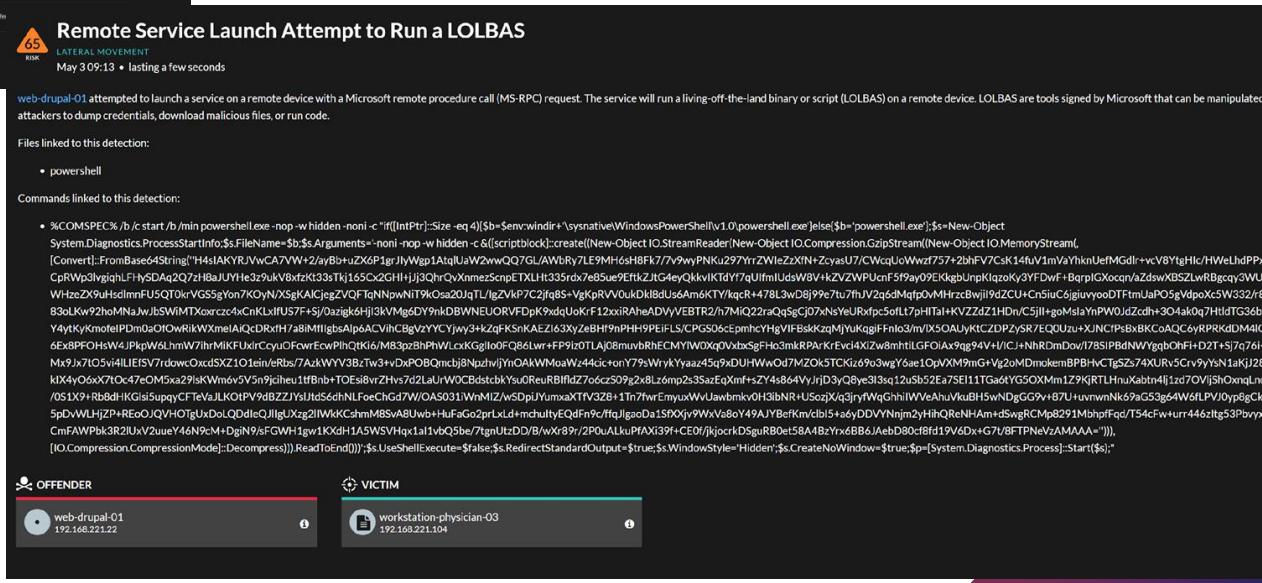
Investigations based on mass visibility and monitoring of devices at a scale that allows for highly nuanced discovery of anomalies that would otherwise be impossible to spot.

*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?

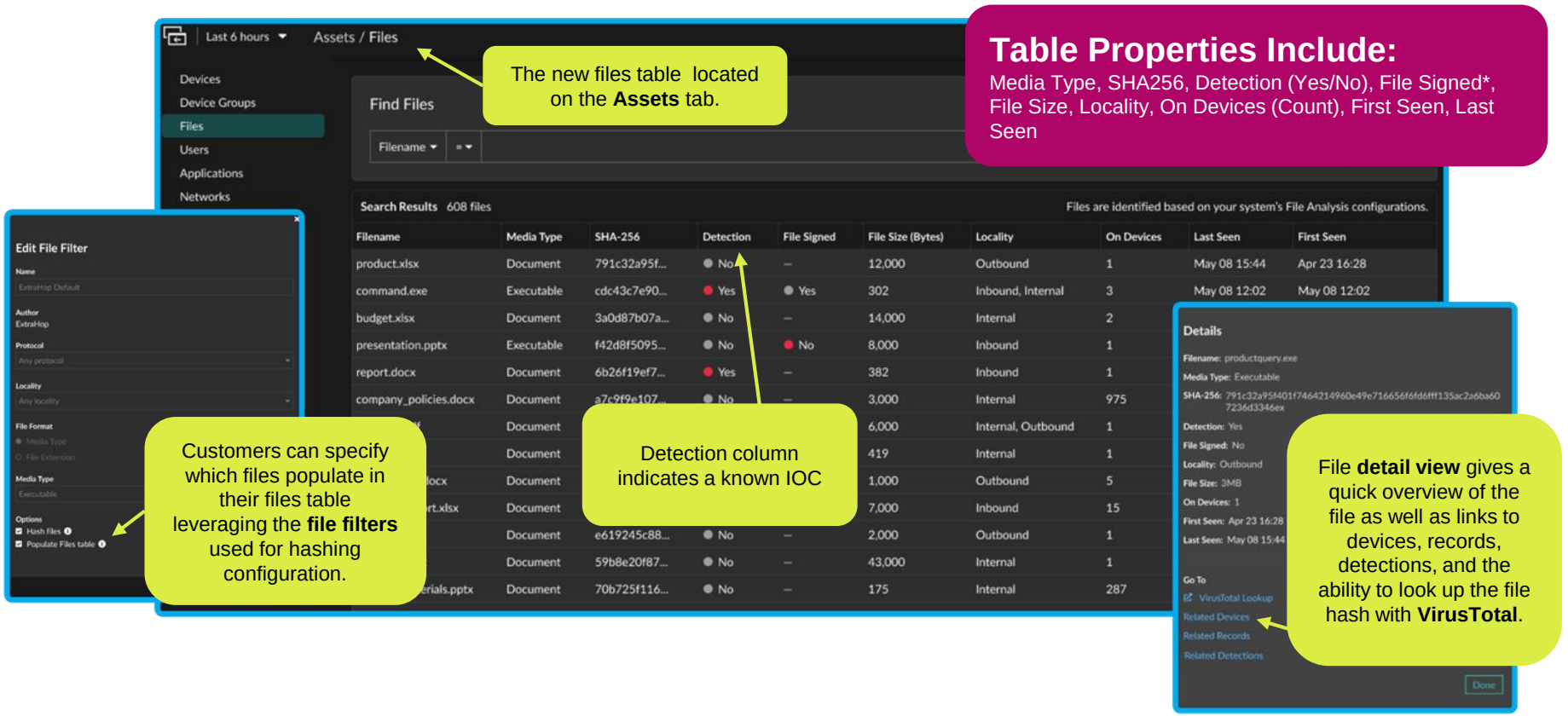
Let NDR do the hard work, while you get on with more interesting things!

Automated attack chain discovery and correlation



Solve and evidence lateral movement with Microsoft protocol decryption

File-Based Detection, Investigation & Threat Hunting



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

> ExtraHop provides insight that is critical to delivering a seamless and secure experience
> for our customers and associates.
>
> **Distinguished Engineer**
> The Home Depot

Thank You

EXTRAHOP