Unexpected Outbound Protocol (UNX-OBP)

Why?

- Successful adversary operations often enough != sophistication
- There's no way around doing the work of knowing your network—be the hunter
- Proactive lead generation
- Reduce dwell time, raise cost to adversary

While HTTP(S)/DNS are top C2 channels, both cybercriminal and nation state actors still routinely use non-web protocols with standard and non-standard ports for both early and later stage operations.

Specific Recent Examples

Threat	Outbound Protocols
Agent Tesla	FTP, SMTP
APT29 CredoMap Stealer	IMAP
Gamaredon	ICMP, VNC
ZINC (North Korean APT)	SSH, VNC
Cuba Ransomware Group	ICMP, SSH
Common Log4Shell Callbacks	LDAP, RMI
AA22-320A (Iranian APT)	LDAP, ICMP

Generally, UNX-OBP applies to these MITRE ATT&CK Techniques

T1016.001: Internet Connection Discovery

T1071: Application Layer Protocol

T1095: Non-Application Layer Protocol

T1571: Non-Standard Port

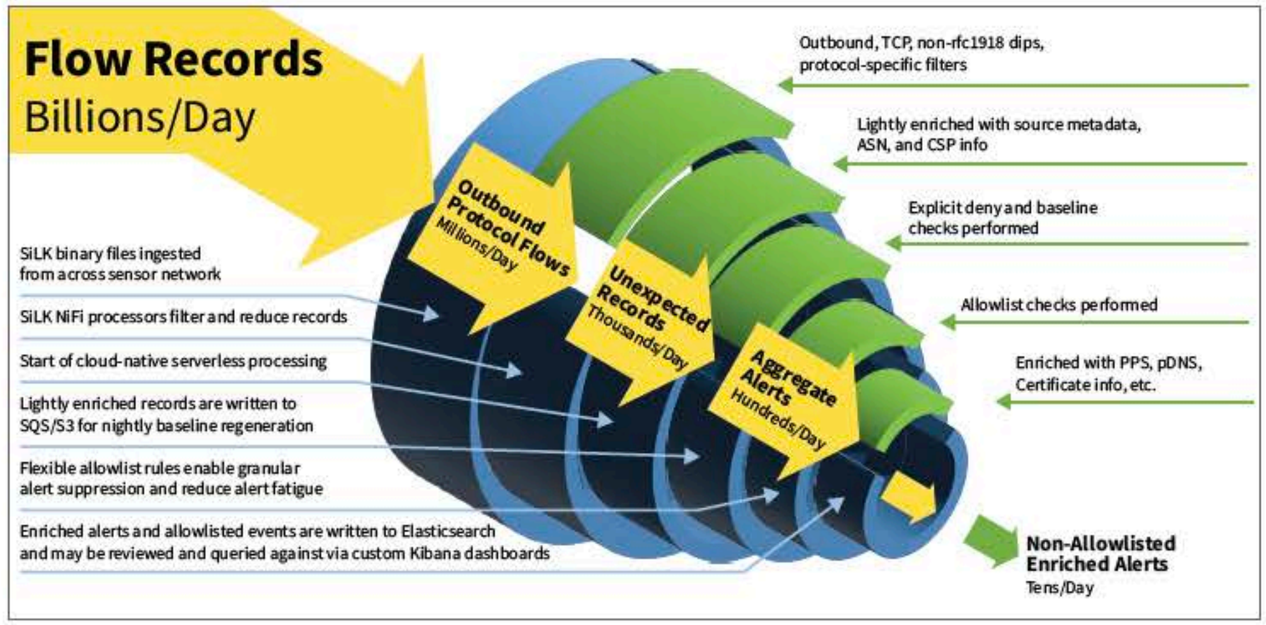
T1572: Protocol Tunneling

T1041: Exfiltration Over C2 Channel

T1042: Exfiltration Over Alternative Protocol

Your network is essentially foreign territory to an adversary, who must discover where they've landed and make certain assumptions about the environment, which almost never fully aligns with how your network actually operates.

Move beyond reactive signature-based analysis and detection. Generate **per protocol baselines** of **outbound traffic** on various anchor flow characteristics and highlight **new, rarely seen, or inconsistent** protocol traffic in near real-time.



Anchor Tuples

2022-10-29T18:28:29.096|179|77.133.124.81|11.79.190.68|55428|445|6|139|67270|112|331.688

Lightly enriched flow

2022-10-29T18:28:29.096|**FLDC**|179|77.133.124.81|11.79.190.68|55428|445|6|139|67270|112|331.688|**11.0.0.0/8**|749|US|arin|DNIC-AS-00749, US

Baseline measurements calculated on the **Full Anchor Tuple (FAT)**

2022-10-29T18:28:29.096|**FLDC**|**179**|**77.133.124.81**|**11.79.190.68**|55428|**445**|6|139|67270|112|331.688|**11.0.0.0/8**|749|US|arin|DNIC-AS-00749, US

As well as the **Partial Anchor Tuple (PAT)**

2022-10-29T18:28:29.096|FLDC|**179**|77.133.124.81|11.79.190.68|55428|**445**|6|139|67270|112|331.688|**11.0.0.0/8**|749|US|arin|DNIC-AS-00749, US

Configurable Thresholds per Protocol

- perc_days_seen—the minimum percentage of days that the PAT of an incoming flow must have been seen in the baseline (typically the last 90 days) in order to be considered "commonly occurring"
- consistency_score—the lowest acceptable consistency score (explained below)

The consistency score starts at 100 and various deviation checks are performed. For each deviation, some number of points is deducted. For packets, bytes, and duration, we only care about deviations which are higher than usual. We weigh deviations in applications seen and bytes more than other deviations.

Alert Types

EXPLICIT_DENY—the incoming flow matched one of the rules this protocol's explicit deny / watch list

NEVER_SEEN_IN_BASELINE—the PAT of the incoming flow is not in the baseline

SEEN_BUT_RARELY_OCCURRING—the PAT of the incoming flow was historically seen occurring less often than the set threshold for the given protocol

SEEN_BUT_INCONSISTENT—the PAT of the incoming flow commonly occurs but there are significant enough deviations among other flow characteristics, based on the consistency score

Alert outputs are only leads and may include both benign and malicious behavior/connections—it is the surrounding context/enrichments and analyst-to-constituent feedback which serve as the primary means to determine benign vs. malicious. Much of this can and should be automated.

"Beyond the Network"—Baseline with or correlate to process network connections and process metadata

Carnegie Mellon University
Software Engineering Institute

Sean Hutchison | shutchison@cert.org