WEEKLY INTELLIGENCE PACK · SAMPLE EDITION

This Tuesday's Drop

Detection rule, incident case study, hunt hypothesis, and career tip — exactly what every subscriber gets every Tuesday. This is one real sample, unedited from the format that ships weekly.

01 Detection Rule of the Week

PLATFORM	MITRE TECHNIQUE	SEVERITY
CrowdStrike Falcon LogScale	**T1059.001 — PowerShell**	**Critical**

WHY IT MATTERS

Office applications and browsers spawning PowerShell is rarely legitimate in an enterprise environment. When it happens, it is almost always post-phishing execution — the moment between a user opening an attachment and a payload reaching out to an external host. This is one of the highest-confidence detections available because the parent process relationship alone does most of the work.

REQUIRED LOG SOURCE

Process creation events (ProcessRollup2) from the Falcon sensor. No additional log forwarding configuration needed beyond standard Falcon telemetry.

QUERY — CROWDSTRIKE LOGSCALE

```
// PowerShell from Office or browser — Critical
#event_simpleName=ProcessRollup2
ImageFileName=/\/powershell\.exe$/i
ParentBaseFileName IN (
  "WINWORD.EXE", "OUTLOOK.EXE",
  "chrome.exe", "msedge.exe"
)
| table @timestamp ComputerName
    UserName CommandLine
| "sort" @timestamp desc
```

EXPECTED OUTPUT

A table of timestamp, host, user, and full command line for every PowerShell process whose parent was an Office application or browser. In a healthy baseline this returns zero rows on most days.

FALSE POSITIVES

None observed across production deployments to date. The one documented exception: internal automation tooling that scripts Office documents directly — verify against your asset inventory before excluding any host.

TUNING NOTES

If your environment uses legacy macro-based reporting tools that legitimately spawn PowerShell from Excel, add the specific host and service account to an allowlist rather than excluding the parent process pattern entirely — that preserves detection for every other host.

INVESTIGATION STEPS

1. Pull the full command line and check for -EncodedCommand or download cradle syntax.
2. Check outbound network connections from the host in the 60 seconds following execution.
3. If an external IP was contacted, isolate the endpoint immediately and revoke the user's active sessions.
4. Pull the original email or download source to identify the delivery vector.

TICKET SUMMARY

> *Suspicious PowerShell execution from [PROCESS] on [HOSTNAME], parent process [WINWORD.EXE/OUTLOOK.EXE/BROWSER]. Escalating per detection SOC-WK24-03. User session [REVOKED/UNDER REVIEW]. Awaiting confirmation of outbound connection status.*

02 Real Incident Case Study

WHAT FIRED

A standard phishing detection rule fired on an inbound email containing a credential harvesting link disguised as a shared document notification. The link itself was not the interesting part — the response after the click was.

WHAT WAS INVESTIGATED

The user entered credentials on the spoofed page. Within four minutes, sign-in logs showed a successful authentication from an unfamiliar ASN. Within nine minutes, a new inbox rule was created forwarding any message containing the words "invoice" or "wire" to an external address. The account itself never showed unusual activity in the SIEM's default risk scoring — this was caught entirely by a hunt against new inbox rule creation, not by an alert.

WHAT ALMOST GOT MISSED

The sign-in itself scored as low-risk by the identity provider's own model because the ASN, while unfamiliar to this specific user, was not flagged as malicious at the time. Without the inbox rule hunt running on a schedule, this would have sat undetected until the finance team noticed a redirected wire request, which is precisely when this pattern usually surfaces in the wild.

03 Hunt Hypothesis

HYPOTHESIS

Inbox forwarding rules created within 15 minutes of a first-time external sign-in are a near-certain indicator of business email compromise, regardless of how the identity provider scores the sign-in itself.

HUNT QUERY — MICROSOFT SENTINEL KQL

```
// New inbox rules following first-time sign-in
CloudAppEvents
| where ActionType in (
  "New-InboxRule", "Set-InboxRule"
)
| where RawEventData contains "ForwardTo"
| project Timestamp, AccountDisplayName, IPAddress
```

WHY IT MATTERS RIGHT NOW

This pattern has shown up twice in the last quarter across different organizations using the same identity provider. Running this hunt weekly costs under five minutes and catches compromise before financial loss occurs, not after.

04 Career Tip

HOW TO PHRASE A TUNING REQUEST WITHOUT SOUNDING LIKE YOU'RE BLAMING THE SIEM TEAM

Don't say "this rule is too noisy." Say "this rule is catching real signal but the false positive rate is making it hard to prioritize — here's the specific pattern I'd exclude and why." Bring the exact field values causing noise, not a general complaint. Tuning requests that come with a proposed fix get actioned in days. Tuning requests that come with a complaint get added to a backlog.
