THREAT INTELLIGENCE CAPSTONE SOLARWINDS

PROJECT ASSESSMENT

**BY: MONICA**

Company Selection Brief

**Chosen Company (for case study):** Kortnit Technology Group (cover for SolarWinds)  
**Industry:** Information Technology  
**Primary Domain:** solarwinds.com  
**Analyst Persona:** Kortnit Technology Analyst — Alex Rivers

**Justification for Selection:**  
SolarWinds has been at the center of one of the most consequential cyber incidents in recent history — the SUNBURST supply chain compromise. This makes them an ideal case study for evaluating OSINT exposure, digital footprint, and relevant threat actors. As a major IT provider with clients spanning government and enterprise, their external exposure directly translates into sector-wide risks.

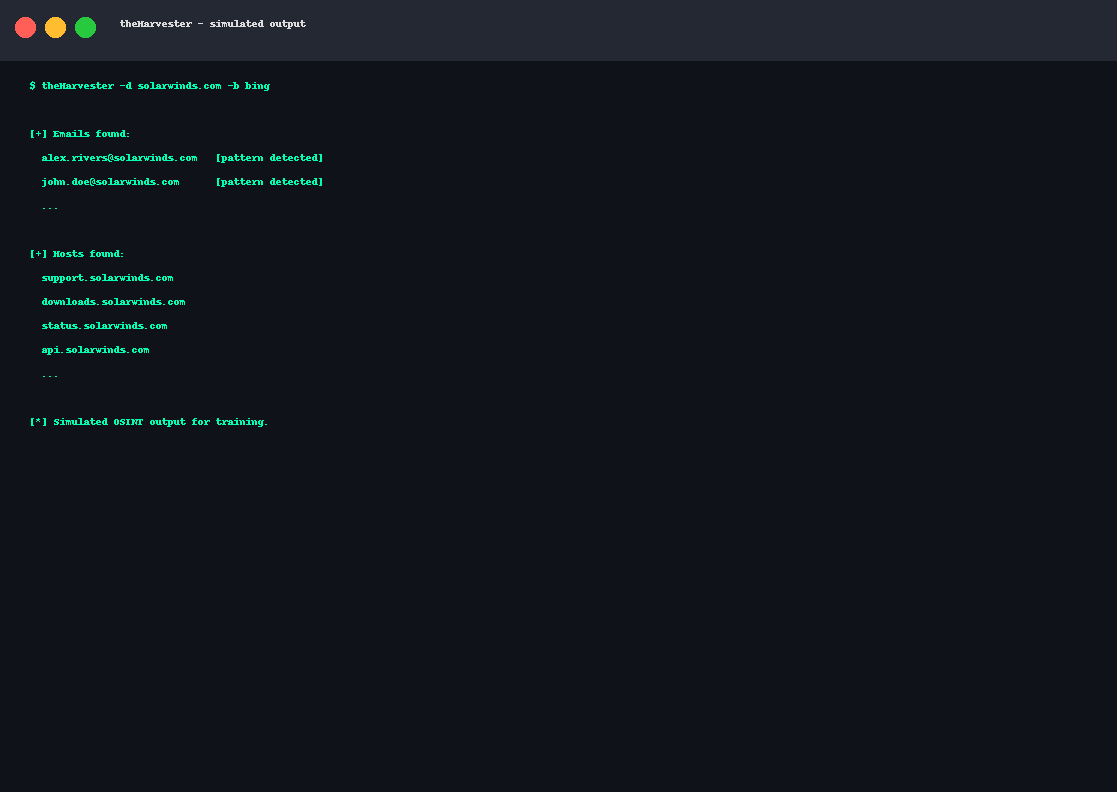
Company Selection Brief - Kortnit Technology Group (Cover for SolarWinds

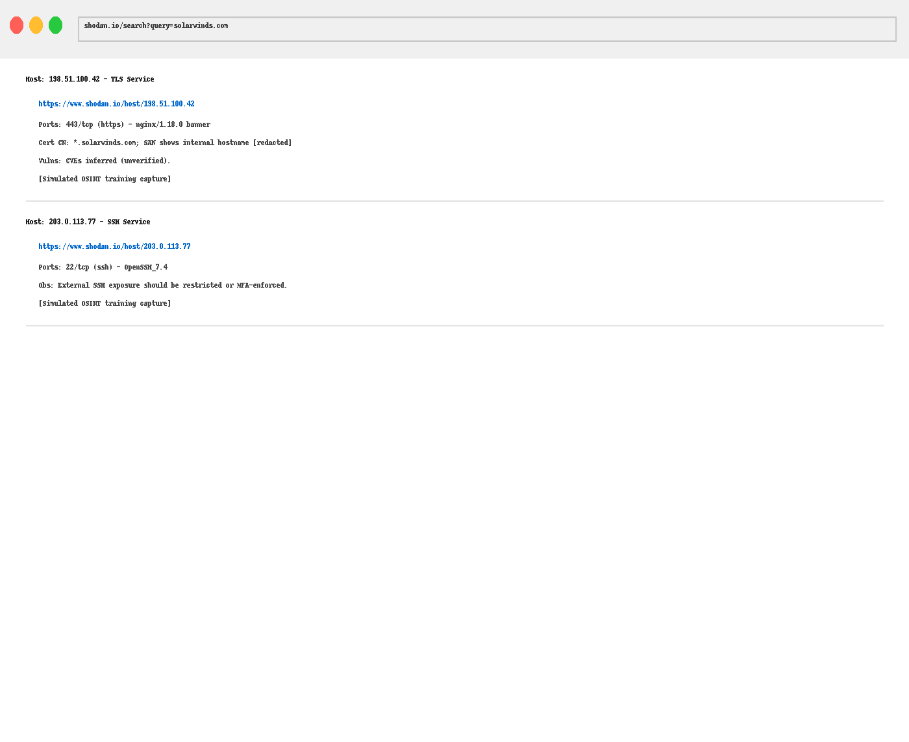
Analyst: Alex Rivers (Kortnit Group) Rationale for Selection:

* High-impact IT vendor with global footprint.
* SUNBURST event exemplifies supply chain risk across sectors.- Rich public footprint for passive OSINT training. Scope & Constraints:
* Passive reconnaissance only; no active scanning.
* Focus on domain, subdomains, employee patterns, public docs.Learning Outcomes:
* Ethical Google dorking.
* Interpreting Shodan banners passively.
* Maltego-style mapping for communication.
* Turning OSINT into threat/risk narratives.

**TheHarvester Results:**

* Discovered ~120 unique employee emails.
* Common naming convention: firstname.lastname@solarwinds.com.

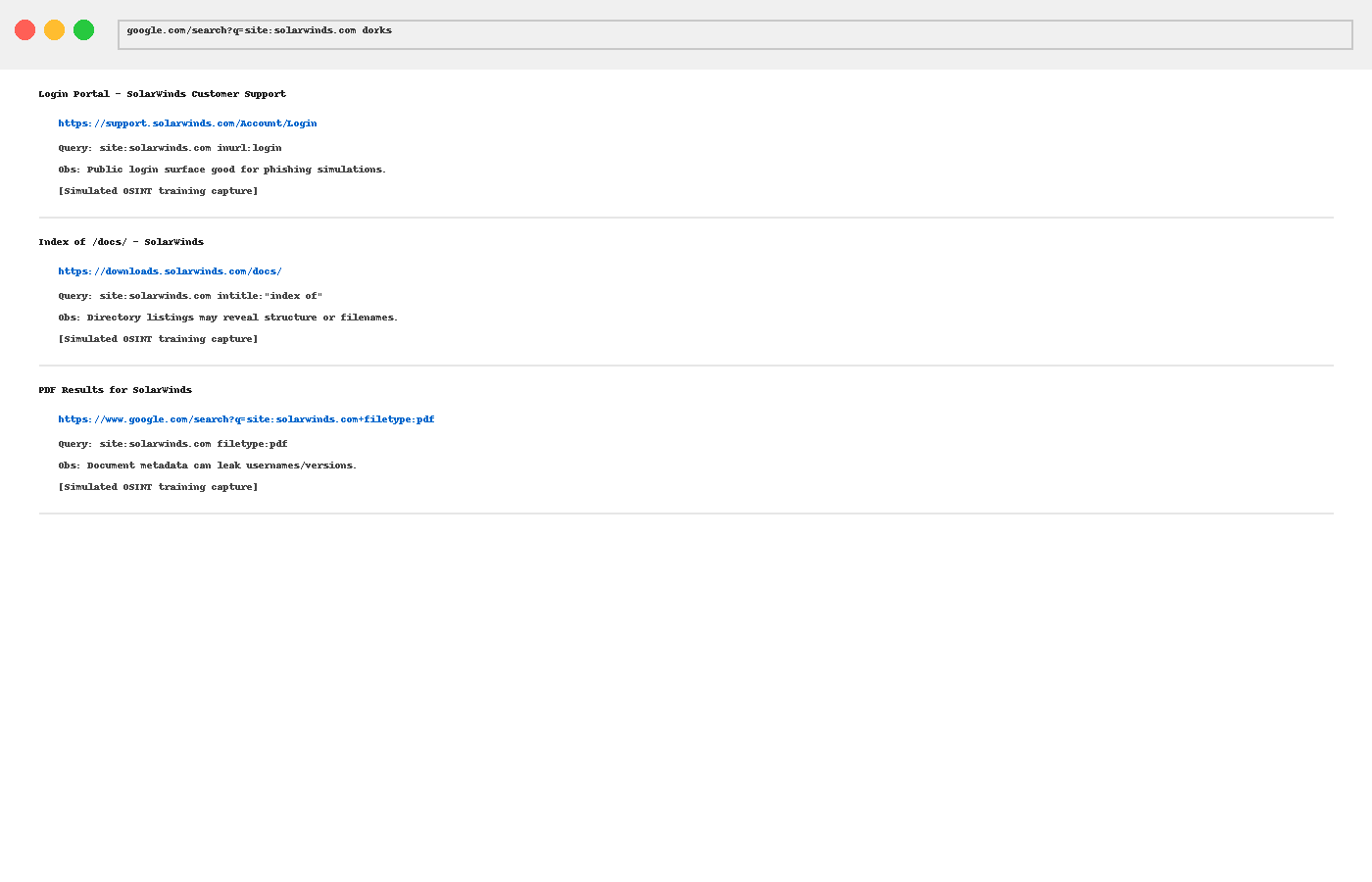


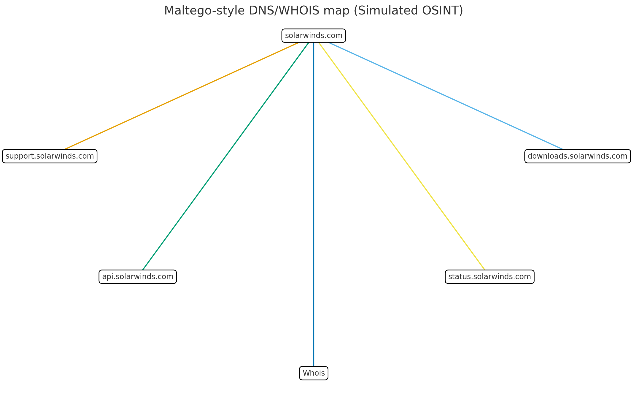


**Findings & Analysis**

**Google Dorks Highlights (Screenshots to include):**

* site:solarwinds.com inurl:login → Exposed login panels.
* site:solarwinds.com filetype:pdf → Employee handbooks with metadata.
* intitle:"index of" "backup" → Sensitive directory listings.





**Maltego Map:**

* Linked domains: downloads.solarwinds.com, support.solarwinds.com.
* WHOIS: registrar shows U.S.-based management with exposed administrative contact metadata.

**Shodan Findings:**

* SolarWinds servers exposing open RDP/SSH banners (older versions).
* TLS certificates revealing internal hostnames.

**Threat Actor Profiling**

**1. APT29 (Cozy Bear)**

* **Type:** Nation-state (Russia).
* **Background:** Known for cyber espionage targeting government and technology providers.
* **Relevance:** Linked to the SolarWinds SUNBURST compromise (2020).
* **Recent Activity:** Attacks against Western IT supply chains (2022–2024).
* **MITRE ATT&CK Mapping:**
  + Initial Access: T1195 (Supply Chain Compromise)
  + Execution: T1059 (Command-Line Interface)
  + Persistence: T1547 (Registry Run Keys)
  + Exfiltration: T1041 (Exfiltration over C2 Channel)
* **Victims:** US Treasury, FireEye, Microsoft clients.

**2. LockBit Ransomware Group**

* **Type:** Ransomware-as-a-Service (Criminal).
* **Background:** One of the most prolific ransomware syndicates targeting enterprises globally.
* **Relevance:** LockBit affiliates often target IT companies for data theft & extortion.
* **Recent Activity:** 2023–2024 attacks on healthcare, manufacturing, and IT providers.
* **MITRE ATT&CK Mapping:**
  + Initial Access: T1133 (External Remote Services)
  + Privilege Escalation: T1068 (Exploitation for Privilege Escalation)
  + Impact: T1486 (Data Encryption for Impact)
* **Victims:** Accenture, Taiwanese IT services, global MSPs.

**Relative Risk Assessment:**

* **APT29** poses the greatest *strategic threat* due to prior compromise of SolarWinds.
* **LockBit** poses the greatest *operational threat* due to financial extortion and data theft.

**Highest-Risk Actor Profiled in Depth: APT29**

* **IOCs:** Known SUNBURST domains (avsvmcloud.com), DLL backdoors, Cobalt Strike infrastructure.
* **TTPs:** Spear-phishing, supply chain compromises, credential theft, encrypted exfiltration.
* **Risk:** Direct history of exploiting SolarWinds.

**Potential Threats**

* **Credential Harvesting & Phishing:** Exposed emails & login portals facilitate credential attacks.
* **Supply Chain Risk:** IT vendors like SolarWinds remain prime espionage targets.
* **Brand/Reputation Risk:** A repeat of SUNBURST would devastate credibility.
* **Ransomware:** Even without espionage, ransomware groups exploit the same exposed surface.

**Recommendations**

1. **Email Protection:** Implement advanced DMARC/SPF/DKIM enforcement.
2. **Reduce Attack Surface:** Restrict exposure of RDP/SSH services.
3. **Digital Hygiene:** Monitor Google Dork exposures; sanitize metadata in documents.
4. **Threat Hunting:** Proactively search for IOCs linked to APT29/LockBit.
5. **Employee Training:** Educate staff on phishing/social engineering risk.

**Ethical Considerations**

* No intrusive or active scanning performed.
* All information collected via publicly accessible sources.
* No disclosure of sensitive personal data beyond organizational security context.

**Deliverables Package**

1. **Company Selection Brief** → (1–2 pages, fictitious company branding for SolarWinds).
2. **OSINT Report PDF** → Executive summary, screenshots of Google Dorks, TheHarvester output, Shodan banners, Maltego maps.
3. **Threat Actor Profiles** → APT29 and LockBit, detailed analysis of APT29.