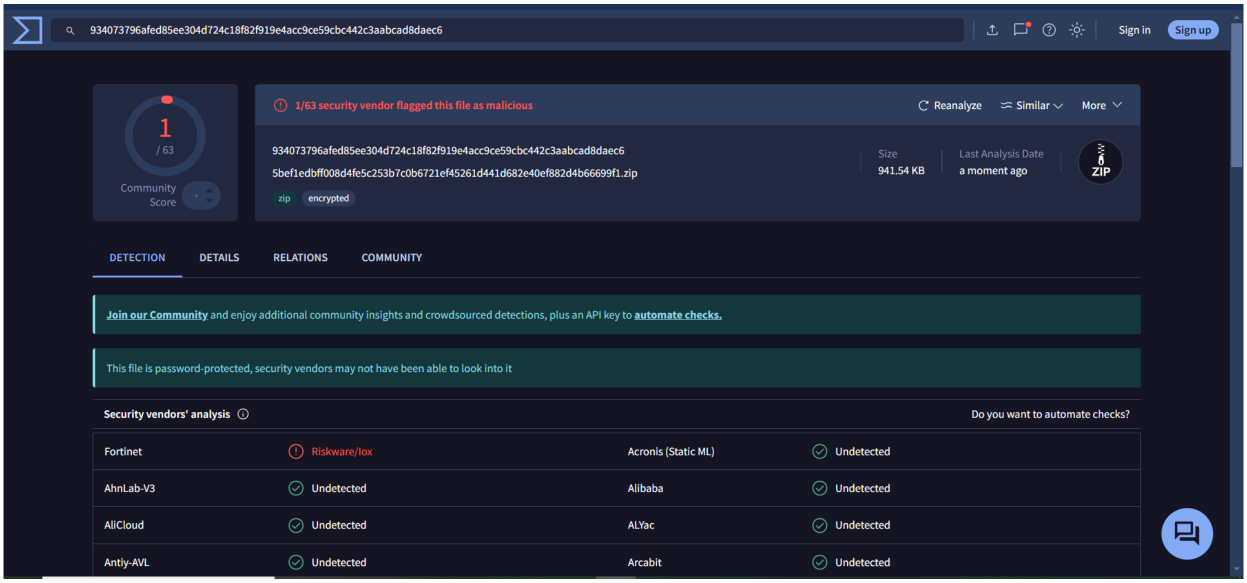
Cyber Threat Analysis Report



934073796afed85ee304d724c18f82f919e4acc9ce59cbc442c3aabcad8daec6

1 / 63

1/63 security vendor flagged this file as malicious

934073796afed85ee304d724c18f82f919e4acc9ce59cbc442c3aabcad8daec6
5bef1edbff008d4fe5c253b7c0b6721ef45261d441d682e40ef882d4b66699f1.zip

zip encrypted

Size 941.54 KB

Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

This file is password-protected, security vendors may not have been able to look into it

Security vendors' analysis

Do you want to automate checks?

Fortinet	Riskware/Iox	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
AliCloud	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected

1. File Overview

- **File Hash:** 934073796afed85ee304d724c18f82f919e4acc9ce59cbc442c3aabcad8daec6
- **File Type:** ZIP (Password-Protected)
- **File Size:** 941.54 KB
- **Encryption:** Yes (VirusTotal indicates that security vendors may not have been able to analyze contents)

2. Detection Results

- **1/63 Security Vendors Detected the File as Malicious**
- **Vendor:** Fortinet
- **Detection:** Riskware/Iox
- **Other Vendors:** Marked as "Undetected"

3. Behavioral Indicators

- The file is password-protected, making it harder for automated scanners to inspect the contents.
- "Riskware/Iox" by Fortinet suggests it could contain potentially unwanted programs (PUPs) or software that may have security concerns.
- Since only 1 out of 63 vendors flagged the file, this could be a false positive, but manual analysis is needed.

4. Potential Impact

- If the file contains malware, it could execute harmful actions such as:

    - **Data Theft:** If it includes spyware or keyloggers.
    - **System Compromise:** If it contains trojans or backdoors.
    - **Persistence Mechanisms:** If it modifies registry keys or system startup behavior.

5. Recommended Actions

- **Further Analysis:** Use a sandbox (e.g., Any.Run, Hybrid Analysis) to execute the file safely.
- **Manual Inspection:** Extract contents in a controlled environment.
- **Monitor Behavior:** Look for unusual system activity post-execution.
- **Check False Positives:** Since only one vendor flagged it, submit to Fortinet for further review.

APT29 - SolarWinds Attack

APT29 (also known as Cozy Bear) is linked to Russia's **SVR intelligence agency** and has conducted cyber espionage against government agencies, think tanks, and private companies. The **SolarWinds attack** was one of the most sophisticated cyber-espionage campaigns in history.

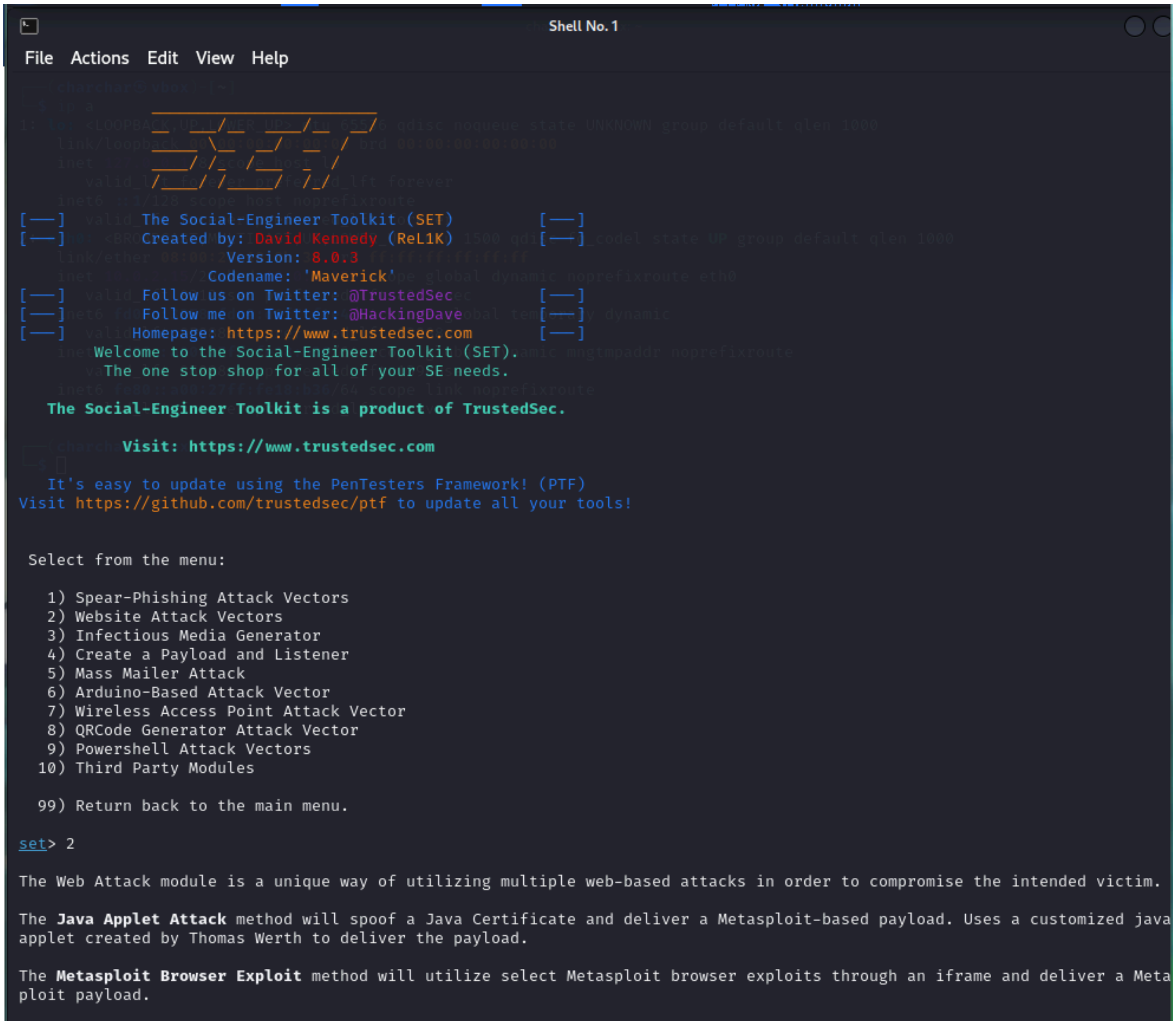
MITRE ATT&CK Mapping of the SolarWinds Attack:

Phase	Tactic (MITRE ATT&CK)	Technique Used
Initial Access	T1195.002 - Supply Chain Compromise	APT29 injected malicious code into **SolarWinds Orion** updates.
Execution	T1059 - Command and Scripting Interpreter	Used **PowerShell** scripts to execute payloads.
Persistence	T1546.008 - Registry Run Keys	Created persistence via registry modifications.
Privilege Escalation	T1078 - Valid Accounts	Stole legitimate credentials for privilege escalation.
Defense Evasion	T1027 - Obfuscated Files or Information	Used encoded PowerShell scripts to avoid detection.
	T1070.004 - File Deletion	Deleted logs and traces to cover tracks.
Credential Access	T1555 - Credentials from Password Stores	Harvested credentials from LSASS memory dumps.
Discovery	T1018 - Remote System Discovery	Identified additional networked systems to laterally move.

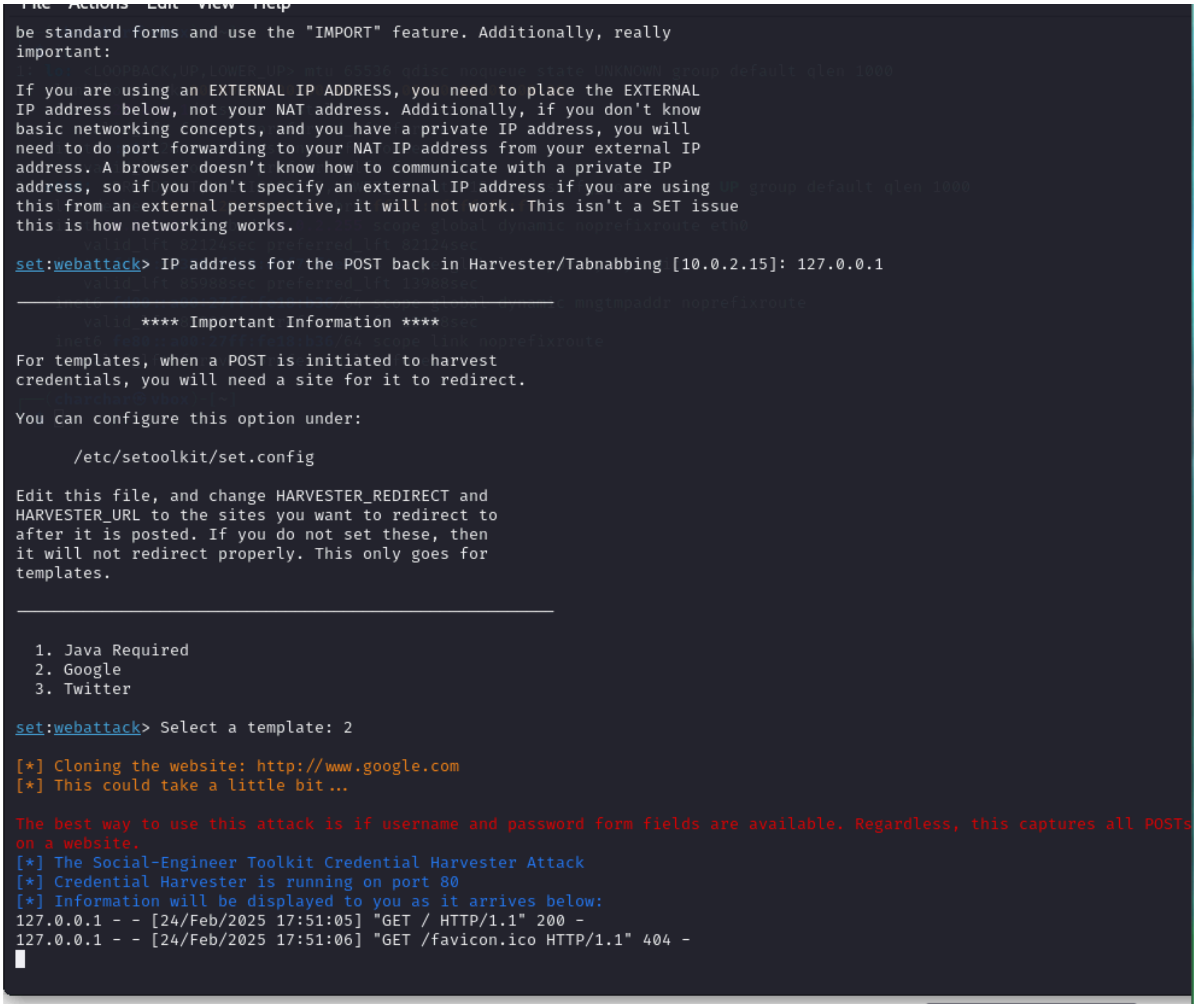
Lateral Movement	T1021 - Remote Services	Used **Remote Desktop Protocol (RDP)** and **WinRM** for movement.
Collection	T1114 - Email Collection	Exfiltrated **Microsoft 365 and Exchange** emails from victims.
Exfiltration	T1041 - Exfiltration Over C2 Channel	Sent stolen data via **encrypted HTTPS connections**.
Impact	T1562.001 - Disable Security Tools	Disabled **endpoint detection and response (EDR)** solutions.

Key Takeaways:

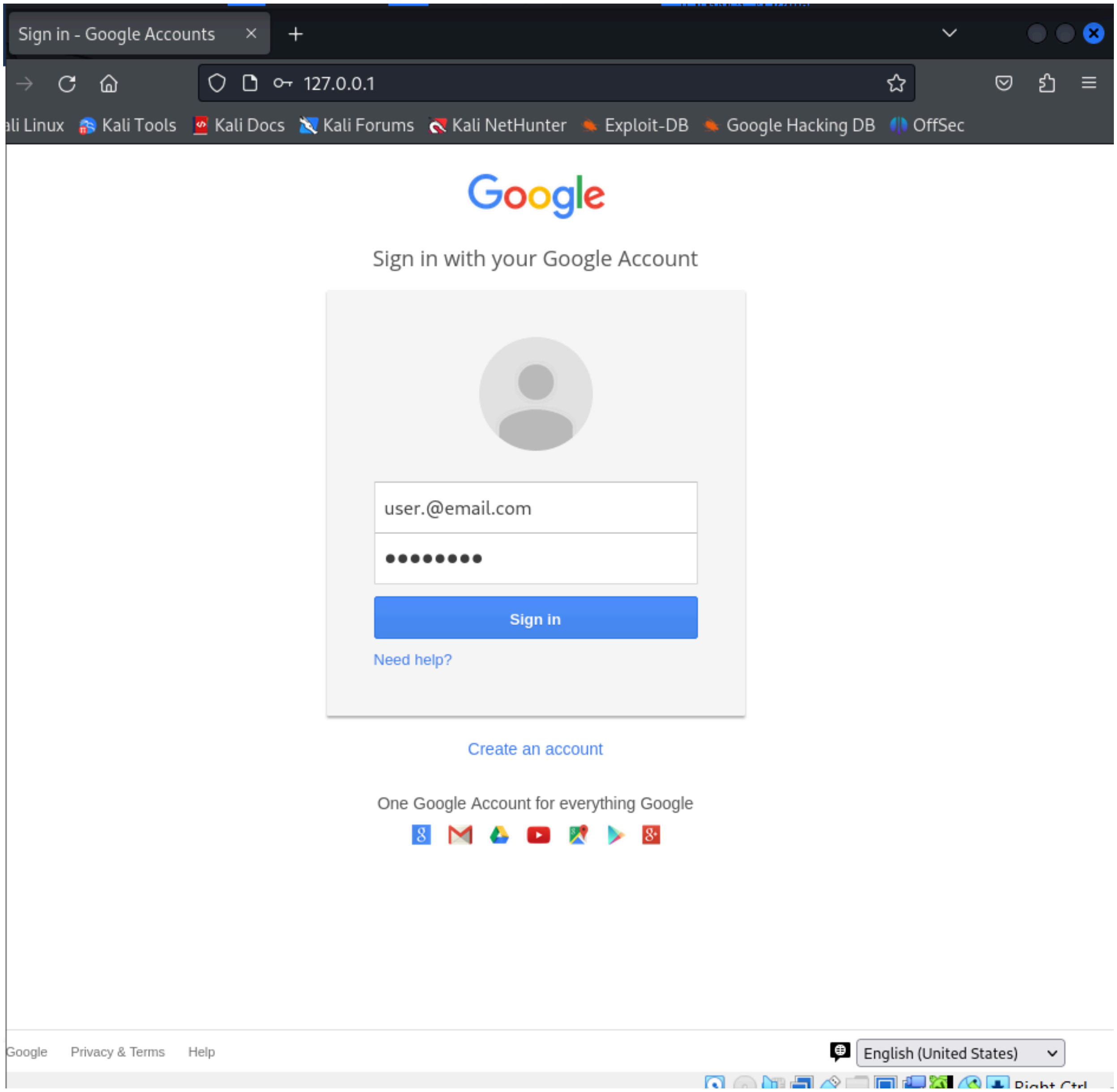
1. **Supply Chain Attack**: Instead of targeting victims directly, APT29 compromised **SolarWinds**, a trusted IT provider, and infected **thousands of organizations** via software updates.
2. **Highly Stealthy Approach**: Used legitimate accounts and obfuscated scripts to avoid detection for months.
3. **Targeted High-Profile Entities**: Victims included **U.S. government agencies**, Microsoft, and cybersecurity firms.



```
[—]    The Social-Engineer Toolkit (SET)          [—]
[—]    Created by: David Kennedy (ReL1K)          [—]
                 Version: 8.0.3
               Codename: 'Maverick'
[—]    Follow us on Twitter: @TrustedSec          [—]
[—]    Follow me on Twitter: @HackingDave         [—]
[—]   Homepage: https://www.trustedsec.com        [—]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java
applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Meta
ploit payload.
```



```
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 127.0.0.1

--------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

--------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs
on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [24/Feb/2025 17:51:05] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Feb/2025 17:51:06] "GET /favicon.ico HTTP/1.1" 404 -
```



Sign in with your Google Account

user.@email.com

●●●●●●●●

One Google Account for everything Google

English (United States)