**Final Project**

**and**

**Report**

**9002 Trojan Delivery**

**Prepared by Quang Pham**

**UID: U31075359**

Table of Contents

[Abstract 3](#_Toc449870271)

[Scenario Introduction 3](#_Toc449870272)

[Threat Actor 3](#_Toc449870273)

[Target 3](#_Toc449870274)

[Campaign 4](#_Toc449870275)

[The Exploit 4](#_Toc449870276)

[Stages of the Attack 4](#_Toc449870277)

[Reconnaissance 4](#_Toc449870278)

[Weaponizing 4](#_Toc449870279)

[Delivery 4](#_Toc449870280)

[Exploit 5](#_Toc449870281)

[Stix Viz Representation 6](#_Toc449870282)

[Soltra/Edge Representation 7](#_Toc449870283)

[Install 8](#_Toc449870284)

[Command and Control 9](#_Toc449870285)

[Actions on Objectives 9](#_Toc449870286)

[Incident Handling Process 9](#_Toc449870287)

[Identification Phase 9](#_Toc449870288)

[Eradication and Recovery Phase 9](#_Toc449870289)

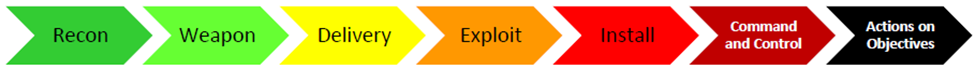
[Lessons Learned Phase 10](#_Toc449870290)

[Exploit References 10](#_Toc449870291)

[References 10](#_Toc449870292)

# **Abstract**

This paper aims to outline the phases of an assault using the "9002 Trojan," which was made possible by the abuse of people's confidence in well-known websites like TinyURL and Google Drive. Combining these services allowed for the delivery of the 9002 Trojan, which was used to carry out a complex malware campaign aimed against political officials and human rights campaigners, mostly in Myanmar and other Asian nations. This assault successfully concealed the attack vector within services that appeared to be innocent by using cleverly shortened URLs to send visitors to a malicious file hosted on Google Drive.1  
The 9002 Trojan, exploiting CVE-2002-0649, capitalizes on weaknesses within digital trust infrastructures.16 Understanding the vulnerability and its distribution method is essential to comprehending how the attackers were able to get past traditional security protections and access targeted computers without authorization. In addition to compromising the system, the Trojan creates a strong command and control channel that permits data exfiltration and other malicious activities. These actions may result in extended unauthorized access to the system and data loss. On July 26, 2016, researchers from Palo Alto Networks' Unit 42 discovered and examined the assault for the first time. They published their results in a blog post.2

The Department of Homeland Security's (DHS) "Kill Chain" concept will be used to carefully dissect the attack lifecycle and describe each stage in this paper, from reconnaissance to actions on objectives:

In addition, the responsibilities of the main actors will be categorized according to STIX (Structured Threat Information Expression) characteristics, allowing for a thorough understanding of the attack's structure and how it affects cybersecurity procedures.

# **Scenario Introduction: 9002 Trojan Attack**

This scenario centers on a sophisticated cyberattack that targets people in Myanmar and other Asian nations by taking advantage of flaws in reliable web services like Google Drive and TinyURL. The assault uses the 9002 Trojan. The Unit 42 team at Palo Alto Networks originally took documentation of the event.3

**Threat Actor**

Given the sophistication and the targets of the attack, the threat actor in this instance is an unidentified entity that is probably state-sponsored. This actor has proven to be capable of using online services to spread malware that targets particular geopolitical areas.

**Target**

The main targets of the 9002 Trojan attack were human rights activists and political personalities in Myanmar, as well as potentially other Asian countries. Specifically, the attacks made use of software vulnerabilities and social engineering.

**Campaign**

The attack used a multipronged strategy that included using social engineering, exploiting web service vulnerabilities, and using Google Drive to distribute malware that was masked by URL shortening services like TinyURL. Installing the 9002 Trojan on the systems of those who were to be targeted was the goal in order to perform data exfiltration and surveillance.4

**The Exploit**

Using cleverly shortened URLs that led to a malicious file housed on Google Drive, the exploit was created. The distribution was concealed by URLs that appeared authentic and, upon clicking, would start the 9002 Trojan download.5

# **Stages of the Attack**

## **Reconnaissance**

## Reconnaissance in the 9002 Trojan scenario most likely entailed the attackers determining targets based on their digital communication vulnerabilities and geopolitical significance. The attackers looked for vulnerabilities in email and web services used by potential targets, including as political figures in Asia and human rights advocates, using data and tools that were made available to the public.6

## **Weaponizing**

## By inserting the 9002 Trojan into an apparently authentic paper, the attackers turned it into a weapon. To improve the likelihood that it would be accessed, this document was probably themed around subjects related to the targets.

## Tools/Techniques: creating malicious scripts, exploiting documents, and incorporating malware into downloadable files placed on managed Google Drive links while hiding them behind TinyURL-provided URL shorteners.7

## **Delivery**

Using TinyURL, the attackers first shortened a URL. This abbreviated URL connected to another actor-controlled server that allowed for additional redirection. hxxp://tinyurl[.]com/zmu4dry was the precise TinyURL that was used.

The target was forwarded to an IP address under the control of the attackers upon clicking the shortened URL, which held a bespoke script for further redirection. The base64 encoded parameters supplied in the URL for this redirection server, hxxp://222.239.91[.]152, were probably used to track clicks and obtain further information about the target's behavior or credentials.

The encoded section contained the recipient's email address and a nested TinyURL link at `hxxp://222.239.91[.]152?<redacted>QGdtYWlsLmNvbWh0dHA6Ly90aW55dXJsLmNvbS9qZmo5b3V2'. The victim's Gmail address was exposed upon decoding, and it redirected once more to hxxp://tinyurl[.]com/jfj9ouv{, another truncated TinyURL link.

The user was sent to a Google Drive URL (hxxps://drive.google[.]com/uc?id=0B0eVt8dSXzFuN2ltVlVkVl8zNVU&authuser=0&export=download) using the last TinyURL link. The malicious payload, a "2nd Myanmar Industrial Human Resource Development Symposium.zip" zip file containing the executable file needed to install the 9002 Trojan, was hosted by this URL.8

## **Exploit**

When the Trojan was first executed, it made sure it wasn't operating in a sandbox, which is a common security precaution that allows malware to be identified by watching how it behaves in a controlled environment. The requirement that the system time must be greater than May 20, 2016, suggests that the basis for this check was probably the system's time setting.

Subsequently, the program introduced further malicious components into the system. A number of programs, including "RealNetwork.exe," "main.dll," and "MPAMedia.dll," that were saved in a folder with an arbitrary name inside the user's profile directory were extracted and run by it. This file-storage technique avoids suspicion by imitating genuine program installations.

By using a method called DLL sideloading, the Trojan took advantage of RealNetwork.exe's authentic look and digital signature to evade security safeguards. A malicious DLL called MPAMedia.dll would be loaded by RealNetwork.exe, and that would then load main.dll. This loading sequence makes sure that the malicious code runs in the background while appearing to be legal processes.

In order to remain persistent on the compromised system, the Trojan altered registry keys to guarantee that RealNetwork.exe launches upon system startup. In particular, it made Software\Microsoft\Windows\CurrentVersion\Run an autorun registry key. The Trojan might stay alive and restart itself after a system reboot thanks to this configuration.

When the Trojan was fully functional, it used a bespoke protocol via TCP port 80 to establish connections with its command and control (C2) server. The string '9002' indicates that this particular Trojan variant is being sent. In order to obtain further harmful instructions, exfiltrate data, and maybe obtain new modules or updates from the attackers, this communication was necessary.9

### 

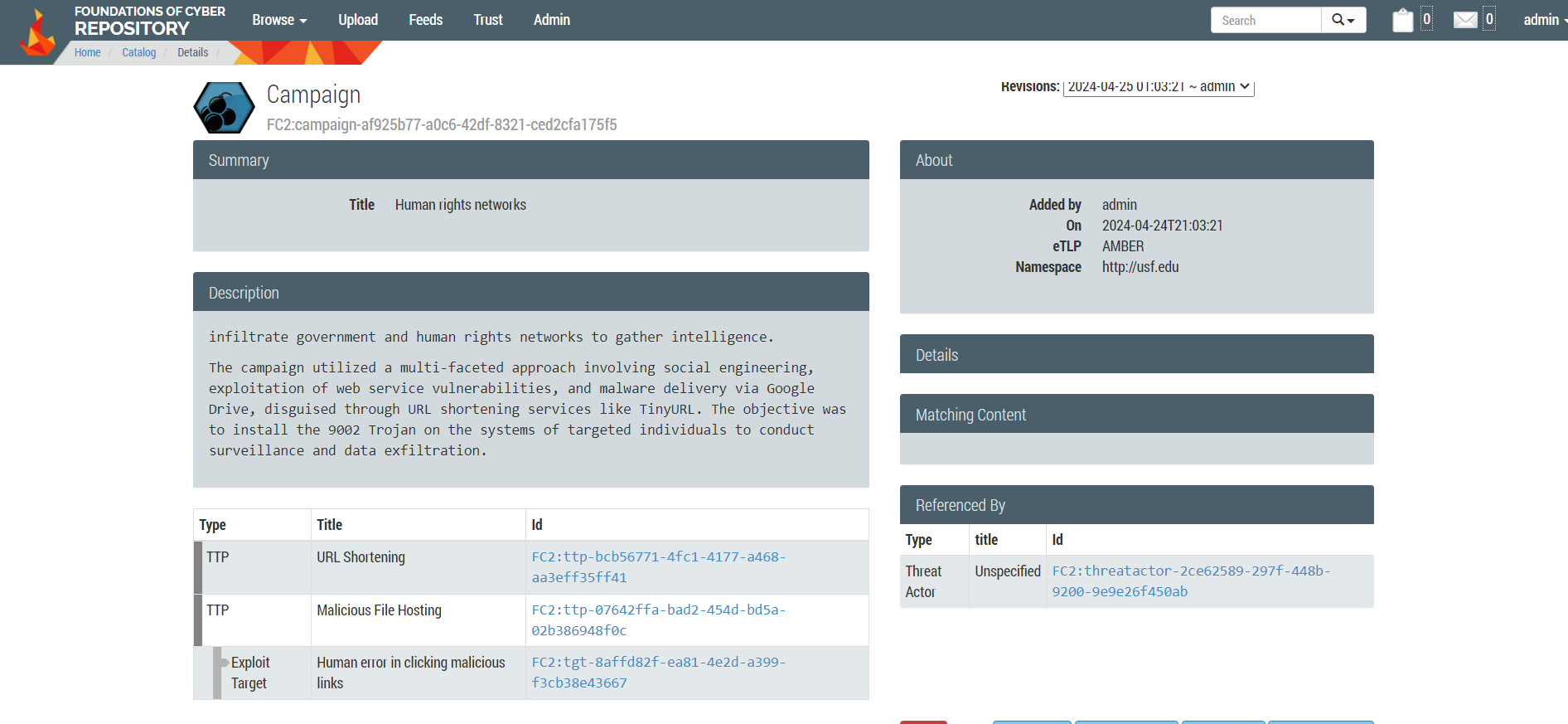
### Stix Viz Representation

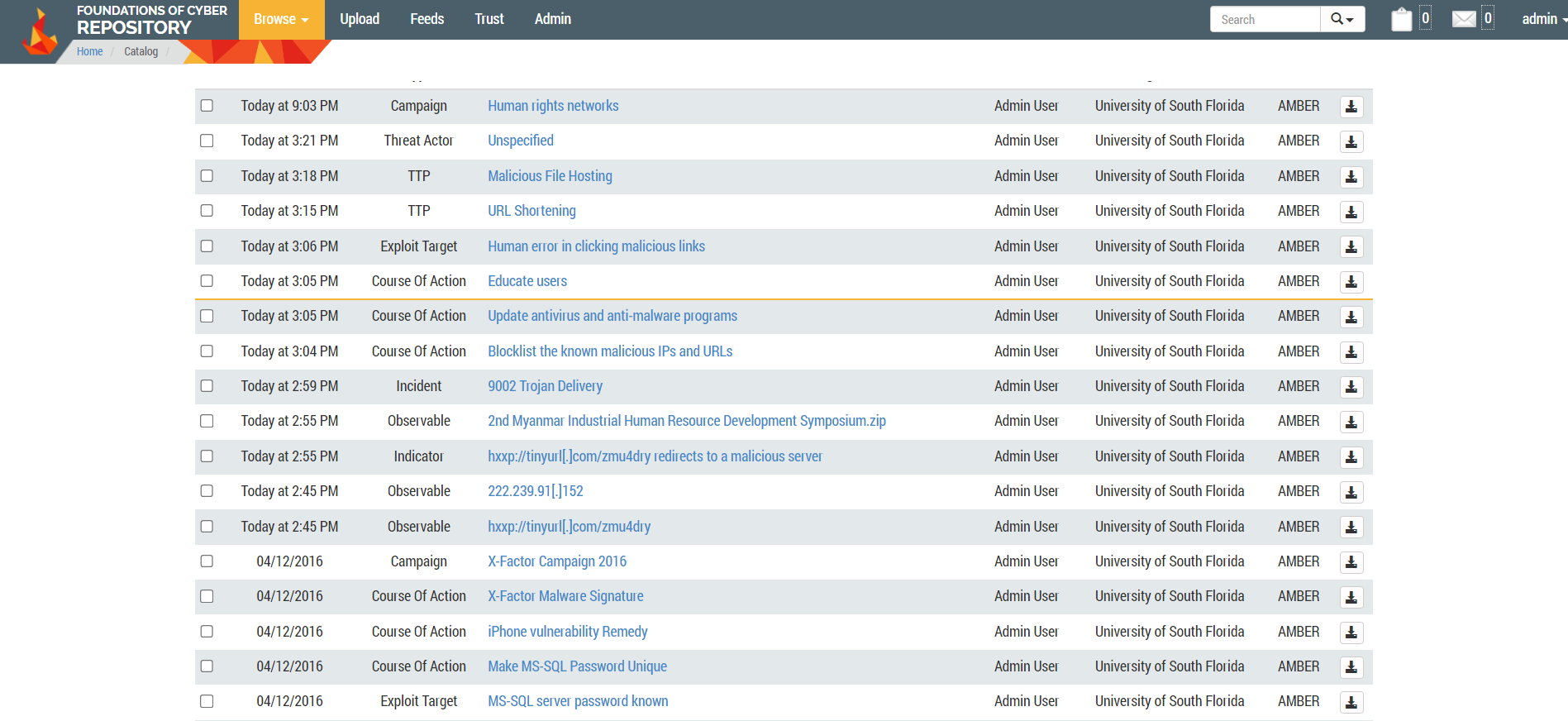
The 9002 Trojan is represented in StixViz image below:



Soltra/Edge Representation

The 9002 Trojan is represented in Soltra/Edge image below:





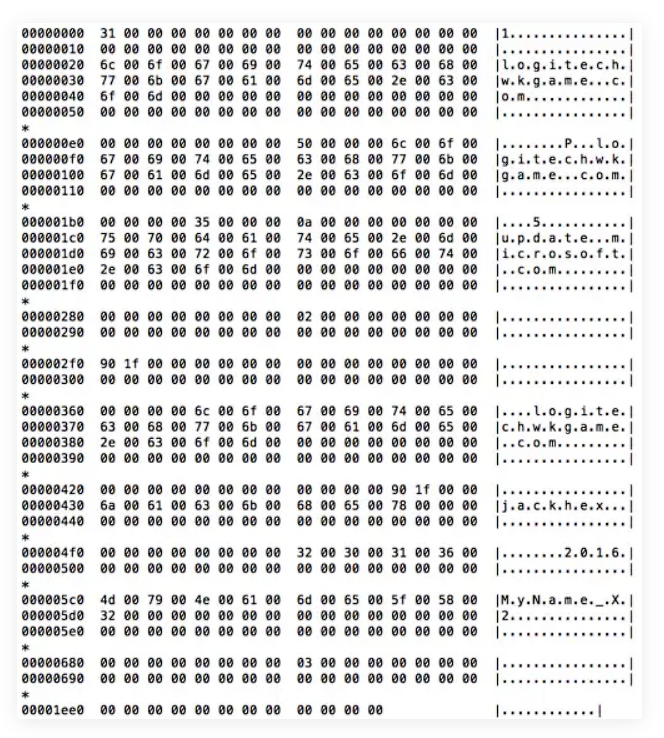
## 

## **Install**

The pivotal moment came when the victim used the TinyURL redirection to download and launch the malicious program called "2nd Myanmar Industrial Human Resource Development Symposium.exe" from the Google Drive link. The victim would manually launch the Trojan, thinking, based on its icon and filename, that the file was a genuine PowerPoint presentation.

In the user's %USERPROFILE% directory, the dropper generated a folder with an arbitrary name. This folder was used to covertly hold extra Trojan components that were required for the program to function. Using a random directory name makes it more difficult to identify installed files from authentic data, which helps prevent discovery.

The C2 server (logitechwkgame[.]com) then handles outbound communications from the infected machine, receiving commands from the attackers and sending stolen data.



The Trojan altered the registry to make sure it stayed active even after system restarts:

RealNetwork.exe was the destination of the autorun registry key that was generated at Software\Microsoft\Windows\CurrentVersion\Run. This configuration makes sure that the executable is launched each time the system boots up, along with the Trojan infrastructure as a whole.10

## **Command and Control**

When the Trojan was fully functional, it used a bespoke protocol via TCP port 80 to establish connections with its command and control (C2) server. The string '9002' indicates that this particular Trojan variant is being sent. In order to obtain further harmful instructions, exfiltrate data, and maybe obtain new modules or updates from the attackers, this communication was necessary.11

## **Actions on Objectives**

In the last stage of the 9002 Trojan assault, called "Actions on Objectives," the attackers use the access they have acquired through earlier phases to carry out the harmful actions they have planned. During this phase, the attack's strategic objectives—which usually include data exfiltration, surveillance, and additional system compromise—are the main focus.12

# **Incident Handling Process**

## **Identification Phase**

increased use of network resources, which can be a sign that control servers are receiving data. finding of unknown programs or files, like "2nd Myanmar Industrial Human Resource Development Symposium.exe," which may have been downloaded and run by unwary people. notifications from antivirus software or intrusion detection systems (IDS) that identify the Trojan or anomalous activities, such as illegal attempts to access specific network resources. System lag or malfunctions, maybe as a result of the Trojan using up system resources or carrying out illegal actions. These will be the clearest indications that an attack may take place.13

## **Eradication and Recovery Phase**

* The 9002 Trojan was found inside the network, and the following actions were done to get rid of the infection and restore the compromised systems:
* Isolation of Affected Systems: Affected systems were cut off from the network to stop any further dissemination or data leaks.
* Forensic Analysis: To determine the extent of the hack and locate all harmful components, a thorough investigation of the compromised systems was carried out.
* Malicious File Removal: Every malicious file connected to the Trojan that was found was eliminated.
* System updates and patching: In order to eliminate any vulnerabilities that the Trojan could have exploited, systems were carefully inspected and updated. Installing the most recent security updates and patches was part of this.
* Credential Resetting: Passwords and other credentials that were possibly compromised were reset as a precaution.
* Restoration from Backups: Before the compromise, data and system configurations were restored using clean backups.
* Network and Security Device Configuration: To prevent unwanted access and enhance monitoring, firewall and router setups were improved. Priority was given to putting strict regulations into place to manage both incoming and outgoing traffic.14

## **Lessons Learned Phase**

# Raising staff awareness of cybersecurity issues and providing them with training to identify phishing efforts and other forms of social engineering. highlighting the significance of timely security patch application and routine system audits in order to reduce vulnerabilities. improving IDS skills to more efficiently identify advanced persistent threats and sophisticated malware. dividing the network into segments to prevent infections from spreading and to regulate lateral movement inside the network.15

# **Exploit References**

1. 9002 Trojan
2. Google Drive Phishing Techniques
3. TinyURL in Cyber Attacks
4. CVE-2012-0158

# **References**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

1. Palo Alto Networks. "Unit 42 Attack Delivers ‘9002’ Trojan Through Google Drive." URL:

https://unit42.paloaltonetworks.com/unit-42-attack-delivers-9002-trojan-through-google-drive/

1. STIX. “Documentation”. URL:

<https://stixproject.github.io/documentation/>

16

1. NIST. “Vulnerability Summary for CVE-2002-0649”. URL:

https://nvd.nist.gov/vuln/detail/cve-2012-0158