



GOVERNMENT WEBSERVER USED As C2 SERVER

AGENT TESLA

MALWARE, TROJAN, EVADER, STEALER, GULoader

Vairav Advisory Report

22nd December 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

EXECUTIVE SUMMARY

In a critical revelation, the analysis underscores a pressing concern involving the Nepal Government's webserver. Disturbingly, our findings indicate that this official web infrastructure has been exploited as a CNC server by malicious actors. The gravity of the situation becomes evident with the identification of over 2000 malicious files engaged in communication with the IP address hosting the compromised webserver. What sets this analysis apart is the revelation that numerous official government websites are now flagged as malicious. This abrupt transformation of legitimate government platforms into potential vectors for cyber threats demands urgent attention and decisive action.

The single largest takeaway from this analysis is the alarming convergence of government infrastructure with malicious activities. The new information at hand not only exposes a vulnerability in the heart of Nepal's digital presence but also signals a potential threat to national security and data integrity. The audience must comprehend the gravity of this situation, as the compromise of government sites not only jeopardizes sensitive information but also undermines public trust in online government services.

Key Takeaways:

- A staggering count of nearly 3000 malicious files is actively communicating with the server's IP address.
- A concerning number of official sites have been identified and flagged as either malicious or phishing entities.
- The server has recently been exploited by Agent Tesla for Command and Control (CNC).
- The malicious files engaging with the IP address of the webserver are linked to the malware families: sality, gen2, and kuku.

Analysis

Many instances of Agent Tesla (Agent Tesla operates as a Remote Access Trojan (RAT) and data theft tool. It is commonly utilized for Malware-As-A-Service (MaaS) to gain initial access) were obtained as a sample, revealing its communication with an official government website in Nepal. Subsequently, a thorough investigation was conducted to gather additional information and artifacts.

35 security vendors and 1 sandbox flagged this file as malicious

b31c4835e17587d6b1f5170da84abb8130519be8ea3fc5da07d47f548ffa18b
Sutarčij analizé-pdf.img.iso

Size: 1.25 MB | Last Analysis Date: 1 day ago

isoimage malware dmg checks-cpu-name detect-debug-environment checks-network-adapters checks-bios long-sleeps attachment calls-wmi contains-pe

Community Score: 35 / 60

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12

Contacted URLs (2)

Scanned	Detections	Status	URL
2023-12-20	17 / 91	200	http://spsc.sudurpashchim.gov.np/geo.bin
2023-12-21	0 / 91	502	http://go.microsoft.com/fwlink/?LinkID=252669&clcid=0x409

46 security vendors and 1 sandbox flagged this file as malicious

Oda1ad1d456b5b7a028efcbfd9c3ee45af7c6830c87c1e7469faa089dbb0fe7e
fordanskningernes hildebrand.exe

Size: 711.54 KB | Last Analysis Date: 1 day ago

peexe overlay checks-cpu-name signed detect-debug-environment checks-network-adapters checks-bios long-sleeps invalid-signature calls-wmi

Community Score: 46 / 72

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Contacted URLs (2)

Scanned	Detections	Status	URL
2023-12-21	0 / 91	200	http://www.nepal.gov.np/
2023-12-20	17 / 91	200	http://spsc.sudurpashchim.gov.np/geo.bin

Figure 1: Contacted domain by Agent Tesla malware.

The website was checked on multiple sandboxes and scanners to find more information.

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to GULOADER - according to source Cluster25 - 13 days ago

This URL is used by GULOADER. Guloader is a shellcode-based downloader frequently utilized to deliver diverse malware. Its encrypted payload, encompassing PE headers, permits threat actors to leverage public cloud services, evade antivirus measures, and maintain payloads for extended durations. Initial versions were VB6 applications with encrypted shellcode. Recent iterations primarily utilize VBScript and NSIS installer in common attacks

GuLoader functions as the gatekeeper for Agent Tesla.

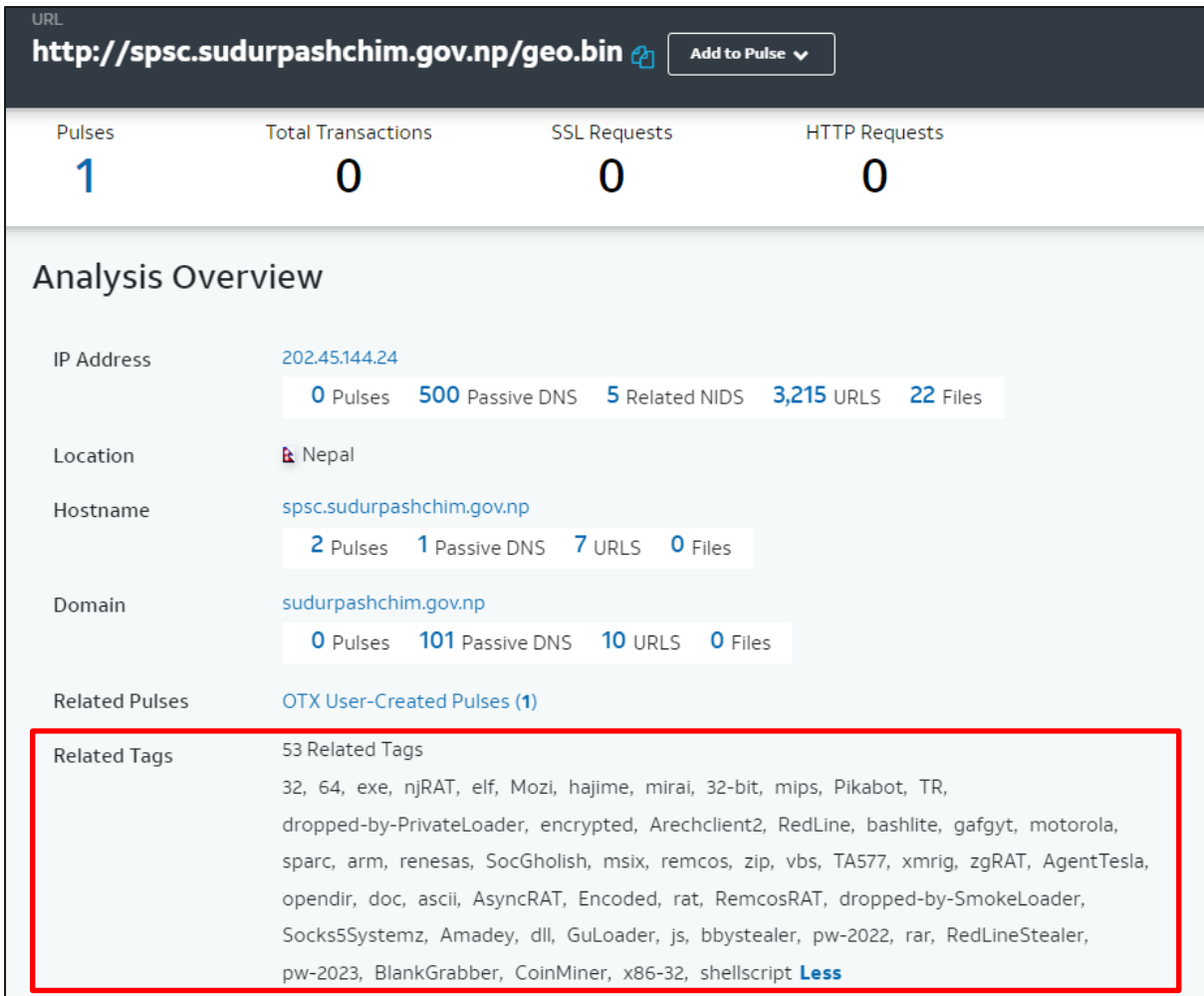


Figure 2: Tags related to the website.

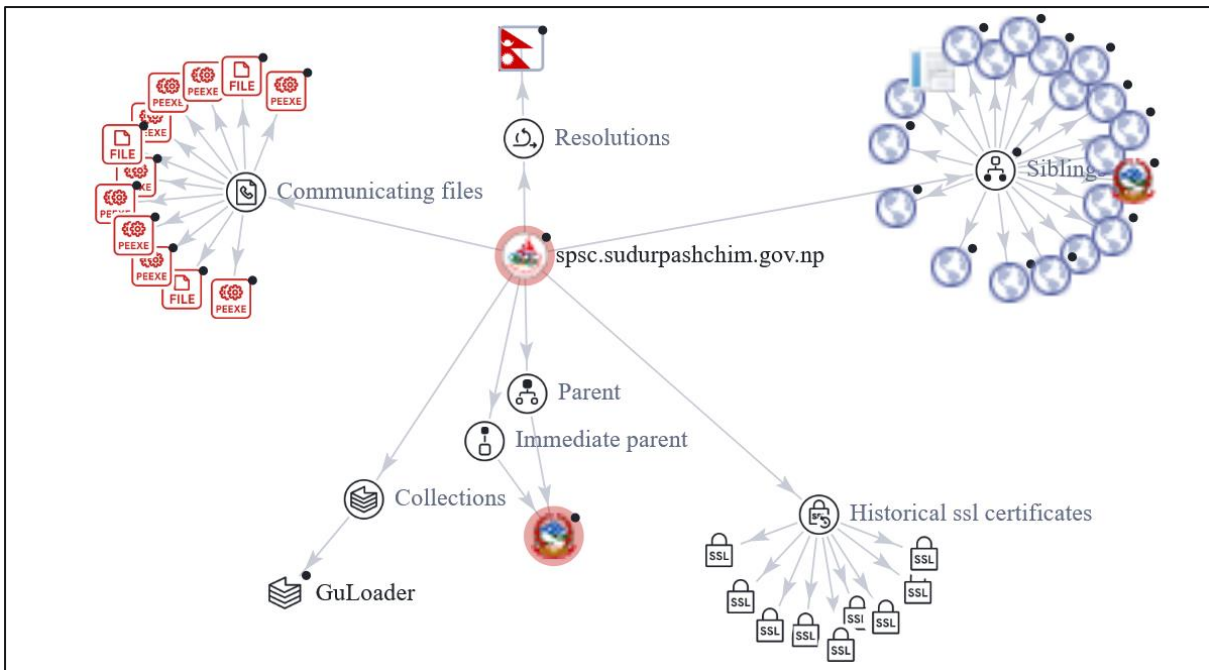


Figure 3: Network Infrastructure.

To delve deeper into the investigation, the IP address hosting the website was examined for additional analysis.

Communicating Files (2.6 K) ⓘ			
Scanned	Detections	Type	Name
2016-01-18	51 / 54	Win32 EXE	00016865ba8e5ed2f6d1cb2ffe8312e944e55b4bfa793ad770760a1b263205ff
2016-06-05	49 / 56	Win32 EXE	isheriff_1617bc0461822a4306c9a217a688364d.bin
2014-10-25	46 / 54	Win32 EXE	Form80.exe
2015-06-07	47 / 57	Win32 EXE	005e74a20f90440ca0849b55a3c71f6225e099df1eee7dac77fe89106c67aa6d
2015-07-15	48 / 56	Win32 EXE	cmview.exe
2015-09-08	45 / 56	Win32 EXE	CatchColor.exe
2014-10-19	45 / 54	Win32 EXE	vt-upload-UdRFI
2014-05-09	44 / 52	Win32 EXE	X-JZ-A
2014-05-31	50 / 53	Win32 EXE	wfplk.pif
2015-06-27	48 / 56	Win32 EXE	drvinst32

More than 2000 malicious files were communicating with the IP Address.

10 / 89
Community Score

⚠️ 10 security vendors flagged this domain as malicious

koshitappu.gov.np

Phishing and Other Frauds government phishing and fraud top-1M

12 / 89
Community Score

⚠️ 12 security vendors flagged this domain as malicious

lmis.nafqlml.gov.np
nafqlml.gov.np

government spyware and malware unknown

8 / 89
Community Score

⚠️ 8 security vendors flagged this domain as malicious

gandakiacademy.gov.np

Government/Legal, Malicious, Suspicious (alphaMountain.ai) top-1M

13 / 89

13 security vendors flagged this domain as malicious

spsc.sudurpashchim.gov.np
sudurpashchim.gov.np

Similar Graph API

Last Analysis Date
1 day ago

Community Score

DETECTION DETAILS RELATIONS **COMMUNITY 1**

Contained In Collections (1)

GuLoader Updated 1 hour ago by CarlosCabal
trusted CloudEye (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwir...
Files: 4.4 K URLs: 2.0 K Domains: 441 IPs: 30

2 / 89

2 security vendors flagged this domain as malicious

pmisfansep.moald.gov.np
moald.gov.np

Phishing and Other Frauds government

Community Score

2 / 89

2 security vendors flagged this domain as malicious

pmisfansep.moald.gov.np
moald.gov.np

Phishing and Other Frauds government

Community Score

6 / 89

6 security vendors flagged this domain as malicious

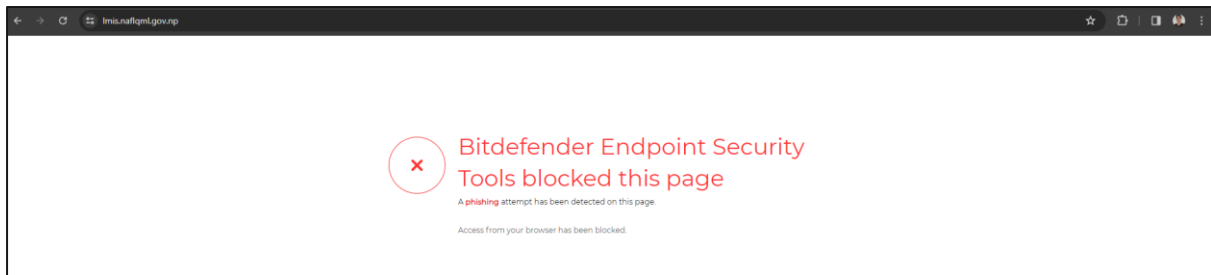
volunteer.karnali.gov.np
karnali.gov.np

Government/Legal, Phishing (alphaMountain.ai) top-1M

Community Score

This indicates that a significant number of genuine websites have been identified as potential security threats, with VirusTotal flagging them as potential phishing platforms.

When attempting to access these websites through a web browser, they are blocked, with the category identified as phishing.



Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2023-12-08 10:01:12	http://spsc.sudurpashchim.gov.np/geo.bin	Online	encrypted GuLoader	abuse_ch
2023-12-07 16:43:09	http://spsc.sudurpashchim.gov.np/PE.bin	Online	encrypted GuLoader	abuse_ch
2023-12-07 07:30:14	http://spsc.sudurpashchim.gov.np/ro.bin	Online	AgentTesla encrypted GuLoader	abuse_ch
2023-12-07 07:30:14	http://spsc.sudurpashchim.gov.np/TUR.bin	Online	AgentTesla encrypted GuLoader	abuse_ch
2023-12-07 07:30:12	http://spsc.sudurpashchim.gov.np/mix.bin	Online	AgentTesla encrypted GuLoader	abuse_ch
2023-11-27 16:39:21	https://nafiqml.gov.np/ctin/	Offline	IcedID TR	k3dg3
2023-05-02 20:11:14	https://bnp.bhimeshwormun.gov.np/gkonf/rentfree...	Offline	obama259 Qakbot USA wsf zip	Cryptolaemus1
2022-12-22 21:18:32	https://mof.gov.np/MEU.php	Offline	B1 BB11 iso Qakbot qbot Quakbot TR U22 zip	Cryptolaemus1
2022-12-21 00:47:17	https://mof.gov.np/mo/index.php	Offline	BB11 img Qakbot qbot Quakbot RR17 TR vhd zip	Cryptolaemus1
2022-12-19 16:38:03	https://mof.gov.np/epmv/index.php	Offline	BB11 img iso Qakbot qbot Quakbot TR TR23 zip	Cryptolaemus1
2022-12-15 17:29:36	https://mof.gov.np/uu/index.php	Offline	S0000 E17 Gozi ISFB iso PM11 TR zip	Cryptolaemus1
2022-12-14 16:08:28	https://mof.gov.np/anim/index.php	Offline	BB10 iso nt005 Qakbot qbot Quakbot TR zip	Cryptolaemus1
2022-12-13 20:30:01	https://mof.gov.np/eoot/index.php?qbot.zip	Offline	675 BB10 iso nt005 Qakbot qbot Quakbot TR zip	Cryptolaemus1
2022-12-07 18:55:25	https://mof.gov.np/ib/index.php?QBOT.zip	Offline	BB09 Qakbot qbot Quakbot TR U12 vhd zip	Cryptolaemus1
2022-12-05 15:19:42	https://gandakiacademy.gov.np/vsu/index.php?QBO...	Offline	BB09 N54 Qakbot qbot Quakbot TR vhd zip	Cryptolaemus1
2021-05-05 21:43:11	https://hetauda.leo.gov.np/_public/back/plugins...	Offline	Dridex	Cryptolaemus1
2020-10-15 13:38:06	http://nifadp.gov.np/gradle-pass/Document/l2n97...	Offline	doc emotet epoch2 heodo	Cryptolaemus1
2020-09-28 22:30:36	http://npncl.gov.np/wp-content/docs/yiUcupFdv3U...	Offline	doc emotet epoch1 heodo	Cryptolaemus1

Figure 4: Flagged government site by abuse.ch.

Hence, malicious actors are exploiting numerous government websites for their command-and-control server, phishing attempt, distributing malware, and for malicious purposes. Since 2020, our government sites have been consistently targeted by these actors. Despite several being taken offline or removed, starting from early December 2023, Agent Tesla has resumed utilizing one of our government websites, specifically `Hxxp://spsc.[.]sudurpashchim.[.]gov.[.]np/`, as a conduit for distributing their malware.

Tactics, Techniques, and Procedure

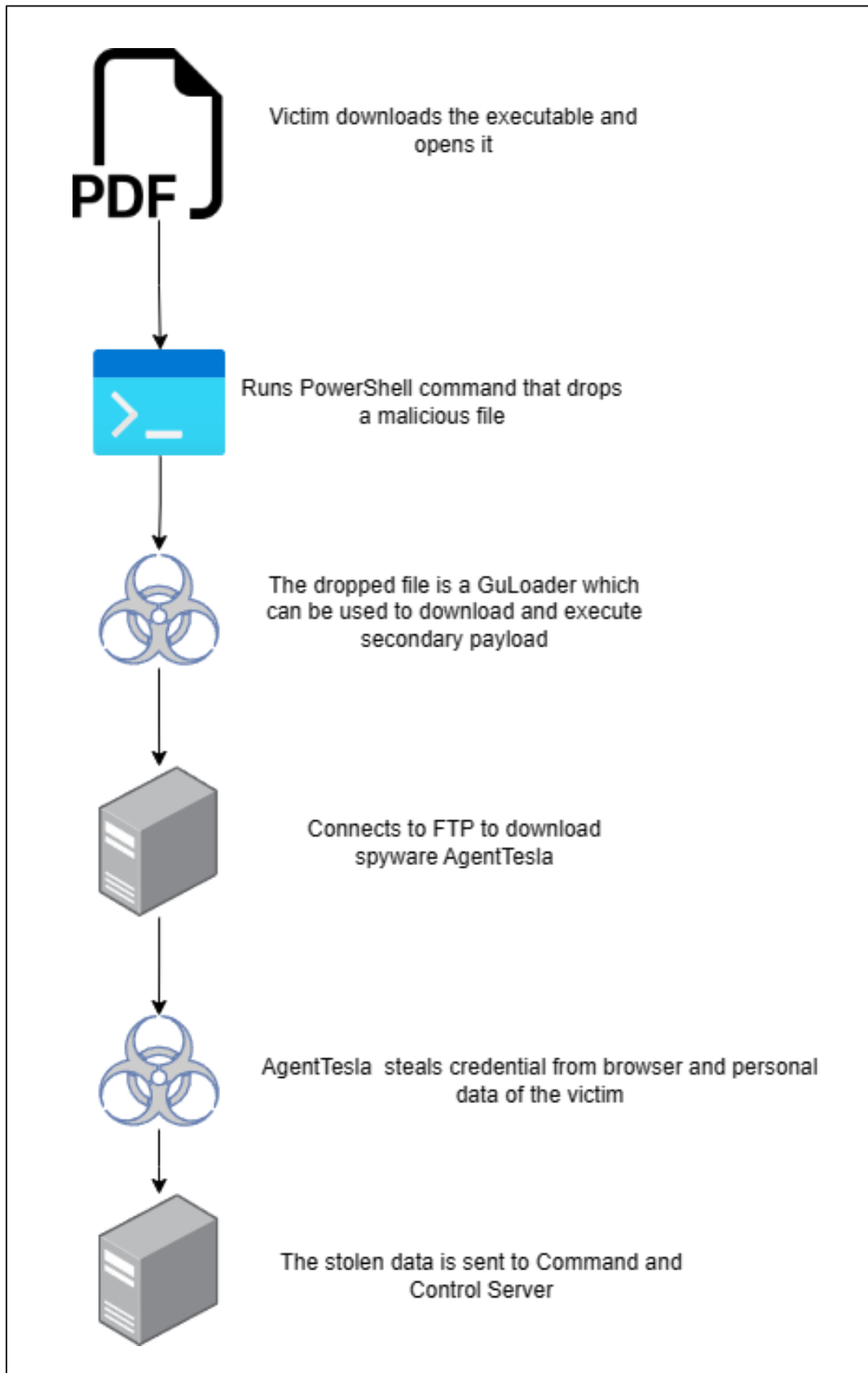
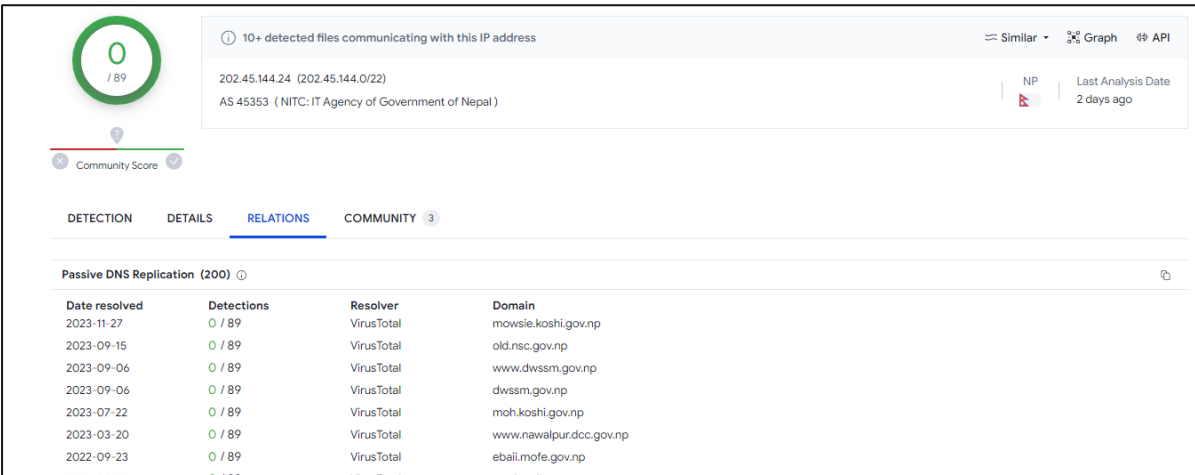


Figure 5: Infection Chain.

Let's delve into the intricate operations of the malware on the victim's PC, uncovering a comprehensive series of actions. Initially, the victim unwittingly acquires the malicious file through a phishing email or a provided link. Upon attempting to open the file, the executable file, distinguished by the MD5 hash "102714cb47ab0624d79ed174a8231ad6", is deployed and executed. This executable discreetly establishes its residence in the "C:\Users\admin\AppData\Local\Temp" directory.

Upon execution, the malware orchestrates a systematic compromise of the victim's system. It commences by extracting the computer name and generating files and folders within the user directory. Simultaneously, it initiates PowerShell in an invisible window. In parallel, an identical file, recognized by the MD5 hash "102714cb47ab0624d79ed174a8231ad6" is duplicated into the "C:\Users\admin\AppData\Roaming" directory.

The malware then extends its reach by connecting to an FTP server with the IP address 87[.]236[.]102[.]132 on port 21. To gain insights into the victim's system, it probes and retrieves information on Internet settings and proxy configurations. Concurrently, GuLoader is activated, establishing a connection to the IP address 202[.]45[.]144[.]24. Notably, further investigation reveals that this IP address corresponds to the location where the websites of the Nepal government are hosted.



The screenshot displays the VirusTotal interface for the IP address 202.45.144.24. The interface shows a community score of 0/89 and a status of "10+ detected files communicating with this IP address". The IP is identified as AS 45353 (NITC: IT Agency of Government of Nepal). The "RELATIONS" tab is active, showing a table of "Passive DNS Replication (200)".

Date resolved	Detections	Resolver	Domain
2023-11-27	0 / 89	VirusTotal	mowsie.koshi.gov.np
2023-09-15	0 / 89	VirusTotal	old.nsc.gov.np
2023-09-06	0 / 89	VirusTotal	www.dwssm.gov.np
2023-09-06	0 / 89	VirusTotal	dwssm.gov.np
2023-07-22	0 / 89	VirusTotal	moh.koshi.gov.np
2023-03-20	0 / 89	VirusTotal	www.nawalpur.dcc.gov.np
2022-09-23	0 / 89	VirusTotal	ebali.mofe.gov.np
2022-09-03	0 / 89	VirusTotal	tourismdharan01.gov.np

In the final stages, Agent Tesla comes into play, clandestinely pilfering personal data and credentials from web browsers. This ill-gotten information is then transmitted to the Command and Control (CnC) server with the IP address **87[.]236[.]102[.]132** on port 56237. Remarkably, this entire sequence of actions unfolds surreptitiously in the background of the victim's PC, operating without their awareness.

MITRE ATT&CK techniques

The malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566) <ul style="list-style-type: none"> Spear phishing Attachment (T1566.001)
Execution	Command and Scripting Interpreter (T1059) <ul style="list-style-type: none"> PowerShell (T1059.001)
Defense Evasion	Hide Artifacts (T1564) <ul style="list-style-type: none"> Hidden Windows (T1564.003)
Credential Access	Credentials from Password Stores (T1555) <ul style="list-style-type: none"> Credentials from Web Browsers (T1555.03)
	Unsecured Credentials (T1552) <ul style="list-style-type: none"> Credentials In Files (T1552.001)
Discovery	Software Discovery (T1518)
	Query Registry (T1012)
	System Information Discovery (T1082)
Command and Control	Application Layer Protocol (T1071) <ul style="list-style-type: none"> Web Protocols (T1071.001) Mail Protocols (T1071.003) DNS (T1071.004)
	Non-Standard Port (T1571)

Indicators of Compromise (IOCs)

IP Addresses

40[.]79[.]141[.]152

20[.]189[.]173[.]14

87[.]236[.]102[.]132

202[.]45[.]144[.]24

23[.]53[.]40[.]72

52[.]109[.]89[.]117

52[.]113[.]194[.]132

2[.]22[.]242[.]227

52[.]109[.]28[.]46

2[.]22[.]242[.]129

Hashes

99471b98351a369f4b5114cdf32223fc

0da1ad1d456b5b7a028efcbfd9c3ee45af7c6830c87c1e7469faa089dbb0fe7e

Domains

ftp[.]vvspijkenisse[.]nl

spsc[.]sudurpashchim[.]gov[.]np

Threat Summary	
Name	Agent Tesla
Threat Type	Malware, Trojan, Evader, Stealer, GuLoader
Detection Names	BitDefender: Trojan.Zmutzy.Pong.3, Gridinsoft: Trojan.U.AgentTesla.tr Microsoft: Trojan:Win32/GuLoader.KA!MTB
Symptoms	Unusual Network Activity, Sluggish System Performance, Unauthorized Software Installs, Modified Proxy Settings, Altered Registry Values, Elevated CPU and Memory Usage, Disabled Security Software, Unrecognized Processes, and Data modifications.
Additional Information	It's important to keep in mind that Agent Tesla may not be the only malware present in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans.
Distribution methods	Spear-phishing techniques
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Effective removal typically requires using robust antivirus or antimalware software capable of detecting and eradicating the malware components. Additionally, restoring the system to a known good state through system backups and performing a thorough analysis of network activity is recommended to ensure complete removal and mitigate potential residual threats.

Vairav Recommendations

We recommend the following to mitigate and prevent ransomware attacks:

1. **Immediate Isolation:** Isolate the compromised devices to prevent further communication with malicious actors and to contain the potential damage.
2. **Thorough Security Audit:** Conduct a comprehensive security audit of all government websites to identify vulnerabilities and assess the extent of the compromise.
3. **Malware Removal:** Employ robust antivirus or antimalware software to initiate a thorough malware removal process on affected servers and workstations.
4. **System Restoration:** Restore affected systems to a known good state using reliable system backups to ensure the removal of malware remnants and to mitigate potential risks.
5. **Network Analysis:** Perform a detailed analysis of network activity to identify any unusual patterns, connections, or suspicious behavior associated with the malware.
6. **Update and Patching:** Ensure that all systems, servers, and software are updated with the latest security patches to address known vulnerabilities that may have been exploited.
7. **User Awareness Training:** Conduct cybersecurity awareness training for government personnel to enhance their understanding of phishing threats and the importance of exercising caution while handling emails and links.
8. **Implement Intrusion Detection Systems (IDS):** Deploy and configure intrusion detection systems to detect and alert any suspicious or unauthorized activities within the network.

9. **Enhanced Monitoring:** Implement enhanced monitoring protocols for government websites, servers, and network traffic to promptly detect and respond to any future security incidents.
10. **Collaborate with Cybersecurity Agencies:** Collaborate with national and international cybersecurity agencies to share threat intelligence and leverage collective expertise in addressing the ongoing security threat.
11. **Regular Security Assessments:** Conduct regular security assessments and penetration testing to proactively identify and address vulnerabilities before they can be exploited.
12. **Communication Strategy:** Develop and implement a transparent and timely communication strategy to inform the public, stakeholders, and relevant authorities about the security incident, the measures taken, and the steps they can take to secure their systems.

It is important to remember that the cyber adversaries behind are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: <https://vairav.net>