ADVANCED PERSISTENT THREAT (APT) SIDEWINDER: THIRD WAVE IN ENTITIES OF NEPAL

SIDEWINDER, RATTLESNAKE, T-APT-04

Vairav Advisory Report

14th February 2025

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

This report uncovers a significant cybersecurity threat orchestrated by APT Sidewinder, a highly sophisticated and persistent threat actor. The group has recently launched a targeted attack mimicking Nepalese government agencies, employing advanced deception tactics to infiltrate official systems. A key element of this campaign is deploying a fraudulent website impersonating Nepal's centralized government email service. This fake login page, designed to harvest usernames and passwords, closely mimics an official government portal to deceive users into disclosing their credentials.

Key Findings

- The campaign specifically aims at compromising government officials by deploying fake authentication portals.
- APT Sidewinder has created a fraudulent Nepal government email login page to steal sensitive login credentials.
- The attackers utilize social engineering, website spoofing, and credential phishing to enhance their success rate.

Threat Actor Profile

<table>
<tr><th colspan="2">APT SIDEWINDER</th></tr>
<tr><td colspan="2">Sidewinder is a suspected Indian threat actor group that has been active since at least 2012. The group has been observed targeting government, military, ISP, and telecom business entities throughout Asia.</td></tr>
<tr><td>Period of Activity: 2012-PRESENT</td><td rowspan="2">TOP 5 Targeted Industries
Military
Government
Education
Healthcare
Crypto
Telecommunication</td></tr>
<tr><td>Other Names:
Rattlesnake, Hardcore Nationalist, HN2, -APT-Q4, APT-C-17, RAZOR Tiger, APT-Q-39, BabyElephant, GroupA21</td></tr>
<tr><td colspan="2">Most Frequently Targeted Countries: Pakistan, Bangladesh, Bhutan, Nepal, Myanmar, Afghanistan, China, Philippines, Singapore, Qatar</td></tr>
</table>

Table 1: Threat Actor Profile

HISTORY OF ATTACK LAUNCHED IN NEPAL

2022 - Phishing & Government Impersonation

Sidewinder used government-themed phishing emails to lure victims into downloading malicious Word documents. The documents contained macro-based payloads that executed malware that connected to command-and-control (C2) servers. The malware stole government login credentials and allowed persistent access to compromised systems.

Discovered Domains of that incident

Malicious Domain	Targeting
wmofa-gov-sa.direct888[.]net	Ministry of Foreign Affairs, Saudi Arabia
wwww.mofa-gov-sa.direct888[.]net	
Mofa-gov-sa/direct888[.]net	
www-police-gov-bd.direct888[.]net	Bangladesh Police
nepalcert-org.fia-gov[.]net	CERT, Nepal
Mopf-gov-mm.direct888[.]net	Ministry of Planning and Finance, Myanmar
Navy-lk.direct888[.]net	Sir Lankan Navy
Nextgen.fia-gov[.]net	ICT Agency of Sri Lanka (ICTA)
www-moha-gov-lk.direct888[.]net	Ministry of Home Affairs, Sir Lanka
Mofa-gov-np.direct888[.]net	Ministry of Foreign Affairs, Nepal
opmcm-gov-np.fia-gov[.]net	Office of the Prime Minister and Council of Ministers
moitt-gov-pk.fia-gov[.]net	Ministry of Information Technology & Telecommunication, Pakistan
wwww.moitt-gov-pk.fia-gov[.]net	

Table 2: Findings of 2023 Attack - Phishing & Government Impersonation

2023 - Targeted incursions aimed at Nepal's governmental entities

Vairav Technology identified a phishing campaign targeting Nepalese government agencies, including the Office of the Prime Minister & Council of Ministers and the Ministry of Foreign Affairs, using a malicious document embedded with macros. The decoy document, suspected to have been stolen from the Prime Minister's Personal Secretariat via a compromised email, was circulated between September 15th and November 18th, 2023.

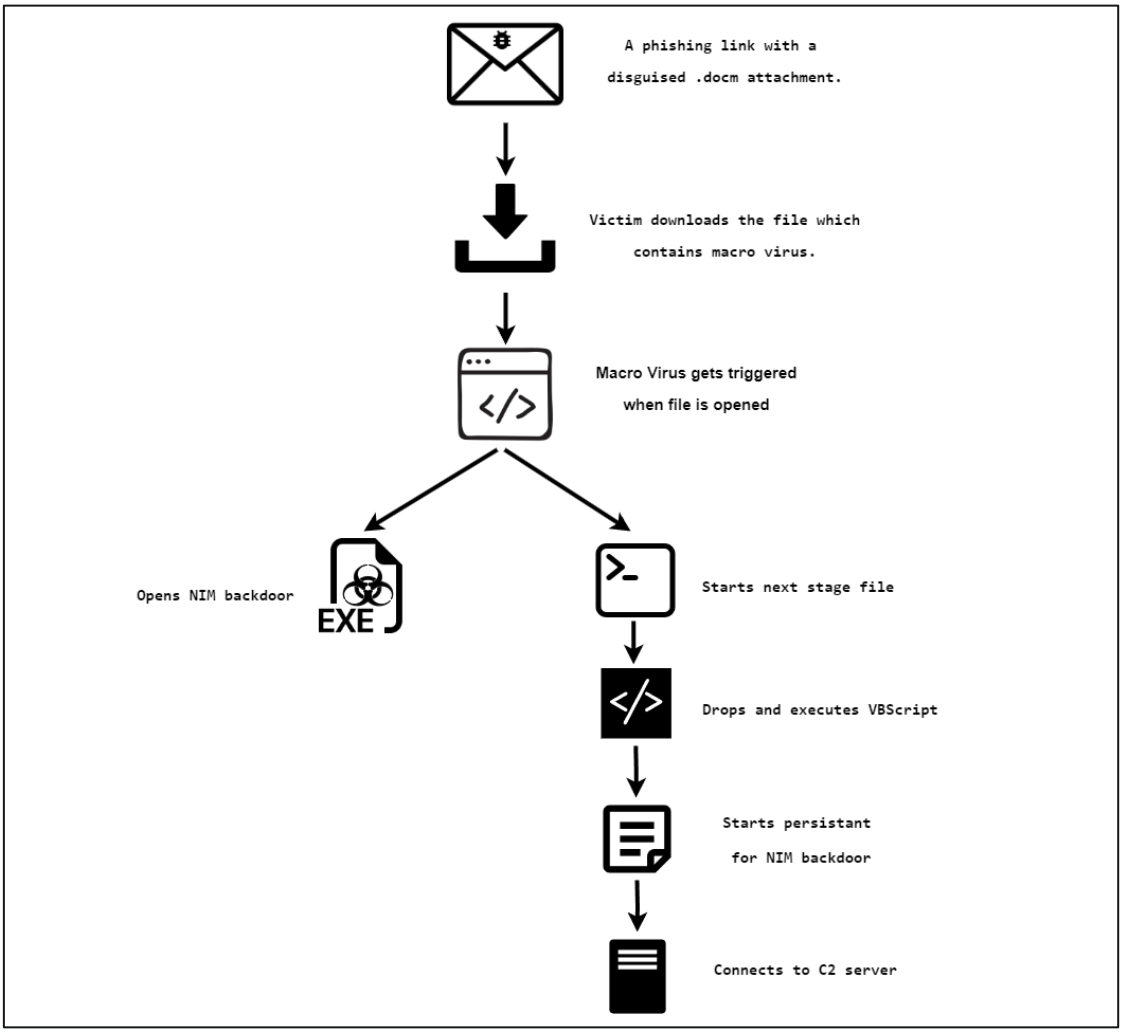

Figure 1: Infection Chain.

File Hash (MD5)	File Type	File Size
e2a3edc708016316477228de885f0c39	Macro document	857.74 KB
5533daa9a34eab3ff725a4e7a873a519	Document	712.50 KB

Table 2: The hash value of the .docm file.

2025 - Nepal Government with Phishing Attack

In 2025, APT SideWinder launched another targeted phishing campaign against Nepalese government agencies, continuing its long-standing focus on South Asian entities. This attack involved a fraudulent Nepal government email login page designed to harvest official credentials.

Figure 2: Fake login page.

TACTICS, TECHNIQUES, AND PROCEDURE

APT **SideWinder** is known for employing a range of advanced tactics and techniques to infiltrate government systems. In this 2025 campaign, the attackers utilized **social engineering**, **phishing**, and **website spoofing** to trick government officials into revealing their credentials.

Attack Methodology

Phishing & Spoofed Website:

- The attackers registered a fraudulent domain (mail.nepla.gov.np.onlinestatus[.]live), mimicking the official Nepal government email system.
- They designed a fake login page (as shown in Figure 2) to steal credentials from government employees.
- The page resembled a legitimate portal, misleading users into entering their usernames and passwords.

Credential Harvesting & Data Exfiltration:

- Once credentials were entered into the phishing page, they were transmitted to a remote command-and-control (C2) server operated by the attackers.
- The stolen credentials could be used for further infiltration, including access to government communication channels and classified documents.

Another post from a security researcher was found posting the new Maldocs from APT Sidewinder on X.

Figure 3: Campaign reported by a security researcher on X (Formerly known as Twitter).

As part of the investigation into APT SideWinder's **2025 Nepal Government Phishing Attack**, the analysis of the **file hash values** reveals critical indicators of compromise (IOCs), including **dropped files and execution chains** that demonstrate the malware's behavior.

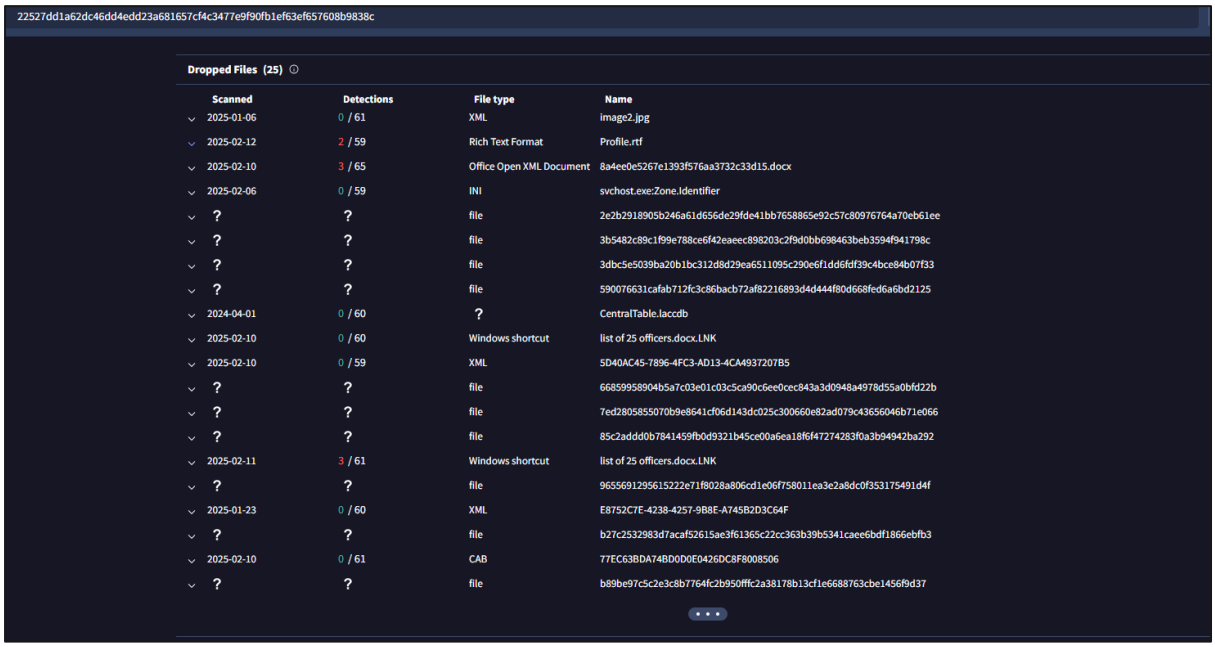

Figure 4: Dropped file from Maldocs.

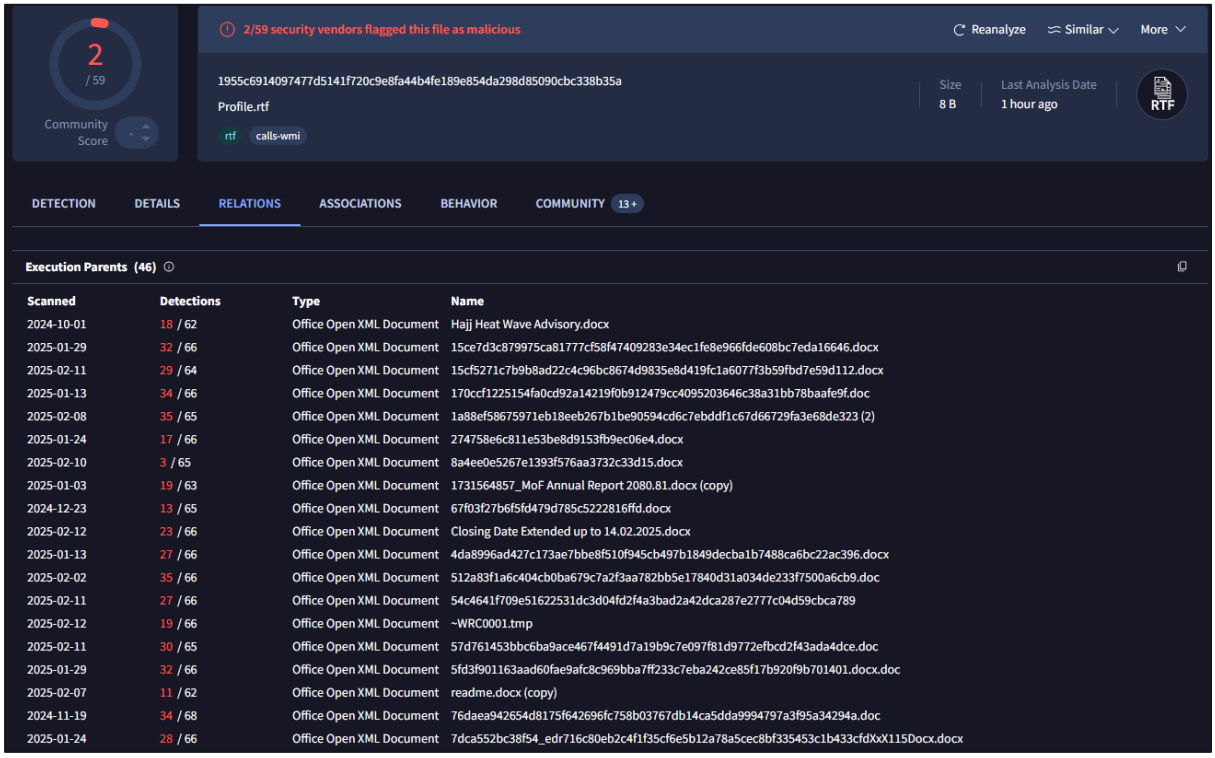

Figure 5: Execution parents of the file.

Correlation Between Dropped Files and Phishing URLs

By analyzing the dropped files and their execution flow, a direct correlation was found between one of the malicious files and a phishing URL masquerading as an official Nepali government site. This indicates that APT SideWinder's campaign involved a multi-layered attack strategy, where malware deployment was linked to credential-harvesting phishing sites.

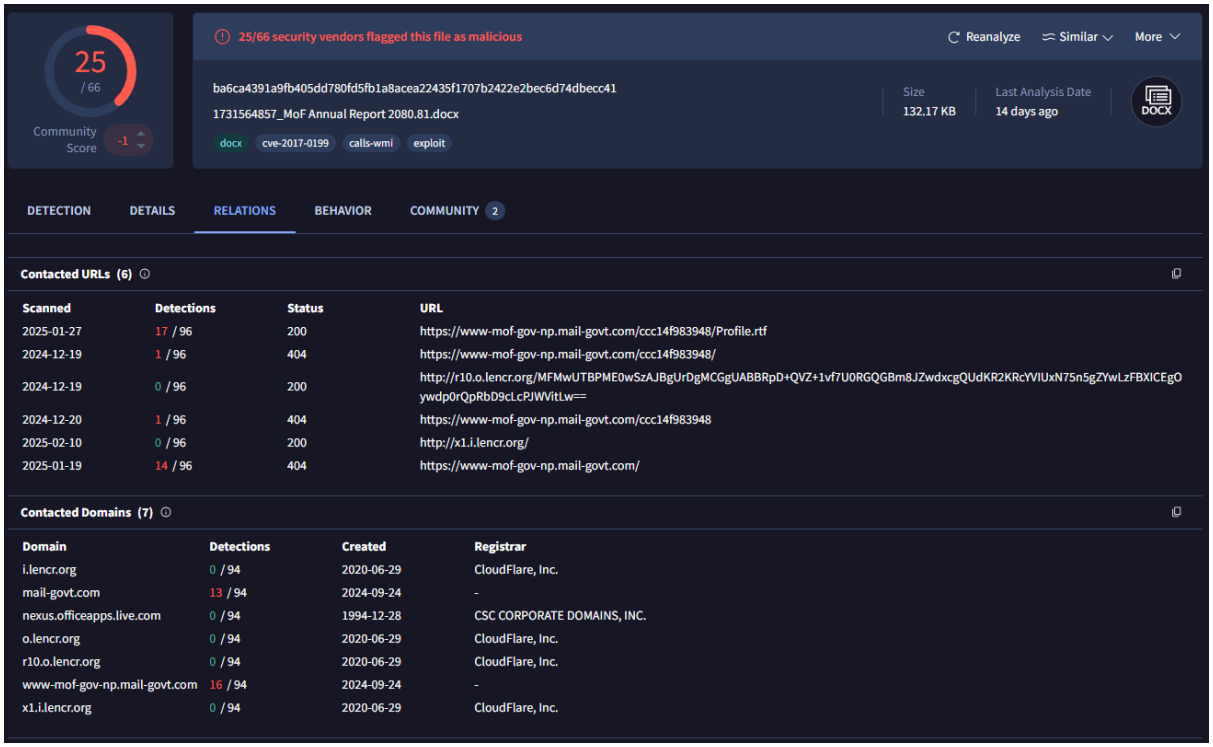

Figure 6: File connected with phishing URL targeting Nepali government sites.

Based on the observed evidence, APT SideWinder appears to follow a two-phase strategy:

- **Phase 1:**

  Credential Harvesting via Phishing Website

- **Phase 2:**

  Malware Propagation via Stolen Email Accounts

This approach allows the threat actor to exploit trust within government agencies, ensuring higher infection rates and deeper infiltration into sensitive networks.

Attack Flow according to the evidence found

Step 1: Phishing page imitates official Nepal government login

- Attackers spoof the Nepal Government's centralized email portal to steal usernames and passwords.
- Employees unknowingly enter their credentials, believing they are accessing an official system.

Step 2: Compromised credentials used for internal phishing

- The stolen credentials are then used to access legitimate government email accounts.
- The attackers send phishing emails from these hijacked accounts, increasing credibility and reducing suspicion among recipients.

Step 3: Phishing emails to distribute malicious documents

- The emails contain macro-embedded Word documents (Maldocs) that appear to be legitimate government files.
- Employees download and open the document, enabling macros, which triggers malware execution

Step 4: Malware deployment & persistent access

- The malicious macro executes a payload, which downloads and installs additional malware.
- The malware may establish command-and-control (C2) communication, allowing remote access and data exfiltration.

Step 5: Lateral movement & further compromise

- Using stolen credentials, attackers expand their access to additional systems.
- They continue the infection cycle, spreading within the government network and potentially compromising critical national infrastructure.

Why This Tactic Is Effective

- **Leverages Internal Trust:** Since phishing emails originate from genuine government email accounts, recipients are more likely to trust and open malicious attachments.
- **Bypasses Traditional Security Controls:** Many email security solutions focus on external threats. When emails originate from trusted sources, security tools may not flag them as malicious.
- **Creates a Continuous Infection Loop:** Once an account is compromised, it is used to infect more victims, ensuring sustained access to government networks.
- **Targeted Attacks for Strategic Espionage:** By targeting government officials, SideWinder gains access to sensitive intelligence, policy documents, and classified communications.

INDICATORS OF COMPROMISE (IOCS)

Type	Value
Hash (SHA-256)	ba6ca4391a9fb405dd780fd5fb1a8acea22435f1707b2422e2bec6d74dbecc41
URL	hxxps://www-mof-gov-np.mail-govt.com/ccc14f983948/Profile.rtf hxxps://mail.nepla.gov.np.onlinestatus[.]live/MOfYcTyI
Domain	mail.nepla.gov.np.onlinestatus[.]live www-mof-gov-np.mail-govt[.]com
IP	51.89.9[.]145, 188.214.38[.]63

DETECTION

Rule 1: Activity_Sequence_by_Sidewinder

```
title: Activity_Sequence_by_Sidewinder
id: sidewinder_activity_sequence
Description: Detects a sequence of malicious activities of the
sidewinder, including VBScript execution, BAT file execution,
ZIP content copying, and executable launch.
author: Rodan Maharjan
date: 2023-11-29
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    - EventID: 1
      Image:
'C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\*.vbs'
    - EventID: 1
      Image: 'C:\Users\windows\AppData\Local\*.bat'
    - EventID: 7
      TargetFilename: 'C:\Users\windows\AppData\Local\*'
      DestinationFilename: 'C:\Users\windows\AppData\Local\*'
      CommandLine: '*\Microsoft\conhost.zip*'
    - EventID: 1
      Image: 'C:\Users\windows\AppData\Local\*.exe'
    - EventID: 1
      CommandLine: '*\*.exe'
  condition: all of them
Tags:
  - malicious
falsepositives:
  - Legitimate use of scripts and executables
level: high
```

Rule 2: Office Macro File Creation

```
title: Office Macro File Creation
id: 91174a41-dc8f-401b-be89-7bfc140612a0
related:
    - id: 0e29e3a7-1ad8-40aa-b691-9f82ecd33d66
      type: similar
status: test
description: Detects the creation of a new office macro files
on the systems
references:
    - https://github.com/redcanaryco/atomic-red-
team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T15
66.001/T1566.001.md
    - https://learn.microsoft.com/en-
us/deployoffice/compat/office-file-format-reference
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022-01-23
tags:
    - attack.initial-access
    - attack.t1566.001
logsource:
    category: file_event
    product: windows
detection:
    selection:
        TargetFilename|endswith:
            - '.docm'
            - '.dotm'
            - '.xlsm'
            - '.xltm'
            - '.potm'
            - '.pptm'
    condition: selection
falsepositives:
```

```
    - Very common in environments that rely heavily on macro
documents
level: low
```

Rule 3: Rundll32 UNC Path Execution

```
title: Rundll32 UNC Path Execution
id: 5cdb711b-5740-4fb2-ba88-f7945027afac
status: test
description: Detects rundll32 execution where the DLL is
located on a remote location (share)
references:
    - https://www.cybereason.com/blog/rundll32-the-infamous-
proxy-for-executing-malicious-code
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022-08-10
tags:
    - attack.defense-evasion
    - attack.execution
    - attack.t1021.002
    - attack.t1218.011
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: '\rundll32.exe'
        - OriginalFileName: 'RUNDLL32.EXE'
        - CommandLine|contains: 'rundll32'
    selection_cli:
        CommandLine|contains: ' \\\\'
    condition: all of selection_*
falsepositives:
    - Unlikely
level: high
```

Rule 4: Office application-initiated network connection to non-local IP

```
title: Office Application Initiated Network Connection To Non-Local IP
id: 75e33ce3-ae32-4dcc-9aa8-a2a3029d6f84
status: test
description: |
    Detects an office application (Word, Excel, PowerPoint) that initiate a network connection to a non-private IP addresses.
    This rule aims to detect traffic similar to one seen exploited in CVE-2021-42292.
    This rule will require an initial baseline and tuning that is specific to your organization.
references:
    - https://corelight.com/blog/detecting-cve-2021-42292
    - https://learn.microsoft.com/de-de/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide
author: Christopher Peacock '@securepeacock', SCYTHE '@scythe_io', Florian Roth (Nextron Systems), Tim Shelton, Nasreddine Bencherchali (Nextron Systems)
date: 2021-11-10
modified: 2024-07-02
tags:
    - attack.execution
    - attack.t1203
logsource:
    category: network_connection
    product: windows
detection:
    selection:
        Image|endswith:
            - '\excel.exe'
            - '\outlook.exe'
            - '\powerpnt.exe'
```

```
            - '\winword.exe'
            - '\wordview.exe'
        Initiated: 'true'
    filter_main_local_ranges:
        DestinationIp|cidr:
            - '127.0.0.0/8'
            - '10.0.0.0/8'
            - '172.16.0.0/12'
            - '192.168.0.0/16'
            - '169.254.0.0/16'
            - '::1/128'  # IPv6 loopback
            - 'fe80::/10'  # IPv6 link-local addresses
            - 'fc00::/7'  # IPv6 private addresses
    filter_main_msrange_generic:
        DestinationIp|cidr:
            - '20.184.0.0/13' # Microsoft Corporation
            - '20.192.0.0/10' # Microsoft Corporation
            - '23.72.0.0/13' # Akamai International B.V.
            - '40.76.0.0/14' # Microsoft Corporation
            - '51.10.0.0/15' # Microsoft Corporation
            - '51.103.0.0/16' # Microsoft Corporation
            - '51.104.0.0/15' # Microsoft Corporation
            - '51.142.136.0/22' # Microsoft Corporation -
https://ipinfo.io/AS8075/51.140.0.0/14-51.142.136.0/22
            - '52.160.0.0/11' # Microsoft Corporation -
https://ipinfo.io/AS8075/52.160.0.0/11
            - '204.79.197.0/24' # Microsoft Corporation
    filter_main_msrange_exchange_1:
        # Exchange Online
        # "urls": [
        #       "outlook.cloud.microsoft",
        #       "outlook.office.com",
        #       "outlook.office365.com"
        # ]
```

```
        DestinationIp|cidr:
            - '13.107.6.152/31'
            - '13.107.18.10/31'
            - '13.107.128.0/22'
            - '23.103.160.0/20'
            - '40.96.0.0/13'
            - '40.104.0.0/15'
            - '52.96.0.0/14'
            - '131.253.33.215/32'
            - '132.245.0.0/16'
            - '150.171.32.0/22'
            - '204.79.197.215/32'
            - '2603:1006::/40'
            - '2603:1016::/36'
            - '2603:1026::/36'
            - '2603:1036::/36'
            - '2603:1046::/36'
            - '2603:1056::/36'
            - '2620:1ec:4::152/128'
            - '2620:1ec:4::153/128'
            - '2620:1ec:c::10/128'
            - '2620:1ec:c::11/128'
            - '2620:1ec:d::10/128'
            - '2620:1ec:d::11/128'
            - '2620:1ec:8f0::/46'
            - '2620:1ec:900::/46'
            - '2620:1ec:a92::152/128'
            - '2620:1ec:a92::153/128'
        DestinationPort:
            - 80
            - 443
    filter_main_msrange_exchange_2:
        # Exchange Online
        # "urls": [
```

```
        #         "outlook.office365.com",
        #         "smtp.office365.com"
        # ]
        DestinationIp|cidr:
            - '13.107.6.152/31'
            - '13.107.18.10/31'
            - '13.107.128.0/22'
            - '23.103.160.0/20'
            - '40.96.0.0/13'
            - '40.104.0.0/15'
            - '52.96.0.0/14'
            - '131.253.33.215/32'
            - '132.245.0.0/16'
            - '150.171.32.0/22'
            - '204.79.197.215/32'
            - '2603:1006::/40'
            - '2603:1016::/36'
            - '2603:1026::/36'
            - '2603:1036::/36'
            - '2603:1046::/36'
            - '2603:1056::/36'
            - '2620:1ec:4::152/128'
            - '2620:1ec:4::153/128'
            - '2620:1ec:c::10/128'
            - '2620:1ec:c::11/128'
            - '2620:1ec:d::10/128'
            - '2620:1ec:d::11/128'
            - '2620:1ec:8f0::/46'
            - '2620:1ec:900::/46'
            - '2620:1ec:a92::152/128'
            - '2620:1ec:a92::153/128'
        DestinationPort:
            - 143
            - 587
```

```
            - 993
            - 995
        Protocol: 'tcp'
    filter_main_msrange_exchange_3:
        # Exchange Online
        # "urls": [
        #       "*.protection.outlook.com"
        #  ]
        DestinationIp|cidr:
            - '40.92.0.0/15'
            - '40.107.0.0/16'
            - '52.100.0.0/14'
            - '52.238.78.88/32'
            - '104.47.0.0/17'
            - '2a01:111:f400::/48'
            - '2a01:111:f403::/48'
        DestinationPort: 443
    filter_main_msrange_exchange_4:
        # Exchange Online
        # "urls": [
        #       "*.mail.protection.outlook.com",
        #       "*.mx.microsoft"
        #  ]
        DestinationIp|cidr:
            - '40.92.0.0/15'
            - '40.107.0.0/16'
            - '52.100.0.0/14'
            - '52.238.78.88/32'
            - '104.47.0.0/17'
            - '2a01:111:f400::/48'
            - '2a01:111:f403::/48'
        DestinationPort: 25
    filter_main_msrange_sharepoint_1:
        # SharePoint Online and OneDrive for Business",
```

```
        # "urls": [
        #       "*.sharepoint.com"
        # ]
        DestinationIp|cidr:
            - '13.107.136.0/22'
            - '40.108.128.0/17'
            - '52.104.0.0/14'
            - '104.146.128.0/17'
            - '150.171.40.0/22'
            - '2603:1061:1300::/40'
            - '2620:1ec:8f8::/46'
            - '2620:1ec:908::/46'
            - '2a01:111:f402::/48'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_1:
        # Microsoft 365 Common and Office Online",
        # "urls": [
        #       "*.officeapps.live.com",
        #       "*.online.office.com",
        #       "office.live.com"
        # ],
        DestinationIp|cidr:
            - '13.107.6.171/32'
            - '13.107.18.15/32'
            - '13.107.140.6/32'
            - '52.108.0.0/14'
            - '52.244.37.168/32'
            - '2603:1006:1400::/40'
            - '2603:1016:2400::/40'
            - '2603:1026:2400::/40'
            - '2603:1036:2400::/40'
```

```
            - '2603:1046:1400::/40'
            - '2603:1056:1400::/40'
            - '2603:1063:2000::/38'
            - '2620:1ec:c::15/128'
            - '2620:1ec:8fc::6/128'
            - '2620:1ec:a92::171/128'
            - '2a01:111:f100:2000::a83e:3019/128'
            - '2a01:111:f100:2002::8975:2d79/128'
            - '2a01:111:f100:2002::8975:2da8/128'
            - '2a01:111:f100:7000::6fdd:6cd5/128'
            - '2a01:111:f100:a004::bfeb:88cf/128'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_2:
        # Microsoft 365 Common and Office Online
        # "urls": [
        #       "*.auth.microsoft.com",
        #       "*.msftidentity.com",
        #       "*.msidentity.com",
        #       "account.activedirectory.windowsazure.com",
        #       "accounts.accesscontrol.windows.net",
        #       "adminwebservice.microsoftonline.com",
        #       "api.passwordreset.microsoftonline.com",
        #       "autologon.microsoftazuread-sso.com",
        #       "becws.microsoftonline.com",
        #       "ccs.login.microsoftonline.com",
        #       "clientconfig.microsoftonline-p.net",
        #       "companymanager.microsoftonline.com",
        #       "device.login.microsoftonline.com",
        #       "graph.microsoft.com",
        #       "graph.windows.net",
        #       "login-us.microsoftonline.com",
```

```
        #       "login.microsoft.com",
        #       "login.microsoftonline-p.com",
        #       "login.microsoftonline.com",
        #       "login.windows.net",
        #       "logincert.microsoftonline.com",
        #       "loginex.microsoftonline.com",
        #       "nexus.microsoftonline-p.com",
        #       "passwordreset.microsoftonline.com",
        #       "provisioningapi.microsoftonline.com"
        # ]
        DestinationIp|cidr:
            - '20.20.32.0/19'
            - '20.190.128.0/18'
            - '20.231.128.0/19'
            - '40.126.0.0/18'
            - '2603:1006:2000::/48'
            - '2603:1007:200::/48'
            - '2603:1016:1400::/48'
            - '2603:1017::/48'
            - '2603:1026:3000::/48'
            - '2603:1027:1::/48'
            - '2603:1036:3000::/48'
            - '2603:1037:1::/48'
            - '2603:1046:2000::/48'
            - '2603:1047:1::/48'
            - '2603:1056:2000::/48'
            - '2603:1057:2::/48'
        DestinationPort:
            - 80
            - 443
        Protocol: 'tcp'
    filter_main_msrange_office_3:
        # Microsoft 365 Common and Office Online
        #  "urls": [
```

```
        #       "*.compliance.microsoft.com",
        #       "*.protection.office.com",
        #       "*.security.microsoft.com",
        #       "compliance.microsoft.com",
        #       "defender.microsoft.com",
        #       "protection.office.com",
        #       "security.microsoft.com"
        #   ]
        DestinationIp|cidr:
            - '13.107.6.192/32'
            - '13.107.9.192/32'
            - '52.108.0.0/14'
            - '2620:1ec:4::192/128'
            - '2620:1ec:a92::192/128'
        DestinationPort: 443
        Protocol: 'tcp'
    condition: selection and not 1 of filter_main_*
falsepositives:
    - You may have to tune certain domains out that Excel may call out to, such as microsoft or other business use case domains.
    - Office documents commonly have templates that refer to external addresses, like "sharepoint.ourcompany.com" may have to be tuned.
    - It is highly recommended to baseline your activity and tune out common business use cases.
level: medium
```

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	User Execution (T1204) • Malicious File (T1204.002)
Persistence	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
Privilege Escalation	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
Defense Evasion	Deobfuscate/Decode Files or Information (T1140)
Discovery	Query Registry (T1012)
	System Information Discovery (T1082)
Collection	Browser Session Hijacking (T1185)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001)
	Ingress Tool Transfer (T1105)

THREAT SUMMARY	
Name	Sidewinder, T-APT-04, Rattlesnake
Threat Type	Trojan, Downloader, Dropper, Macro Virus
Detection Names	Fortinet: VBA/Valyria.6953!tr, AVG: VBS:Obfuscated-gen [Trj], BitDefender: VB:Trojan.Valyria.6953, KasperskyUDS:DangerousObject.Multi.Generic.
Symptoms	Decoy Documents, Dynamic URL Requests, Unusual Network Activity, Scripted Attacks, Nim Backdoor Activation, Persistence Mechanisms, Unrecognized Processes, Data modifications.
Additional Information	The Nim backdoor's functionality, while relatively simple, is part of a potentially long-term and strategic operation. The consistency in the characteristics of the macro code and the Nim backdoor suggests a tried-and-tested approach by the attacker.
Distribution methods	Spear-phishing techniques, Document Exploitation
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. **Beware of phishing attacks:**
    - Exercise caution when encountering emails containing unexpected attachments or links, especially from unknown or unverified sources.
    - Refrain from clicking on links shared through social media channels if the source is unfamiliar.
2. **Avoid execution of unknown files**
    - Do not execute email attachments or run files with exaggerated titles, particularly those received from untrusted or unfamiliar sources.
    - Exercise discretion when dealing with files related to governmental activities or high-profile events, as they may be used as decoys in cyber-attacks.
3. **Important backup files**
    - Regularly back up critical files to a secure and isolated location to mitigate the impact of potential data loss in the event of a cyber-attack.
4. **Patch and update systems**
    - Promptly apply security patches and updates to operating systems and software to address known vulnerabilities and enhance overall system security.
5. **Utilize threat intelligence platforms**
    - Leverage the Threat Intelligence File In-depth Analysis Platforms to identify and analyze files from unknown sources, particularly those in multiple formats compatible with Windows and Android platforms.
6. **Exercise caution with unknown applications**
    - Exercise caution when installing applications from informal or untrusted sources.
    - Verify the authenticity of applications through the Threat Intelligence Analysis Platform before running or installing them.

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: sales@vairavtech.com

Website: https://vairavtech.com