Confucius Uses Pegasus Spyware-related Lures to Target Pakistani Military

By By: Daniel Lunghi Aug 17, 2021 Read time: 5 min (1215 words)

Published: 2021-08-17 · Archived: 2026-04-05 15:47:11 UTC

APT & Targeted Attacks

While investigating the Confucius threat actor, we found a recent spear phishing campaign that utilizes Pegasus spyware-related lures to entice victims into opening a malicious document downloading a file stealer.

Introduction

While investigating the Confucius threat actor, we found a recent spear phishing campaign that utilizes Pegasus spyware-related lures to entice victims into opening a malicious document downloading a file stealer. The NSO Group's spyware spurred a collaborative investigationnews article that found that it was being used to target high-ranking individuals in 11 different countries.

In this blog entry, we take a look at the lures used by the malicious actor and provide a short analysis of the file stealer used in the campaign, which was launched in early August.

The contents of the spear phishing email

The campaign involves a two-step attack. During the first phase, an email without a malicious payload containing content copied from a legitimate Pakistani newspaper's article is sent to the target. The sender address, which is spoofed, impersonates the PR wing of the Pakistani Armed Forces (info@ispr.gov.pk).

Two days later, a second email — purportedly a warning from a Pakistani military about the Pegasus spyware — containing a cutt.ly link to a malicious encrypted Word document and the password for decryption will be sent to the target. The sender address impersonates a service similar to that on the first email (alert@ispr.gov.pk).

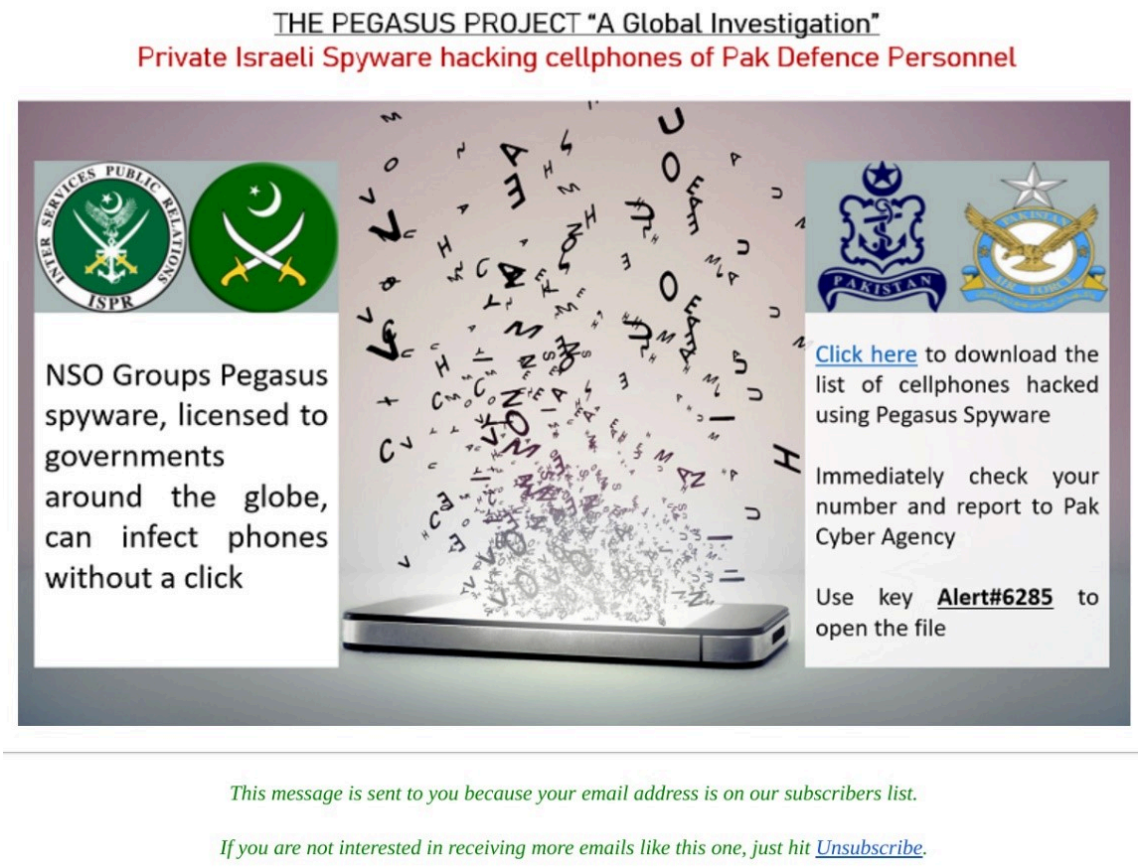

Figure 1. Spear-phishing email from early August. Notice the insertion of logos from the Pakistani Army, Air Force, Navy, and PR department.

If the target clicks on either the link or on the "unsubscribe" link, it will download a Word document from the domain parinari[.]xyz.

The emails are sent either from an ExpressVPN exit node in Pakistan, or from a mail server under the attacker's control.

Examining the encrypted document containing macros

After entering the password mentioned in the message, a document containing macros is displayed on screen.

Figure 2. Malicious document containing macros

If the victim enables macros, the malicious code will be loaded. If the victim enters any phone number and clicks "SUBMIT," the text field will be replaced by the message "Phone Number Not Found."

Behind the scenes, a .NET DLL file named skfk.txt, which is filled with content found inside the "Comments" property of the document, is created in the temporary directory. The file is then loaded in memory via PowerShell.

Stage 1 is a simple download & execute program. It downloads an ASCII file from the same domain and converts it into binary before loading it on to the memory and jump to a dynamic function.

Stage 2 is also .NET DLL file that downloads a third file from parinari[.]xyz, converts it from ASCII to binary, and then creates a scheduled task to load it.

Stage 3 is similar to stage 1, with the only change being the URL to retrieve the next stage.

Stage 4 is the final payload (analyzed in the next section). it is never written in clear text to the file disk.

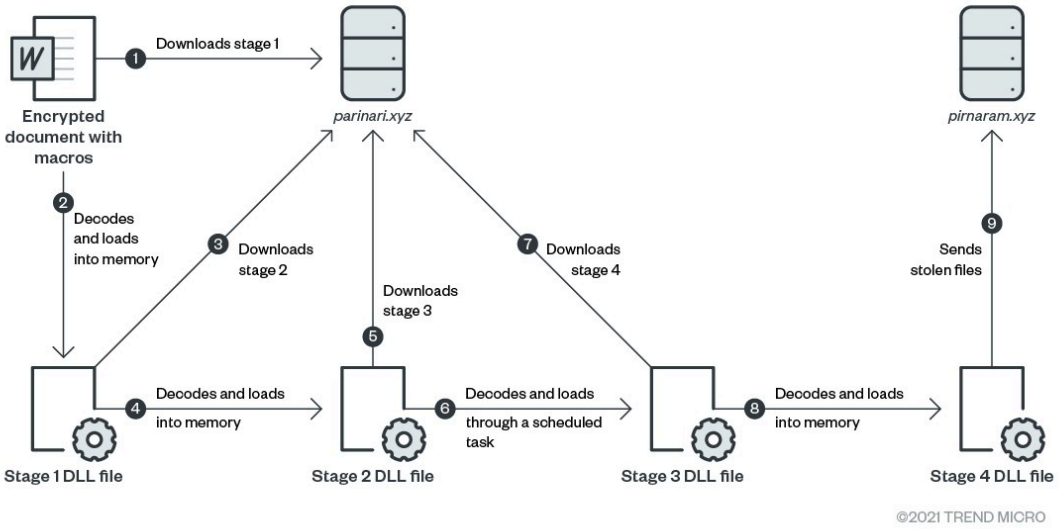

Figure 3. File stealer loading scheme

It should be noted that most of the compilation timestamps of these DLL files have been modified by the attacker to a year in the far future (2060, 2099 …), and the server IP addresses are often hidden behind CloudFlare.

Analysis of the file stealer

The final payload is a .NET DLL file designed to steal documents and images with the following extensions:

File extension	Description
TXT	Text file
PDF	PDF file
PNG	Image file in PNG format
JPG	Image file in JPG format
DOC	Word document
XLS	Excel document

XLM	Excel document with macros
ODP	OpenDocument Presentation
ODS	OpenDocument Sheet
ODT	OpenDocument Text
RTF	Rich Text Format file
PPT	PowerPoint document
XLSX	Excel document
XLSM	Excel document with macros
DOCX	Word document
PPTX	PowerPoint document
JPEG	Image file in JPEG format

The “Documents,” “Downloads,” “Desktop,” and “Pictures” folders of every user are checked. The DLL file also examines drives other than C:.

```
public void sdsdjkfhds()
{
    string userName = Environment.UserName;
    List<string> pfhl = new List<string>();
    string pattern = "*";
    pfhl = this.Gpufh();
    "C:\\\\Users\\\\" + userName;
    string tdn = Environment.MachineName + "__" + userName;
    this.CUD(tdn, 0);
    foreach (string text in Directory.GetDirectories("C:\\Users\\"))
    {
        if (text != "C:\\Users\\Default" || text != "C:\\Users\\Public")
        {
            this.GF(text + "\\Documents\\", pattern, "Documents", pfhl);
            this.GF(text + "\\Downloads\\", pattern, "Downloads", pfhl);
            this.GF(text + "\\Desktop\\", pattern, "Desktop", pfhl);
            this.GF(text + "\\Pictures\\", pattern, "Pictures", pfhl);
        }
    }
    DriveInfo[] drives = DriveInfo.GetDrives();
    char[] trimChars = new char[]
    {
        ':',
        '\\'
    };
    foreach (DriveInfo driveInfo in drives)
    {
        if (driveInfo.Name != "C:\\")
        {
            this.GF(driveInfo.Name, pattern, driveInfo.Name.TrimEnd(trimChars), pfhl);
        }
    }
    Environment.Exit(0);
}
```

Figure 4. Code showing the main function of the file stealer

When a file matching one of the listed extensions is found, its MD5 hash is calculated and compared to an exclusion list retrieved from the command-and-control (C&C) server pirnaram[.]xyz.

If the hash is not listed, the file is sent via the C&C to a directory named after the concatenation of the machine name and the username. The exclusion list is different for every machine name-username string.

Other campaigns

During our monitoring of Confucius, we came across a campaign delivering the same payload, using a different lure. In this instance, the campaign impersonated the Pakistani Defense Housing Authority. Again, this threat actor's interest in military personnel is obvious.

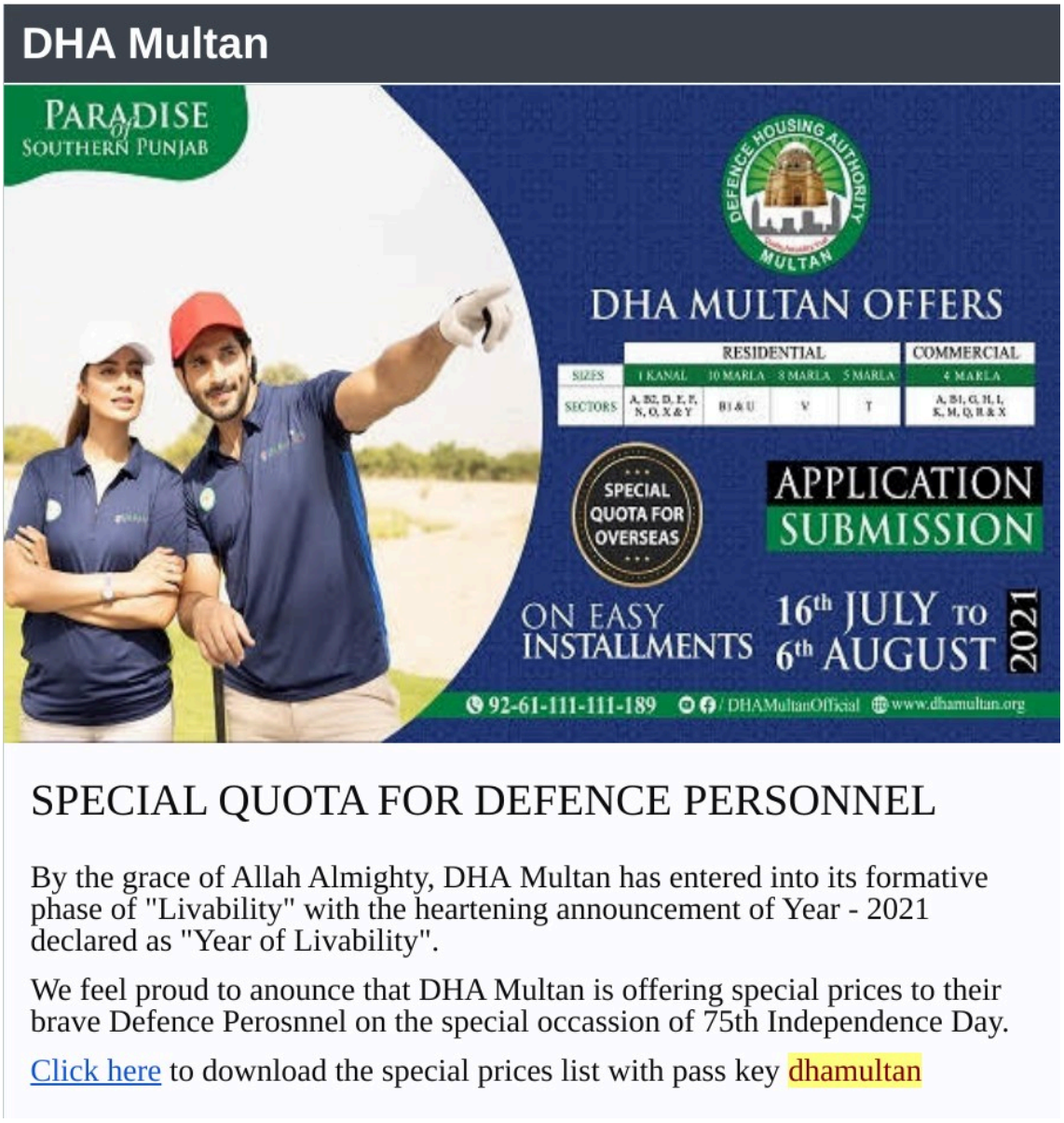

Figure 5. Spear-phishing email from early August

The lures used in an older campaign from April 2021 impersonated the Federal Board of Revenue. There were minor differences in tools, tactics, and procedures: the malicious document was directly attached to the spear phishing email — still encrypted — and the decryption password was sent in a different email. The first stage was also hidden in the "Comments" section. However, the second stage contained the final payload, which was once again a file stealer with the exact same structure (a .NET DLL). Instead of exfiltrating the files through PHP scripts, they were done via FTP server.

It should be noted that in some occasions, the threat actor sent spear-phishing emails from the domain name mailerservice[.]directory which we attributed to the Patchwork threat actor in previous research. We disclosed multiple links between Patchwork and Confucius threat actors in the past, so this came as no surprise to us.

The creative use of social engineering lures and how to defend against them

In our previous research, we already found Confucius, which is known for targeting Pakistan military for espionage purposes, employing multiple file stealers. While the code quality of its payloads is not of the highest standard, this threat actor uses innovative techniques when crafting its malicious documents, such as hiding malicious code in the comments section, or using encrypted documents to prevent automatic analysis. Therefore, it's highly likely that Confucius will continue to experiment and try out different kinds of social engineering lures in future campaigns.

Despite the variety of lures used by the threat actor, best security practices still apply to these attacks. Users should always be wary and avoid clicking on any link or downloading any file from unsolicited emails or suspicious sources. Red flags such as unusual sender domains or grammatical and spelling errors are also a sign that the email is malicious in nature, or at the very least, should be approached with proper security protocols in mind.

The following security solutions can also protect users from email-based attacks:

- **Trend Micro™ Cloud App Security**products – Enhances the security of Microsoft Office 365 and other cloud services via computer vision and real-time scanning. It also protects organizations from email-based threats.
- **Trend Micro™ Deep Discovery™ Email Inspector**products – Defends users through a combination of real-time scanning and advanced analysis techniques for known and unknown attacks.
-

Indicators of Compromise

SHA256	Detection name
dacf7868a71440a7d7d8797caca1aa29b7780801e6f3b3bc33123f16989354b2	Trojan.W97M.CONFUCIUS.A
0f6bcbdf4d192f8273887f9858819dd4690397a92fb28a60bb731c873c438e07	Trojan.W97M.CONFUCIUS.B
508bcc1f3906f5641116cde26b830b43f38f9c68a32b67e03a3e7e3f920b1f4a	Trojan.W97M.CONFUCIUS.B
654c7021a4482da21e149ded58643b279ffbce66badf1a0a7fc3551acd607312	Trojan.W97M.CONFUCIUS.C
712172b5b1895bbfcced961a83baa448e26e93e301be407e6b9dc8cb6526277f	Trojan.Win32.DLOADR.TIOIBELQ
Server hosting malicious documents	
parinari[.]xyz	

Server used for file exfiltration
pirnaram[.]xyz
Domain names linked to other campaigns
pemra[.]email
ispr[.]email
fbr[.]news
defencepk[.]email
pakistanarmy[.]email
pmogovpk[.]email
mailerservice[.]directory
file-dnld[.]com
funtifu[.]live
cnic-update[.]com
cnic-ferify[.]live
fbr-update[.]com

download.fbr[.]tax
support-team[.]tech
api.priveetalk[.]com
latest_info@fbr.news
notice@fbr.news
alert@fbr.news
thenewsinernational@mailerservice.directory

Tags
