# Chinese hackers hide on military and govt networks for 6 years

By Bill Toulas

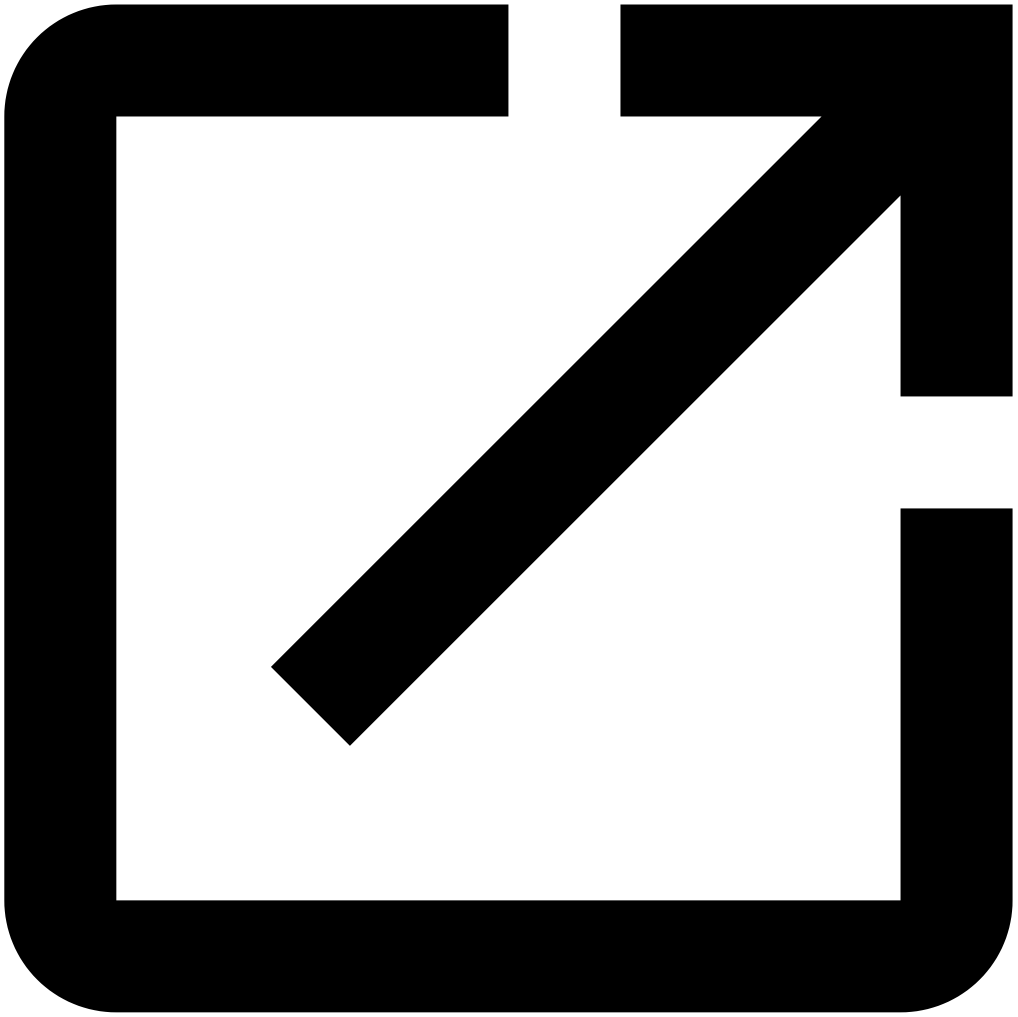
Published: 2024-05-22 · Archived: 2026-04-05 12:49:55 UTC

A previously unknown threat actor dubbed "Unfading Sea Haze" has been targeting military and government entities in the South China Sea region since 2018, remaining undetected all this time.

Bitdefender researchers who discovered the threat group report that its operations align with Chinese geo-political interests, focusing on intelligence collection and espionage.

As is typical for Chinese state-sponsored threat actors, "Unfading Sea Haze" demonstrates operational, TTP, and toolset overlaps with other activity clusters, most notably, APT41.


DIE LINKE.
0:00



## Abusing MSBuild for fileless malware

Unfading Sea Haze attacks start with spear-phishing emails carrying malicious ZIP archives that contain LNK files disguised as documents.

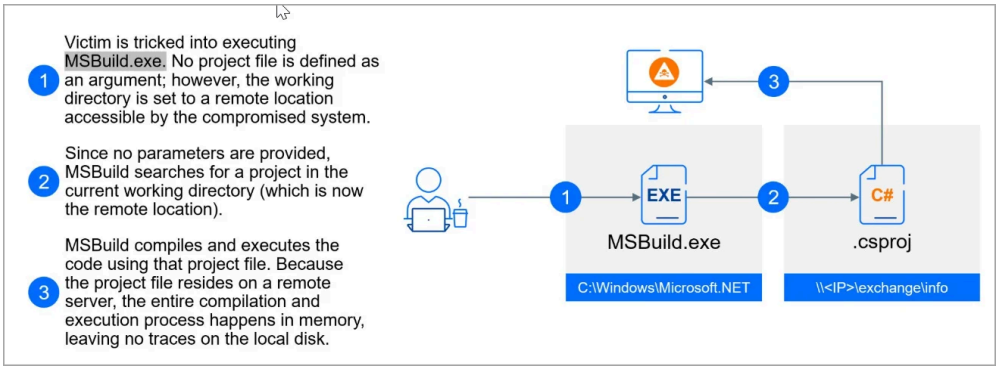
As of March 2024, the latest lures used in these attacks concern U.S. political topics, while the ZIPs were deceptively named to appear as Windows Defender installers/updaters.

These LNK files contain a long obfuscated PowerShell command that will check for the presence of an ESET executable, ekrn.exe, and if it exists, halts the attack.

If the executable is not found, the PowerShell script will perform an interesting trick to launch fileless malware directly into memory using Microsoft's legitimate msbuild.exe command-line compiler.

"In this attack, the criminals start a new MSBuild process with a twist: they specify a working directory located on a remote SMB server (like \154.90.34.83\exchange\info in the above example)," explains Bitdefender.

"By setting the working directory to a remote location, MSBuild will search for a project file on that remote server. If a project file is found, MSBuild will execute the code it contains entirely in memory, leaving no traces on the victim's machine."




**Abusing msbuild.exe to launch fileless malware**

*Source: Bitdefender*

That code executed by MSBuild is a backdoor program named 'SerialPktdoor,' which gives the attackers remote control over the compromised system.

The attack also employs scheduled tasks that execute innocuous files to side-load malicious DLLs and use local administrator account manipulation to maintain persistence.

Specifically, the hackers reset the password for the local administrator account, which is disabled by default in Windows, and enable it. The account is then again hidden from the login screen via Registry modifications.

This provides the threat actors with a hidden admin account that can be used to further their attacks.

Bitdefender highlights the atypical strategy of using commercial Remote Monitoring and Management (RMM) tools, like the Itarian RMM, in the attack chain to gain a foothold on the compromised network.

## Unfading Sea Haze's Arsenal

Once access has been established, Unfading Sea Haze uses a custom keylogger named 'xkeylog' to capture the victim's keystrokes, an info-stealer targeting data stored in Chrome, Firefox, or Edge, and various PowerShell scripts that extract information from the browser database.

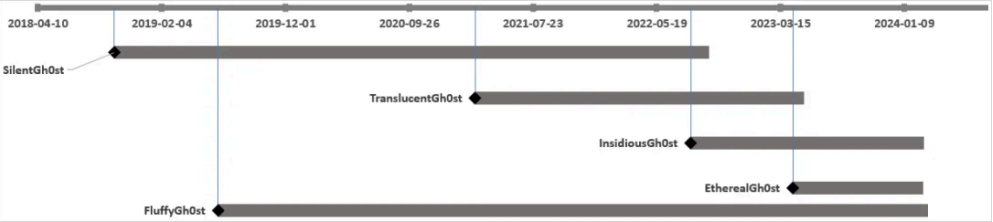
```
Add-Type -AssemblyName System.Security
$path = "C:\Users\<redacted>\AppData\Local\Google\Chrome\User Data\Local State"
$pathver = "C:\Users\<redacted>\AppData\Local\Google\Chrome\User Data\Last Version"
$regex = """encrypted_key"":""(.*?)"""
$enckey = select-string -Path $path -Pattern $regex -AllMatches | % { $_.Matches } | % { $_.Value }
Foreach ($key in $enckey) {
    $strkey= $key.SubString(17,$key.Length-18)
    $bytes = [System.Convert]::FromBase64String($strkey)
    $enc  = [byte[]]::new($bytes.Length-5)
    [System.Array]::Copy($bytes,5,$enc, 0, $bytes.Length-5)
    $dec = [Security.Cryptography.ProtectedData]::Unprotect($enc, $null,  [Security.Cryptography.DataProtectionScope]::LocalMachine)
    $basestr =[System.Convert]::ToBase64String($dec)
    $basestr  |out-file C:\programData\aa.txt
}
 Get-Content -Path $pathver |out-file C:\programData\bb.txt
```

**Extracting encrypted data from Chrome**
*Source: Bitdefender*

Starting in 2023, the hackers moved to stealthier tools like the abuse of msbuild.exe to load C# payloads from remote SMB shares, as well as variants of the Gh0stRAT malware.

Bitdefender has seen the deployment of:

- **SilentGh0st** – The oldest variant offering extensive functionality through a rich set of commands and modules
- **InsidiousGh0st** – Go-based evolution of SilentGh0st that also features TCP proxy, SOCKS5, and PowerShell improvements.
- **TranslucentGh0st**, **EtherealGh0st**, and **FluffyGh0st** – Newest variants featuring dynamic plugin loading and lighter footprint for evasive operation.




**Gh0stRAT variants deployment timeline**
*Source: Bitdefender*

In earlier attacks, the hacker also used Ps2dllLoader, a tool that loads .NET or PowerShell code into memory, and 'SharpJSHandler,' a web shell that listens for HTTP requests and executes encoded JavaScript code.

Interestingly, a custom tool checks for newly plugged USB and Windows Portable Devices (WPD) every ten seconds and sends device details and specific files to the attackers.

To exfiltrate data from breached systems, Unfading Sea Haze uses a custom tool named 'DustyExfilTool' that performs secure data extraction via TLS over TCP.

More recent attacks show that the threat actors have switched to a curl utility and the FTP protocol for data exfiltration, now also using dynamically generated credentials that are changed frequently.

Unfading Sea Haze shows stealth, persistence, and adaptability, leveraging fileless attacks, advanced evasion methods, and modular malware design.

To stop these attacks, organizations must adopt a multifaceted security strategy involving patch management, MFA adoption, network segmentation, traffic monitoring, and deployment of state-of-the-art detection and response products.

---