# ToolShell Used to Compromise Telecoms Company in Middle East

## China-based threat actors also compromised networks of government agencies in countries in Africa and South America.

- Threat Intelligence
- 22 Oct 2025
- 7 Min Read

Share

China-based attackers used the ToolShell vulnerability (CVE-2025-53770) to compromise a telecoms company in the Middle East shortly after the vulnerability was publicly revealed and patched in July 2025.

The same threat actors also compromised two government departments in the same African country during the same time period. Zingdoor, which was deployed on the networks of all three organizations, has in the past been associated with the Chinese group Glowworm (aka Earth Estries, FamousSparrow).

Another tool used in this campaign, KrustyLoader, has also previously been linked to activity by a group called UNC5221, which has been described as a China-nexus group.

The attackers also gained access to the networks of two government agencies in South America and a university in the U.S. recently. In these attacks, the attackers used other vulnerabilities for initial access and exploited SQL servers and Apache HTTP servers running the Adobe ColdFusion software to deliver their malware. Notably, in the South American victims, the attackers used the filename “mantec.exe”, possibly to mimic a Symantec filename (“symantec.exe”) in an attempt to hide their malicious activity. This binary (mantec.exe), which is a legitimate copy of a BugSplat executable, a tool used for bug tracking, was used to sideload a malicious DLL.

Evidence suggests that a state technology agency in an African country, a government department in the Middle East and a finance company in a European country were also compromised by the same attackers.

## What is ToolShell?

ToolShell was patched by Microsoft in July 2025, but by the time it was patched it had already been exploited in the wild as a zero-day vulnerability. ToolShell affects on-premise SharePoint servers and gives an attacker unauthenticated access to vulnerable servers, allowing them to remotely execute code and access all content and file systems. ToolShell was a variant of another vulnerability (CVE-2025-49704) that had been patched in July 2025.  Another related vulnerability (CVE-2025-53771) was also patched at the same time as ToolShell. This is a path traversal bug that allows an authorized attacker to perform spoofing over a network. It too was a variant of an older patched vulnerability (CVE-2025-49706).

Shortly after patching the vulnerabilities, Microsoft said that at least three Chinese groups had been exploiting ToolShell. Microsoft said at the time that two Chinese espionage groups had been exploiting the vulnerability - Budworm (aka Linen Typhoon) and Sheathminer (aka Violet Typhoon). In addition to this, a third China-based actor, known as Storm-2603, was also exploiting the vulnerabilities to carry out attacks in which it was distributing the Warlock ransomware.

## Toolset

Malicious activity in the telecoms company in the Middle East began on July 21, 2025, just two days after patches were published for ToolShell, with the deployment of a likely webshell by the attackers.

The attackers loaded the Zingdoor backdoor onto the network by sideloading it using a legitimate Trend Micro binary. Zingdoor is a HTTP backdoor written in Go, which was first seen in April 2023, and first documented by Trend Micro in August that year being used in a campaign that they attributed to Glowworm. Zingdoor can collect system information, upload and download files, and run arbitrary commands on compromised networks. As well as Zingdoor, the attackers also deployed what appears to be the ShadowPad Trojan. The loader for the Trojan was sideloaded using a legitimate BitDefender binary (SHA256: 3fc4f3ffce6188d3ef676f9825cdfa297903f6ca7f76603f12179b2e4be90134).

ShadowPad is a modular remote access Trojan (RAT) that is closely associated with China-based APT groups. Because of its modular nature, ShadowPad can be continuously updated with new functionalities. This capability makes it a powerful tool. It is associated with various threat groups, particularly the APT41-

nexus groups such as Blackfly, Grayfly and Redfly. It was documented being used by Glowworm in 2024, which was the first time that particular group had been observed using the malware. It has more recently been used in attacks where ransomware has been deployed. Typically, ShadowPad is loaded onto victim networks via DLL sideloading. DLL sideloading is a technique where the attackers use the DLL search order mechanism in Windows to plant and then invoke a legitimate application that executes a malicious DLL payload.

On July 25, KrustyLoader was dropped by the attackers. KrustyLoader was first documented in January 2024. It is an initial-stage malware, written in Rust, which has the primary purpose of delivering a second-stage payload. KrustyLoader can carry out various anti-sandbox and anti-analysis checks, can make a copy of itself and set itself up to self-delete when its activity is finished, and can decrypt and download additional malware. Its previous activity has been linked to China-based threat actors, and in earlier campaigns it was also used to download the Sliver post-exploitation framework, which is also seen deployed against this target.

Sliver is an open-source cross-platform adversary emulation/red team framework that can legitimately be used for security testing. However, it is often abused by threat actors who use it as a command-and-control framework.

A variety of publicly available and living-off-the-land tools are also used by the attackers in this activity, including:

- **Certutil**: Microsoft Windows utility that can be used for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.
- **GoGo Scanner**: A publicly available automated scanning engine aimed at Chinese speaking users, for use by red teams. It is available on GitHub.
- **Revsocks**: A publicly available cross-platform SOCKS5 proxy server program/library written in C that can also reverse itself over a firewall.
- **Procdump**: Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but can also be used as a general process dump utility.
- **Minidump**: A script from the post-exploitation framework PowerSploit used for dumping processes. Attackers usually dump lsass.exe to find credentials.
- **LsassDumper**: A utility designed to dump the Local Security Authority Subsystem Service (LSASS) process memory to a file.

An exploit for the Windows LSA Spoofing Vulnerability, CVE-2021-36942 (aka PetitPotam), was also executed. PetitPotam is an exploitation technique that allows for a threat actor within a compromised network to steal credentials and authentication information from Windows Servers such as a Domain Controller to gain full control of the domain. This is likely used for lateral movement or privilege escalation.

## ToolShell impact further revealed

These attacks demonstrate that the ToolShell vulnerability was being exploited by an even wider range of Chinese threat actors than was originally thought.

There is some overlap in the types of victims and some of the tools used between this activity and activity previously attributed to Glowworm. However, we do not have sufficient evidence to conclusively attribute this activity to one specific group, though we can say that all evidence points to those behind it being China-based threat actors.

The large number of apparent victims of this activity is also notable. This may indicate that the attackers were carrying out an element of mass scanning for the ToolShell vulnerability, before then carrying out further activity only on networks of interest. The activity carried out on targeted networks indicates that the attackers were interested in stealing credentials and in establishing persistent and stealthy access to victim networks, likely for the purpose of espionage.

# Indicators of Compromise (IOCs)

**File indicators**

6240e39475f04bfe55ab7cba8746bd08901d7678b1c7742334d56f2bc8620a35 - LsassDumper

929e3fdd3068057632b52ecdfd575ab389390c852b2f4e65dc32f20c87521600 - KrustyLoader

db15923c814a4b00ddb79f9c72f8546a44302ac2c66c7cc89a144cb2c2bb40fa - Likely ShadowPad

e6c216cec379f418179a3f6a79df54dcf6e6e269a3ce3479fd7e6d4a15ac066e – ShadowPad Loader

071e662fc5bc0e54bcfd49493467062570d0307dc46f0fb51a68239d281427c6 - Zingdoor

1f94ea00be79b1e4e8e0b7bbf2212f2373da1e13f92b4ca2e9e0ffc5f93e452b - PetitPotam/CVE-2021-36942 exploit

dbdc1beeb5c72d7b505a9a6c31263fc900ea3330a59f08e574fd172f3596c1b8 - RevSocks

6aecf805f72c9f35dadda98177f11ca6a36e8e7e4348d72eaf1a80a899aa6566 - LsassDumper

568561d224ef29e5051233ab12d568242e95d911b08ce7f2c9bf2604255611a9 - Socks Proxy

28a859046a43fc8a7a7453075130dd649eb2d1dd0ebf0abae5d575438a25ece9 - GoGo Scanner

7be8e37bc61005599e4e6817eb2a3a4a5519fded76cb8bf11d7296787c754d40 - Sliver

5b165b01f9a1395cae79e0f85b7a1c10dc089340cf4e7be48813ac2f8686ed61 - ProcDump

e4ea34a7c2b51982a6c42c6367119f34bec9aeb9a60937836540035583a5b3bc - ProcDump

7803ae7ba5d4e7d38e73745b3f321c2ca714f3141699d984322fa92e0ff037a1 – Minidump

7acf21677322ef2aa835b5836d3e4b8a6b78ae10aa29d6640885e933f83a4b01 - mantec.exe – Benign executable

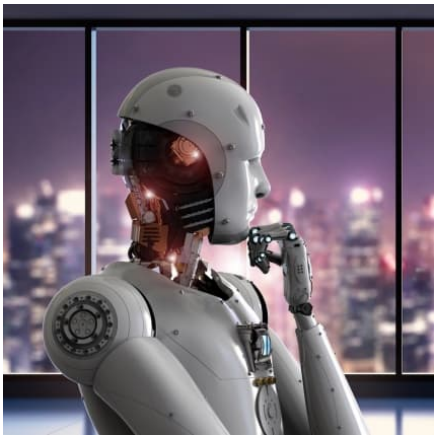
6c48a510642a1ba516dbc5effe3671524566b146e04d99ab7f4832f66b3f95aa - bugsplatrc.dll

**Network indicators**

http://kia-almotores.s3.amazonaws[.]com/sy1cyjt - KrustyLoader C&C server

http://omnileadzdev.s3.amazonaws[.]com/PBfbN58lX - KrustyLoader C&C server

## About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

### You might also enjoy

## ToolShell: Critical SharePoint Zero-Day Exploited in the Wild

- 21 Jul 2025
- 3 Min Read