SoftServe hit by ransomware, Windows customization tool exploited

By Lawrence Abrams

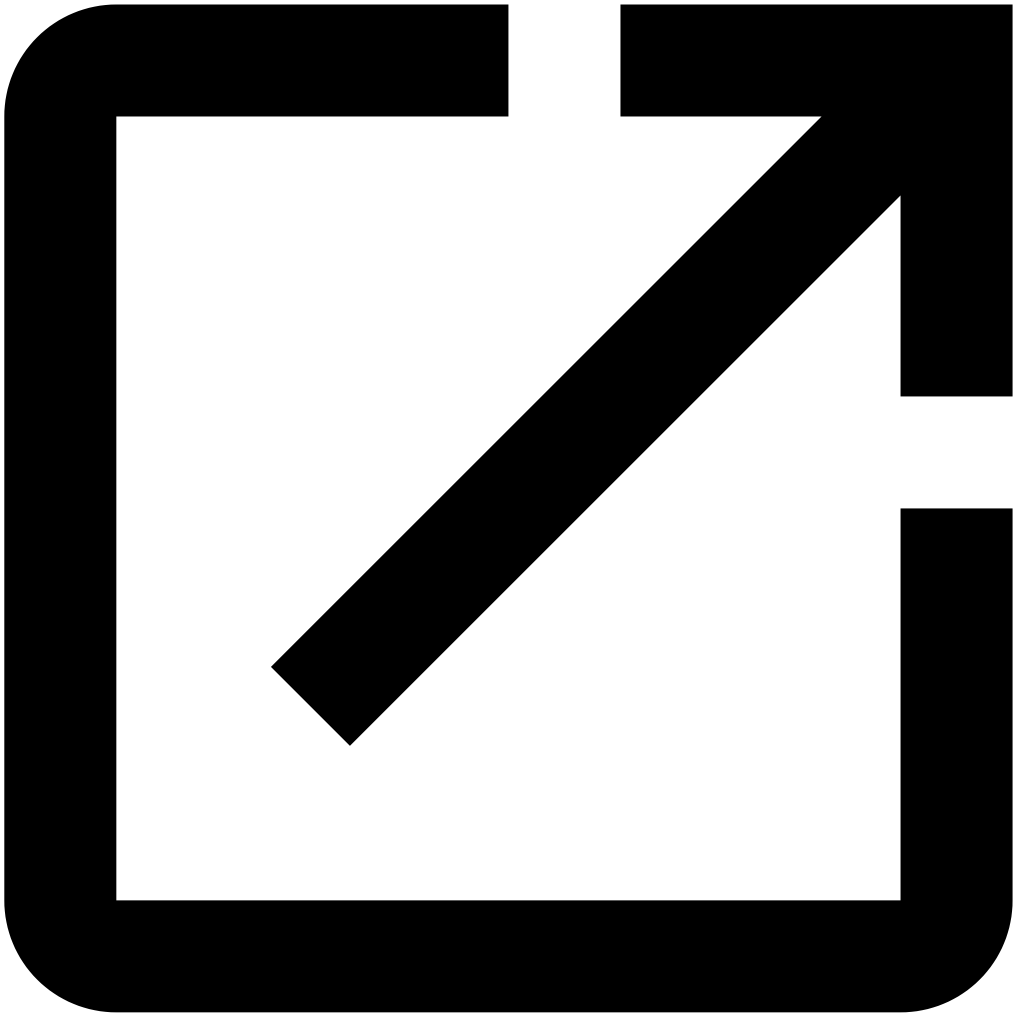
Published: 2020-09-10 · Archived: 2026-04-05 14:42:59 UTC

Ukrainian software developer and IT services provider SoftServe suffered a ransomware attack on September 1st that may have led to the theft of customers' source code.

With over 8,000 employees and 50 offices worldwide, SoftServe is one of Ukraine's largest companies offering software development and IT consulting.

News about a cyberattack on SoftServe first began circulating on the 'Telegram DC8044 Kyiv Info' channel, where an alleged message sent by the company to employees was shared.


DIE LINKE.
0:00



"Today at 1AM in the morning SoftServe came under cyber attack. Attackers got access to company infrastructure and managed to launch encrypting ransomeware along with some other malware.
We have taken some of our services offline to stop spread of attack, unfortunately your work will be suffering from our containment steps in coming hours ...
We also blocked tunnels to our customers networks to avoid spread of malware to their infrastructure."

In a subsequent statement to Ukrainian technology news site AIN, SoftServe confirmed that a cyberattack had occurred that caused them to disconnect their clients to prevent its spread.

“Yes, there was an attack today. The most significant consequences of the attack are the temporary loss of functionality of a part of the mail system and the halt of some of the auxiliary test environments. As far as we can estimate, this is the greatest impact of the attack, and other systems or client data were not affected.”

"To avoid the spread of the attack, we isolated some segments of our network and restricted communication with client networks. We are preparing a message to our clients about the situation. Simultaneously with the resumption of services, we are investigating the incident itself, so we are not ready to comment on who exactly did this," Adriyan Pavlikevich, Senior Vice President of IT at SoftServe, told AIN.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731.

An incident report found today by security researcher MalwareHunterTeam and shared with BleepingComputer, confirms that SoftServe suffered a ransomware attack.

This incident report states that the ransomware attack appended the "*.s0fts3rve555-*** (like s0fts3rve555-76e9b8bf)" extension to encrypted file's names.

It has not been confirmed, but this extension pattern matches those used by the Defray ransomware, also known as RansomEXX, which was recently used against Konica Minolta.

The report also includes a PowerShell script used to find files that were changed during the attack, indicating that the attack occurred between 2 AM and 9 AM.

1. Run powershell script for identification of file changes for period of attack

```
PS C:\Windows> Get-ChildItem -Recurse -ea SilentlyContinue | where{$_.LastWriteTime -
ge [datetime]$("9/1/2020 2:00:0 AM") -and $_.LastWriteTime -le [datetime]$("9/1/2020
9:00:0 AM")} | Select -Property LastWriteTime,FullName
```

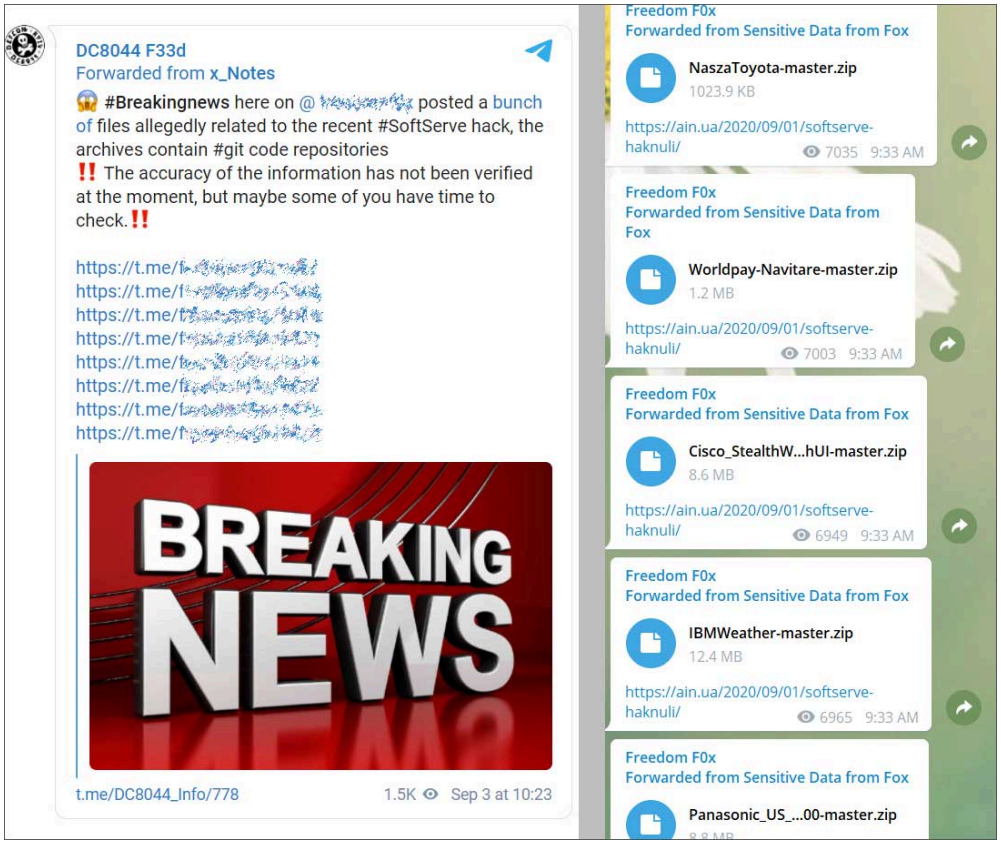
PowerShell script

BleepingComputer has contacted SoftServe with further questions about the attack but has not heard back.

Customers' source code allegedly stolen

In a later post to the DC8044 Telegram channel, links were shared to source code repositories that were allegedly stolen during this attack,

These zip files are for projects that claim to be for Toyota, Panasonic, IBM, Cisco, ADT, WorldPay, and more.



Leak of files allegedly stolen during SoftServe attack

BleepingComputer has not independently confirmed whether this data belongs to SoftServe, but there are references to the company in some of the leaked source code repositories.

Windows customization tool exploited in attack

According to the SoftService incident report, the attackers exploited a DLL hijacking vulnerabilitie in the legitimate Rainmeter application to deploy their ransomware.

Rainmeter is a legitimate Windows customization tool that loads a Rainmeter.dll when launched.

During the attack, the threat actors replaced the legitimate Rainmeter.dll with a malicious version compiled from the source code to deploy the ransomware.

"Distributed ransomware DLL(Rainmeter.dll) compiled from legitime Rainmeter - a desktop customization tool for Windows. Malicious DLL loading from legitime EXE (used popular cyberattack method DLL side-loading) using additional instruments like CobaltStrike Beacon, PowerShell, etc. Such technique is hard to detect by any antivirus as of now," the SoftServe incident report states.

According to detections from VirusTotal, the Rainmeter.dll is identified as the backdoor Win32/PyXie.A.

In a 2019 report from BlackBerry, PyXie is a Python remote access trojan (RAT) known to exploit DLL hijacking vulnerabilities in other software such as LogMeIn and Google Update.

BlackBerry researchers state that they have seen evidence that this RAT has been used in ransomware attacks.

"Analysts have observed evidence of the threat actors attempting to deliver ransomware to the healthcare and education industries with PyXie," the report states.

Source: https://www.bleepingcomputer.com/news/security/softserve-hit-by-ransomware-windows-customization-tool-exploited/