CompuCom MSP hit by DarkSide ransomware cyberattack

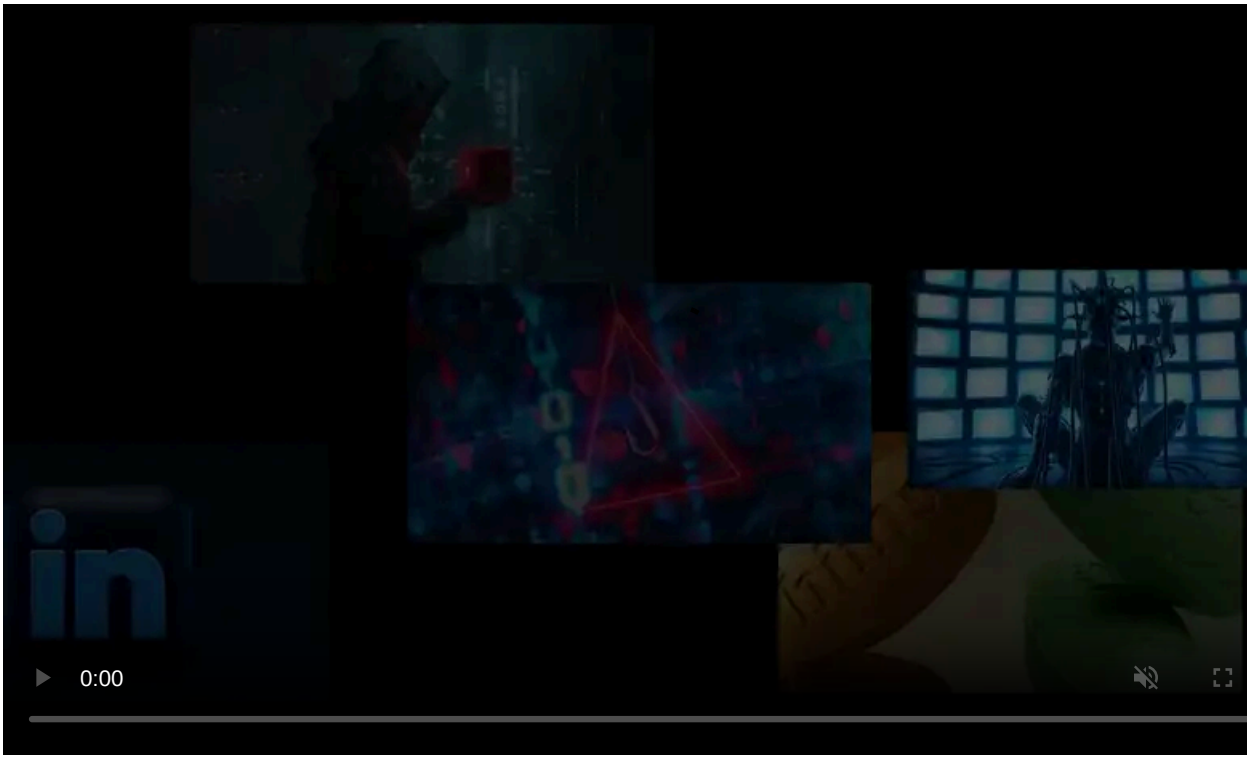
By Lawrence Abrams

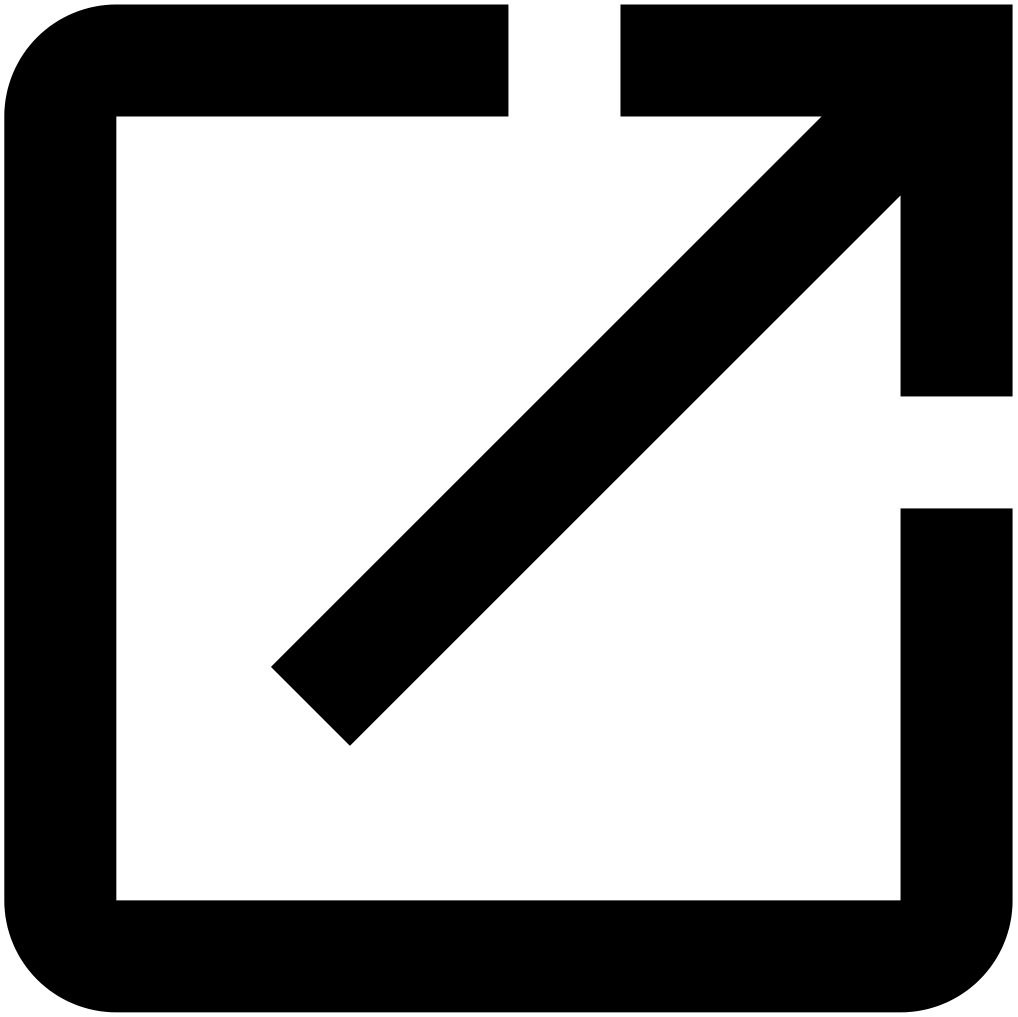
Published: 2021-03-04 · Archived: 2026-04-05 17:24:33 UTC

Update 3/4/21: This article was originally published on 3/3/21 and has been updated with new info.

US managed service provider CompuCom has suffered a DarkSide ransomware attack leading to service outages and customers disconnecting from the MSP's network to prevent the spread of malware.

CompuCom is an IT managed services provider (MSP) that provides remote support, hardware and software repair, and other technology services to companies. CompuCom is a wholly-owned subsidiary of The ODP Corporation (Office Depot/Office Max) and employs approximately 8,000 people.


0:00



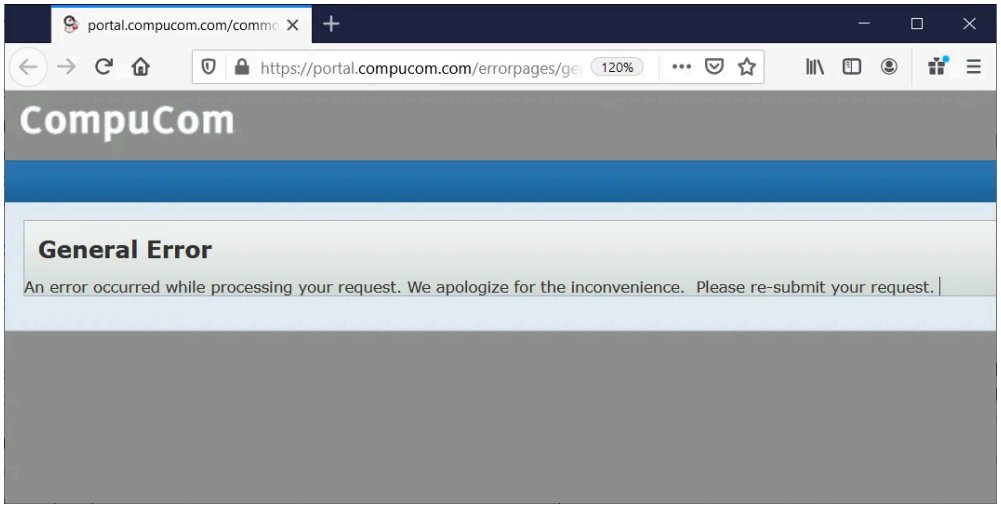
Some of the past and existing customers of CompuCom include well-known names, such as Home Depot, Target, Citibank, Wells Fargo, Truist Bank, and Lowe's.

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

The attack occurred over the weekend

Over the weekend, CompuCom suffered an outage that prevented customers from accessing the company's customer portal to open troubleshooting tickets.

When visiting the portal, the website greeted customers with a general error message stating, "An error occurred while processing your request."



Error message on CompuCom client portal

BleepingComputer was told that CompuCom began contacting customers to alert them that they had been compromised by malware soon after the attack. However, customers were not told what type of attack occurred and whether it was ransomware.

In later conversations with affected customers, BleepingComputer learned that CompuCom had disconnected their access to some customers to prevent the malware's spread. Another customer told us that they had detached from CompuCom's VDIs (Virtual Desktop Infrastructure) to ensure their data was not affected by the attack.

Multiple people also told BleepingComputer that this was a ransomware attack, but we could not confirm independently if this is true.

After reaching out to CompuCom about the attack, the company issued a statement to BleepingComputer stating that they suffered a 'malware incident' and that there is no evidence of it spreading to customers' systems.

You can read the full CompuCom statement below:

> "Certain CompuCom information technology systems have been affected by a malware incident which is affecting some of the services that we provide to certain customers. Our investigation is in its early stages and remains ongoing. We have no indication at this time that our customers' systems were directly impacted by the incident.
>
> As soon as we became aware of the situation, we immediately took steps to contain it, and engaged leading cybersecurity experts to begin an investigation. We are also communicating with customers to provide updates about the situation and the actions we are taking.

> We are in the process of restoring customer services and internal operations as quickly and safely as possible. We regret the inconvenience caused by the interruption and appreciate the ongoing support of our customers." - CompuCom

CompuCom confirms ransomware attack in FAQ

Today, a CompuCom customer shared a 'Customer FAQ Regarding Malware Incident' that provides more details about the attack than the company shared in their press release.

According to the FAQ, CompuCom was breached by threat actors who installed Cobalt Strike beacons on several systems in their environment.

These beacons allow remote threat actors access to the network to steal data, spread to other machines, and ultimately deploy the ransomware, which the threat actors deployed on February 28th.

"Based on our expert's analysis to date, we understand that the attacker deployed a persistent Cobalt Strike backdoor to several systems in the environment and acquired administrative credentials. These administrative credentials were then used to deploy the Darkside Ransomware," the CompuCom FAQ reads.

Cobalt Strike is increasingly being deployed through a variety of Trojans installed via phishing campaigns. These Trojans include BazarLoader, TrickBot, ZLoader, and QBot.

Now that DarkSide Ransomware has been confirmed to be behind the attack, it is likely that the threat actors harvested unencrypted files before encrypting the devices.

If data was stolen and a ransom is not paid, we will likely see this data published on their ransomware data leak site in the next few weeks.

In the past, other companies hit by DarkSide include Discount Car and Truck Rentals, Brookfield Residential, and the Brazilian Eletrobras and Copel energy companies.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
