NEWS RELEASE

Cisco Consumer Security Alert: Millions of Users Threatened by Breach of Consumer Application, Piriform's CCleaner

2017-09-18

SAN JOSE, CA -- (Marketwired) -- 09/18/17 -- Cisco's (NASDAQ: CSCO) industry leading cybersecurity research team, Cisco Talos, today is alerting consumers and businesses to its discovery of a major cybersecurity attack that could affect millions of users worldwide.

WHAT HAPPENED
Attackers hijacked and hid malware inside Piriform's CCleaner application which was available for download between August 15 - September 12, 2017. Piriform is a company owned by Avast. Anyone who downloaded the 5.33 version product or updated their existing product during this timeframe became infected.

On September 13, 2017, Cisco Talos notified Avast so that it could begin corrective action. At this time the version containing the malware has been removed and is no longer available for download. However, many consumers remain at risk -- and will remain at risk even after updating their CCleaner software.

CONSUMER IMPACT
Billing itself as the "world's most popular PC cleaner and optimization tool," Avast's CCleaner is trusted by consumers to speed up PC and smartphone performance by removing unneeded/necessary files. As recently as November 2016, CCleaner boasted 2 billion downloads with a growth rate of 5 million users per week.

Once the malware was installed, attackers could potentially gain access to the user's computer and other connected systems to steal sensitive personal data and/or credentials that could be used for online banking or other online activities.

Like the Nyetya malware in late June, in this instance attackers hacked into a legitimate, trusted

application and made it malicious. These types of attacks are often successful because consumers trust that these well-known and broadly-used applications are safe. Criminals are exploiting this trust.

WHAT TO DO

Because the malware remains present, even after users update the CCleaner software, Talos advises all users to wipe their entire computer -- remove and reinstall everything on the machine -- and to restore files and data from a pre-August 15, 2017 backup, before the current version was installed.

It is critical to remove this version of the CCleaner software and associated malware, since it's structure means it has the ability to hide on the user's system and call out to check for new malware updates for up to a year.

RESOURCES

For additional information on this attack, visit the Cisco Talos Blog post: CCleaner: a vast number of machines at risk

RSS Feed for Cisco: http://newsroom.cisco.com/rss-feeds

For media interviews with Cisco Talos, please contact
Tony Welz
703-877-8101
tony@w2comm.com

Source: Cisco