Major German manufacturer still down a week after getting hit by ransomware

By Written by Catalin Cimpanu, ContributorContributor Oct. 21, 2019 at 12:15 p.m. PT

Archived: 2026-04-05 18:53:37 UTC

Image: Pilz

Pilz, one of the world's largest producers of automation tools, has been down for more than a week after suffering a ransomware infection.

See als

-

"Since Sunday, October 13, 2019, all servers and PC workstations, including the company's communication, have been affected worldwide," the Germany-based company wrote on its website.

"As a precaution, the company has removed all computer systems from the network and blocked access to the corporate network."

All the company's locations across 76 countries were impacted and were disconnected from the main network, unable to file orders and check customer statuses.

It took Pilz staff three days to regain access to its email service, and another three days to restore email service for its international locations. Access to the product orders and delivery system was restored only today.

Production capabilities weren't impacted, but unable to check orders, they've been hampered and going at slower rates.

Blame BitPaymer

The German company -- known for its automation relays, controllers, and sensors -- is the latest in a long line of BitPaymer victims, Maarten van Dantzig, Lead Intelligence Analyst at FoxIT, told *ZDNet* today.

Van Dantzig was able to tie the Pilz infection to BitPaymer after he found and analyzed a BitPaymer sample uploaded on VirusTotal. The sample contained a ransom note with Pilz-related contact details, customized for the company's network.

BitPaymer is a ransomware strain that appeared in the summer of 2017 and has been tied to several high-profile incidents at Scottish hospitals, the PGA, two Alaskan towns (Matanuska-Susitna and Valdez), Arizona Beverages, in attacks leveraging an iTunes zero-day, and, most recently, at French TV station M6.

But BitPaymer is not your regular ransomware strain. BitPaymer's authors engage in what's called "big game hunting," a term coined by Crowdstrike and which describes the act of going only after high-value targets -- in the hopes of extracting a large ransom payment, instead of extorting home consumers for meager profits.

BitPaymer's Dridex partnership

During the past two years, BitPaymer has been distributed exclusively via the Dridex botnet, van Dantzig told ZDNet.

An ESET report from January 2018 claimed the ransomware was the work of the Dridex authors themselves.

Currently, most experts believe the Dridex gang spends their time sending email spam that infects users with the Dridex trojan, compiles a list of victims, and then deploys BitPaymer on the networks of large companies, in the hopes of extracting huge ransoms after encrypting their files.

Historically, this tactic has been pretty lucrative, and BitPaymer has been tied to ransomware demands going as high as $1 million, Van Dantzig told *ZDNet* today in a phone call.

This cybercrime model of botnet-ransomware partnership is extremely popular these days. A similar "working relationship" also exists between the operators of the Emotet and TrickBot botnets and the Ryuk ransomware gang.

A surge in activity since April this year

You can easily see BitPaymer's modus operandi in the chart below, consisting of submissions to ID-Ransomware, an online service sponsored by the MalwareHunterTeam and Emsisoft where ransomware victims can upload samples and detect the type of ransomware they've been infected.

bitpaymer-last-year.jpg

BitPaymer submissions to ID-Ransomware in the last 12 months

Source: ID-Ransomware (supplied)

Most ID-Ransomware activity charts are smooth, as there are daily submissions from victims who get infected after opening emails or installing ransomware-infected files.

However, for BitPaymer, this is different. The spikes show occasional infections as the ransomware is deployed on a handful of carefully selected targets, rather than spammed out in every direction. This pattern is specific to "big-game hunting" ransomware operations.

Van Dantzig says companies must understand that once they recover from a BitPaymer infection, their job is not done. System administrators must also remove the Dridex trojan from infected hosts, otherwise they'll be reinfected again.

In fact, van Dantzig has seen this happen in the past.

Pilz was not immediately available for comment at the time of publishing.

Cybercrime and malware, 2019 predictions

Security

Source: https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/