Active malware operation let attackers sabotage US energy industry

By Dan Goodin

Published: 2014-06-30 · Archived: 2026-04-05 20:54:14 UTC

The Havex RAT gathers information about the infected computers and the networks they are connected to and sends it to servers under the control of the attackers. Among other things, it extracts data from a victim's Outlook address book and virtual private networking (VPN) programs. A program that appears to be have been developed in-house, Havex is also known as Backdoor.Oldrea and the Energetic Bear RAT. Dragonfly members also infected some computers with Trojan.Karagany, a RAT available in underground markets that has most likely been modified. It's capable of collecting passwords, taking screenshots, and cataloging documents stored on infected computers.

Dragonfly operators hacked websites of at least three different companies providing ICS software. The first provided a product used to provide VPN access to programmable logic controller devices (PLC). The unnamed provider discovered the attack shortly after it was mounted, but by then there had already been 250 downloads of the trojanized software. The second provider was a European manufacturer of specialist PLC devices. Symantec estimated that a compromised package containing a computer driver was available for download for at least six weeks last June and July. The last firm was also based in Europe and develops systems to manage wind turbines, biogas plants, and other energy infrastructure. The compromised software was available for about 10 days in April, Symantec said.

In addition to trojanizing legitimate software used by its victims, Dragonfly has relied on traditional methods of infecting its targets. Those include spam campaigns that trick recipients into installing malicious applications and so-called watering hole attacks, which plant exploits on websites known to be frequented by targets. The discovery that the group has more recently begun infecting suppliers underscores the evolution that's typical in many malware operations.

"The Dragonfly group is technically adept and able to think strategically," the Symantec report stated. "Given the size of some of its targets, the group found a 'soft underbelly' by compromising their suppliers, which are invariably smaller, less protected companies."
