GOVERNMENT

Trisis has mistakenly been released on the open internet

A nuclear reactor system. Trisis malware, which could damage industrial control systems like this pictured, is freely available on the internet. (Getty)

Chris Bing Jan 16, 2018 | CyberScoop

An elite, government authored cyberweapon has been sitting online in public view for nearly anyone to copy since Dec. 22 because multinational energy technology company Schneider Electric mistakenly posted a sensitive computer file to VirusTotal, three sources familiar with the matter told CyberScoop.

Schneider Electric obtained the file in question, titled “Library.zip,” after collecting evidence during a data breach investigation in the Middle East that focused on an incident at an oil and gas refinery. Library.zip holds the backbone of a dangerous malware framework known as “Trisis” or “Triton,” according to research by U.S. cybersecurity companies Dragos Inc. and FireEye.

The upload to VirusTotal, a public malware repository, provided the remaining puzzle piece needed for someone to reconstruct Trisis from publicly available artifacts. After being

posted to VirusTotal, Library.zip proliferated — it was picked up and re-uploaded to various platforms, including GitHub and VirusTotal.

Experts say the unique malware was carefully designed to manipulate safety controllers produced by Schneider Electric that essentially manage industrial equipment in nuclear power plants, oil and gas production facilities, and paper mills. It is just the fifth known malware variant capable of forcing physical damage by taking over industrial control systems (ICS). Trisis could be used by hackers to force a Schneider Electric safety instrumented system (SIS) to malfunction, leading machinery to breakdown or even explode.

According to analysts with FireEye, Symantec and Dragos, Trisis is likely the work of a nation-state.

"In line with industry protocol, a Schneider Electric employee posted a file to VirusTotal in the interest of enabling its security vendor members to analyze and respond to the new malware. Shortly afterwards, Schneider Electric received a request from a third party to take the file down, and promptly complied with that request," a Schneider Electric spokesperson told CyberScoop.

FireEye's internal digital forensics and investigations unit, named Mandiant, was originally called in by the Middle Eastern victim company in September 2017 to respond to the initial Trisis infection. CyberScoop reported Tuesday that a Saudi oil and gas facility owned in part by the state-backed petroleum company Saudi Aramco was Trisis' "patient zero."

While Schneider Electric's upload of Library.zip was removed from VirusTotal in less than 24 hours, various researchers and observers had quickly copied the code. CyberScoop identified GitHub accounts that are currently hosting the file.

Sources say Library.zip is harmless on its own, but when combined with another already publicly available computer file found at the scene of the breach, titled "Trilog.exe," it allows for anyone to recreate the core Trisis virus.

Someone likely associated with the investigation at the victim company uploaded the Trilog.exe file to VirusTotal on Aug. 29; months before Trisis was first publicly revealed.

FireEye chose not to share the Library.zip file or Trilog.exe file because it understood the dangers associated with spreading both pieces online. They did, however, release a YARA rule that made it easy to figure out when and if Trilog.exe and Library.zip were uploaded to VirusTotal. Typically, cybersecurity professionals will use YARA rules to scan for certain malicious files within a specific digital environment.

Dragos, which also obtained early samples of Trisis but through an intermediary, was similarly restrained in the publication of evidence. Dragos chose not to share the Library.zip file for fear of what damage it might cause.

Security researchers constantly post and disseminate malware across the internet for continued analysis and investigation. However, sources tell CyberScoop the VirusTotal discovery was alarming due to what an attacker could achieve with the Trisis framework. Additionally, there had been a concentrated, internal effort to keep Library.zip private.

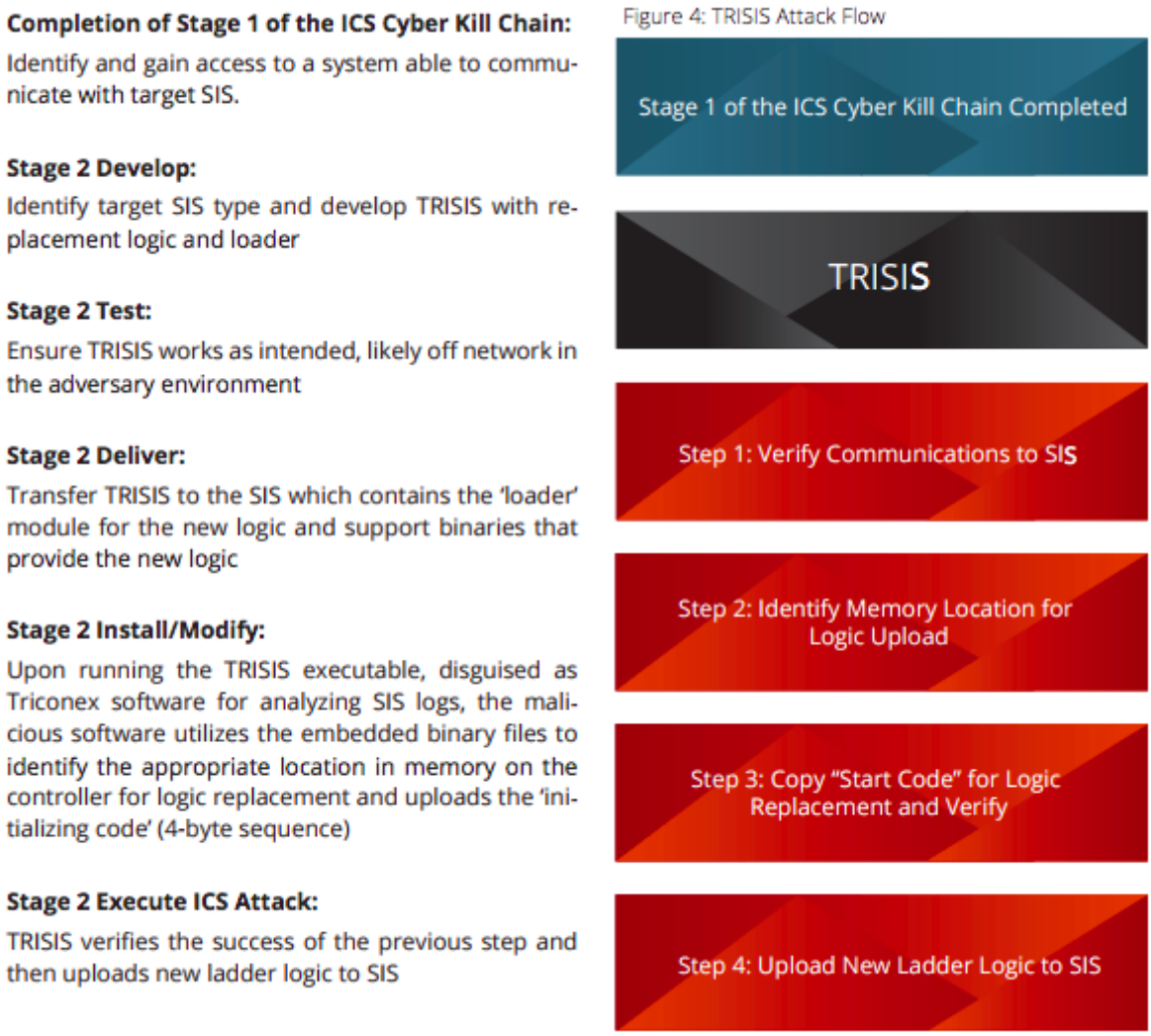
Three sources familiar with the Trisis investigation told CyberScoop that the publication of Library.zip by Schneider Electric — after Trilog.exe had already been publicized — effectively "lowered the barrier" for advanced hacking groups to create their own destructive, ICS-tailored malware.

"It caused a total panic," said one source. "It just was incredibly stupid for [Schneider Electric] to do it."

The sources, however, clarified that it would not be easy for any random hacker to pick up Trisis and then use it to its full potential.

There is still a lot of work that would need to go into turning Trisis into an actionable cyberattack, including but not limited to writing new shell code that causes some action on the safety systems.

In other words, the Trisis malware framework is just one component of what would need to be a highly sophisticated, multi-step intrusion that first compromises industrial control equipment before covertly planting Trisis.



Infographic via Dragos report

A technical report authored by Dragos shows how hackers armed with Trisis would still need to complete a list of actions before being able to cause any sort of physical damage to a factory, oil refinery or plant that uses Schneider Electric's safety controllers. Trisis in

itself does not force damage but it creates unsafe conditions that can lead to serious

The U.S. government, through the Department of Homeland Security and National Security Agency, is still studying Trisis, sources told CyberScoop.

-In this Story-

cyberattack, Dragos Inc., FireEye, research, Schneider Electric, Trisis, Triton

RELATED NEWS

GOVERNMENT

Norton takes over...

by **Patrick Howell O'Neill** • 20 hours ago

GOVERNMENT

Booz Allen scores $621M...

by **Chris Bing** • 1 day ago

GOVERNMENT

DHS threatened with...

by **Michelai Graham** • 1 day ago