



FINISHED INTELLIGENCE REPORTS

HC3 Analyst Note - Conti Ransomware



TLP:WHITE

May 25, 2021

Conti ransomware has recently been brought back into the spotlight due to its attack on Ireland's national health system - the Health Service Executive (HSE). Conti leverages many of the tools and techniques common among major ransomware operators such as

encryption, double-extortion via the use of a leak site, ransomware-as-a-service partnerships and many of the frequently-successful infection vectors such as phishing and remote desktop protocol (RDP) compromise, among others. One of several recommendations given by Sophos security researchers to protect networks from Conti is to keep regular backups of important and current data on an offline storage device.

Alert ID 9667f0a4

[View Alert](#)

Tags Conti, Analyst Note, HC3

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.

Certificate in Diversity Management in Health Care Program

certificate-in-diversity-management-in-health-care-program-brochure-5-1

Ginger

Lemon

Yogurt

cilantro

Onion-

Fresh-dill

Fresh-parsley

Kosher-salt

Spray-bottle

Turmeric

Coriander

cumin

Garlic

Celery

Carrots

Potato

Smoked-paprika

Apple-cider-vinegar