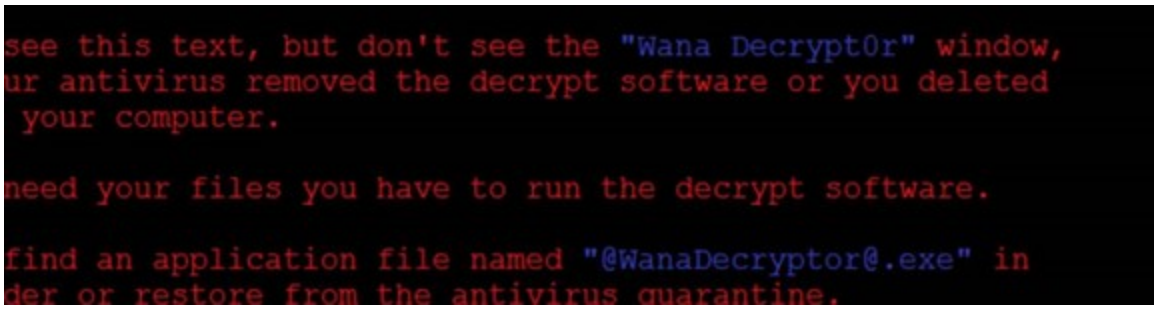
HHS Update and call Saturday: international cyber threat to healthcare organizations

May 12, 2017

Executive Summary

Ransomware can infect computers multiple ways and may or may not require user interaction. This message outlines several vectors of attack and what users can do to help protect themselves. Dial in information for a Sector-wide call for 1100 ET, May 13, 2017 is included.

Example of Ransomware



Where can I find the most up-to-date information from the U.S. government?

www.us-cert.gov/

hsin.dhs.gov (NCCIC portal for those who have access. We are not posting anything to the HPH portal at this time.)

How can I help protect myself from email-based ransomware attacks?

Ransomware can be delivered via email by attachments or links within the email. Attachments in emails can include documents, zip files, and executable applications. Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system. To help protect yourself, be aware of the following:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.
- Don't click on links in emails if you weren't expecting them – the attacker could camouflage a malicious link to make it look like it is for your bank, for example.
- Keep your computer and antivirus up to date – this adds another layer of defense that could stop the malware.

How can I help protect myself from open RDP ransomware attacks?

Recently, attackers have been scanning the Internet for Remote Desktop Protocol (RDP) servers open to the Internet. Once connected, an attacker can try to guess passwords for users on the system, or look for backdoors giving them access. Once in, it is just like they are logged onto the system from a monitor and keyboard. To help protect yourself, be aware of the following:

- If you do not need RDP, disable the service on the computer. There are several ways of doing this based on which version of Microsoft Windows you are using.
- If RDP is needed, only allow network access where needed. Block other network connections using Access Control Lists or firewalls, and especially from any address on the Internet.
- To find which version of Microsoft you are using: https://support.microsoft.com/en-us/help/13443/windows-which-operating-system

What is HHS doing to secure our systems?

- HHS Office of the Chief Information Officer implemented enterprise block across all OpDivs and StaffDivs and is ensuring all patching is up to date.
- HHS is working with Department of Homeland Security to scan HHS' CIDR IP addresses through the DHS NCATS program to identify RDP and SMB
- HHS notified VA and DHA and shared cyber threat information.
- HHS is coordinating with National Health Service (England) and UK-CERT.
- HHS through its law enforcement and intelligence resources with the Office of Inspector General and Office of Security and Strategic Information, have ongoing communications and are sharing and exchanging information with other key partners including the US Department of Homeland Security and the Federal Bureau of Investigation

Sector Call, 1100 ET, May 13, 2017

We will hold a call for the Healthcare and Public Health Sector Saturday, May 13 to include a situational awareness brief from HHS and discussion. This will be an operator-moderated call-- to speak on this call, you will need to press *1. You may share this call information with healthcare cyber professionals across the sector. Additional calls will be scheduled as needed.

Date: May 13, 2017

Time: 11am Eastern Time

Call in Number: 1-888-576-3153

Participant Code: 8645045

To talk on this call you will need to press *1

Requests for Information, impacts, and indicators

Please notify us at cip@hhs.gov if:

- you identify a new attack vector identified for this Ransomware other than Email, or the following Ports: SMB share and RDP; or
- if there are any impacts to patient care or supply chain distribution because of ransomware.

Please share any indicators or cyber threat information with the HHS Healthcare Cybersecurity and Communications Integration Center at HCCIC-mgmt@hhs.gov.

If you are the victim of ransomware

If your organization is the victim of a ransomware attack, please contact law enforcement immediately. We recommend organizations contact their FBI Field Office Cyber Task Force immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber crime. Victims are also encouraged to report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.