_____
From: Vassilenko, Olga (TBS)
Sent: April 27, 2018 10:32 AM
To: EOC Operations (MOHLTC)
Subject: Cyber Security Threat Advice - Orangeworm

OPS Cyber Security Division assessed a newly described malware by a threat group dubbed Orangeworm and recommends that the threat advisory note (starts below) be distributed to the health organizations to help them address potential cyber security risks.

Definitions:
CYBER SECURITY THREAT ADVICE (no active exploits)
Purpose: to enable organizations to prepare for and mitigate cyber threats
* Information about known vulnerabilities and other cyber threats, risks and incidents.
* List of additional resources to help recipients better understand the cyber risks and make informed decisions about how to take timely preventative action.
TRAFFIC LIGHT PROTOCOL (TLP)
* RED - personal for named recipients only
* AMBER - limited distribution
The recipient may share AMBER information with others within their organization, but only on a 'need-to-know' basis.
* GREEN - community wide
Information in this category can be circulated widely within a particular community.
However, the information may not be published or posted publicly on the Internet, nor released outside of the community.
* WHITE - unlimited
Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

CYBER SECURITY THREAT ADVICE - ORANGEWORM
TLP: GREEN

Date: April 27, 2018

OPS Cyber Security Division is providing this information for potential use at the sole discretion of recipients in order to protect against cyber threats. This notification is provided in order to help health care organizations enable cyber preparedness and resilience.

EXECUTIVE SUMMARY

Healthcare companies in the U.S., Europe and Asia are getting hit with a backdoor that comes from a long-observed group, which security vendor Symantec calls Orangeworm.

Orangeworm appears to infiltrate networks by taking advantage of vulnerabilities and then installing Trojan.Kwampirs backdoor malware. The Kwampirs malware was found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines.

Additionally, Orangeworm was observed to have an interest in machines used to assist patients in completing consent forms for required procedures.

WHAT IS THE ISSUE?

* Operating since 2015, a threat group dubbed Orangeworm has been newly attributed to hacking and infiltrating healthcare groups around the world. Companies specifically targeted include hospitals, healthcare providers, pharmaceuticals, IT services firms serving the healthcare industry, and more.

* Analysts are still investigating the campaign tactics, techniques, and procedures of the Orangeworm group to determine their objectives whether espionage of the medical systems themselves, to steal patient data, or potential future sabotage or ransom.

* The Orangeworm group is using a repurposed Trojan called Kwampirs to set up persistent remote access after they infiltrate victim organizations. Kwampirs is not especially stealthy and can be detected using indicators of compromise and activity on the target system. The Trojan evades hash-based detection by inserting a random string in its main executable so its hash is different on each system. However, Kwampirs uses consistent services names, configuration files, and similar payload DLLs on the target machine that can be used to detect it.

* The Kwampirs malware was found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines. Additionally, Orangeworm was observed to have an interest in machines used to assist patients in completing consent forms for required procedures.

* According to Deloitte, identifying and mitigating the risks of fielded and legacy connected devices represents healthcare's biggest cybersecurity challenge.

ADVICE FROM INTELLIGENCE PARTNERS

At this stage there has been no evidence of any malicious exploitation. There are only one or two reported cases in Canada where Orangeworm might have been discovered. If active exploitation is seen globally, the Canadian Cyber Incident Response Centre (CCIRC) and other intelligence partners will issue a cyber flash, which will include indicators of compromise (IOC). CCIRC will encourage organizations to block these additional IOC's from accessing information on an organization's network.

Symantec provides the following list of IoCs: https://urldefense.proofpoint.com/v2/url?u=https-3A__content.connect.symantec.com_sites_default_files_2018-2D04_Orangeworm-2520IOCs.pdf&d=DwIFAg&c=0hCx1u36-XAMUG1zdNEI2VR5Zeej6Q9MkDa5wSI1xHs&r=3PCvL67TQo31KUNWn9CvKVvl5EjuDeCjYCYexwLOWUo&m=DwhjCyGHD59ufBd3wad2tDwS-E9mwjbG9E_bgxRYYFc&s=9bDPLCx0HU243FKuKjXmo11fgyP1Mk1cFKqhq03xQJM&e=

REFERENCES

The following references provide details of Orangeworm developments to help organizations mitigate potential cyber risks:

https://urldefense.proofpoint.com/v2/url?u=https-3A__securityaffairs.co_wordpress_71698_cyber-2Dcrime_orangeworm-2Dtargets-2Dhealthcare.html&d=DwIFAg&c=0hCx1u36-XAMUG1zdNEI2VR5Zeej6Q9MkDa5wSI1xHs&r=3PCvL67TQo31KUNWn9CvKVvl5EjuDeCjYCYexwLOWUo&m=DwhjCyGHD59ufBd3wad2tDwS-E9mwjbG9E_bgxRYYFc&s=JfQLIGts7w4PIoQymrpiVQykNWDNXOP47xxG9yvZDvY&e=
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.theregister.co.uk_2018_04_24_orangeworm-5Fmedical-5Fmalware&d=DwIFAg&c=0hCx1u36-XAMUG1zdNEI2VR5Zeej6Q9MkDa5wSI1xHs&r=3PCvL67TQo31KUNWn9CvKVvl5EjuDeCjYCYexwLOWUo&m=DwhjCyGHD59ufBd3wad2tDwS-E9mwjbG9E_bgxRYYFc&s=HrzvkVaXbFXjMuf_Lt-n-b17B-SD2PeEDGhywv3Bqek&e=
https://urldefense.proofpoint.com/v2/url?u=https-3A__blog.qualys.com_indication-2Dof-2Dcompromise_2018_04_24_orangeworm-2Dtargeting-2Dhealthcare-2Dindustry-2Dsince-2D2015-2Dnow-2Dexposed&d=DwIFAg&c=0hCx1u36-XAMUG1zdNEI2VR5Zeej6Q9MkDa5wSI1xHs&r=3PCvL67TQo31KUNWn9CvKVvl5EjuDeCjYCYexwLOWUo&m=DwhjCyGHD59ufBd3wad2tDwS-E9mwjbG9E_bgxRYYFc&s=gCkSgsaCGfzwe-TreIZ_Z3GjSAnMi4NMa0dZeFfmGwk&e=

FOR FURTHER INFORMATION
If you find any of these indicators on your networks, or have related information, please contact cyberadvice@ontario.ca

NO WARRANTY
This Cyber Advisory contains third party content and links. OPS Cyber Security Division does not control or maintain third party links and makes no representation or warranty that the link will still work when you click on it or the service or content is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether you want to follow any link or agree to receive or rely on any service or content that is made available to you.