Security Response Attack Investigation Team

POSTED: | MIN READ | THREAT INTELLIGENCE

Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia.

First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage.

> "Orangeworm installs the Kwampirs custom backdoor in large firms in the healthcare sector in the U.S., Europe & Asia. https://symc.ly/2K1oJjU"

SHARE

CLICK TO TWEET

Sights set on healthcare

Based on the list of known victims, Orangeworm does not select its targets randomly or conduct opportunistic hacking. Rather, the group appears to choose its targets carefully and deliberately, conducting a good amount of planning before launching an attack.

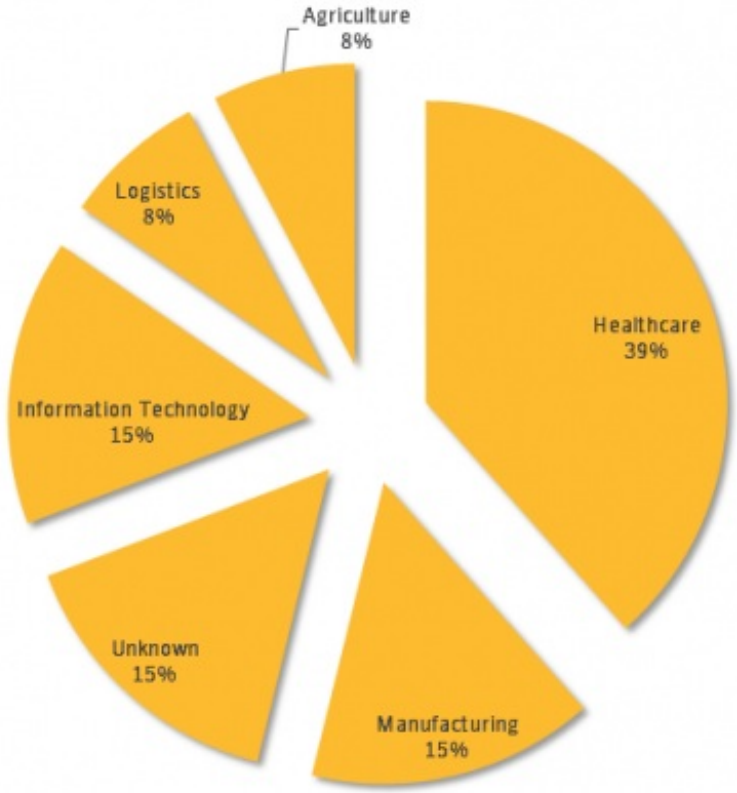


Figure 1. Nearly 40 percent of Orangeworm's victims operate within the healthcare industry

According to Symantec telemetry, almost 40 percent of Orangeworm's confirmed victim organizations operate within the healthcare industry. 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. The exact motives of the group are unclear.

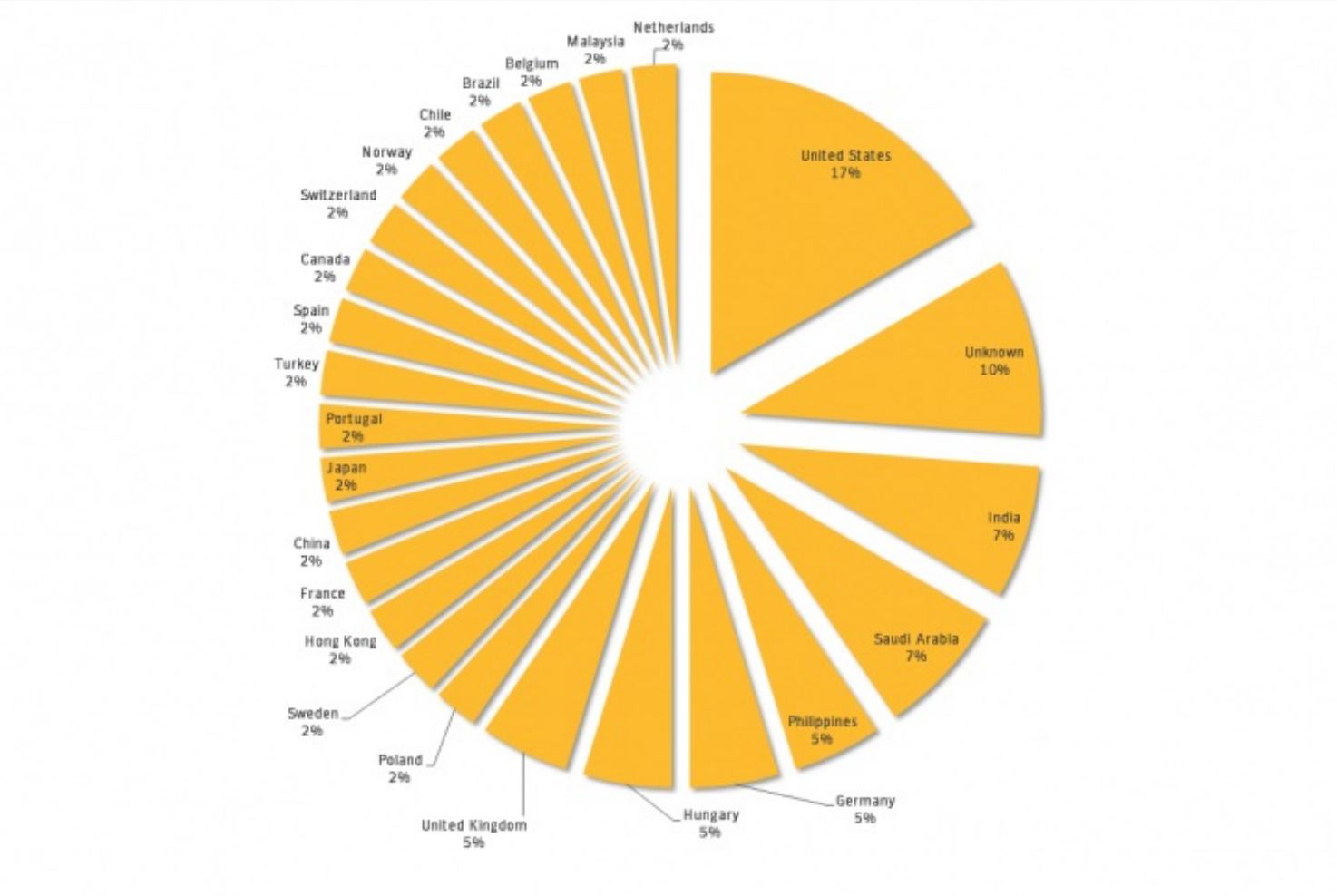


Figure 2. The biggest number of Orangeworm's victims are located in the U.S.

The biggest number of Orangeworm's victims are located in the U.S., accounting for 17 percent of the infection rate by region. While Orangeworm has impacted only a small set of

victims in 2016 and 2017 according to Symantec telemetry, we have seen infections in multiple countries due to the nature of the victims operating large international corporations.

> The biggest number of Orangeworm's victims are located in the U.S., accounting for 17 percent of the infection rate by region.

Healthcare providers caught in the crosshairs

We believe that these industries have also been targeted as part of a larger supply-chain attack in order for Orangeworm to get access to their intended victims related to healthcare. Orangeworm's secondary targets include Manufacturing, Information Technology, Agriculture, and Logistics. While these industries may appear to be unrelated, we found them to have multiple links to healthcare, such as large manufacturers that produce medical imaging devices sold directly into healthcare firms, IT organizations that provide support services to medical clinics, and logistical organizations that deliver

healthcare products.

Post-compromise activities

Once Orangeworm has infiltrated a victim's network, they deploy Trojan.Kwampirs, a backdoor Trojan that provides the attackers with remote access to the compromised computer.

When executed, Kwampirs decrypts and extracts a copy of its main DLL payload from its resource section. Before writing the payload to disk, it inserts a randomly generated string into the middle of the decrypted payload in an attempt to evade hash-based detections.

To ensure persistence, Kwampirs creates a service with the following configuration to ensure that the main payload is loaded into memory upon system reboot:

Service name	WmiApSrvEx
Display name	WMI Performance Adapter Extension
Start type	SERVICE_AUTO_START
Binary pathname	%Windows%\System32\<filename.dll>
Command	rundll32.exe "%Windows%\System32\<filename>",ControlTrace -Embedding -k

The backdoor also collects some rudimentary information about the compromised computer including some basic network adapter information, system version information, and language settings.

Orangeworm likely uses this information to determine whether the system is used by a researcher or if the victim is a high-value target. Once Orangeworm determines that a potential victim is of interest, it proceeds to aggressively copy the backdoor across open network shares to infect other computers.

It may copy itself to the following hidden file shares:

- ADMIN$
- C$WINDOWS
- D$WINDOWS
- E$WINDOWS

Information gathering

At this point, the attackers proceed to gather as much additional information about the victim's network as possible, including any information pertaining to recently accessed

computers, network adapter information, available network shares, mapped drives, and files present on the compromised computer.

We have observed the attackers executing the following commands within victim environments:

Command	Description
cmd.exe /c "arp -a" 2>nul	Display recently contacted addresses per available network interface
cmd.exe /c "systeminfo" 2>nul	Display detailed configuration information for the system and its operating system (e.g. OS version information, registered owner details, manufacture details, processor type, available storage, list of installed patches, etc.)
cmd.exe /c "hostname" 2>nul	Display system's configured hostname
cmd.exe /c "ver" 2>nul	Display system version information
cmd.exe /c "route print" 2>nul	Display routing table for available network interfaces
cmd.exe /c "getmac" 2>nul	Display the systems configured MAC address
cmd.exe /c "ipconfig /all" 2>nul	Display IP address configuration information for any available network interfaces
cmd.exe /c "netstat -nao" 2>nul	Display a list of active and listening connections (TCP and UDP)
cmd.exe /c "tasklist /v" 2>nul	Display list of running system processes
cmd.exe /c "tasklist /svc" 2>nul	Display list of running system services
cmd.exe /c "net share" 2>nul	Display list of available network shares
cmd.exe /c "net users" 2>nul	Display list of available user groups
cmd.exe /c "set" 2>nul	Display list of configured environment variables
cmd.exe /c "net accounts" 2>nul	Display account policy information (e.g. maximum

cmd.exe /c "net accounts" 2>nul	Display account policy information (e.g. maximum password age, length of password, lockout duration, etc.)
cmd.exe /c "net config workstation" 2>nul	Display system network configuration information (e.g. computer name, current username, version information, domain configuration, etc.)
cmd.exe /c "net localgroup administrators" 2>nul	Display list of local accounts with administrative access
cmd.exe /c "net localgroup users" 2>nul	Display list of local group user accounts
cmd.exe /c "net localgroup /domain" 2>nul	Display domain local groups
cmd.exe /c "net use" 2>nul	Display list of available network mappings
cmd.exe /c "net view" 2>nul	Display list of available servers on the network
cmd.exe /U /c dir /s /a c:\ >> "C:\windows\TEMP\[RANDOM].tmp" 2>nul	List files and directories in C:\
cmd.exe /c "cmd /c date /t" 2>nul	Display system date

No concern about being discovered

Kwampirs uses a fairly aggressive means to propagate itself once inside a victim's network by copying itself over network shares. While this method is considered somewhat old, it may still be viable for environments that run older operating systems such as Windows XP. This method has likely proved effective within the healthcare industry, which may run legacy systems on older platforms designed for the medical community. Older systems like Windows XP are much more likely to be prevalent within this industry.

Additionally, once infected, the malware cycles through a large list of command and control

(C&C) servers embedded within the malware. It appears while the list is extensive, not all of the C&Cs are active and continue to beacon until a successful connection is established. Despite modifying a small part of itself while copying itself across the network as a means to evade detection, the operators have made no effort to change the C&C communication protocol since its first inception.

Both of these methods are considered particularly “noisy” and may indicate that Orangeworm is not overly concerned with being discovered. The fact that little has changed with the internals of Kwampirs since its first discovery may also indicate that previous mitigation methods against the malware have been unsuccessful, and that the attackers have been able to reach their intended targets despite defenders being aware of their presence within their network.

> Kwampirs uses a fairly aggressive means to propagate itself once inside a victim's network by copying itself over network shares.

No hallmarks of a nation-state actor

While Orangeworm is known to have been active for at least several years, we do not believe that the group bears any hallmarks of a state-sponsored actor—it is likely the work of an individual or a small group of individuals. There are currently no technical or operational indicators to ascertain the origin of the group.

Protection

Symantec customers are protected against Orangeworm and Symantec has also made efforts to notify identified targets of its operations.

Customers with Intelligence Services or WebFilter-enabled products are protected against activity associated with the Orangeworm group. These products include:

- Web Security Service (WSS)
- ProxySG
- Advanced Secure Gateway (ASG)
- Security Analytics
- Content Analysis
- Malware Analysis
- SSL Visibility

- PacketShaper

Symantec has the following specific detections in place for tools used by Orangeworm:

Anti-virus (AV):

- Trojan.Kwampirs

Intrusion prevention system (IPS):

- System Infected: Trojan.Kwampirs Activity
- System Infected: Trojan.Kwampirs Activity 2
- System Infected: Trojan.Kwampirs Activity 4

Indicators of Compromise

File Attachments

Indicators of Compromise for Orangeworm | PDF | 556.65 KB

About the Author

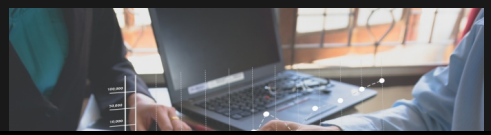
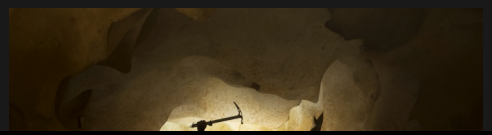
Security Response Attack Investigation Team

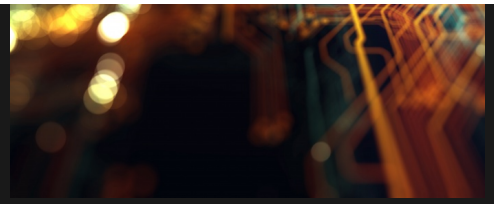
The Attack Investigation Team is a group of security experts within Symantec Security Response whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis which helps customers respond to attacks.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

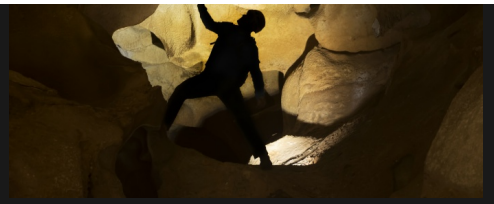



POSTED: | 20 MIN READ

Microsoft Patch Tuesday – April 2018

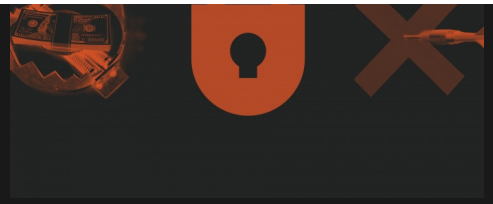
POSTED: | 2 MIN READ

Latest Intelligence for March 2018



POSTED: | 0 MIN READ

Browser-based coin mining without a browser?



POSTED: | 4 MIN READ

ISTR 23: Insights into the Cyber Security Threat Landscape