Patchwork cyberespionage group expands targets from governments to wide range of industries

symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

July 24, 2016

Symantec Official Blog

Symantec finds that Patchwork now targets a variety of industries in the US, China, Japan, South East Asia, and the UK.

By: Joji HamadaSymantec Employee

- Created 25 Jul 2016
- : 简体中文, 繁體中文, 日本語, 한국어

The Patchwork attack group has been targeting more than just government-associated organizations. Our research into the group found that it's been attacking a broad range of industries—including aviation, broadcasting, and finance—to drop back door Trojans.

Symantec Security Response has been actively monitoring Patchwork, also known as Dropping Elephant, which uses Chinese-themed content as bait to compromise its targets' networks. Two security companies, Cymmetria and Kaspersky, each recently released reports on the campaign, most of which are in line with our observations.

Patchwork group widens scope to include broad range of industries in multiple regions

Targets
As other researchers observed, Patchwork originally targeted governments and government-related organizations. However, the group has since expanded its focus to include a broader range of industries.

While most of the interest still lies in the public sector, more recent attacks were found targeting the following industries:

- Aviation
- Broadcasting
- Energy
- Financial
- Non-governmental organizations (NGO)
- Pharmaceutical
- Public sector
- Publishing
- Software

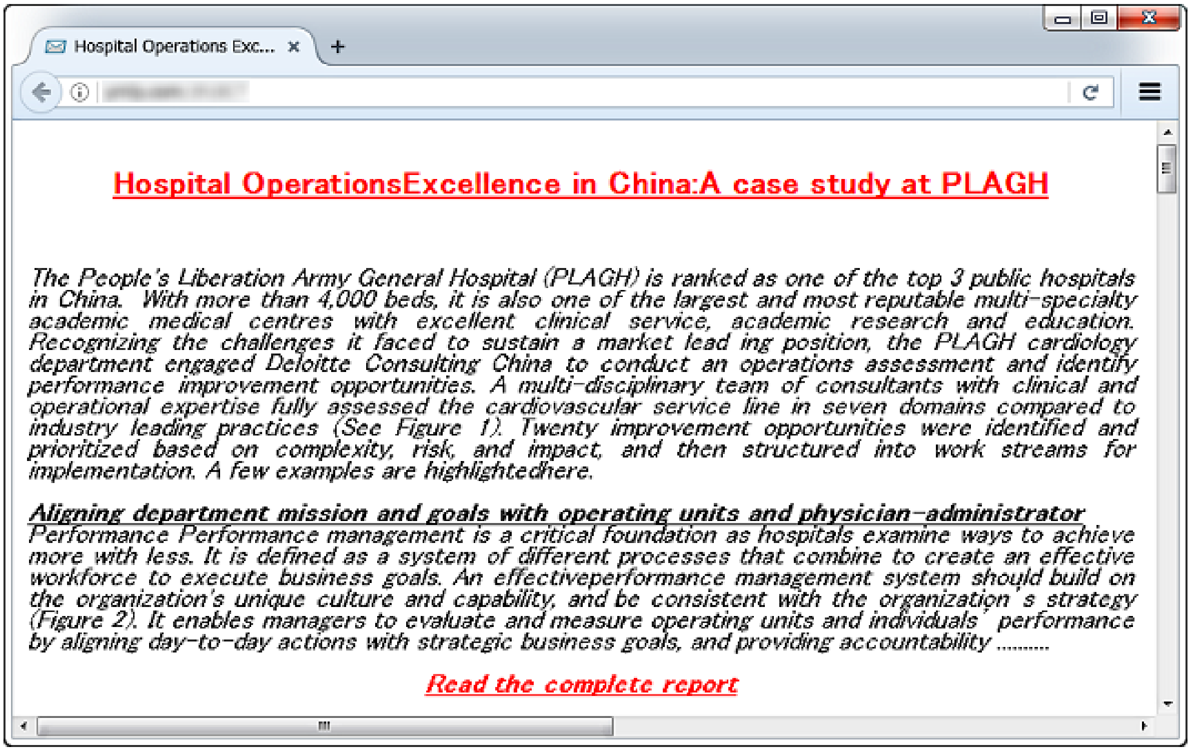
According to Symantec telemetry, targeted organizations are located in dispersed regions. Although approximately half of the attacks focus on the US, other targeted regions include China, Japan, Southeast Asia, and the United Kingdom.

Aviation, NGOs, energy, financial, among industries targeted by Patchwork cyberespionage group

Attack vector

Our first observation of an attempted attack related to this campaign dates back to November 2015, although Symantec telemetry data indicates that the campaign may have already existed in early 2015 or perhaps even earlier.

The threat actor mainly relies on a legitimate mailing list provider to send newsletters to a select number of targets. The newsletter includes a link to the attacker's website, which has content focusing on topics related to China to draw the target's interest. These websites are hosted on the same domains as the mailing list provider. Each website is customized for the intended target, and contains specialized topics related to the targeted industries.



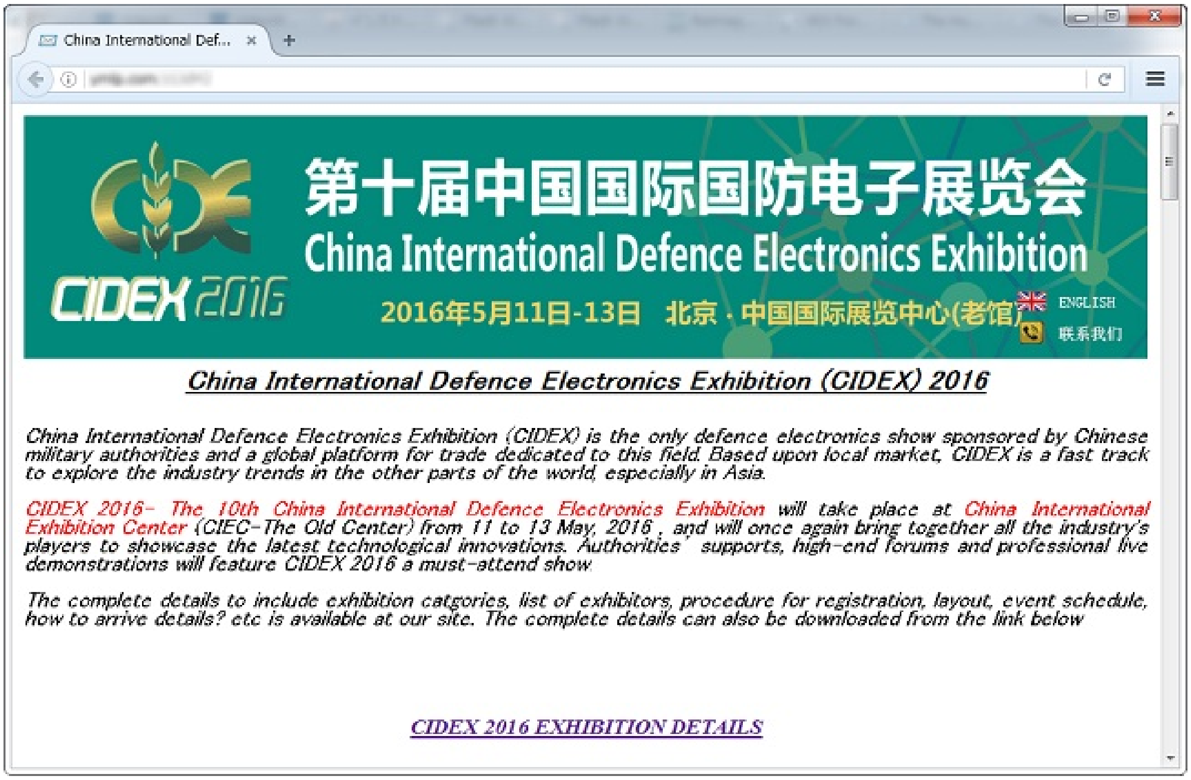
Hospital OperationsExcellence in China:A case study at PLAGH

The People's Liberation Army General Hospital (PLAGH) is ranked as one of the top 3 public hospitals in China. With more than 4,000 beds, it is also one of the largest and most reputable multi-specialty academic medical centres with excellent clinical service, academic research and education. Recognizing the challenges it faced to sustain a market lead ing position, the PLAGH cardiology department engaged Deloitte Consulting China to conduct an operations assessment and identify performance improvement opportunities. A multi-disciplinary team of consultants with clinical and operational expertise fully assessed the cardiovascular service line in seven domains compared to industry leading practices (See Figure 1). Twenty improvement opportunities were identified and prioritized based on complexity, risk, and impact, and then structured into work streams for implementation. A few examples are highlightedhere.

Aligning department mission and goals with operating units and physician-administrator
Performance Performance management is a critical foundation as hospitals examine ways to achieve more with less. It is defined as a system of different processes that combine to create an effective workforce to execute business goals. An effectiveperformance management system should build on the organization's unique culture and capability, and be consistent with the organization's strategy (Figure 2). It enables managers to evaluate and measure operating units and individuals' performance by aligning day-to-day actions with strategic business goals, and providing accountability ....

Read the complete report

Figure 1. A customized website with content related to a Chinese public hospital



第十届中国国际国防电子展览会

China International Defence Electronics Exhibition

2016年5月11日-13日　北京 · 中国国际展览中心(老馆)

CIDEX 2016

China International Defence Electronics Exhibition (CIDEX) 2016

China International Defence Electronics Exhibition (CIDEX) is the only defence electronics show sponsored by Chinese military authorities and a global platform for trade dedicated to this field. Based upon local market, CIDEX is a fast track to explore the industry trends in the other parts of the world, especially in Asia.

CIDEX 2016- The 10th China International Defence Electronics Exhibition will take place at China International Exhibition Center (CIEC-The Old Center) from 11 to 13 May, 2016 , and will once again bring together all the industry's players to showcase the latest technological innovations. Authorities' supports, high-end forums and professional live demonstrations will feature CIDEX 2016 a must-attend show.

The complete details to include exhibition catgories, list of exhibitors, procedure for registration, layout, event schedule, how to arrive details? etc is available at our site. The complete details can also be downloaded from the link below

CIDEX 2016 EXHIBITION DETAILS

Figure 2. A customized website with content related to the Chinese military

The malicious sites link to files hosted on different domains, which appear to be solely used for malicious purposes. The domains are registered under names that pose as legitimate sources for Chinese intelligence. Several domains predominantly used in the attacks are hosted on two servers with the IP addresses 212.83.146.3 and 37.58.60.195.

These websites host two different types of malicious files: a PowerPoint file (.pps) and a rich text file with a Word .doc extension.

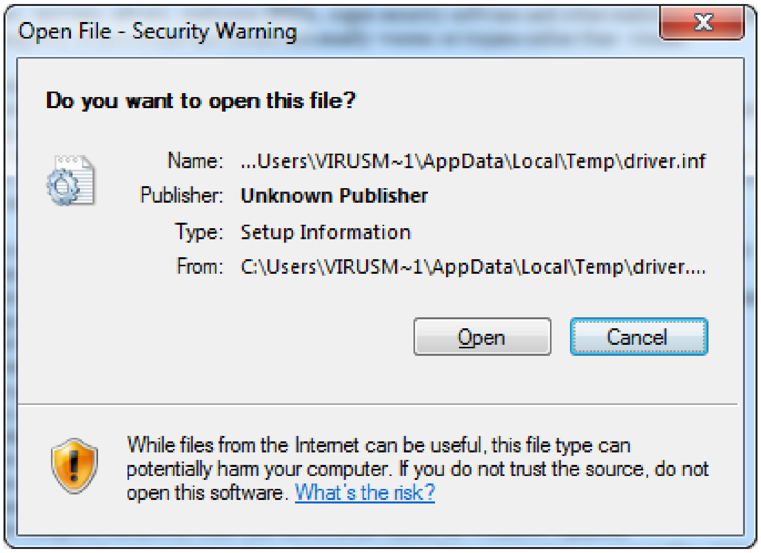
The PowerPoint files appear to exploit the Microsoft Windows OLE Package Manager Remote Code Execution Vulnerability (CVE-2014-4114), which was used in the Sandworm attacks against American and European targets in October 2014. The rich text files typically attempt to exploit the Microsoft Office Memory Corruption Vulnerability (CVE-2015-1641), which was patched in April 2015. We have also confirmed an older flaw being exploited, the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158).

From what we can confirm, the documents contain copies of publicly available content taken from legitimate websites. Topics range from military/defense, hospital, naval disputes, and even malware removal.

Malicious PowerPoint files

The .pps files likely exploit the Microsoft Windows OLE Package Manager Remote Code Execution Vulnerability (CVE-2014-4114). However, the exploit for this particular campaign is a slight variation of similar exploits observed in the past. The exploit takes advantage of how the patch is designed to only warn users, rather than completely prevent malware infections without user interaction.

Nothing happens when the file is opened on PowerPoint 2016. However, when the file is opened on older versions of PowerPoint, it displays a security warning asking whether the user wants to open driver.inf depending on the environment, such as the version of the operating system and the patch applied.



Open File - Security Warning

Do you want to open this file?

Name: ...Users\VIRUSM~1\AppData\Local\Temp\driver.inf
Publisher: **Unknown Publisher**
Type: Setup Information
From: C:\Users\VIRUSM~1\AppData\Local\Temp\driver....

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Figure 3. Opening the .pps file on PowerPoint versions earlier than 2016 displays this prompt

If the user chooses to open the file, the computer will be compromised. If the user chooses not to open it, the computer will not be infected. However, Backdoor.Enfourks will be dropped, though not executed, into the temporary directory when the .pps file is opened. This poses a risk of compromise to the intended target.

We have confirmed this issue on all versions of PowerPoint tested in the lab. Users should manually remove any potential dropped files which would typically be named “sysvolinfo.exe”.

Malicious Word .doc file

Besides the .pps file, the threat actor uses rich text files to deliver the malware. While other researchers have reported that these files exploit CVE-2012-0158, Symantec has also observed CVE-2015-1641 being exploited to drop Backdoor.Steladok.

Main payloads

Both the .doc and .pps files mainly drop two malware families. Typically, the PowerPoint Slide file drops Backdoor.Enfourks, an AutoIT executable which is usually bloated with meaningless data and targets mainly 32-bit systems. The .doc file drops Backdoor.Steladok.

While both back door Trojans wait for commands from the threat actor, they can search for files and upload them to the specified server once activated. For unknown reasons, both threats use Baidu, the Chinese software vendor, in their routines. The Trojans confirm an internet connection by pinging Baidu’s server and create a registry entry with the vendor’s name to run every time Windows starts. As two file types are used to deliver two different payloads, there are likely multiple individuals or groups contributing to the malware development efforts.

Mitigation

Users should adhere to the following advice to prevent Patchwork’s attacks from succeeding:

- Delete any suspicious-looking emails you receive, especially if they contain links or attachments. Spear-phishing emails are frequently used by cyberespionage attackers as a means of luring victims into opening malicious files.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities which are frequently exploited by attackers.
- Keep your security software up to date to protect yourself against any new variants of this malware.

Protection

Symantec and Norton products detect Patchwork’s malware as follows:

Antivirus:

Intrusion prevention system:

- System Infected: Backdoor.Steladok Activity
- System Infected: Backdoor.Enfourks Activity

Indicators of compromise

The following details suspicious domains, IP addresses, and files, which may indicate that Patchwork has compromised a computer:

Suspected domains and IP addresses:

- chinastrats.com
- epg-cn.com
- extremebolt.com
- info81.com
- lujunxinxi.com
- militaryworkerscn.com
- milresearchcn.com
- modgovcn.com
- newsnstat.com
- nudtcn.com
- socialfreakzz.com
- 81-cn.net
- cnmilit.com
- nduformation.com
- expatchina.info
- info81.com
- climaxcn.com
- expatchina.info
- miltechcn.com
- miltechweb.com
- securematrixx.com
- 46.166.163.242
- 212.129.13.110

Detection name	MD5	File name
Trojan.PPDropper	0bbff4654d0c4551c58376e6a99dfda0	
Trojan.PPDropper	1de10c5bc704d3eaf4f0cfa5ddd63f2d	MilitaryReforms2.pps
Trojan.PPDropper	2ba26a9cc1af4479e99dcc6a0e7d5d67	2016_China_Military_PowerReport.pps
Trojan.PPDropper	375f240df2718fc3e0137e109eef57ee	PLA_UAV_DEPLOYMENT.pps
Trojan.PPDropper	38e71afcdd6236ac3ad24bda393a81c6	militarizationofsouthchinasea_1.pps
Trojan.PPDropper	3e9d1526addf2ca6b09e2fdb5fd4978f	How_to_easily_clean_an_infected_computer.pps
Trojan.PPDropper	475c29ed9373e2c04b7c3df6766761eb	PLA_Forthcoming_Revolution_in_Doctrinal_Affairs.pps

Detection name	MD5	File name
Trojan.PPDropper	4dbb8ad1776af25a5832e92b12d4bfff	maritime_dispute.pps
Trojan.PPDropper	4dbb8ad1776af25a5832e92b12d4bfff	Clingendael_Report_South_China_Sea.pps
Trojan.PPDropper	543d402a56406c93b68622a7e392728d	2016_China_Military_PowerReport.pps
Trojan.PPDropper	551e244aa85b92fe470ed2eac9d8808a	Assessing_PLA_Organisational_Reforms.pps
Trojan.PPDropper	6877e60f141793287169125a08e36941	Clingendael_Report_South_China_Sea.pps
Trojan.PPDropper	6d8534597ae05d2151d848d2e6427f9e	cn-lshc-hospital-operations-excellence.pps
Trojan.PPDropper	74fea3e542add0f301756581d1f16126	Clingendael_Report_South_China_Sea_20160517Downloaded.pps
Trojan.PPDropper	812a856288a03787d85d2cb9c1e1b3ba	
Trojan.PPDropper	8f7b1f320823893e159f6ebfb8ce3e78	
Trojan.PPDropper	b163e3906b3521a407910aeefd055f03	china_security_report_2016.pps
Trojan.PPDropper	d456bbf44d73b1f0f2d1119f16993e93	
Trojan.PPDropper	e7b4511cba3bba6983c43c9f9014a49d	Chinastrats.com netflix2.pps
Trojan.PPDropper	ebfa776a91de20674a4ae55294d85087	Chinese_Influence_Faces_2.pps
Trojan.PPDropper	eefcef704b1a7bea6e92dc8711cfd35e	Top_Five_AF.pps

Table 1. Malicious PowerPoint slides associated with this campaign

Detection name	MD5	File name
Trojan.Mdropper	2099fcd4a81817171649cb38dac0fb2a	
Trojan.Mdropper	3d852dea971ced1481169d8f66542dc5	China_Vietnam_Military_Clash.doc
Trojan.Mdropper	4ff89d5341ac36eb9bed79e7afe04cb3	Cyber_Crime_bill.doc
Trojan.Mdropper	7012f07e82092ab2daede774b9000d64	china_report_EN_web_2016_A01.doc
Trojan.Mdropper	735f0fbe44b70e184665aed8d1b2c117	Cyber_Crime_bill.doc
Trojan.Mdropper	7796ae46da0049057abd5cfb9798e494	
Trojan.Mdropper	e5685462d8a2825e124193de9fa269d9	PLA_Forthcoming_Revolution_in_Doctrinal_Affairs2.doc
Trojan.Mdropper	f5c81526acbd830da2f533ae93deb1e1	Job_offers.doc

Table 2. Malicious rich text files associated with this campaign

Detection name	MD5
Backdoor.Steladok	0f09e24a8d57fb8b1a8cc51c07ebbe3f
Backodor.Enfourks	233a71ea802af564dd1ab38e62236633
Backdoor.Steladok	2c0efa57eeffed228eb09ee97df1445a
Backodor.Enfourks	3ac28869c83d20f9b18ebbd9ea3a9155
Trojan.Gen.2	465de3db14158005ede000f7c0f16efe
Trojan.Gen.2	4fca01f852410ea1413a876df339a36d
Backodor.Enfourks	61e0f4ecb3d7c56ea06b8f609fd2bf13

Detection name	MD5
Backodor.Enfourks	6b335a77203b566d92c726b939b8d8c9
Backodor.Enfourks	a4fb5a6765cb8a30a8393d608c39d9f7
Backodor.Enfourks	b594a4d3f7183c3af155375f81ad6c3d
Backodor.Enfourks	b7433c57a7111457506f85bdf6592d18
Backodor.Enfourks	b7433c57a7111457506f85bdf6592d18
Backodor.Enfourks	c575f9b40cf6e6141f0ee40c8a544fb8
Backodor.Enfourks	d8102a24ca00ef3db7d942912765441e
Backdoor.Steladok	f47484e6705e52a115a3684832296b39
Backodor.Enfourks	f7ce9894c1c99ce64455155377446d9c
Infostealer	ffab6174860af9a7c3b37a7f1fb8f381

Table 3. Payloads associated with this campaign

- Tags: Products, Endpoint Protection, Security Response, APT, Backdoor.Enfourks, Backdoor.Steladok, CVE-2012-0158, CVE-2014-4114, CVE-2015-1641, South East Asia, UK, USA
- Subscriptions (0)