Operation Tropic Trooper

Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers

Kervin Alintanahin
Targeted Attack Defense Response Team

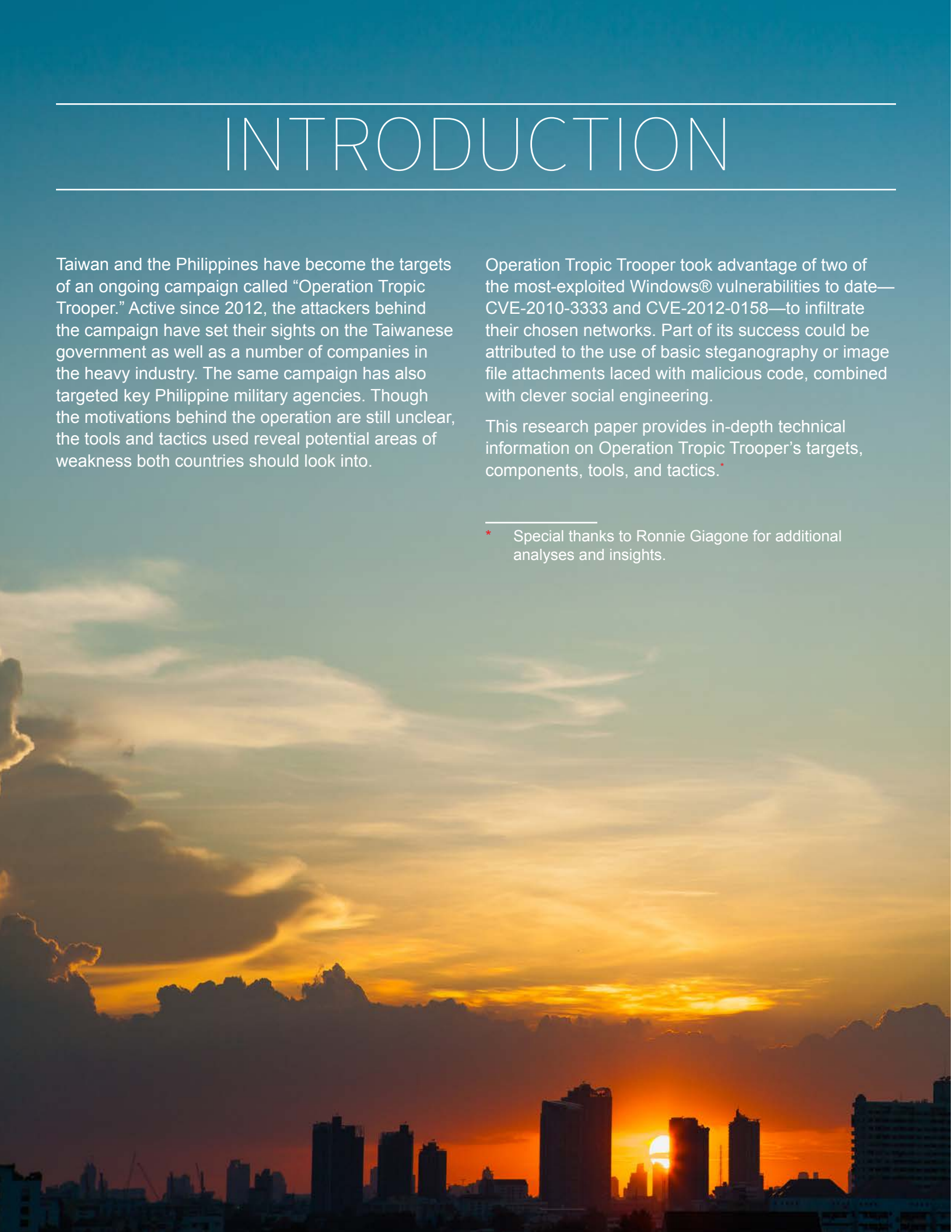
Contents

INTRODUCTION

Taiwan and the Philippines have become the targets of an ongoing campaign called "Operation Tropic Trooper." Active since 2012, the attackers behind the campaign have set their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies. Though the motivations behind the operation are still unclear, the tools and tactics used reveal potential areas of weakness both countries should look into.

Operation Tropic Trooper took advantage of two of the most-exploited Windows® vulnerabilities to date—CVE-2010-3333 and CVE-2012-0158—to infiltrate their chosen networks. Part of its success could be attributed to the use of basic steganography or image file attachments laced with malicious code, combined with clever social engineering.

This research paper provides in-depth technical information on Operation Tropic Trooper's targets, components, tools, and tactics.*

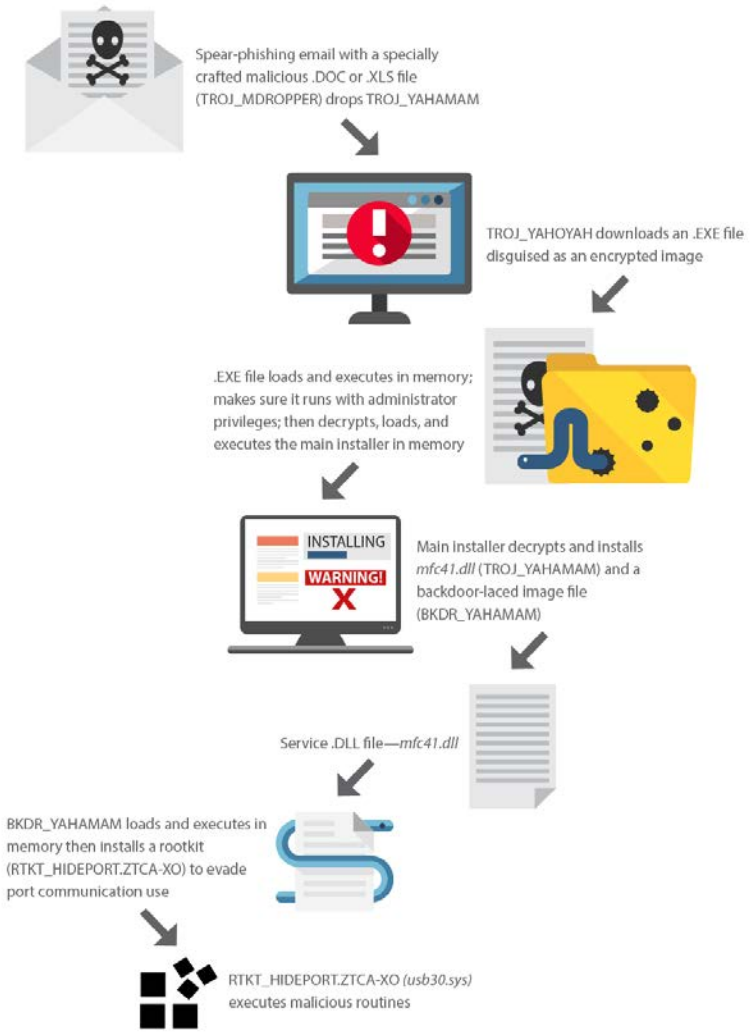


* Special thanks to Ronnie Giagone for additional analyses and insights.

Targets

Malware used in Operation Tropic Trooper shared similar characteristics with those used in attacks targeting various organizations in Vietnam and India as early as 2011. [1]

Operation Tropic Trooper targets government institutions, military agencies, and companies in the heavy industry in Taiwan and the Philippines. [2]

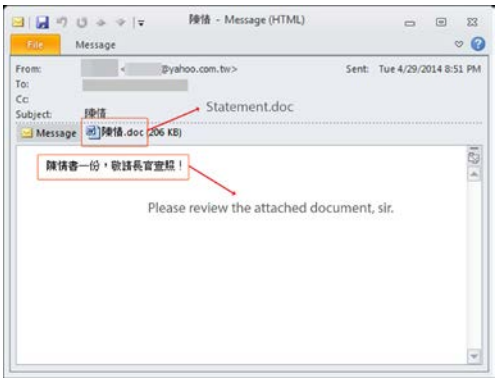


Operation Tropic Trooper campaign flow

Campaign Components

Point of Entry

The actors behind Operation Tropic Trooper used spear-phishing emails with weaponized attachments to exploit old vulnerabilities, particularly CVE-2010-3333 and CVE-2012-0158. [3–5] These bugs have been two of the most exploited vulnerabilities since their discovery. [6–7]



Spear-phishing email sample

To infiltrate target networks, the attackers relied on crafty social engineering tricks. They used contextually relevant subjects, content, and aptly named attachments such as “Statement” to convince chosen recipients to download and open the files supposedly sent for review.

The following filenames were also used:

- *3AD 28 March 2013, SI re ASG Plan Bombing in Zamboanga City.doc*
- *Troops Disposition 26 FEB 13.doc*
- *2nd qtr 2013 AR PF15.doc*
- *Draft AS-PH MLSA - v3 DAGTS_CFO_ILOG_DSA Clean.doc*
- 關於*104*年中央政府總預算*.doc* (translation: *About 104 years total central government budget.doc)*
- 實驗室電話表*.doc* (translation: *Laboratory telephone table.doc)*

- *[REDACTED]*自荐信及个人简历*.doc* (translation: *[REDACTED] cover letter and your resume.doc)*

Opening the attachment runs an embedded malicious executable file, normally a downloader that accesses a malicious site to download an image file. Some attachments open decoy documents to hide their malicious nature.

Department of Transportation and Communications
Philippine Coast Guard
HEADQUARTERS COAST GUARD DISTRICT NORTH WESTERN LUZON
Poro Point, City of San Fernando, La Union
Telefax: (072) Email:

MEMORANDUM

To : Director

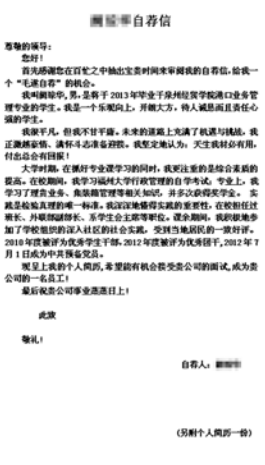
From : Commander, Coast Guard District North Western Luzon

Subj : Preparedness Plan for the Rainy Season

Date : May 27, 2013

Submitted herewith are the consolidated Preparedness Plan of different Stations and Detachment of this District.

Team Deployment	Number of Personnel	Equipment	Communication Equipment
CGDNWLZN	SDU-NWLZN	1 Pathfinder	1 unit VSAT, Tel No (072) Cellphone with nr
	COMED-NWLZN		2 Base RADIO
CGS San Fernando	Team 1(5 Personnel)	MBca TF Sapp Kanagatan, BFAR Patrol Boat, 6 Lifejackets, 1 Life Buoy Cano	1 Base RADIO, 2 VHF Handheld Radio, Cellphone with nr PLDT Landline with nr
	Team 2(4 Personnel)	MBca TF Sapp Kanagatan, BFAR Patrol Boat, 6 Lifejackets, 1 Life Buoy Cano	1 Base RADIO, 2 VHF Handheld Radio, Cellphone with nr PLDT Landline with nr
CG Det Damortis	3 personnel	4 life Jackets, 2 Life Buoy Cano and Hired banca (when necessary)	1 VHF Handheld Radio, 1 VHF Base Radio and cellphone with nr
CG Det Dasigayos	3 personnel	4 Life Jackets, 2 Life Buoy Cano, 1 Binocular and hired banca (when necessary)	1 VHF Handheld Radio, 1 VHF Base Radio and cellphone with nr
	Team 1(5 Personnel)	1 MUKAT, 1 Motorcycle and 1	1 Base RADIO, 6



自荐信

尊敬的领导：

您好！

首先感谢您在百忙之中抽出宝贵时间来审阅我的自荐信，给我一个"毛遂自荐"的机会。

我叫阚翠华，男，是将于 2013 年毕业于泉州经贸学院海口业务管理专业的学生。我是一个乐观向上，开朗大方，待人诚恳而且责任心强的学生。

我很平凡，但我不甘平庸。未来的道路上充满了机遇与挑战，我正激扬豪情，满怀斗志准备迎接。我坚定地认为：天生我材必有用，付出总会有回报！

大学时期，在抓好专业课学习的同时，我更注重的是综合素质的提高。在校期间，我学习福州大学行政管理的自学考试，专业上，我学习了理员业务、食品药管理等相关知识，并多次获得奖学金。实践是检验真理的唯一标准，我深深地感得实践的重要性，在校担任班班长、外联部副部长、系学生会主席等职位，课余期间，我积极地参加了学校组织的深入社区的社会实践，受到当地居民的一致好评。2010 年度被评为优秀学生干部，2012 年度被评为优秀团干，2012 年 7 月 1 日成为中共预备党员。

现呈上我的个人简历，希望能有机会获受贵公司的面试，成为贵公司的一名员工！

最后祝贵公司事业蒸蒸日上！

此致

敬礼！

自荐人：

（另附个人简历一份）

Sample decoy documents (left: for Filipino targets; right: for Taiwanese targets)

Initial Payload: TROJ_YAHOYAH

The downloader typically attached to emails related to Operation Tropic Trooper is detected by Trend Micro as TROJ_YAHOYAH, a downloader with 32- and 64-bit support. It has an encrypted configuration file and uses HTTP GET requests to download other files that are then decrypted and executed in memory.

Installation Routine

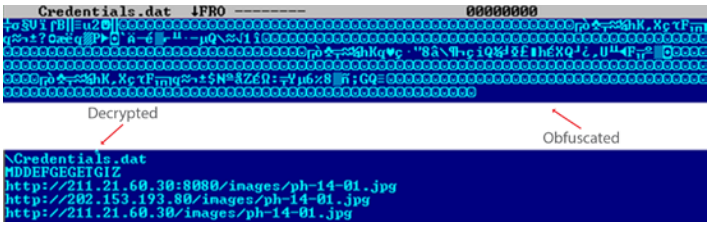
When executed, TROJ_YAHOYAH checks if the infected system's Windows OS is 64-bit capable or not. If it is, the Trojan will decrypt a 64-bit copy of itself using a simple XOR cipher with a single-byte key at *"0x90."*

If the infected system is not 64-bit capable, the Trojan will just drop a 32-bit executable copy of itself *(%APP DATA%\Microsoft\Credentials\Credentials.exe,* detected as TROJ_YAHOYAH), along with an encrypted configuration file *(%APP DATA%\Microsoft\Credentials\Credentials.dat).* The configuration file was encrypted using the same simple algorithm featured in the previously cited Rapid7 report on KeyBoy.

```
mov     al, dec_key[edx*4]
mov     [ebp+var_5], al
mov     ecx, [ebp+arg_0]
add     ecx, [ebp+var_4]
mov     dl, [ecx]
mov     [ebp+var_6], dl
movzx   eax, [ebp+var_6]
xor     eax, 1
mov     [ebp+var_8], al
movzx   ecx, [ebp+var_5]
movzx   edx, [ebp+var_8]
imul    ecx, edx
mov     [ebp+var_7], cl
mov     eax, [ebp+arg_0]
add     eax, [ebp+var_4]
mov     cl, [ebp+var_7]
mov     [eax], cl
jmp     short loc_100035AF
```

Code that decrypts the configuration file using "0x95,0x99,0x9d,0xc3,0xc7, 0xcb,0xd7,0xe5,0xbd,0xa9, 0xb5,0xeb,0xf7,0xe3,0xe7, 0xed" as key

Unlike the KeyBoy Trojan though, which searches for the string, *"IJUDHSDJFKJDE,"* TROJ_YAHOYAH searches for *"MDDEFGEGETGIZ."* These strings, found at the beginning of the decrypted code, represent the configuration file. Absence of the said file terminates the infection process.



TROJ_YAHOYAH's decrypted configuration file

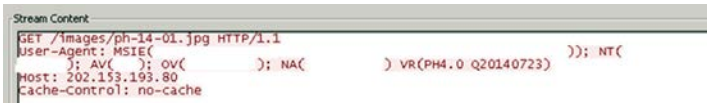
TROJ_YAHOYAH's configuration file, when decrypted, contains the links to sites from which it can download the files it needs to continue its routines. After decryption, it executes a dropped copy using the *-Embedding* parameter then attempts to delete itself.

The downloader's name was inspired by its self-deletion routine after dropping its payload. YAHOYAH was derived from the Visayan term "hayohay," which loosely translates to an easily discarded "servant" in English. [8]

Download Routine

TROJ_YAHOYAH attempts to access links and download files via HTTP GET requests. To move to another attack phase, it uses the following user-agent strings:

- ***MSIE:*** Checks for the system's Internet Explorer® version
- ***NT:*** Checks for the system's Windows OS version
- ***AV:*** Checks for installed antimalware solutions
- ***OV:*** Checks for the system's Microsoft™ Office® version
- ***NA:*** Checks for the system's hostname
- ***VR:*** Hard-coded string only used when accessing download sites to track which downloader was used on a target.



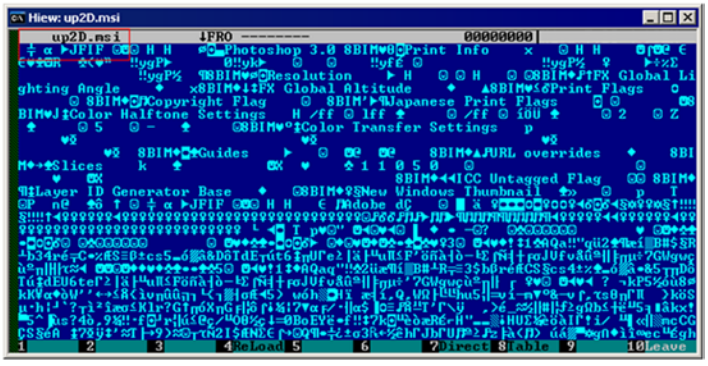
HTTP GET request sample

TROJ_YAHOYAH checks for the following antimalware solution processes:

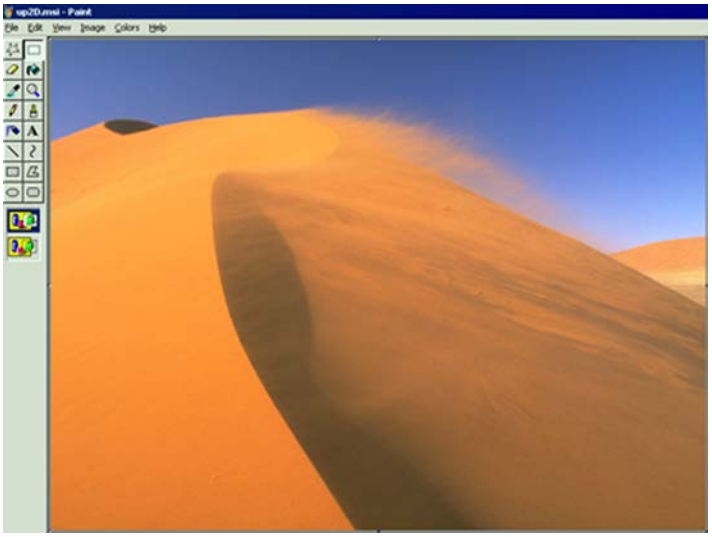
- *360rp.exe*
- *360tray.exe*
- *ALMon.exe*
- *ALsvc.exe*
- *ashserv.exe*
- *Avastsvc.exe*
- *avgam.exe*
- *avguard.exe*
- *avp.exe*
- *avpmapp.exe*
- *consctl.exe*
- *CyberoamClient.exe*
- *econceal.exe*
- *econser.exe*
- *ekrn.exe*
- *escanmon.exe*

- *mcshield.exe*
- *nod32krn.exe*
- *pccntmon.exe*
- *rtvscan.exe*
- *SAVAdminService.exe*
- *SavService.exe*
- *sfctlcom.exe*
- *swi_service.exe*
- *uiwatchdog.exe*

TROJ_YAHOYAH temporarily saves downloaded files in a specially created folder named *"%APP DATA%\tasks\up{random characters}.msi."*



Sample .MSI file with a malicious .JPG header



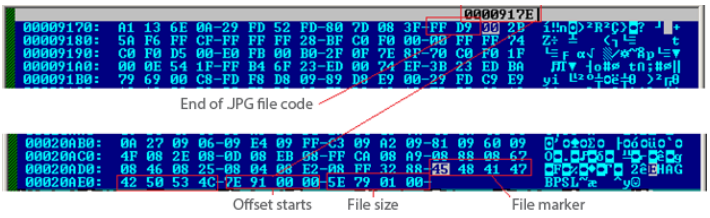
Sample .MSI file opened on Microsoft Paint

The image is supposed to be an 800 x 600 wallpaper that is way heavier than the real one named *"Wind.jpg"* normally found in Windows XP systems' *%WINDOWS%\wallpaper\web* folder. The actors behind Operation Tropic Trooper may be using a simple steganography technique to mask the backdoor's routines in order to evade antimalware and network perimeter detection. [9] We have seen the actors use other images found in the same folder such as *"Ascent.jpg," "Friend.jpg,"* and *"Home.jpg."*

A more in-depth analysis of the downloaded file reveals that malicious code has been appended to it. This allows TROJ_YAHOYAH to check offset *0x0F* bytes from the end of the file code to identify a marker where the malicious binary code will be added, thus increasing the file's size.

Other images used in attacks

TROJ_YAHOYAH looks for the string, *"EHAGBPSL,"* and decrypts the appended binary code. When decrypted, an .EXE file is executed in memory. It automatically runs if the user has administrator privileges. If the user has limited privileges though, it will first attempt to obtain administrator privileges by bypassing User Account Control (UAC) but only on Windows 7. It will then decrypt another XOR-encrypted file using the key *"0x90"* in memory then check if the *"StartWork"* function was exported then execute it.



Malicious code appended to that of the .JPG file

Maintaining Persistence

The last file that TROJ_YAHOYAH executes in memory is the main installer. It contains two more files that install a .DLL file detected as TROJ_YAHAMAM. This file is registered as a service named *"INCS"* to maintain persistence. It also drops the following XOR-encrypted malware-laced image files:

- *% windows %\System32\mfc41.dll* (detected as TROJ_YAHAMAM)
- *% windows %\inf\mfc41.inf* (a configuration file)
- *% windows %\Fonts\mfc41.tff* (a copy of the configuration file)
- *%windows%\Web Wallpaper\images.jpg* (contains BKDR_YAHAMAM)

A batch (.BAT) file is used to start the *INCS* service. TROJ_YAHAMAM uses a trick similar to that of TROJ_YAHOYAH in order to decrypt files. When decrypted, TROJ_YAHAMAM executes the backdoor payload.

Backdoor Payload: BKDR_ YAHAMAM

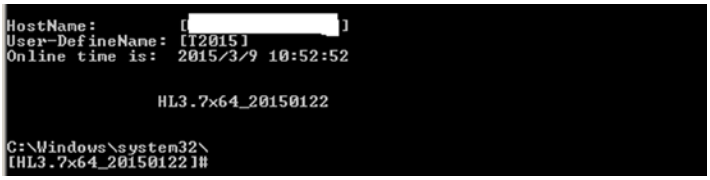
BKDR_YAHAMAM is usually encrypted then embedded in an image file. When decrypted, it is loaded and executed in memory by a .DLL file that is registered as a service (TROJ_YAHAMAM). It exfiltrates data from infected systems, downloads and uploads files, and has a remote shell. It also drops a rootkit component named *"usb.sys,"* detected as RTKT_HIDEPORT.ZTCA-XO. The rootkit creates the service, *usb30,* and hides evidence of port communication to evade detection and remain persistent.

Command-and-Control Communication

When executed, BKDR_YAHAMAM checks if it runs under *svchost.exe.* It uses the configuration file, *%windows %\Fonts\mfc41.tff,* which contains the following information:

- *C&C1*
- *C&C2*
- *C&C3*
- *ControlPort*
- *DownloadURL1*
- *DownloadURL2*
- *DownloadURL3*
- *LoginPass* (for authentication purposes)
- *Port1*
- *Port2*
- *Port3*
- *USB*
- *UserMark*

BKDR_YAHAMAM encrypts C&C communication using multiplication with a 1-byte key. Attackers can use the *"?"* and *"Help"* commands to see the various options the backdoor offers as shown in its code.

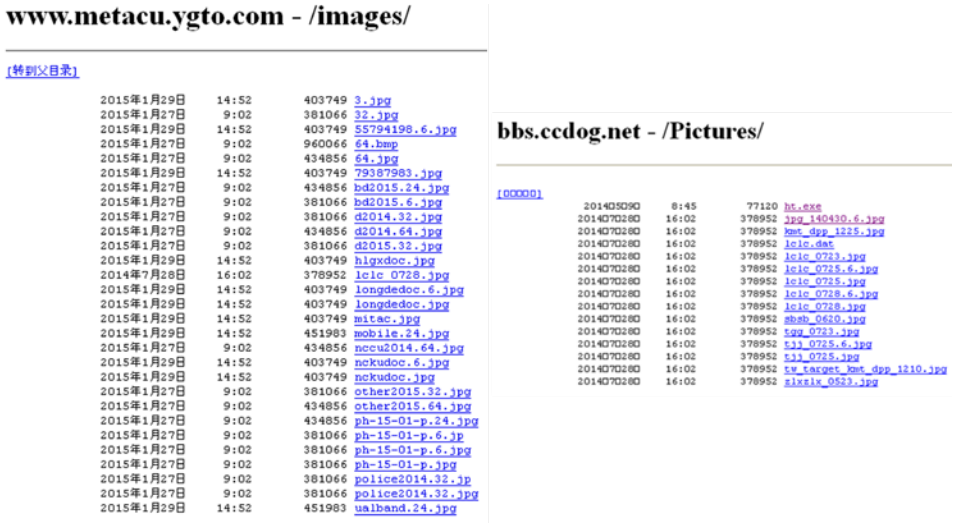


Tool used to emulate command-and-control (C&C) communication with a 64-bit version of BKDR_ YAHAMAM

We were able to download some files from two of the C&C servers that TROJ_YAHAMAM accesses. These had some image files that the 32- and 64-bit versions of the backdoor can choose from for use in attacks.

```
? or Help                                       --> Help Menu
CleanEvent                                      --> Clean Log
GetUser                                         --> List Accounts
DelUser [UserName]                              --> Delete Account

EnumService                                     --> 8 List Services
ViewService [ServiceName]                       --> View Specific Service
DelService [ServiceName]                        --> Delete Service

Put [RecvIP] [Port] [FileName]                  --> Send File To FileClient
GetFile [IP] [Port] [FileName]                  --> Get File From FileServer
Get [http://IP/A.exe] [File.exe]           --> Get File From IIS
DownLoad [RemoteFile]                      --> DownLoad File From Remote
UpLoad [LocalFile]                              --> UpLoad File From Local
DecryptFile [SrcFile] [DstFile]                 --> Decrypt File

Run [Program] [Parameter]                       --> Execute As System
Arun [Program] [Parameter]                      --> Execute As LogonUser
CmdRun [CmdProgram] [Parameter]                 --> Execute Cmd Program

Ft [ModifyFile] [ReferFile]                     --> Change File's Time
Dt [ModifyDir] [ReferDir]                       --> Change Dir's Time

Lcx [CtrlIP] [CtrlPort] [DestIP] [DestPort]
StopLcx                                         --> Stop Lcx Func

-------------------------------------------------------------------------------------------

SysInfo                                         --> 1 View System Infor
GetInfo                                         --> 2 View Machine Infor
SoftInfo                                        --> 3 View Installed SoftWare

OneKey                                          --> Collect All Info
OneKeyDisk                                      --> Get All Disk FileInfo

Pslist                                          --> 7 List Process
Pskill [PID]                                    --> Kill Process
Modlist [PID]                                   --> List Process Module

Netstat                                         --> 5 View TCP
ListIP                                          --> 6 List IP Info
Ipconfig                                        --> Show IPconfig
TcpKill [LocalHost] [Port] [RemoteHost] [Port] --> Clear A TCP Connection

-------------------------------------------------------------------------------------------

Shell [cmd.exe]                                 --> 4 Get A Shell 44 Shell to Work Dir
ShellA                                          --> Get Shell As LogonUser

Winlogon [Domain] [User] [Pass]                 --> Get User Shell With Pass
WhoAmI [PID]                                    --> Display Self Work Info
ShellTo [IP] [Port]                             --> Send Shell To Client
New [IP] [Port]                                 --> Send New To Client
Pshell [IP] [Port]                              --> Send PowerShell to NcmdClient
Ncmd [IP] [Port]                                --> Send Shell to NcmdClient

-------------------------------------------------------------------------------------------

ViewTermPort                                    --> View Terminal Port
SetTermPort [Port]                              --> Set Terminal Port
InstallTerm [Port]                              --> Install Terminal Service
StopTerm                                        --> Stop Terminal Service

-------------------------------------------------------------------------------------------

ConfigView                                      --> 9 View Self Config
Set [Option]                                    --> Set Config
KingView [KingConfigFile]                       --> View King's Config
KingSet [KingConfigFile] [Option]               --> Set King's Config

-------------------------------------------------------------------------------------------

StartUSB                                        --> Start USB Func
StopUSB                                         --> Stop USB Func
ScreenCapture                                   --> 11 Get DesktopScreen

-------------------------------------------------------------------------------------------

CD                                              --> Change Dir
Dir [Parameter] [/s]                            --> Display Info
Ldir                                            --> Display Local Files
Dirxe                                           --> Dir Work Dir
Dirxb                                           --> Dir Bmp Dir
Copy [Sour] [Dest] [/s]                         --> Copy Sour to Dest
Del [File(Dir)]                                 --> Delete Files or Dir
Md [DirName]                                    --> Made a Dir
Rd [DirName]                                    --> Delete a Dir
Type [FileName]                                 --> Display File's Content

-------------------------------------------------------------------------------------------

Ver                                             --> Show Version
Reboot                                          --> Reboot System
Exit                                            --> Exit Control
Sleep [Min]                                     --> 0 Sleep 1440, Entry Sleep
SleepTo [Date]                                  --> SleepTo Date, eg.20140506
ResetConnect                                    --> 12 Reset Fail Counts to Zero

-------------------------------------------------------------------------------------------

Remember To Run Pstore!!

List Help Completed
```

The following table lists the unique SHA-1 hashes that TROJ_YAHAMAM downloads, along with their backdoor payloads.



C&C servers TROJ_YAHAMAM accesses to download malicious payloads

Filename	SHA-1 Hash	Backdoor Payload	Trend Micro Detection Name
3.jpg	*c5359ecc1651a98125bf7ea2668f85af64a7a533*	HL3.7x86_20140711	BKDR_YAHAMAM
32.jpg	*872cbe46a84fb88836db2a15e92d8c80d4209af3*	HL3.7x86_20150122	BKDR_YAHAMAM
bd2015.24.jpg	*8ee9bdab29970c95f9ed5915813543609b7f438c*	HL3.7x86_20150122	BKDR_YAHAMAM
lclc_0725.jpg	*fedb2c7b5f6a11ddefd29eb034e85f17c612e3ba*	HL3.7x86_20140508	BKDR_YAHAMAM
SmartNavport0205.32.gif	*75940e926894b65652bb84d96fe42fe709a183f5*	HL3.7x86_20150122	BKDR_YAHAMAM
ualband.24.jpg	*6d82e1aafd910b93ebf2ece773d43e9ccbbf84f3*	HL3.7x64_20140711	BKDR_YAHAMAM

Interestingly, a BKDR_POISON variant was found on the sites' folders as well, leading us to believe that the attackers also use it for Operation Tropic Trooper.

Filename	SHA-1 Hash	Trend Micro Detection Name
wshif.dll	*a7b4381b1f9161992b358eda9bd58a6b219a13d3*	BKDR_POISON.TUFN
wship.dll	*4eedf918aeb1a2bedc6278e89ebf3005d0b95d41*	BKDR_POISON.TUFN

BKDR_YAHAMAM can steal practically any type of file saved on infected systems. Apart from stealing data, it can also perform more harmful actions like kill processes and services, delete files and directories, and put systems to sleep, among others.

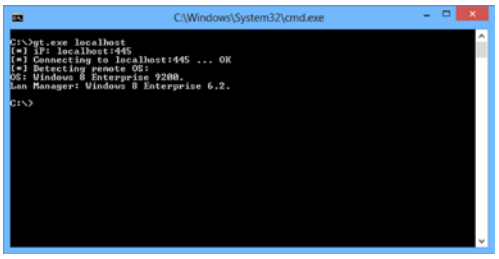
BKDR_YAHAMAM also attempts to install an accompanying executable rootkit *(%windows %\system32\drivers\usb30.sys,* detected as RTKT_HIDEPORT.ZTCA-XO). RTKT_HIDEPORT.ZTCA-XO is also XOR encrypted and found at byte key, *"0x90,"* to hide the port that the backdoor should use according to the configuration file. It will only hide communication activities occurring in the first of three port entries indicated in the configuration file. After creating and starting the rootkit service, BKDR_YAHAMAM then attempts to delete the rootkit and the related service. This will not stop the rootkit from running in the background.

BKDR_YAHAMAM variants with rootkits for 32-bit systems run on 32-bit versions of Windows XP. On Windows 7 64-bit systems, however, the backdoor works but the rootkit does not.

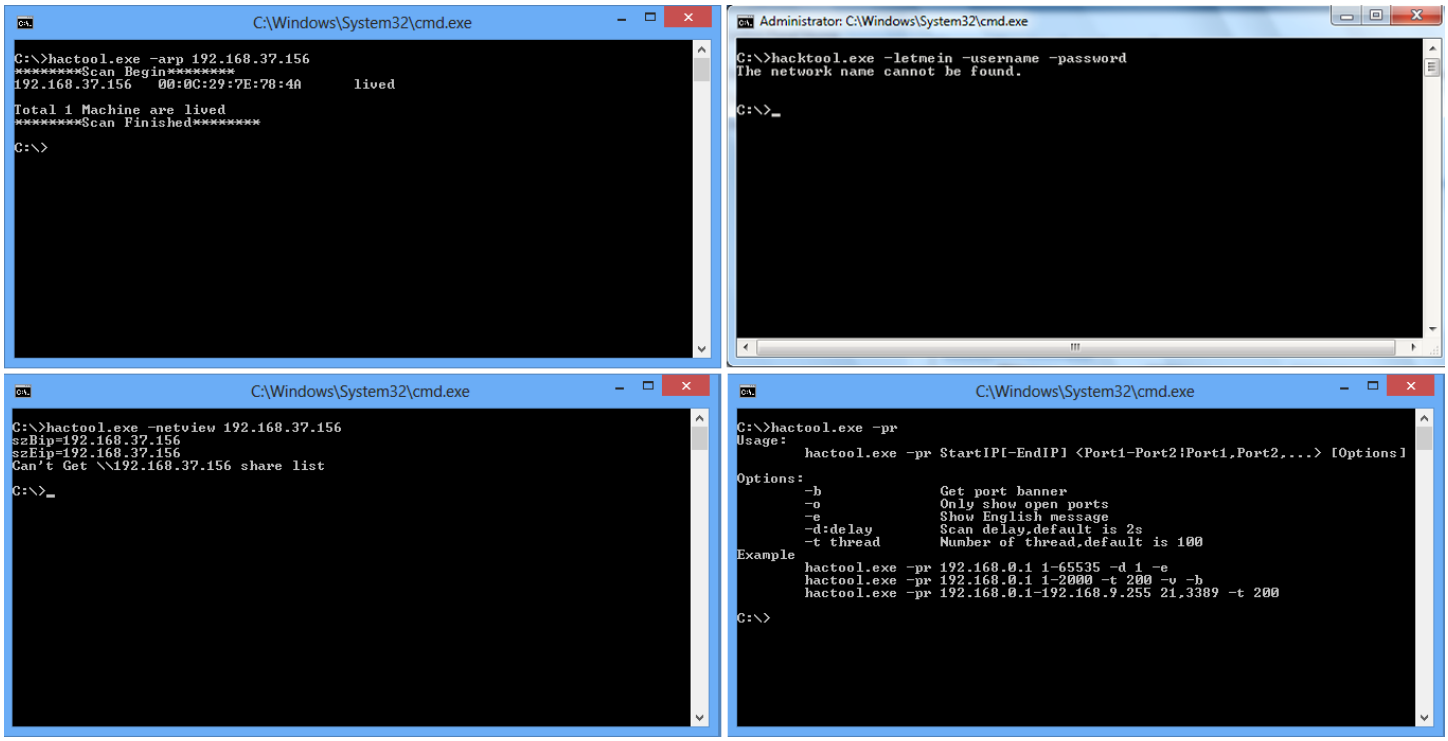
Lateral Movement

In the course of doing research, we also managed to get hold of the following tools that the actors behind Operation Tropic Trooper used in an attack:

- **HKTL_GETOS:** Detects a target system's OS version. [10]
- **HKTL_SHARESCAN:** Performs the following:
  - ***-pr:*** Scans for open ports on target systems.
  - ***-letmein:*** Scans for saved usernames and passwords on target systems.
  - ***-arp:*** Views the Address Resolution Protocol (ARP) on each target system.
  - ***-netview:*** Scans target systems for shared resources.



HKTL_GETOS's OS-version-sniffing routine



HKTL_SHARESCAN's routines (top left: -pr; *top right:* -letmein; *bottom left:* -arp; *bottom right:* -netview

These hacking tools were possibly remotely downloaded by the attackers onto infected systems. They aided in lateral movement and further intelligence gathering. Data such as credentials saved on infected systems can be stolen via Address Resolution Protocol (ARP) poisoning or main-in-the-middle (MiTM) Layer 2 and pass-the-hash attacks. [11–12] The stolen credentials allow attackers laterally move throughout a network. The threat actors no longer have to hack their way in, they have the ability to log in as legitimate users.

Possible Connections

Based on the specially crafted documents we were able to gather, Operation Tropic Trooper has been active since 2012. We have seen malware samples from 2011 that behaved the same way and used similar file markers. [13]

The following table provides more detailed information on Operation Tropic Trooper's downloader, TROJ_YAHOYAH.

SHA-1 Hash	Campaign ID Hard-Coded into Malware
17ee08b92aeefb8d3d73a02beb03e634b453b5fe	PH4.0 Q20121012
3a8bed630679a30c8f945a7f9fe9eef18dd18ef8	PH4.0 Q20131218
3ff3519749764f64f5f208347f39bd77f7e2fa92	PH4.0 Q20130527
47747dccd1fc57a6456cf2a06d654966193545e5	PH4.0 Q20120730
542ca28d4154e4e4382f9dfe4e0C37983046e93d	PH4.0 Q20131218
56680180af5a792dca8e6112c57810b5e06bca1b	PH4.0 Q20120730
593ab027f90d8651e685581b8f09d87a2c95f244	PH4.0 Q20140723
5c5a4ceea45c3f0e67085b9d323da13eedcf6e1b	PH4.0 Q20121012
6099001d54d39bcdd7c874672e8b28789e79721f	PH4.0 Q20121012
7d5fd316f12ff39e5a9b43dabd66eccdcdb164e7	PH4.0 Q20141104

SHA-1 Hash	Campaign ID Hard-Coded into Malware
973e522edeb08bea948098ce7c8b83866857de9c	PH4.0 Q20130527
aef101fb24bd39e3cc14c26796c0336f2cb1d540	PH4.0 Q20131218
b1fdb46cbe73cc14f784bebac47e33606b259967	PH4.0 Q20121012
b767e1325bf103e672183e9487093ac068b75bc8	PH4.0 Q20140723
ba71031ec0dccf09fbc48af61a22e5faa6b055a4	PH4.0 Q20140910
bb8fddcd993a3ca94c6dd583f36df76bb5227ca5	PH4.0 Q20130527
c4ae20ef0a90f095a88a9ea9920e97733a4d5626	PH4.0 Q20141104
d50c657ff3068bd03ef74cfa5a289bbda87f33ef	PH4.0 Q20121012
f8ac7ccf99485f485a435e05420bf3c103a3a549	PH4.0 Q20131218

Defending Against Operation Tropic Trooper

Threat Intelligence Gathering

Network and system administrators can protect against Operation Tropic Trooper by blocking user access to related C&C servers. They should also keep an eye out for related strings as well as services and their corresponding paths.

Download Links

TROJ_YAHOYAH downloads the following image files:

- *113.10.183.104/imgs/phh121018.jpg*
- *113.10.221.89/images/kong.jpg*
- *113.10.221.89/images/phonedpp.jpg*
- *113.10.221.89/Pictures/dzh_0925.jpg*
- *113.10.221.89/underwater.jpg*
- *173.252.220.169/underwater.jpg*
- *198.211.3.83/images/ph06.jpg*
- *202.153.193.73/images/kong.jpg*
- *202.153.193.73/images/phonedpp.jpg*
- *208.187.167.126/images/dfsy.jpg*
- *208.187.167.126:88/images/dmjs.jpg*
- *208.187.167.126/images/phzy.jpg*
- *50.117.38.164/Pictures/dzh_0925.jpg*
- *61.218.145.179/monitor/images/Smartxy130619.gif*
- *61.221.169.31/images/kongj.jpg*
- *61.221.169.31/images/phonedpp.jpg*
- *61.222.31.83/monitor/images/Smartxy130619.gif*
- *69.221.169.31/underwater.jpg*

- *air88.ddns.us/images/af130218.jpg*
- *air88.ddns.us/js/af130901.jpg*
- *air88.ns01.us:53/js/af130901.jpg*
- *air88.ns01.us/images/af130218.jpg*
- *air88.ns01.us:53/js/af130901.jpg*
- *air99.ns01.us/js/af130901.jpg*
- *info.acmetoy.com/imgs/phh121018.jpg*
- *msc.ddns.us:443/images/ph06.jpg*
- *nevermore.onmypc.org/images/ph06.jpg*
- *ph11.dns1.us:53/images/phzy.jpg*
- *ph11.dns1.us/images/dfsy.jpg*
- *ph11.dns1.us/images/dmjs.jpg*
- *ph11.ns01.us:443/images/phzy.jpg*
- *ph11.ns01.us:5050/images/dmjs.jpg*
- *ph11.ns01.us/images/dfsy.jpg*
- *ware.compress.to/imgs/phh121018.jpg*
- *www.amberisic611.4dq.com/monitor/images/Smartzh140222.gif*
- *www.bannered.4dq.com/monitor/images/Smartzh131225.gif*
- *www.bannered.4dq.com/monitor/images/Smartzh140222.gif*
- *www.cham.com.tw/images/dzh_0925.jpg*
- *www.forensic611.3-a.net/monitor/images/Smartzh131225.gif*
- *www.forensic611.3-a.net/monitor/images/Smartxy130619.gif*
- *www.forensic.zyns.com/monitor/images/Smartzh131225.gif*
- *www.metacu.ygto.com/monitor/images/Smartzh140222.gif*

Strings

TROJ_YAHOYAH looks for the following strings to continue performing its malicious routines:

- *EHAGBPSL*
- *MDDEFGEGETGIZ*

Services

Network and system administrators can also look out for the following services, which are related to TROJ_YAHAMAM:

- **ServiceName:** *INCS*
  - **DisplayName:** IPSEC Network Connections Services;
  - **ImagePath:** *%SystemRoot%\System32\svchost.exe -k incsvc*
- **ServiceName:** *usb30*
  - **DisplayName:** *usb30*
  - **ImagePath:** *%SystemRoot%\\System32\DRIVERS\usb30.sys*

Solution Use

We also recommend a Custom Defense strategy that uses a comprehensive “Detect—Analyze—Respond” life cycle to address threats particular to an organization. This can provide in-depth threat profile information as well as advanced threat detection at the network level to discover malicious content (malware), communication, and attacker activity that are not typically visible to traditional security solutions.

The following table shows how a custom defense solution such as Trend Micro™ Deep Discovery can aid in detecting the components of Operation Tropic Trooper.

Attack Component	Deep Discovery Component	Description
Spear-phishing emails	Email Inspector	Detects spear-phishing emails used to infiltrate, establish a foothold in, and launch targeted attacks against targets; has email-inspection capabilities that detect malicious content, attachments, and URLs that pass unnoticed through standard email security solutions
Malicious image files	Analyzer	Detects even previously unknown threats by analyzing a broad range of file types, sizes, and sources using customizable sandbox environments that attackers design and build to match organization's desktop and device platforms
Malware • BKDR_POISON.TUFN • BKDR_YAHAMAM • RTKT_HIDEPORT.ZTCA-XO • TROJ_YAHOYAH	Analyzer	Detects even previously unknown threats by analyzing a broad range of file types, sizes, and sources using customizable sandbox environments that attackers design and build to match organization's desktop and device platforms
	Inspector	Identifies suspicious activities anywhere on networks, including those related to lateral movement and C&C; also detects traffic generated by malware-download-related behaviors via HTTP GET requests

CONCLUSION

Operation Tropic Trooper is not highly sophisticated. But the fact that it has attained some degree of success and has managed to infiltrate crucial organizations in both Taiwan and the Philippines shows the urgent need for targeted entities to rectify their shortcomings in terms of security.

As with other targeted attacks, Operation Tropic Trooper brings great risks, especially since its targets include government institutions and military agencies. Although we were not able to collect enough information to determine the identities and motivations of the actors behind Operation Tropic Trooper, we were able to gather enough intelligence to help potential victims defend against the campaign. Knowing that attackers are still using old techniques and exploiting known vulnerabilities will make it easier for the targeted organizations to pinpoint and fix security gaps in their networks.

Building threat intelligence is crucial in the fight against targeted attacks. Identifying the tools, tactics, and procedures (TTPs) that threat actors use based on external reports and internal historical and current monitoring can help create a strong database of indicators of compromise (IoCs) that can serve as basis for action. Using the right tools for advanced threat protection should also be part of an expanded security monitoring strategy. This includes establishing and empowering incident response teams and training employees, partners, and vendors on social engineering and computer security. [14]

APPENDIX

Malicious Files

Filename	SHA-1 Hash	Trend Micro Detection Name
credentials.exe	17ee08b92aeefb8d3d73a02beb03e634b453b5fe 25c2540125a4f6db5bd9e71b9130ba19aed4af2c 3a8bed630679a30c8f945a7f9fe9eef18dd18ef8 3ff3519749764f64f5f208347f39bd77f7e2fa92 43f565273e9b2bcfa9640c41ebb591f5dccca23e 47747dccd1fc57a6456cf2a06d654966193545e5 542ca28d4154e4e4382f9dfe4e0c37983046e93d 56680180af5a792dca8e6112c57810b5e06bca1b 5c5a4ceea45c3f0e67085b9d323da13eedcf6e1b 6099001d54d39bcdd7c874672e8b28789e79721f 77eaac29dc3f46fdd4782b3a633a9c4b35fbdf20 7d5fd316f12ff39e5a9b43dabd66eccdcdb164e7 973e522edeb08bea948098ce7c8b83866857de9c a31d398abf230f18bee6487732ad477e98a4f784 a7713afd111b40da066449cc4450338316e51462 aef101fb24bd39e3cc14c26796c0336f2cb1d540 b1fdb46cbe73cc14f784bebac47e33606b259967 ba71031ec0dccf09fbc48af61a22e5faa6b055a4 bb8fddcd993a3ca94c6dd583f36df76bb5227ca5 c4ae20ef0a90f095a88a9ea9920e97733a4d5626 d50c657ff3068bd03ef74cfa5a289bbda87f33ef dd011e35df5b529f4a92d480428c63faa8a6da3f f8ac7ccf99485f485a435e05420bf3c103a3a549	TROJ_YAHOYAH.A
(Image).jpg	0360098a17c5c68004350f3eb34ab6c2b5b7b6f6 2f853796b9598a85ce90c499f4e4e194b1348e0c 5adcea95439abf2c2c335af187dbeb92cb5587c0 70b0dafe10f2399bb3ae767be376b6f5cd68db19 84842226e9b626b2b4fca325fb1d13058aabf1be a149a79149ab080004adee3051bf0fd874177e97	BKDR_YAHAMAM.A
mfc41.dll/rpcrt32.dll	0f7f277c57a7656e116894bb3460a15669bffaa3 49f4db863e4ac5b2c55e1bc7540ee865f5126dba 52084036ed353e24423e0bd1f10ea741096e8fbd 7835e3ca339626f87738644092bdf91a8a15eaac aa7e591951c085e0ab50748e6e0d96be99ad3f1a ac1bfb13e8d79a2cbd33cf3e4ef94a6f0c32abfc afe298099de7af1c43c97dce3e649f0c83164707 e771cff898649a5a00b4421db186859b1b04cac9	TROJ_YAHAMAM.A

Filename	SHA-1 Hash	Trend Micro Detection Name
(Exploit).doc	159a91f9c9a83493c03f83c22f478019b7f6e8ca 2665e536de618760cfe4b57c8f679d95fbb3da0b 2bd3f8356d4a3415e07311ffdc2d4834c0141029 305dcb0e9257875d0699567d7d10e69e6014eed1 312cc84043490b7a3b54fecff977cab75785f0c0 3631faf525863d8bd24e571e04b41bdced047734 4236be3aa2abc45e49a27d9bf87b6e5003d805c5 7676bd47deaf69a8a3a17a3f9e261b7aca1dac24 7b48460b5f6f8bc68fedb78a07f7884f57c66b57 8136ce73e502882fa187f7b53b549376bfb52ba2 a5ce827db51b204af7fef1a5b12b10a2566430bc	TROJ_MDROPPER.RDY

REFERENCES

[1] Nex. (7 June 2013). *Rapid7 Community.* "KeyBoy, Targeted Attacks Against Vietnam and India." Last accessed on 7 April 2015, https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india.

[2] Investopedia, LLC. (2015). *Investopedia.* "Heavy Industry." Last accessed on 22 April 2015, http://www.investopedia.com/terms/h/heavy_industry.asp.

[3] Loucif Kharouni. (10 January 2014). *TrendLabs Security Intelligence Blog.* "Targeted Attack Methodologies for Cybercrime." Last accessed on 7 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/whatever-works-targeted-attack-methodologies-for-cybercrime/.

[4] Kyle Wilhoit. (15 December 2013). *TrendLabs Security Intelligence Blog.* "Cybercriminals Using Targeted Attack Methodologies (Part 1)." Last accessed on 7 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-using-targeted-attack-methodologies-part-1/.

[5] Maersk Menrige. (17 June 2014). *TrendLabs Security Intelligence Blog.* "Template Document Exploit Found in Several Targeted Attacks." Last accessed on 7 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/template-document-exploit-found-in-several-targeted-attacks/.

[6] Ryan Flores. (9 May 2012). *TrendLabs Security Intelligence Blog.* "Snapshot of Exploit Documents for April 2012." Last accessed on 7 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/snapshot-of-exploit-documents-for-april-2012/.

[7] Trend Micro Incorporated. (2014). *Trend Micro Security Intelligence.* "Cashing in on Digital Information: An Onslaught of Online Banking Malware and Ransomware." Last accessed on 7 April 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf.

[8] Wikimedia Foundation, Inc. (12 October 2014). *Wikipedia.* "Alipin." Last accessed on 8 April 2015, http://en.wikipedia.org/wiki/Alipin.

[9] Jennifer Gumban. (3 March 2014). *TrendLabs Security Intelligence Blog.* "Sunsets and Cats Can Be Hazardous to Your Online Bank Account." Last accessed on 10 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/sunsets-and-cats-can-be-hazardous-to-your-online-bank-account/.

[10] Trend Micro Incorporated. (2015). *Threat Encyclopedia.* "HKTL_GETOS." Last accessed on 10 April 2015, http://about-threats.trendmicro.com/ArchiveGrayware.aspx?language=cn&name=HKTL_GETOS.

[11] Jeff King and Kevin Lauerman. (2015). *Cisco.* “ARP Poisoning (Man-in-the-Middle) Attack and Mitigation Techniques.” Last accessed on 20 April 2015, http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html.

[12] SANS Institute. (2010). *SANS Institute InfoSec Reading Room.* “Pass-the-Hash Attacks: Tools and Mitigation.” Last accessed on 20 April 2015, http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283.

[13] McAfee, Inc. (2014–2015). *McAfee for Business.* “Generic Dropper!dyh!4929C723EA9D.” Last accessed on 1 April 2015, http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=570595.

[14] Trend Micro Incorporated. (2015). *Trend Micro Security News.* “Targeted Attack Campaigns and Trends: 2014 Annual Report.” Last accessed on 14 April 2015, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attack-campaigns-and-trends-2014-annual-report.

Created by:

TrendLabs

The Global Technical Support & R&D Center of **TREND MICRO**

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569.8900