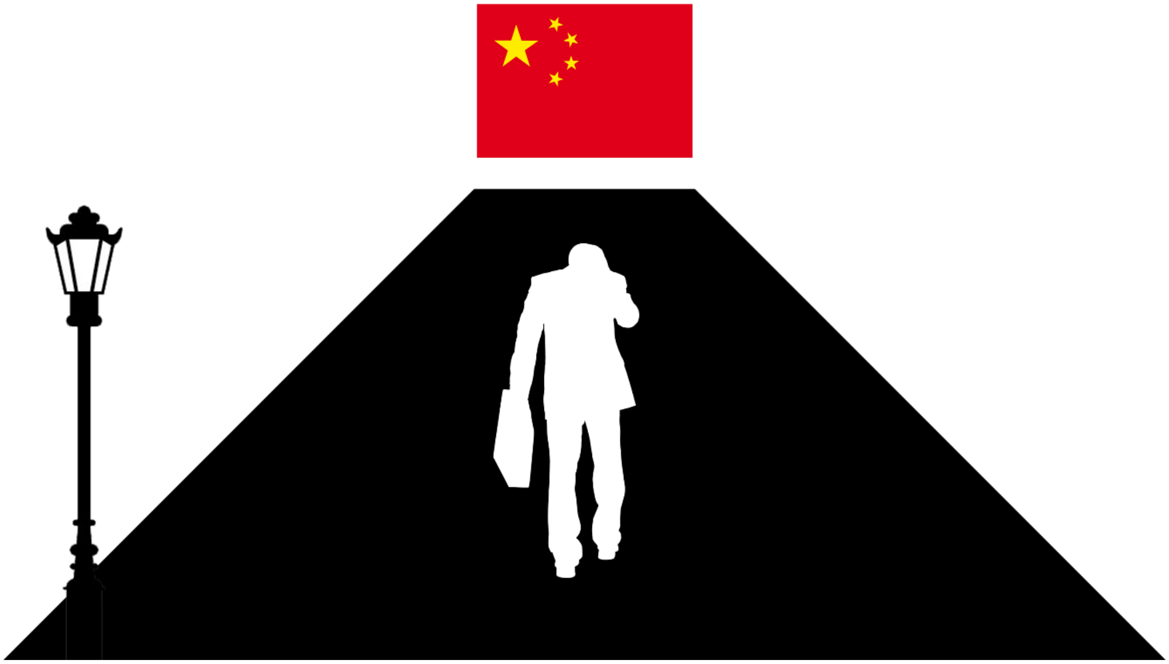
Norton Labs

OPERATION EXORCIST

7 YEARS OF TARGETED ATTACKS AGAINST THE ROMAN CATHOLIC CHURCH



EXECUTIVE SUMMARY

Researchers from the combined labs of NortonLifeLock and AVIRA have uncovered several clusters of malicious activity against the Holy See and the Roman Catholic Church.

The activity appears to date back several years—long before what has been previously documented—but with several new initiatives launched recently.

We assess with high confidence that the threat actors are aligned with Chinese strategic interests and may encompass one or multiple groups. Likewise, we assess with high confidence that the goal of the activity is surveillance, as the Catholic Church has been diplomatically active in countries that are of special interest for the Chinese government.

INTRODUCTION

During 2020, several researchers and security vendors reported on targeted malware used against the Roman Catholic Church. [1] [2] [3] [4]. These revolved around a few known toolsets commonly associated with Chinese threat actors, notably the PlugX malware, but also covered some previously undocumented malware families.

The Catholic Church has historically had a turbulent relationship with Chinese authorities, where it was demanded that the Church could only operate within the strict guidelines of the Communist Party.

In recent years, Pope Francis has had a strong focus on the Catholic Church in Asia, with numerous visits of countries in the region. At the same time, the Vatican has worked to improve affairs with the Chinese government. Since 2014, diplomatic talks have been held over the thorny subject of appointment of bishops [5] [6], and finally in 2018 the Vatican reached a provisional agreement with the Chinese government [7]. The deal was renewed for an additional two years in 2020.

Considerable criticism has been raised against the deal, citing concerns over the human rights situation in China and the crackdown on religious communities. [8]

This is the political context for the malware campaigns we will be detailing in this paper.

CHAPTER 1:
THE LINKIPV6 PLUGX/POISONIVY CAMPAIGN (2014-2016)

Patient Zero

On February 10, 2021, Norton antimalware technology detected the presence of a malicious DLL on a user machine in France. This turned out to be a PlugX malware.

PlugX

PlugX is a well-known Chinese trojan used by a whole host of threat actors. It is usually distributed as a package of several files. These files are composed to exploit a phenomenon called *DLL search order hijacking* (also called sideloading) [9].

One of the files in the bundle will be a legitimate program from a trusted software vendor. When this program is run, it attempts to load a Dynamic Link Library (DLL), which is a software component belonging to its own installation. The program will find a malicious DLL with the same name, inadvertently loading that instead. The malware thus gets the unwitting help of a trusted executable to run. The malicious DLL then typically loads an encrypted file from disk which contains the final payload.

There are many sideloader configurations used by malware (more than 60 that we've seen), and a lot of major software products by trusted vendors have historically been misused this way. Most of these issues were fixed a long time ago, but old executables still work and are still exploited by threat actors.

Sample found on user computer:
sha256: 6b851e5b7d429f56a3fd7453314afc4b8c96cb3a702609cfba2545b0bbe15828

This is a standard PlugX loader named *vsodscpl.dll*, designed to be loaded by a legitimate *scncgf32.exe* from the McAfee VirusScan suite. We do not have the payload blob (named *mcafee.lib*) in this case. However, there is a complete dropper on VirusTotal (VT) for this exact loader [10]. This dropper is configured to use the following Command & Control (C2) addresses:

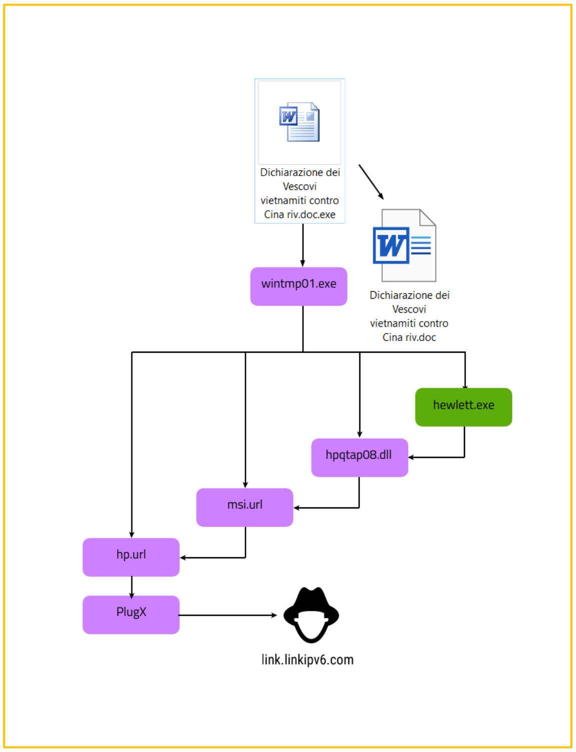
sg3appstore[.]net
us3appstore[.]net
bz3appstore[.]info
maildantri[.]org

While we cannot be certain that the VT dropper was the one used in our case, there is good reason to believe the samples are related: Two of the C2 domains above are also used in PoisonIvy campaigns we will detail later. These overlap with Vatican-oriented activity.

In addition to that sample, we saw IPS events from the machine showing that it was reaching out to the following domain:

```
link.linkipv6[.]com
```

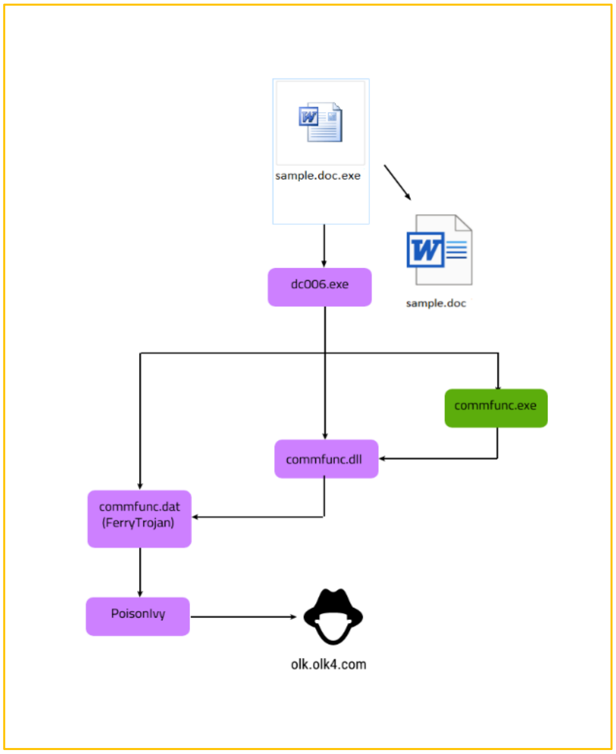
Data from VirusTotal showed that this C2 is connected to a large cluster of PlugX and PoisonIvy activity, apparently targeting the Catholic Church and its activities in Asia. This cluster is much older than previously reported Catholic-related targeting. Most of the samples were submitted to VT in 2016. However, the malicious loader DLL has a compilation timestamp from December 2013, and the various lures appear to be mainly from 2014. More than 100 malware samples were found to belong to this cluster. They tend to follow the same two basic designs as shown below, with just the lure documents differing between samples.


Dichiarazione dei Vescovi vietnamiti contro Cina riv.doc.exe
Dichiarazione dei Vescovi vietnamiti contro Cina riv.doc
wintmp01.exe
hewlett.exe
hpqtap08.dll
msi.url
hp.url
PlugX
link.linkipv6.com

Left: The dropper is a PE executable which is named according to some church-related topic (in Italian.)

It extracts another executable called *wintmp01.exe* to disk. In addition, a real document is opened to stop the user from becoming suspicious. Wintmp01.exe is a WinRAR SFX archive containing four files:

Hewlett.exe is a renamed legitimate *hpqtax08.exe* from Hewlett-Packard. It loads the malicious *hpqtap08.dll,* which in turn loads the first of two binary shellcode blobs - *msi.url*. This contains an intermediate executable written in Delphi, which depending on the situation attempts to load the final shellcode blob *hp.url* either directly or through thread injection mechanisms. Once decoded, *hp.url* contains a classic early PlugX executable.



Right: The dropper is a PE executable similar to the left case.

It extracts another executable called *dc006.exe* to disk. In addition, a real document is opened to stop the user from becoming suspicious. Dc006.exe is a Delphi executable containing an encoded exe resource which is run in memory. This resource again extracts three files:

Commfunc.exe is a renamed legitimate *cammute.exe* from Lenovo. It loads the malicious *commfunc.dll,* which in turn loads a binary shellcode blob *commfunc.dat*.

This contains a loader executable written in Delphi, which contains and calls an embedded SHELLCODE resource, containing Poison Ivy.

The loader uses the internal name **FerryTrojan.** In theory it can be used to load any type of shellcode.

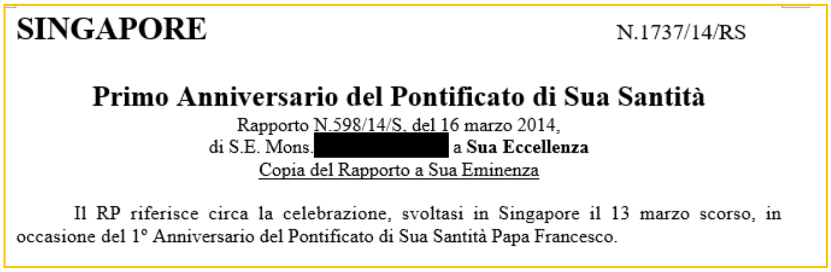
PoisonIvy

PoisonIvy (PI) was originally a “remote administration tool” developed by the Swedish hacker Shapeless in 2005, with several other contributors [11]. It was freely available on the web and was quickly adopted by many threat actors because of its features. It is lightweight and supports being deployed as a small executable shellcode. PI injectors also sometimes use sideloading.

Targeting

We have little hard data on the actual targets for this campaign, but we can make high-confidence conclusions based on the topics and design of the lure documents.

Many lures follow a format that seems to adhere to the internal Vatican document standard:



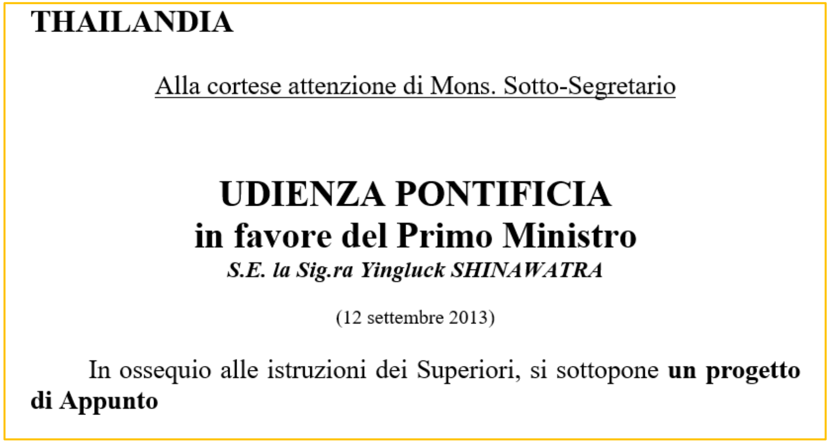
SINGAPORE N.1737/14/RS

Primo Anniversario del Pontificato di Sua Santità
Rapporto N.598/14/S. del 16 marzo 2014,
di S.E. Mons.[redacted] a **Sua Eccellenza**
Copia del Rapporto a Sua Eminenza

Il RP riferisce circa la celebrazione, svoltasi in Singapore il 13 marzo scorso, in occasione del 1° Anniversario del Pontificato di Sua Santità Papa Francesco.

Above: Naming convention follows the scheme SEQUENCE_NUMBER/YEAR/ DEPARTMENT. In our case, the ‘Department’ field is ‘RS’ (Rapporti con gli Stati - Relations with States). This is a report on anniversary celebrations for Pope Francis in Singapore.

Correspondence possibly directed at external recipients:



THAILANDIA

Alla cortese attenzione di Mons. Sotto-Segretario

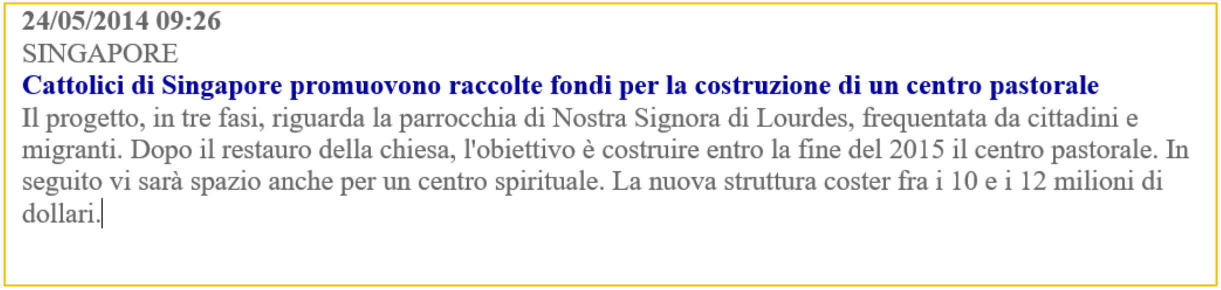
UDIENZA PONTIFICIA
in favore del Primo Ministro
S.E. la Sig.ra Yingluck SHINAWATRA

(12 settembre 2013)

In ossequio alle istruzioni dei Superiori, si sottopone **un progetto di Appunto**

Above: Notice of Papal Audience given to then Prime Minister Yingluck Shinawatra of Thailand. The meeting indeed took place on Sept. 12th, 2013 [12]

News reports taken from public sources:



24/05/2014 09:26

SINGAPORE

Cattolici di Singapore promuovono raccolte fondi per la costruzione di un centro pastorale

Il progetto, in tre fasi, riguarda la parrocchia di Nostra Signora di Lourdes, frequentata da cittadini e migranti. Dopo il restauro della chiesa, l'obiettivo è costruire entro la fine del 2015 il centro pastorale. In seguito vi sarà spazio anche per un centro spirituale. La nuova struttura coster fra i 10 e i 12 milioni di dollari.

Above: A news story seemingly taken from AsiaNews [13]

Many of these lures seem to be either stolen legitimate documents, or documents deliberately doctored to resemble official Vatican correspondence.

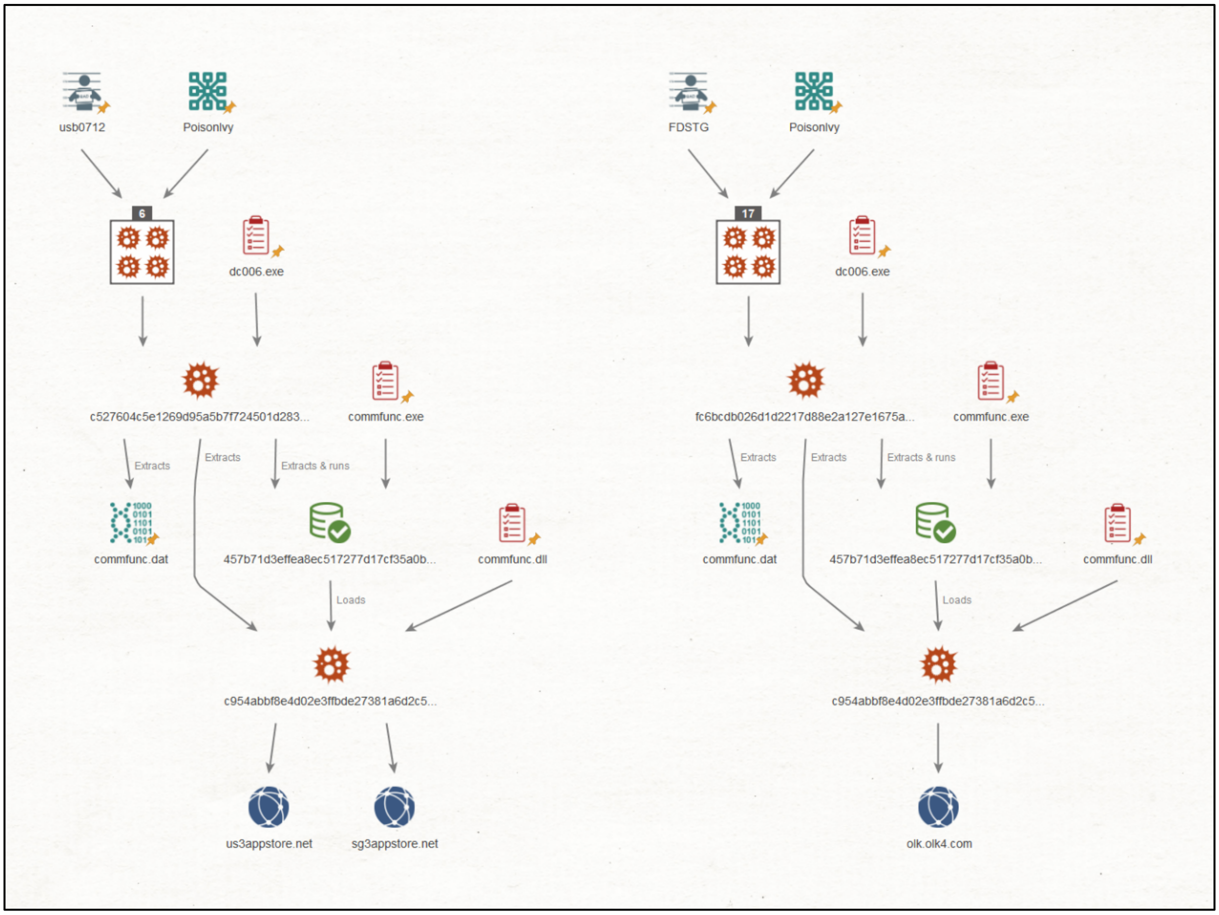
As mentioned, it is not evident which individuals were targeted by these malware packages.

There is a strong focus on the Church's activities pertaining to countries in the South-East Asia region: Vietnam, Thailand, Philippines, Japan, East Timor, and Singapore. However, since most of these lures are in Italian and often follow an apparent internal Vatican communication format, it is reasonable to assume that the recipients are Italian-speaking representatives of the Holy See.

A full document list is provided in the Appendix.

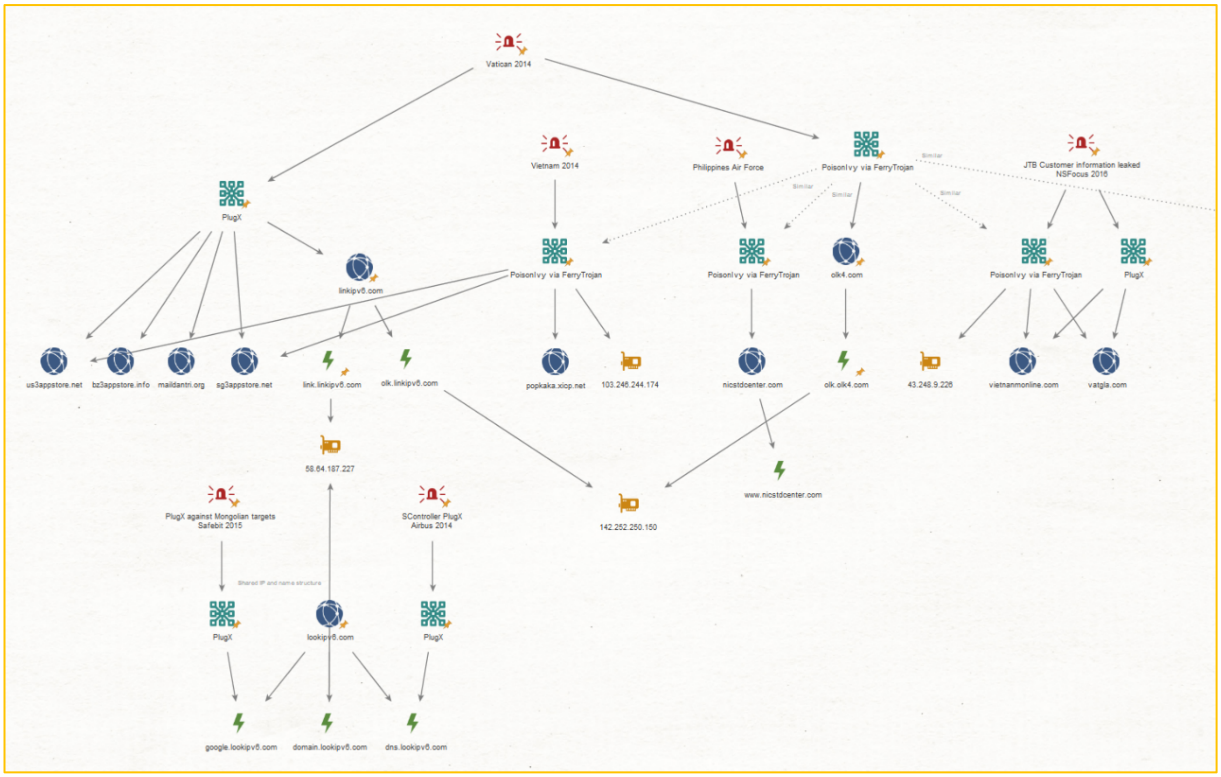
Connections to other activity

The **wintmp01** PlugX and **dc006** PoisonIvy droppers have a long history. There are several separate branches going back to at least 2014 mainly targeting Vietnam. These seem to be more focused on internal Vietnamese issues, and not specifically on religious matters or the Vatican. In the case of PoisonIvy, the malware configuration usually contains a campaign tag that gives a hint as to which cluster they belong to.

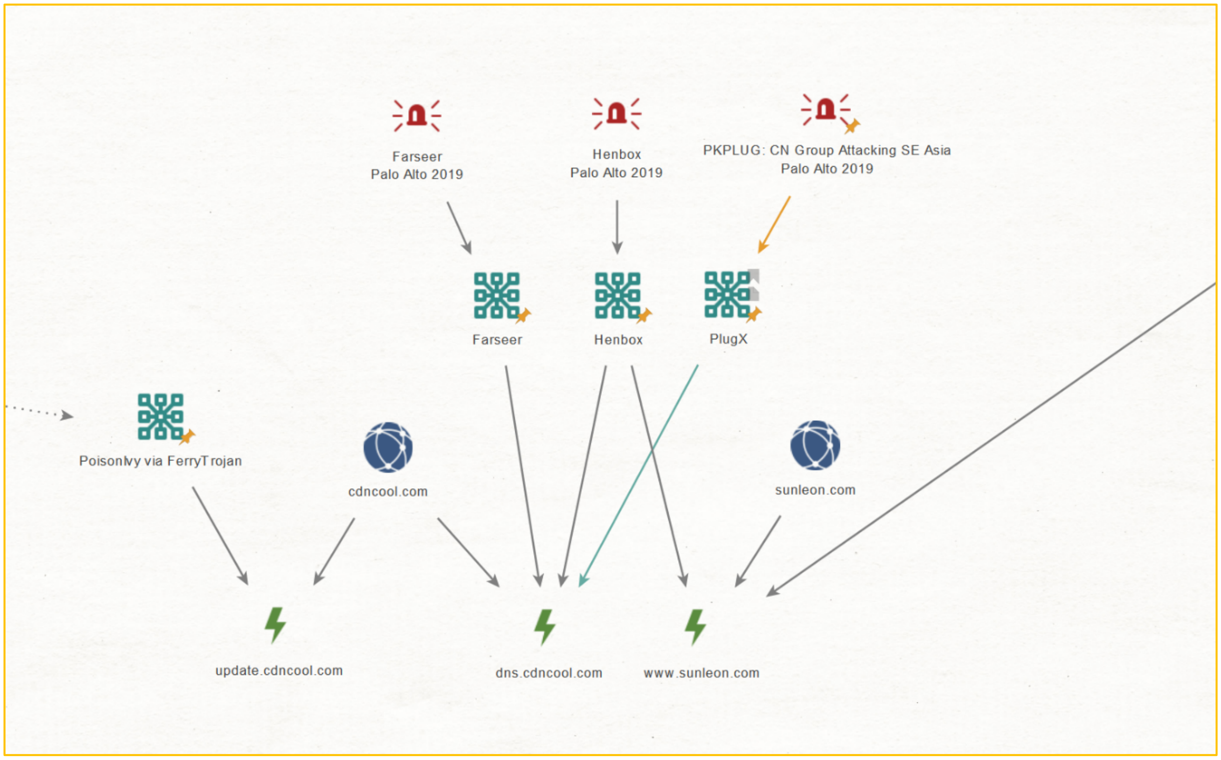


Above: Similarity between the **usb0712** Vietnamese campaign and the **FDSTG** Vatican campaign. Note the *appstore[.]net domains, also used in the previously mentioned PlugX dropper [10].

The FerryTrojan loader used in some of the Vatican PoisonIvy samples is a common factor among several other clusters of activity. The same is the case for the network infrastructure used.



Some historic connected cases



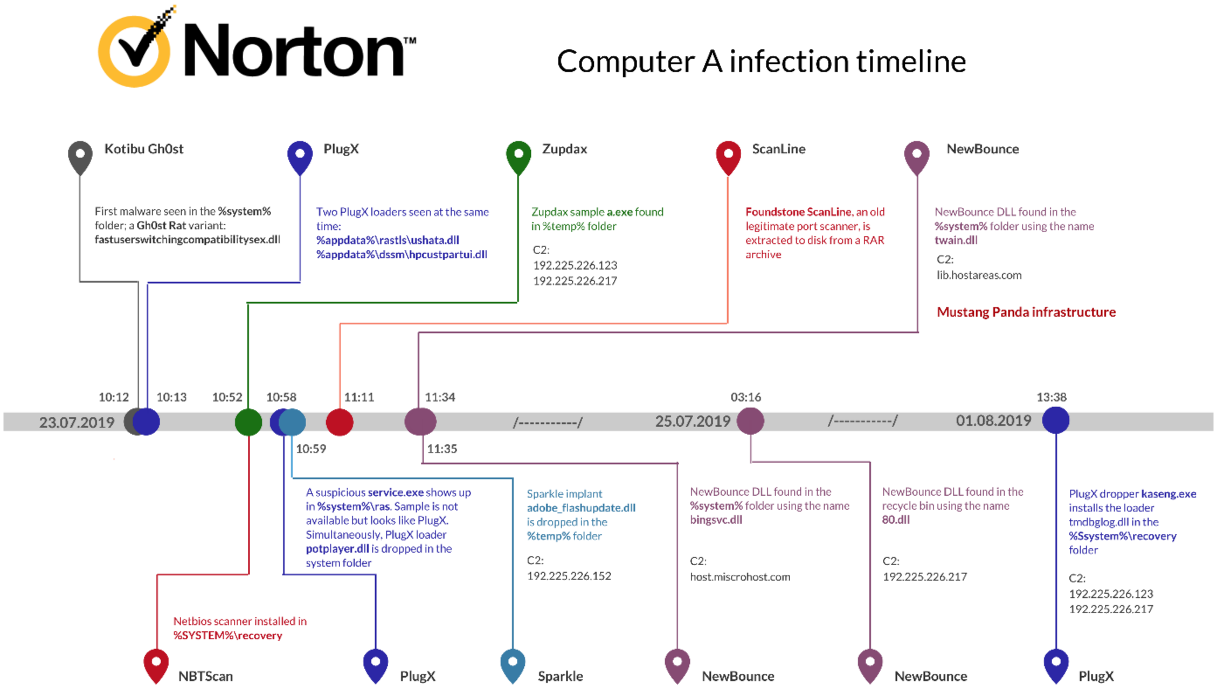
The FerryTrojan PoisonIvy loader provides a link to more recent attacks.

1	Vatican and Vietnamese PlugX and PoisonIvy campaigns are almost identical in structure.
2	Vatican PlugX activity using the C2 linkipv6[.]com overlaps on IP with Mongolian PlugX activity at lookipv6[.]com [14] [15].
3	The breach of the Vietnamese travel agency JTB and subsequent user data leak was reportedly done using FerryTrojan PlugX over the C2's vietnanmonline[.]com and vatgla[.]com. [16]
4	FerryTrojan PoisonIvy samples were used in a campaign against Philippines Air Force. There are 100+ associated samples that reach out to the associated C2 [17], complete with lure documents.
5	The cdncool[.]com domain is used for both FerryTrojan PoisonIvy, as well as PlugX, Farseer and Henbox. [18] [19] [20]

CHAPTER 2:
THE VATICAN INTRUSIONS (2019-2020)

Throughout 2019, Norton researchers detected abnormal activity in telemetry data originating from computers located in the Vatican. Closer inspection of the logs revealed that a handful of computers had several clearly malicious implants installed. Some of these belonged to previously known families such as PlugX while others had not been publicly documented before.

A total of 17 computers showed signs of intrusion to varying degrees. In this paper, we will be referring to these as machines A to Q.


Computer A infection timeline

First malware seen in the **%system%** folder; a **Gh0st Rat** variant: **fastuserswitchingcompatibilitysex.dll**

Two PlugX loaders seen at the same time:
%appdata%\rastls\ushata.dll
%appdata%\dssm\hpcustpartui.dll

Zupdax sample **a.exe** found in %temp% folder

C2:
192.225.226.123
192.225.226.217

Foundstone ScanLine, an old legitimate port scanner, is extracted to disk from a RAR archive

NewBounce DLL found in the **%system%** folder using the name **twain.dll**

C2:
lib.hostareas.com

Mustang Panda infrastructure

A suspicious **service.exe** shows up in **%system%\ras**. Sample is not available but looks like PlugX. Simultaneously, PlugX loader **potplayer.dll** is dropped in the system folder

Sparkle implant **adobe_flashupdate.dll** is dropped in the **%temp%** folder

C2:
192.225.226.152

NewBounce DLL found in the **%system%** folder using the name **bingsvc.dll**

C2:
host.miscrohost.com

NewBounce DLL found in the recycle bin using the name **80.dll**

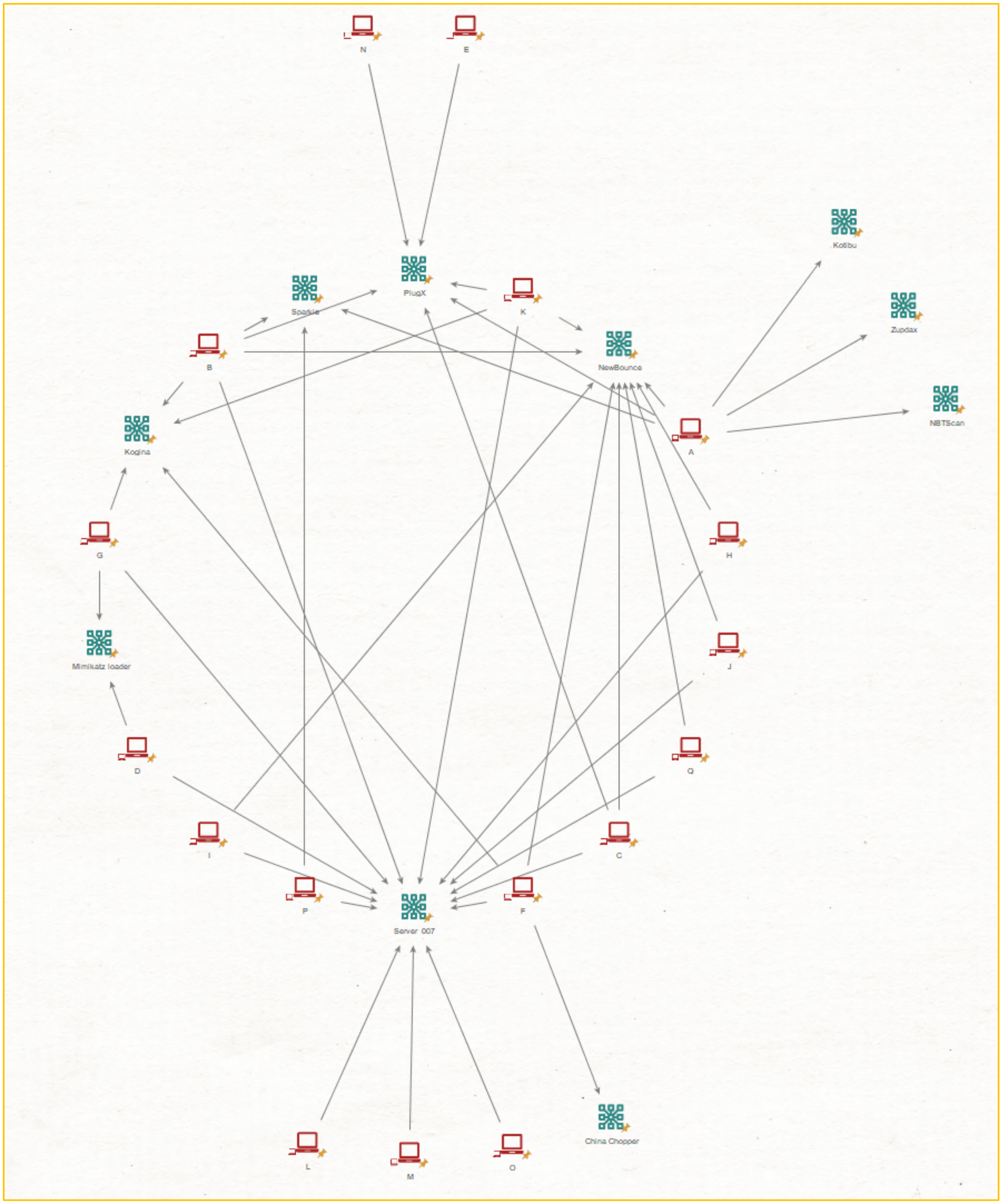
C2:
192.225.226.217

PlugX dropper **kaseng.exe** installs the loader tmdbglog.dll in the **%Ssystem%\recovery** folder

C2:
192.225.226.123
192.225.226.217

Netbios scanner installed in **%SYSTEM%\recovery**

This activity revolves around a main command and control hub located at the IP addresses 192.225.226[.]123 and 192.225.226[.]217. Over time, these addresses have been used to control malware installations spread over at least four different families.



The other computers we identified contained these and a few malware families to different degrees.

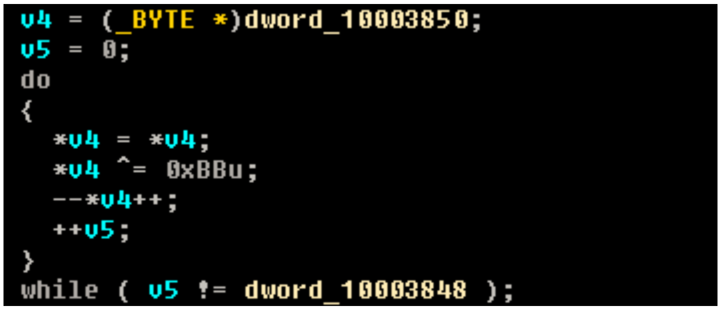
PLUGX

The PlugX installers in this case have been of different types, which suggests that the attackers have an arsenal of different malware builders at their disposal.

Sample:
sha256: f96adc9e046ecc6f22d3ba9cfea47a4af75bcba369f454b7a9c8d7ca3d423ac4

This is a bundled installer executable which contains the legitimate application ptwatchdog.exe renamed to msvsct.exe, a malicious TmDbgLog.dll and an encrypted PlugX executable payload named TmDbgLog.dll.obj. The installer extracts and executes a Visual Basic script (msvvcs.vbs) which in turn extracts the other components.

The PlugX payload is decoded by XOR'ing each byte with 0xbb and subtracting 1.



```
v4 = (_BYTE *)dword_10003850;
v5 = 0;
do
{
  *v4 = *v4;
  *v4 ^= 0xBBu;
  --*v4++;
  ++v5;
}
while ( v5 != dword_10003848 );
```

Command-and-control (C2) servers are 192.225.226[.]123 and 192.225.226[.]217.

Several other PlugX loader DLLs were seen on the affected computers, though without the original dropper and payload. Without these we cannot be certain about the specifics of the malware. Some of the DLLs have instead shown up in full dropper packages on VirusTotal and while these have not necessarily been used against Vatican targets, it is likely that there is some connection between them. For example:

Loader sha256:
ad48650c6ab73e2f94b706e28a1b17b2ff1af1864380edc79642df3a47e579bb
Dropper sha256:
0a00204517283c9a8d1e2d1a8743249c14de0edcec4a8292500083437735663c
Dropper sha256:
75f2e752983a9f46082e7b35820f23db577a5aff9ad946b05b0d3871a9df686b

These are very similar to the dropper above, though they are WinRAR self-extracting executables (SFX), not bundled installers.

C2 servers are:
lib.hostareas[.]com and 123.1.151[.]64
web.miscrosaft[.]com and 154.213.21[.]207

Loader sha256:
29b5ffcda77acf5d1d14f8e1e57d2bed803dd493863377fdf48b3ca97126bdde

This is an impersonation of *HPCustPartUI.dll* from Hewlett-Packard. It uses a different loader logic from the previous configuration (no VBS script and payload is encoded using the assembly instructions [sub 0x71, xor 0xb5, add 0x71]). The payload is named *HPCustPartic.UI*.

Several droppers are available that incorporate this loader:

Dropper sha256:
3f46de9df24fd146d75c906663e8f1ace300b147f0cea0370f38cb0088a158a4
Dropper sha256:
6537fcbb157bde7acabc3a1a8bef266d7825573ed5ecee1408c495db3c913c60
Dropper sha256:
ade0514ccb90c39a61ab8a4c16818fbcd352984e2a26b2ffcd92165975e07fd5
All of these are configured to use 192.225.226[.]217 and/or 192.225.226[.]123 as C2 servers.

Loader sha256:
653fe0ab7b634e50ba09f962c6357bcf76ce633768aa41dd01d1a93ef83a0a54

This is an impersonation of *comserv.dll* from Rising Information Technology.

The dropper also contains the legitimate executable *RStray.exe* as well as the payload *comserv.dll.url.* The payload is not decoded before being called, but the code is obfuscated.

Dropper sha256:
8c16116b95b94511c3dfe5aa1fdb05078a88747bbd2ef9ebe305f90f1bbf604a
C2 server: 192.225.226[.]152

ZUPDAX

This remote access trojan has been in use since at least early 2014, but it has managed to stay under the radar of the security community, apart from a brief mention in two reports. [18] [20]

The malware has evolved over time, as has the functionality it offers. The version used in our case is apparently the same as described by the Korean security vendor Hauri in Hauri Security Magazine [21] in 2018. Like PlugX, this malware often uses DLL sideloading as a part of the infection process.

The Zupdax “P1Rat” installer

The initial dropper is a bundled installer we have called the “P1Rat” variant due to the installer and included loader DLL containing the following debug paths:

D:\Leee\515远程文件\P1Rat_2017_07_28A\src\MyLoaderBypassNorton\Release\loaderexe.pdb

D:\Leee\515远程文件\P1Rat_2017_07_28A\src\MyLoader_bypassKIS\snake\res\SiteAdv.pdb

The following files exist as resources in the installer:

Resource #	Installed filename	Description
103	siteadv.exe	Legitimate and signed Mcafee Siteadvisor Executable
105	siteadv.dll	Malicious loader DLL
106	ok.obj	RC4-encrypted payload (key: ”GoogleMailData”)
107	n/a	Configuration data XOR 0x64

Resources 103, 105 and 106 are extracted to disk using the above names, and siteadv.exe is executed. This causes the malicious sideadv.dll to be loaded.

Sideadv.dll contain its own copy of the configuration resource. The config data contains:

- Names of executables
- Installation path
- Name of the encrypted payload
- Main payload export function to call
- Whether payload will be loaded from disk or memory
- Registry install key
- Installation check mutex name

Siteadv.dll will be loaded with one of four possible parameters:

Install	Install loader exe in registry run key and load payload (from file or memory)
Run	Load a decrypted payload dll file from disk and call its export function. Name of dll and export is defined in config resource
Mrun	Decrypt and load payload dll file to memory and call its export function. Name of dll and export is defined in config resource
Install_and_del	Install loader exe in registry run key and load payload from memory, as well as delete a file (typically the installer)

The “Boar” and “Badger” installers

Zupdax has previously been distributed in other installers going by the names “Boar” and “Badger”. As far as we know, these have not been used in the Vatican campaign(s), but we mention them here for completeness.

“**Boar**” executables have contained the following debug paths:

d:\tenshine\The Boar\bin\install.pdb
d:\tenshine\The Boar\bin\ushata.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\install.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\ushata.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\byebye.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\SvcDll.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\install_test.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\ushata_noload.pdb
e:\workspace\boar服务生成用byebye.exe过uac\bin\test.pdb

Instead of containing payload components as resources, Boar incorporates these as encoded and compressed blobs in the installer file. These are extracted and installed according to information in an INI file. Where “P1Rat” spoofs siteadv.dll for sideloading, “Boar” spoofs ushata.dll, a Kaspersky component. The malicious DLL is inadvertently loaded by the signed legitimate Kaspersky executable avpui.exe which is also included in the installer.

The “**Badger**” installer is structurally similar to the “P1Rat” installer, down to the using the same resource structure and the same RC4 password for the payload decryption. The PDB string is:

c:\Users\PC-2015\Desktop\Badger\En-v2\免杀\MyLoader_bypassKIS\bin\loaderdll.pdb

The malware associated with this installer is a trojanized *Able Desktop* installation. This sample was previously detailed by ESET [26], described as dropping PlugX aka Korplug. The payload does however appear to be Zupdax. The campaign in that case was seemingly aimed at Mongolian targets and was attributed to LuckyMouse aka Emissary Panda/APT27 or alternatively a threat actor known as TA428.

Zupdax main payload

The payload is a PE DLL executable of approximately 300kb, written in C++. It exports one function named *load.*

The malware utilizes the open-source library UDT for network communication. UDT is described as a *"UDP based application-level data transport protocol for distributed data intensive applications over wide area high-speed networks."* [22]

The malware will in some configurations try to disguise this as legitimate traffic by connecting to port 53 (DNS) on the command & control server, as well as deliberately naming the C2 domains with the ns* (nameserver) prefix. Data transferred is encrypted using RC4 with the encryption key "Microsoft".

Zupdax has historical connections to several other targeted operations which will be briefly covered below.

The variant used in the Vatican campaign supports the following commands:

Command	Action
0x0	Stop all actions and deinstall service
0x17	Save data to file
0x19	Deinstall service
0x29	Verify received plugin and call its export function "Fu**ME". (Export name is a profanity slightly redacted. It is case insensitive, any case combination is loaded)
0x38	Download and execute file
0x68	Start program named AVANTI.EXE (this is usually the loader executable)

NEWBOUNCE

This malware is a backdoor that also includes rootkit components.

The name “NewBounce” is derived from the PDB path included in several samples:

```
f:\sj\newbounce\hidefile\amd64\mhide64.pdb
F:\sj\newbounce\Release\setup3.pdb
```

The string “bounce” is also present as debug messages found in the code; such as “Run bounce” and “work bounce Mode ”

Installer sha256:
5e3d5f7d04ed48f27652f21d72c5915be147d0dd5bf0e92f1c26b38d5f4e1d7a

This is a simple installer that checks system architecture (x32/x64) and installs the correct service DLL accordingly. The DLLs are copied from existing files present on disk named MSVC3.DAT and MSVC6.DAT.

Service DLL:

The service DLL contains the main functionality of the malware. It contains the following features:

- It can connect to up to three different download servers (optionally via proxy) and download a shellcode blob embedded in a JPG file. The file will be named “out.jpg” on disk.
  The last four bytes of the JPG indicate the offset in the file where the code blob starts. This code is LZ-compressed and is read into memory and decompressed before being called.
- Upon installation it collects basic descriptive data about the target computer, such as Windows version, computer name, system language and ansi code page, drive types and free disk space, username, memory status, CPU type and RDP port and uploads these to C2 server.
- The malware sets up AES-encrypted command&control communications using the key phrase:

  “*GAEncryptfasdfafhhIlove!!@#$!@$!@$#%!asdfasdfasdfsdfaasdfaasdfasfsafasdfasdfdasfdasfjjjvzcxvjzjdfasdfasdfsadfasfsdafdasfasdfasfd*”

- The message handling loop responds to commands from operator. Features include uploading and downloading of files, opening a command shell, listing files and processes, copying and deleting files.

The DLL is installed in the %system% folder using names like *twain.dll* or *bingsvc.dll*, and registry entries are added to load it:

Registry\Machine\System\CurrentControlSet\Services\twain

Sample: File hider rootkit component
sha256 96c0a4bde1d8fedd58215f91d3aaa49e65fb44275ecb15302ebabfc02350c47b

When first executed, NewBounce installs a rootkit minifilter driver and calls this to hide files related to the malware. This rootkit driver is installed in the *drivers* folder using the file name "*hfile_device.sys*". The driver subscribes to IRP_MJ_DIRECTORY_CONTROL events (0xC) via a postprocessing callback and checks the file name returned against its own list of file names. If the name is found in the list, the directory entry is ignored and thus never appears in ordinary directory/folder listings.

Userland applications interacting with this rootkit can add new file name strings to the hidden files list by calling the driver through DeviceIoControl with IOControlCode 0x22E024. Sending the string "CLEAR ALL" instead of a filename will empty the list.

The file is digitally signed using a code certificate issued to 上海域联软件技术有限公司 – or Shanghai Yulian Software Technology Co., Ltd. This certificate is almost certainly shared in the underground. A large amount of different malware is signed with it and it has been used in multiple cyberattacks [23] [24]. It was originally valid only until 2012 and has also been revoked.

This file hider rootkit is identical between the different NewBounce samples we have seen in the Vatican case.

Interestingly, the service also tries to invoke two *other* rootkit drivers to hide registry entries and network connections. These drivers are called PCI358129.SYS and NSIP.SYS, but they are not dropped by any of the malware samples in the Vatican intrusion. Without the drivers installed, the calls to them will simply fail.

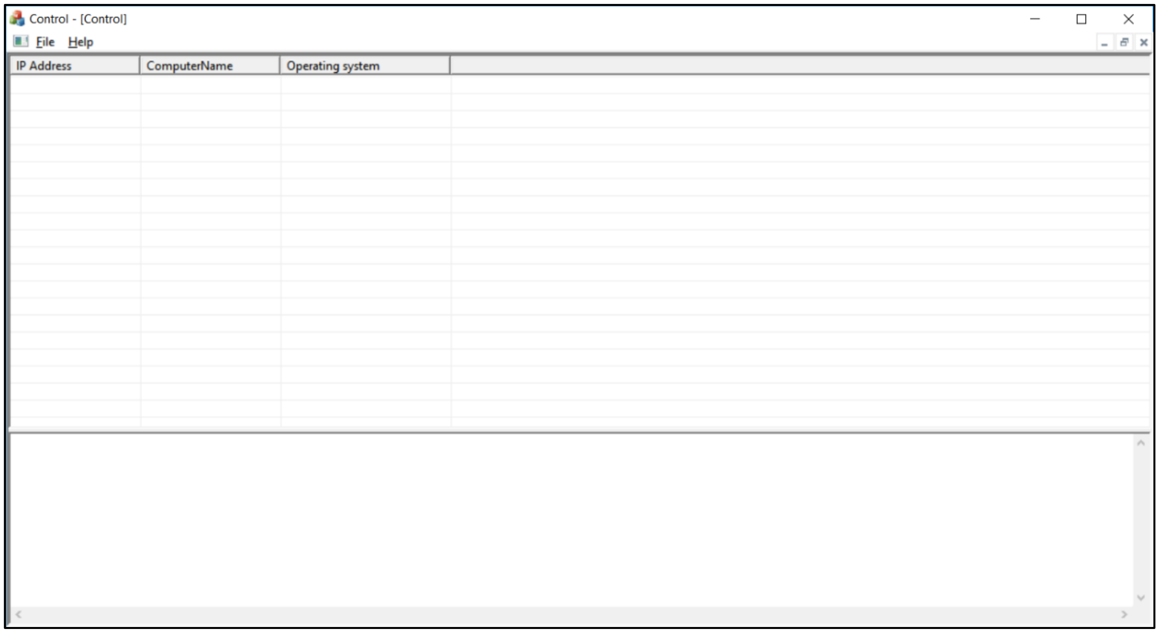
However, we found an earlier NewBounce sample which *does* drop drivers matching the descriptions. They have similar names, PDB paths and are signed with the same certificate as the file hider, but at least the registry hider does not appear to be fully finished.

```
f:\sj\wfpga\hidereg\amd64\hidereg64.pdb
f:\sj\wfpga\nsiproxy\amd64\nsiproxy64.pdb
```

Sample: NewBounce dropper
sha256: c425e30a202f00b9d272bc864965ad9087c1596466f842871121c523b47638c2
Sample: Network hider rootkit component
sha256 ddb6bc2db796885a3e706c99918a8e3ba80826a9813ead7cb6b9999e1cae4b7f

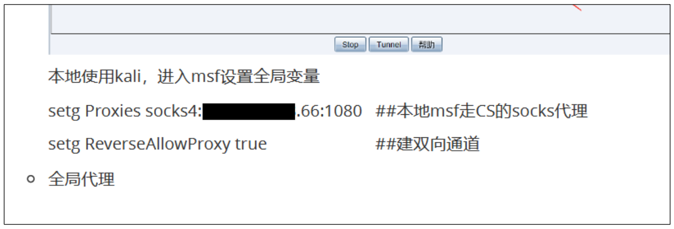
Sample: Registry hider rootkit component
sha256 cec59ba4fe49f48332f2a60df7ebb72ac86e6049b8ec09b0aa2bd9c9214e112e
Sample: Controller
sha256: 6156ca511faca6ca9ff08263157df5c8cb77f7dbbb08950d59159ce4331a4fcf

Someone submitted what appears to be a NewBounce controller to VirusTotal. This uses the same hardcoded AES key for communication.



Above: The NewBounce controller GUI

An IP address associated with a NewBounce C2 can be found in 2019 training materials from a Chinese security group. This article discusses how to use Cobalt Strike.



本地使用kali，进入msf设置全局变量

```
setg Proxies socks4:[redacted].66:1080   ##本地msf走CS的socks代理
setg ReverseAllowProxy true              ##建双向通道
```

- 全局代理

There could be several possible explanations for this – e.g. re-use of the IP – but it is interesting.

KOGINA

This is a credential stealer with a loader component.

The name “Kogina” is derived from the PDB path included in some samples:

```
D:\gina\x64\Loader.pdb
Z:\c\ok\gina\x64\Loader.pdb
```

The loader injects a shellcode to the Windows Service Host process svchost.exe. The embedded shellcode is responsible for dropping the payload and establishing persistence on the system.

- Injects code to svchost
- Drops payload to system32 directory
- Establishes persistence by installing as a SSP DLL in "HKLM\System\CurrentControlSet\Control\Lsa\Security Packages"
- The payload is an unencrypted DLL inside of the shellcode.

Payload:

The payload DLL contains the main credential stealer with the capability to send the username and password to the C&C server. It is installed as a password filter DLL.

We have seen two hardcoded names for the payload:

```
kavsrvc.dll
wmvdmooe3.dll
```

Depending on the included configuration the stolen credentials can be saved to a file on disk, transmitted to C2 via UDP over port 53, or they can be sent via HTTP POST.
Our samples connect over HTTP to *hxxp://mail.chin-coj[.]com/mskmsonemissio.php*.
Usernames and passwords are encrypted and base64 encoded and concatenated with "flag=" eg. "flag=base64encode(encrypt(username[password]))".

SERVER007

This is a backdoor written in C++. It appears to have been in development at deployment time because it contains a lot of debug statements. We have seen both 32- and 64-bit versions, but only the installed DLL – we do not have copies of the dropper. This malware has been one of the most commonly found on targeted machines (11/17).

It is installed as a service in the Windows System folder, and when run, it sets up communication with C2 server over HTTP. Network traffic is LZ-compressed and base64 encoded.

The malware profiles the local system and uploads the data to C2. This includes:

- Local hostname/ip
- Computer name
- System language ID
- System ANSI code page
- Windows Version (Major and Minor Versions, Build number, Platform ID)
- Drive types
- Free disk space
- Default RDP port

It then sets up a command loop that can:

- run local shells
- list files/folders
- delete files
- rename files
- upload and download files
- execute local commands

The name **Server_007** stems from a string present in many samples which appears to be a campaign tag or similar. This string is also included in the data sent back to C2 but is otherwise not used. The most prevalent such tag is “server_007” and is probably the default value. Two samples contain the tag “ppoomm” here, which is similar to www.ppoomm[.]va, the website of “Pontificie Opere Missionarie” aka the Pontifical Mission Societies. We do not have individual target information apart from affected computers being geographically located in the Vatican, so we do not know if this is meaningful.

SPARKLE

Sparkle is another malware that has been in development for quite some time. Variations go back to at early 2015. This malware was briefly mentioned and given the name Sparkle in a 2019 article by BlackBerry Cylance Threatvector Team [25]. We saw Sparkle used on three computers (A, B, P) in our cluster.

It is typically installed as a DLL by an executable dropper. The dropper is responsible for extracting the DLL from an LZ-compressed blob and execute it via rundll32.exe. It will add a registry run key for persistence.

```
HCKU\Software\ts\explorer\run Adobe =
%SYSTEM%\rundll32.exe %TEMP%\Adobe_FlashUpdate.dll Start
```

Alternatively, a shortcut file - “Internet Explorer.lnk” - with the same function may be placed in the %STARTUP% folder.

Once installed, the main payload connects back to C2 server and sets up communication. Early variants use regular unencrypted (but LZ-compressed) TCP traffic for this, while newer variants send this information over HTTP.
There is some variation between versions, but usually the features include:

- List system drives
- List files
- Delete files
- Execute CMD statements
- Copy & move files
- Upload files to a remote server
- Download files from a remote server

As with several other malwares in this investigation, some Sparkle samples also contain noteworthy PDB strings:

```
F:\六道\Obiit-IV\Release\svchost_1.pdb
F:\六道\Obiit-III\Release\Install_New.pdb
F:\六道\Obiit-IV\Release\Install_New.pdb
E:\六道\HTTP探针远程取证软件\Release\Install_New.pdb
C:\Users\123\Desktop\Obiit-YY\Obiit-III-2.000\Release\Install_New.pdb
C:\Users\Bala\Desktop\Obiit-III\Release\Install_New.pdb
F:\666666\Obiit-III-SD\Release\Install_New.pdb
```

Based on the PDB strings, the project seems to have been named “Obiit” – or alternatively “六道“ – “six ways”, possibly referring to the six stages of Buddhist existence.

GRAVY INJECTOR

This is a simple injector that starts nslookup.exe and loads a malicious DLL into the nslookup process. We do not have a copy of this payload DLL, but it is named “MsPEng.dll” on disk.

The injector’s PDB string gives a hint at what the functionality is supposed to be:
C:\Users\enWin7x64\Desktop\GravityProxyXE\x64InjectDll\MsPEng\x64\Release\MsPEng.pdb

It is likely that the payload is a proxy of some sort. To avoid naming collision with an unrelated malware already named “Gravity”, we have named this malware “Gravy”.

CONNECTIONS TO OTHER ACTIVITY

The malware and network infrastructure used by the threat actors in this incident has overlaps with other current and historical activity from China-related groups.

1 A PlugX dropper 6537fcbb157bde7acabc3a1a8bef266d7825573ed5ecee1408c495db3c913c60 configured with a C2 used against the Vatican was sent as email attachment to Korean recipients.

2 A PlugX dropper ade0514ccb90c39a61ab8a4c16818fbcd352984e2a26b2ffcd92165975e07fd5 configured with a C2 used against the Vatican appears to refer to a Belgian Catholic organization.

3 A Zupdax sample was involved in campaigns apparently against Mongolian targets [26]. Final payload is structurally very similar to a sample used against the Vatican, though it is almost two years newer.

Mongolia sha256:
07f87f7b3313acd772f77d35d11fc12d3eb7ca1a2cd7e5cef810f9fb657694a0
Vatican sha256:
f56d87a87b52e86e669fb9b01e28caa8817e83a6fb8e1873faec70b15ae6bb72

4 An old Zupdax sample was at a point in time **hosted** on a Cambodian government website.

sha256:
9fa51060685808ab72ab9f862ced67241306c5fd927ae28c17252bac6cbf9354
C2: mail.vip53[.]cn

The same host served other malicious content apparently related to Cambodia [27].

5 A Zupdax sample is configured to use C2 servers that have been associated with FF-Rat activity [28]. This sample is structurally identical and has the same compile time as the Vatican Zupdax sample.

sha256:
84b8bfe8161da581a88c0ac362318827d4c28edb057e23402523d3c93a5b3429
C2: pop.playdr2[.]com|mail.playdr2[.]com|ns2.gamepoer7[.]com

FF-Rat aka FormerFirstRat has been attributed to the group known as DragonOk or Bronze Overbrook [29].

6	NewBounce samples are configured to use C2 servers that have been associated with the threat group Mustang Panda aka Bronze President [2] [30], and have also been mentioned in the context of RedDelta [31]. sha256: d6f468c274536c6ce2705d2780b44b52d5d27d7614cae10ea57dc1689e703ba1 C2: mail.svrchost[.]com|host.svchosts[.]com sha256: 5298bf36c489af136bcb69f9eb8d7700606006e3f702af771a9c0c74d784401b C2: lib.hostareas[.]com The RedDelta activity was also reported used against Hong Kong Catholic targets [2].
7	Most of our Server007 samples were compiled January 2019 and connect to the C2 server at the IP address 45.192.160[.]214. Throughout early 2020 this IP shared SSL certificate with another IP address at 154.213.21[.]70. This IP hosted the domain lib.jsquerys[.]net - a similar domain name configuration as the NewBounce C2 lib.hostareas[.]com. These domains were also documented used for other RedDelta activity [31], including the use of Cobalt Strike.
8	The Gravy injector sample contains traits found in other malware. sha256: 0253e700764a008b2e724e1d24718594ff8ff4b138298b5a0d79f0a42503938f The first pdb string segments: “C:\Users\enWin7x64\Desktop\...” are identical to pdb strings found in these samples: sha256: 5c2a6b11d876c5bad520ff9e79be44dfbb05ee6a6ff300e8427deab35085bef6 sha256: 9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d These samples have been associated with supply chain attacks on the gaming industry as well as other targeted attacks against Vietnamese entities [32] [33], and have also been associated with Vatican attacks [2]. The PDB strings are however quite generic.
9	The P1Rat loader used for Zupdax has been used to install other malware – notably **Rshell**, another previously undocumented backdoor. sha256: b1d6ba4d995061a0011cb03cd821aaa79f0a45ba2647885171d473ca1a38c098

	Rshell uses the RC4 password “GoogleMailData” for its configuration data, same as the password used for the encrypted payload and the P1Rat Zupdax payloads. [34] The targets appear to be Russian or Russian speaking, and one of the droppers refers to the Russian aerospace entity ROSCOSMOS.
10	Sparkle samples share C2 infrastructure with Henbox/Farseer clusters via the C2 www.sunleon[.]com. This is the second link between Henbox activity and the Vatican campaigns.

CONCLUSION

The targeting of persons connected to the Roman Catholic Church has been ongoing since at least 2014. In Chapter 1 we detailed campaigns that appeared to target Italian-speaking persons likely connected to the Vatican. In Chapter 2 we detailed intrusions seen on computers *inside* the Vatican City.

We assess the following with high confidence:

- The 2014-2016 PlugX and PoisonIvy campaigns against Vatican and Vietnamese targets were performed by the same threat actors. There are multiple close overlaps in toolsets and infrastructure.
- The 2018-2020 Vatican intrusion activity is linked with previous reporting on the threat actors RedDelta and Mustang Panda. [2] [31] . There are multiple infrastructure overlaps.

We assess the following with medium confidence:

- The two cases are likely linked and performed by the same or cooperating groups. There are overlaps in toolset preferences, targeting, and at least one infrastructure/unique malware contact point.

Several names for the threat actors have been used. Recorded Future introduced the name RedDelta, while noting that the group overlaps with the previously known group Mustang Panda. We have chosen not to distinguish between these groups.
There are many connections to other intrusion activity, both historic and more current. This is nothing new for this region and there appears to be a great deal of resource sharing between groups, and some groups appear to have wide-ranging interests.
We do not expect the attacks against the Catholic Church to end as long as it continues to engage with and influence the lives of people in China and other South East Asian countries.

In today’s open world, one should expect targeting of all sorts of interest groups and individuals, not only targets associated with governments and corporations.

PROTECTION STATEMENT

Norton protection products detect and remove the malware described in this paper, as well as block known malicious network traffic.

APPENDIX 1: INDICATORS OF COMPROMISE

Indicators from Chapter 1: The Linkipv6 PlugX/PoisonIvy campaign
Sample hashes: Items in green are included with high confidence; yellow medium and white low.

PlugX droppers (sha256)	C2	Target
04b03dc7eab99b55165bc5b51d990682f817c09a5ebf31f0cd6034764245fec1	link.linkipv6[.]com	Vatican
04b08225f717ea139c35c801ce224c365e94dc8f3d5b41d41b51b057c52076f4	link.linkipv6[.]com	Vatican
0560be591a7746088681855a96d01fd9232a6cb21de4f62e21c272aa18c4ee7e	link.linkipv6[.]com	Vatican
0a2d362c5af17a39886750f154fdbfcae8ae9be42813fcf9901bb1b91b7b7f18	link.linkipv6[.]com	Vatican
0a7d9eb7d9c293b165b6c610bb6987d904970ba0f154f6a1c05ebd4587c7fa35	link.linkipv6[.]com	Vatican
0bd7f98f9245b0f30728c6291beeadf088878ff1f325d36e238a1401a741440d	link.linkipv6[.]com	Vatican
11a9ec3aa5a978a793d015563f7e285322d0fe0c8004ba23488ac45fa4a7ef78	link.linkipv6[.]com	Vatican
13bfa7b470e422b653f0a55db42c7435fb320bd2fc68e2bda3318aacb45425a3	link.linkipv6[.]com	Vatican
1447258cd13a41596ac00d3a2bc0cde050234ae594ddb3b2caa1fc429b68af6c	link.linkipv6[.]com	Vatican
150890306145f327d030d2dbd6726d3ee5acebfe3b3998152b8bee0a0bb097f3	link.linkipv6[.]com	Vatican
16a8821ebde52961d4209a47cb002973f40c519228201112d005216bdcbbcc24	link.linkipv6[.]com	Vatican
244b7d8508e81575c4f37173ea126a8502d5cd9beed2b4303a2d030ed0953fc3	link.linkipv6[.]com	Vatican
28609f6c7548f2a450fc71548c17b971b451b2f9db4c81bc0870748d12c7315d	link.linkipv6[.]com	Vatican
2af54e0773e74934a6f1dd3b553f864a331cf2f544818c696e3077043fec606f	link.linkipv6[.]com	Vatican
2dbb3b198cc95da56cda5a3208d0b7edb15232d08e9fd1a3ed68ce47b676e93f	link.linkipv6[.]com	Vatican
30b3d4159ab36b931e87974d9ab8a0254a3b7ef9b98f74ff3ae7801c2aab7164	link.linkipv6[.]com	Vatican
400e8525a119ab86eda7e864228a09a143231e5f25831fd671c067698b1951fa	link.linkipv6[.]com	Vatican
44ff818e4fb2799439fd44759bc26610e348dce7720fc461d53345a02328607d	link.linkipv6[.]com	Vatican
4e58eab7f4adfafed03f6e94dffacfbe784761b237dbe2a2cc678dbec2c86e5f	link.linkipv6[.]com	Vatican
4fb96b8fa9740d7c01a2561a5acfa6a842d90fa64c24c52923812a327cf075d2	link.linkipv6[.]com	Vatican
5bec8720ceb8a6637b21c8a240ba652c47345b80475961421b99b2e2927c91ec	link.linkipv6[.]com	Vatican
5f2b3ee6c92fce500480736c586c53a92735535862ccc2fe80cab07941fde0eb	link.linkipv6[.]com	Vatican
61148f8fbec43c9254b4de2ca278cee0cc03bf0107eecb58381ea78ca134b5f5	link.linkipv6[.]com	Vatican
64544265796e21792fab4e8072b1c6932f6b0877943eeb7e4be911d2b922fe55	link.linkipv6[.]com	Vatican
64de19aea536278c4360f6483ca603d84e554258ecee5ffe4abfeaa808b10a9b	link.linkipv6[.]com	Vatican
6a3aa888a8befcb5455d6593303e962df8fe82477a294df94a710cc2684cb9ea	link.linkipv6[.]com	Vatican
6c6345e17678b9d4503664bc638164267e8b9cc08ca3e37582ec410d35841bb1	link.linkipv6[.]com	Vatican
7a23e528a414b7fc1d6759dc87e530a9ca723cbf1509e98f134e02403a97ed48	link.linkipv6[.]com	Vatican
7b67a65887465cb0b60597473082845e3127a9d5cce9a61aa00751ed7945f81e	link.linkipv6[.]com	Vatican
7f396db327f8c419060f0c2cd576d890dc88f2d984dd8382f95063074f27f82a	link.linkipv6[.]com	Vatican
822cc72d508c54f1fbfc84e6c22fd410ce52969a80f6e38280d0b5e3bf4f46c3	link.linkipv6[.]com	Vatican
8ae998bca091b3ec865ce62bfeb6b97dd085106b0828b7f35b478431499472d7	link.linkipv6[.]com	Vatican
8b79eafa600177f9d4464cc76d0e6d2e611d5718b4961c2e03019667c2e2b066	link.linkipv6[.]com	Vatican
9038f8b6201a52993935b9c3b718bc964b0c619bbe9bfa2ff7be2d8bf8b8e041	link.linkipv6[.]com	Vatican
91c9375476c2b34785e1940a5664bb2fe355872c7231e0a1bb4f45999458f03a	link.linkipv6[.]com	Vatican
96b1a672368504eebf068e52ac6a75e08fbe18c3c3322d064524c872b4ed025e	link.linkipv6[.]com	Vatican
98c3444074cde26f657394f0f5fc0a1b017ed8069b4fdd33df47edb1356e30e1	link.linkipv6[.]com	Vatican

a4d8d68bf25898cf948527030854a97cfe255b8d86c1329b0ef198ae5fd89897	link.linkipv6[.]com	Vatican
ac2a91dc51fcc1a9d2fedabda302f0e90a6a88ec153fd79262e6bab9f7090f2a	link.linkipv6[.]com	Vatican
b938df60cc2e0147a9e618ee71f31e27d0d2024bfeeca97c0fb927976eb1cc5c	link.linkipv6[.]com	Vatican
b98bbfdeaaab46148791566c258ab12478716e43b0f6f2750f1fffab20dfc7a3	link.linkipv6[.]com	Vatican
b98e2b124788c81b589c834ab6ad6c6d4d4a452180d818bf4b6abc1b396a5434	link.linkipv6[.]com	Vatican
c311c93b7ebe6d27a35baaa42853cc19aeb6a5e5d997edf9c6a948f3ad0a1bcb	link.linkipv6[.]com	Vatican
c857fba2228b9adab754da04241d292d7bef9a20c2941736e1702cc3ce60162c	link.linkipv6[.]com	Vatican
cec55e05d30e4afd9f76b2589f2eea49d66ccf4b8e8f5729aeff8e9c708b566b	link.linkipv6[.]com	Vatican
d0d57aeddbd713a906f9b04b6818457bb2e76636e02b7eabf2ae43202fe237cb	link.linkipv6[.]com	Vatican
df782a31cd8a8bf0c7cd9fb05ced2ceb1f9295ac68278c4437adf92eebe41e0b	link.linkipv6[.]com	Vatican
eeb3d5f6378b8ad3e6cba2ff7c9d31833c26046e7bad2dc8c5b5e576b5800928	link.linkipv6[.]com	Vatican
f675ee799bb6db1d2697947b55944568bb19bae03712c6c2b024857161920faa	link.linkipv6[.]com	Vatican
ad214d54e1a29964520e4806bb85259600dff52b3cea6e3ecdc805049497636d	link.linkipv6[.]com	Vatican
b11d17ada474b01aee9c0c87d533854155bb3fa27c0d4a07b4f35df7b37da8f9	link.linkipv6[.]com	Vatican
b8858e95c303765ee68a8456c49d9201e809651b4daddca5e5915030e2f627ba	link.linkipv6[.]com	Vatican
b8dfd3912c538da22f96ae4a099e0cec1ff7d572d9d72133cf831da06a199ce9	link.linkipv6[.]com	Vatican
bae2db602e9db78bc9e2557b6b4898eb5694cf47c376a0af6ddf795493a2e86c	link.linkipv6[.]com	Vatican
eb967e42feda6a666d525a69d73ba75160be0a1654fe8422a2e0279b83e5e5bf	link.linkipv6[.]com	Vatican
ee9f5f897fe13c66cfda807fd6da83ee7b87ee409b11e94ff1269d61ffd0296d	link.linkipv6[.]com	Vatican
f5126ab1f663b9dcdec513098df5923be298af187370a0b7637f10c5b12098df	link.linkipv6[.]com	Vatican
f6db88a1871afe9b59084224101531c6716d84e7c2a1e9f34e3f3d53516bd389	link.linkipv6[.]com	Vatican
fb4c677e29b9eb5e0a8a2d7fc1b63cf75ba190471d3574d4d5c6cb90da506bcb	link.linkipv6[.]com	Vatican
fd9821bad8dde783c87fee49cb41b019331cc96b72643c4cb5a6378867b0b4df	link.linkipv6[.]com	Vatican
fff79c1568d7e2883cea82276f51bf05e14d0ab35e46f012d11385a739d4d961	link.linkipv6[.]com	Vatican
083d8dfde3c7992cdc76aef998eafb747c78b797e46f06721d82ccb2befdbfc9	link.linkipv6[.]com	Vatican
535b0baa1e58f141e4a32fc3f24d4e5b47c2180eb8299e288c3f1141cb1b9c64	link.linkipv6[.]com	Vatican
55ad8d21e696b37d0c9577af6a7634c900a3631412744714d617987247fa58cc	link.linkipv6[.]com	Vatican
57fc0ed0279606e60b492b3a722cec71091b8464b23eb4f1d532f2161296690f	link.linkipv6[.]com	Vatican
590bf31129a74d69c68dcd2f9af9fc1748a4cf335f558ad3eb2371c22fbcf2f7	link.linkipv6[.]com	Vatican
6b88c6389c7102916613e08bbd11509c901dc3e2531b35b5b9c1a381dc1fc44b	link.linkipv6[.]com	Vatican
be4740c509a15aee2ec9278a66795d66095f201cf58c083167e51be72084d98d	link.linkipv6[.]com	Vatican
102ed4057e8499dcb23e2d7ff640cad7b53805e3980fa42ee80d09f29bf92155	link.linkipv6[.]com	Vatican
18a133da3797344508a070da7efc84f9fb104ffef2154fae802402f7b7c9c8ba	link.linkipv6[.]com	Vatican
18ed09c2468e0e5d716e324a47f0cb0f90f37d5a67b3d70146cca73b64addec5	link.linkipv6[.]com	Vatican
217e6824340a646feb4b45c53e5ba58ab32b9f3a2fe465b9fff9c5aec60c5f48	link.linkipv6[.]com	Vatican
248245ff4b565abcfd4975cc987233efc63bfc664c4f45acba52541953603a90	link.linkipv6[.]com	Vatican
297bea0b2943cc429e6d24e1908c084ac36acaba49e45c780aba1b07f7fbf257	link.linkipv6[.]com	Vatican
29a8f94893c5e5c7d760203bfb177f042e26020848dc9372474f8868f7b5c1c0	link.linkipv6[.]com	Vatican
2e85e448cf685d265ed29338ea406a5a0613e06e7632d5d3f7edad323c8d0b06	link.linkipv6[.]com	Vatican
31b44826f55c8b21f432c59c4aa798de9738d607563b6577d5b60f37caf877a6	link.linkipv6[.]com	Vatican
3650f2f1e569d04d10760c31bb4e8cd732fda5b5d3dea651ec0ca863e7c50d24	link.linkipv6[.]com	Vatican
4bd48b659eeb7783cf036f3e0fb87b61a37b8cdb2efed91fda71e48018de6e92	link.linkipv6[.]com	Vatican
886ee18a6ff174afcf8c89a61d0df32826d6ce641a072843913cab010ffcc403	link.linkipv6[.]com	Vatican
936036f3e8ec0814fa356ddb951ae41c90b3900afc69180d3275d4f9f70f9bbe	link.linkipv6[.]com	Vatican

9d63ec45eb9d1b7b6f3e89e6cb46fcb1b84a7ceac9cd656d939eafd412dfbc82	link.linkipv6[.]com	Vatican
d13975b122635623ee8029dc855f793f17b9717d37f609ef73ba9d0b618b088f	link.linkipv6[.]com	Vatican
da56ad2741f01c33001de0289a4aa4d379694adebc04b6ed63862a655c08cf44	link.linkipv6[.]com	Vatican
dab73ab2656babd4e466d3bcd0bdd47329d4b7b5b0183d56593c849ea2f0c55b	link.linkipv6[.]com	Vatican
dcd1cc80835f21360d1cf0ac03ebc972c7ef0f7ebc6ca9cb240ffef7548ed1fd	link.linkipv6[.]com	Vatican
e021369f49a01271644376dd15f19e777e6e70daa04fea08515848f55e585289	link.linkipv6[.]com	Vatican
e08c16f9ddd0396e0c1dd90dc206f0eb3a32f544e54e909e6d89bfe456e39749	link.linkipv6[.]com	Vatican
e1781fadf7ff7f7f0134c1226518bfc45a96bcbd5ca032655cb6964b81b9cb94	link.linkipv6[.]com	Vatican
e7a63f06cfedb4add863cc214805d3313272ad18a6c8ee8d1e64d8482f12b1a6	link.linkipv6[.]com	Vatican
eda4f59c57a45737e9ca3334e224de5e47428c83b80e197c346d9eb70614447c	link.linkipv6[.]com	Vatican
f6559039f1577b64fef89cb1781cf1d0bbea670c5e7ab331a346ca8b9f77072b	link.linkipv6[.]com	Vatican
20fd8bb27046068cf1b2e6bec8cd5fc37537518a6eb86429893368547248d507	sg3appstore[.]net us3appstore[.]net	Vietnam
0b4b63b13674c56d9940cc84af5de0a24f693f0f7655c4ae5f792de4f111cee1	us3appstore[.]net bz3appstore[.]info sg3appstore[.]net maildantri[.]org	Vietnam

PoisonIvy droppers (sha256)	Campaign	C2	Target
fc6bcdb026d1d2217d88e2a127e1675a84ac12a8c3d1baa38b7583a47c73a95f			
481f6a7a8eb78ebdb982ebac0b4a4a1a0bbd2ccd85b81b22eb3c8ffb932c605f			
c527604c5e1269d95a5b7f724501d2835a6c2271b8a4748b63006226b3543acd			
c954abbf8e4d02e3ffbde27381a6d2c5c18213682bf5aa2bfb99e54be31a0878			
546079f7478555350c47e81e6619dcdd580ec9a73a7ec47a87487c83f891a62e	FDSTG	olk.olk4[.]com	Vatican
aaa6ebfc4dc8667b02e2f48770f65261d88329e723c461f427f07bfdf2da2914	FDSTG	olk.olk4[.]com	Vatican
bd0bfe71d1c5be1159b9e54bb69d248604cdbbe56bf3bd702dec81e0857a8f8d	FDSTG	olk.olk4[.]com	Vatican
00d78b376a44da4eeb9a81d84efc05920d2ddfd1c7ceecabffa746a653b90854	FDSTG	olk.olk4[.]com	Vatican
44e38c2a353735f4d95d6307610ae749568612ea38f22d717f028a2d23f5e352	FDSTG	olk.olk4[.]com	Vatican
4b141b9e87053010a91157cefb68c30c6ca27ab2951aee0105a37ea563034f39			Vatican
51ad3ca8d2a9f18d323c7bdc45dd581adbf7b0e39f6b5fa0b4206b061a03cbde			Vatican
68a0ae05aecf7abd9df83ea73ce54dc190c7f26f431be7493fc62ac20a2178ee			Vatican
69f92e69bad59f433e856262e8ae37c714becb3802f40307c44eae81623b4ad5	FDSTG	olk.olk4[.]com	Vatican
6c7cbfc2d8dc9991aff3baae1374a68922d0a67ec4c33f6ccb87f1a947412060			Vatican
805d3eb4903eb37dee15d8918d3e020facafa4a932719bccc0762c376067a8b5			Vatican
858593c8c3fc4a4022903dc690b8896d96a89b31d170d06ad7910447d5c8cbf4			Vatican
9029898e78e433f0bc7bba5dd9557278b0ffbfe3c7281b298e9736bc014c35eb			Vatican
bb259df4e2e61a14639bee8d28ef73750b504a69c7ad894f6f11f472815be84d			Vatican
c764116ca08afd5f46b0954ae496c724dd7cf3675faf13119689a8c556e72a51			Vatican
ed1b04527f195aabc0a34f0e0a94ec9b2a81692110e77d43699344336d8e9fc1			Vatican

fd31f38a4d49a37156704ec07bfb7bb6a38e759e577a3bf2f69daae550e340a2			Vatican
638c13fba454fb2aa92be5badcc0d89e75bb6bb1ffd9248240b0dfa7f04f604d		us3appstore[.]net	Vietnam
e60cff459f7cd69e1928101859294724ba4137ea8c8a600778f044ff7c4c12b4	usb0712	sg3appstore[.]net us3appstore[.]net	Vietnam
baef39ba772d6ce968a0ea8f270febe7ac3a450f326fc9eb71947c7fc021d9f2	usb0712	sg3appstore[.]net us3appstore[.]net	Vietnam
8bf9409d180b89a82a62175ec2f76ecd2a6cccc4728f2f1f86f6d248f9b6362d		us3appstore[.]net	Vietnam
8c00438ac47325b200586d14279bb8eb2401aac0a3fdab967d8f0fda8f631694	usb0712	sg3appstore[.]net us3appstore[.]net	Vietnam
f2c04d13fb2494bef47866ea05565965bea6e32ffa6ca5fabde0fc459a6dbac0		us3appstore[.]net	Vietnam
f907e59484a50afc50d373df9d556ae44bcc717b21eaf8190a154f230c83da1c		us3appstore[.]net	Vietnam
328fbe840a7c74e06c05e13e1b86adaedcf7410a56bb946da41af35766ac72dd	0811	sg3appstore[.]net us3appstore[.]net	Vietnam
4cfdc9e1257eeeab0af3647bbb06a114cd6bac134907bbe6f7b435a8dcb172db			
4fa7fbc53cbdabb078672673e6750ac734daf620e83bbea12b971391d16dd21b	testub	sg3appstore[.]net us3appstore[.]net	Vietnam
c47273ba9dafe017627020ca391a93462bf93de8480ed7e67ccdbea1b7105790	612	us3appstore[.]net	Vietnam
ff7ae2a93bd9d9d48eac6ed5a327ed994c0810f46789ef2a1b2f5dabeaa180c0			
abb0b520b0ce07cc75508ce65e745416c624554451fd84fed4a66e5eb4dc0ca2	0603	sg3appstore[.]net us3appstore[.]net	Vietnam
873e60018422e2c8a20b1d5b534934cc458c8a68ecbf86fccaad48197a4abc1c	140512	us3appstore[.]net	Vietnam
a1d1a4574bf12d3a73f3d8c6aee8f94f8cad6fb954add2e1a3d9e3a6ba95fc0d	140503	sg3appstore[.]net us3appstore[.]net	Vietnam
4e93e81467df7266f77c620f641b43b0125ed4759e7f14cb7a9a74c1d6ba1444			
a1ff375df189bbc7794c2de2fc3acfbcffb908e1aa3f79fce03dffa5bd2254ca	Jdntw	maildantri[.]org	
32011cbdd718852b787f7f822cf0a8cf8d5200a42f9a9cdca84375d941745fee			
9662bc8045aaae9c85f4af0d00dd0b83233375a2e613a21d7ad8acd63d38c57b	0518	www.nicstdcenter[.]com www.mistflying[.]com	
a70e4854f923ca744e24a17e45f35b71b42f2740921dd8893cd5ffbb682ab807	huawei	md.sony36[.]com	
f775233770c68ec90fa6d35e5fd94d4ff08f0dfc8a13c030d7e3f528637163bb	-	miconx.vicp[.]cc miconx.gnway[.]org miconx.gnway[.]net	
28125ad7ea11c485a854fa1354284b33f0ebf9c1a4783b6f2c20c6eddef021bc		vietnanmonline[.]com vatgla[.]com 43.248.9[.]226	Vietnam
bf36ebf2ac5ddc3df792b726b7f8b7789c6004152108ee54114f341ce4e17d8c		vietnanmonline[.]com vatgla[.]com 43.248.9[.]226	Vietnam
8abcbfe0f44726f898c1c288c4a5d3a84f1aa11a60156e28d125fffbf0b81ce6		vietnanmonline[.]com vatgla[.]com 43.248.9[.]226	Vietnam
6c58f0e82f54ff10252d5263b367049f4d30bc469b0a47e0d7f8c3ccd9d576c3	0726	vietnanmonline[.]com vatgla[.]com	Vietnam
c29ffe3aac7cc20cce54b9d9c3848ae64551eeb780264e351547914b7f742f7e		vatgla[.]com	Vietnam
4945c76afbc0ad140ac35ee4a07e3f2043a145c22101ff00f58939cb4834b849	0726	vietnanmonline[.]com vatgla[.]com	Vietnam
6710fdc8d383b6bc82ecff82b24a799ec8122bef538f6fd3991ea72f93450d1c		vietnanmonline[.]com vatgla[.]com	Vietnam
557f9b9512b3884e3bd80eb8d5527ecf29d0587bec7628a629ba8c09f28f7428			
032db8a2be0d8cabe66ea6b3a9befd9f36aaa2f650fd80ee4d929ca0f8619c49			
f488bafd1fc23dc2fcbb1ce5d77d8f3b7ebbc28811cbeac403f7dd889a1ca230			
98ca9314ecbd884e8280918c3fca52149982b132df6ec0e92b2a81e6152132e2			

03c8c275900502299767679ea6438d8845d2bb299a8de13b22ed56934aaf3992	PHI0805	www.nicstdcenter[.]com	PAF

Network indicators:

link.linkipv6[.]com
olk.olk4[.]com
vietnanmonline[.]com
vatgla[.]com
43.248.9[.]226
maildantri[.]org
sg3appstore[.]net
us3appstore[.]net
bz3appstore[.]info
popkaka.xicp[.]net
lookipv6[.]com

Document lure names:

1166-14-RS.doc
1223-14-RS.doc
1257.14.doc
1711-14-RS.doc
1737-14-RS.doc
1829-14-RS.doc
2360-14-RS.doc
2362-14-RS.doc
2568-14-RS.doc
2877-14-RS.doc
2985-14-RS.doc
3070-12-RS (2).doc
690-14-RS.doc
Accordo-Cronologia della proccedura.doc
amministratore diocesano di Alaminos.doc
amministratore diocesano di Kidapawan.doc
Appunto-Hung Sua Eminenza.doc
Appunto-Hung Sua Santità.doc
Appunto-Incontro del 17 settembre con Delegazione vietnamita-lavoro.doc
Appunto-PM Abe-Udienza Pontificia.doc
Appunto-PM Abe-Udienza Pontificia2.doc
Appunto-PM Abe-Udienza Pontificia3.doc
Appunto-PM Abe-Udienza Pontificia4.doc
Appunto-PM Abe-Udienza Pontificia5.doc
Appunto-Udienza Pontificia S.Eminenza (2).doc
Appunto-Udienza Pontificia SPadre, Sig.ra PM Shinawatra (2).doc
Appunto-Udienza Pontificia SPadre, Sig.ra PM Shinawatra OK (2).doc
Appunto-undienza amb Singapore.doc
appunto-visita Nguyen Sinh Hung.doc
Assemblea Plenaria della CBCP lavoro.doc
Assemblea Plenaria VN-757 riv.doc
auguri del Sig. PhamDung all'Ec.mo Segretario per i RR.SS. occasione nomina di Segretario di Stato Parolin.doc
avviso-ambasciatore Long.doc
camicia-appunto SP e SEm (2).doc
camicia-appunto SP e SEm 9-9-13 (2).doc
Cao.Appunto-Udienza Pontificia S.Ecc.zza, Sig.ra PM Shinawatra OK.riv3 (2).doc
Cao.Appunto-Udienza Pontificia S.Em, Sig.ra PM Shinawatra OK.riv3 (2).doc
Cao.Appunto-Udienza Pontificia SEm, Sig.ra PM Shinawatra OK.riv2 (2).doc
Cao.Appunto-Udienza Pontificia SPadre, Sig.ra PM Shinawatra OK.riv (2).doc
Cao.provv- Dipolog gio.doc
Cao.Provvista-Diocesi Vinh Long riv.doc
Cao.Situazione Sing 622 riv.doc
CAO-VIETNAM-NOTA VERBALE PUBBLICAZIONE ARCIVESCOVO HOCHIMINH VILLE.doc
Colpo di Stato Thailandia riv.doc
Corea S-APPUNTO COMFORT WOMEN allegato 3721.doc
Crisi politica-finale.doc
desiderio dell'Ambasciatore Thanh di salutare il Santo Padre.doc
Dichiarazione dei Vescovi vietnamiti contro Cina riv.doc
Direttorio Singapore 2014 riv.doc

Elezioni Thailandia 0986-feb-11-lavoro riv.doc
Festa del PP 598 riv.doc
festa del PP Thai gio.doc
Hung-lista di 8 membri-U-Pontificia.doc
Incontro V-2014- date dell' incontro -riv.doc
Incontro V-2014- date dell' incontro-1.doc
legge Amnistia 0725T nov lavoro2.doc
Lettera di Mons. Sotto-Segretario all'Ambasciatore riv.doc
lettera Sac. Doan Van.doc
NAM-Conferenza ministeriale Algeria.doc
Nuovo numero fax.doc
Offerta-residenza del RP HCM City riv.doc
osservazioni varie - Papal Foundation.doc
presa possesso-arcidiocesi Zamboanga.doc
proposta Mons. Barnabé Vescovo di Vinh Long-Prima Sezione.doc
Provv-Hanoi sup- kham.doc
Provv-Hanoi suplementare riv.doc
Provvista Hanoi 686-dic- lavoro4- gio.doc
Provvista Hanoi 686-riv.doc
Provvista Talibon riv.doc
Provvista-Coadiutore Xuan Loc 2014 riv.doc
pubblicazione - Ausiliare Long Xuyen.doc
pubblicazione rinuncia Card. Man + Mons. Doc Hochiminh Ville.doc
richiesta consenso gov. Coadiutore Xuan Loc.doc
richiesta consenso gov. Vescovo di My Tho.doc
richiesta PF-Sr. Hong MTG-DL.doc
Sing-Cattolici di Singapore promuovono raccolte fondi per la costruzione di un centro pastorale.doc
Situazione 716 finale-riv.doc
situazione politica 1148T finale.doc
Situazione Singapore 593 riv.doc
thai-Aggiornamento situazione politica thailand.doc
thai-anniversario 30 anni della visita JP2 riv.doc
Trasmissione consenso- Ausiliare di Long Xuyen.doc
Trasmissione consenso- Vescovo di My Tho.doc
URGE-Nota Verbale visita ai Musei Vaticani.doc
Vescovo di Danang Tri 706 gen riv.doc
Vietnam Visit 1989-2012.doc
Visita diocesi 717-riv.doc
Visita diocesi 756 riv.doc
Visita diocesi VN 759 finale.doc
visita in VN 733 marzo gio.riv.doc
visita Musei delegazione vietnamita NV riv.doc
visita Sig. Thanh 698 riv.doc

Indicators from Chapter 2: The Vatican intrusions.

Server007

Sha256	Filename	C2	Location
Payload DLL’s			
26b1f9754bb3931e4e41fd962436d2d1cecdabd8c46d22147b76907660f8caaa	wercplsupportex.dll	45.192.160[.]214	va
941a87d7e101b5ab26cae8be7bdd07dd52c63c03f7c77b7f60685cd976726f70	wercplsupportex.dll	45.192.160[.]214	va
a4edf18c5d625a18e2a2824075dfc973ff26f5c0b8023e4bb33ec772345ca03e	wercplsupportex.dll	45.192.160[.]214	va
4e7210bf099d45fa24eb7e99bb1e63b35298af2d4ba543802b23ce5b65571f93	wercplsupportex.dll	139.180.139[.]176	va
83ce4899b4083dd9d26d3ef3ea86ab2b9aab885ccba6a6f37264f417d3465ce0	n/a	www2.edao614[.]com	n/a
83e851ae7461a730022c567d4271aa30c950ba9c46f87c484c91da1a502b00f6	netsvc_os.5.dll	45.192.160[.]214	va

PlugX

Sha256	Filename	C2	Port	Loc.
Installers				
f96adc9e046ecc6f22d3ba9cfea47a4af75bcba369f454b7a9c8d7ca3d423ac4	kaseng.exe	192.225.226[.]123 192.225.226[.]217	80 443	va
6537fcbb157bde7acabc3a1a8bef266d7825573ed5ecee1408c495db3c913c60	kr.exe hanbiromon.exe	192.225.226[.]123 192.225.226[.]217	53 80 443	kr
8c16116b95b94511c3dfe5aa1fdb05078a88747bbd2ef9ebe305f90f1bbf604a		192.225.226[.]152	80 443	n/a
2404881d8ada053a15393696176342c87e179613d6ce6d0225dea74afdebdb9c		103.56.55[.]76	80 443	n/a
c80e3f51e3132ff146a93dfdde7c7878e16005bba92241833bf2f77a9e503278		safer.ddns[.]us 192.225.226[.]123 192.225.226[.]217	80 443	n/a
07cbbf072888b801d35f98ee29ade4f9b7fffafcc360c272e5307bfa1c2d1efa		safer.ddns[.]us 192.225.226[.]217	80 443	n/a
3f46de9df24fd146d75c906663e8f1ace300b147f0cea0370f38cb0088a158a4		192.225.226[.]217	80 443	n/a
Loader dll’s				
26dff84d992ad99e0fa1d01c9f3cd708b0614a8e05616d166793813ca10238a0	tmdbglog.dll			
29b5ffcda77acf5d1d14f8e1e57d2bed803dd493863377fdf48b3ca97126bdde	hpcustpartui.dll			va
653fe0ab7b634e50ba09f962c6357bcf76ce633768aa41dd01d1a93ef83a0a54	comserv.dll			va
92afd70ab9636e2c50995e94eb5cf281e2e7a0791ebd94126c45e5a24f53304f	tmdbglog.dll			
a7af90a0883778f75314560639150afc448ee12f0af1544dfa3b5b6b75e4b931	tmdbglog.dll			
ab1282afced126da7d330d7be338dfe1f3623970a696710e55a67fb549118f1d	tmdbglog.dll			va
ad48650c6ab73e2f94b706e28a1b17b2ff1af1864380edc79642df3a47e579bb	tmdbglog.dll			va
da1db9ebf26b10257b241d2e20368ab64e17fb4a148cf703de713d726dad236e	tmdbglog.dll			
fc5cadb7f7f6e5f7b0df795be3518322546ae4eaf9ab8b4f302392512dd5610c	tmdbglog.dll			

Sparkle

Sha256	Filename	C2	Port	Loc.
Payload dll				
305a4621079fd3f9b86f4f277559a696518f963cc62e6b9ee3a79e1316b4ac40	adobe_flashupdate.dll	192.225.226[.]152	443	va
f983da6dca83fab02428aa511d0716ea11eb0a262d24990733e65f5e7368a954	adobe_flashupdate.dll	192.225.226[.]153	80	va
Dropper executable				
de54c4df277f94279d9ebfd09b179f40bd97ae477dda219b25580b77c0fd3c0a	shovsts.exe	192.225.226[.]153	80	va

Kotibu/Gh0st Rat (QgptkagOckl variant).

Sha256	Filename	C2	Location
a291f94597974691ff581b308a5101753e7def9a9275c35d39858213254f4bb0	fastuserswitchingcompatibilitysex.dll	n/a	va

Kogina

Sha256	Filename	C2	Port	Loc.
Dropper executable				
3b75861c7ecff5303a0f1184d595c8d1496e08bb667a3afbfa84754b8b251df1	loader.exe	mail.chin-coj[.]com	80	va
ae97c9c9958d70ff4d7beba9d884b39195a64a60ad5ad03f477da3bd0ad70de8	loader.exe	mail.chin-coj[.]com	80	va
aff5c46be9d3cc3272597428c87d5f57ff21cc5c1c8a6f80f6e20924cb9c6bfd	loader.exe	N/A		va
Payload dll				
715fcf03c4bfa831dd23069f32012df77167a6769871ef36e8e4bddacf0c6c23	wmvdmooe3.dll	mail.chin-coj[.]com	80	va
c694d59281ab851f48af6e09129364fc2c27ef53028b07700ea5dc27830ab547	kavsrvc.dll	mail.chin-coj[.]com	80	va
65e705d3cb6b604af8437359dfe20f3daa0f26a94d41b7af1f7ac4f90e795fdc	wmvdmooe3.dll	N/A		va

“NewBounce”

Sha256	Filename	C2	Port	Loc.
Payload DLL’s				

5298bf36c489af136bcb69f9eb8d7700606006e3f702af771a9c0c74d784401b	twain.dll	lib.hostareas[.]com	80	va
9179358e6a4edb2b5ab1a6a7dd89affc8774f05878ca6578c59c0b0a2f0afc15	bingsvc.dll	host.miscrohost[.]com	80	va
d6f468c274536c6ce2705d2780b44b52d5d27d7614cae10ea57dc1689e703ba1	bingsvc.dll	mail.svrchost[.]com host.svchosts[.]com	80	n/a
1a8a518a7cc78a85f1c8dfe101a73813279599eececef1503548acfa848b1591	bingsvc.dll	login.achkus[.]com str.notepluses[.]com	80	va
da3911c8c77767ec218b8608fbfaf573450d0d91f6bc604d56822e5a00d65cfe	80.dll	192.225.226[.]217	80	va
c425e30a202f00b9d272bc864965ad9087c1596466f842871121c523b47638c2	conf.dll	122.0.0[.]22	80	n/a
f2e49841b342155d251b9dfda6ef2f8a632dcf93ec0b32b0d6c96fdc0e4e5a7d		121.127.253[.]119	80	n/a
481cbf4eb0f2c09174bf56b645a4f0fb3f4a17e4fdde91adcfa50c20fe8be172	s.exe	121.127.253[.]119	80	n/a
48bb8ff92c747fcd9da17e1cf7b7eba3fa039f502e9e5beb44ce3b17a8eb5d3c	s_exe.dll	121.127.253[.]119	80	n/a
e2d4b63023b3b81bebc9b5dcd810ac0b6d1edbede7a00edfa8999312e1b64f23	msvc3.dll	121.127.253[.]119	80	n/a
fa309edc46b58a364b91ef870e833d48727e6469ea8b76526ab8e88272d42542		121.127.253[.]119	80	n/a
Service executable				
4a7cf906c8cc871176d0702245953eeee5065f9651186cd8ae594e6835b8a8eb	s32.exe	192.225.226[.]217 192.225.226[.]123	8443	n/a
Rootkit component dropped by the above files				
96c0a4bde1d8fedd58215f91d3aaa49e65fb44275ecb15302ebabfc02350c47b	hfile_device.sys			va
cec59ba4fe49f48332f2a60df7ebb72ac86e6049b8ec09b0aa2bd9c9214e112e	pci358129.sys			n/a
ddb6bc2db796885a3e706c99918a8e3ba80826a9813ead7cb6b9999e1cae4b7f	nsip.sys			n/a
Service loader				
5e3d5f7d04ed48f27652f21d72c5915be147d0dd5bf0e92f1c26b38d5f4e1d7a	setup3.exe			va

Zupdax

Sha256	Filename	C2	Port	Location
Dropper EXE				
f56d87a87b52e86e669fb9b01e28caa8817e83a6fb8e1873faec70b15ae6bb72	a.exe	192.225.226[.]123 192.225.226{.[217	53	va
84b8bfe8161da581a88c0ac362318827d4c28edb057e23402523d3c93a5b3429	slack.exe	pop.playdr2[.]com mail.playdr2[.]com ns2.gamepoer7[.]com	110 25 53	n/a
d6af2d1df948e2221a4bdaa3dd736dc0646c95d76f1aa1a1d314e5b20185e161		192.225.226[.]218	443	n/a
f2ce101698952e1c4309f8696fd43d694a79d35bb090e6a7fd4651c8f41794a3		ns9.mcafee-update[.]com	53	n/a
4f8905c6e60ff76041603401ddb1e10dd137ed1755828c6ed93b1b65f033c7eb		ns1.symantec-inc[.]com	80	n/a
Sideloader DLL				
d62d56fd06381b78068f0fe3d9df14bbda8d2a9dcab5bd22db2f2a4391f53578	siteadv.dll			va
137a3cc8b2ecd98f7d6b787d259e66ca2c1dae968c785d75c7a2fecb4cbbcaf0	siteadv.dll			n/a
2360fa60a1b6e9705bf6b631fcfe53616f37738cf61bc0444ea94ce09c699c7f	siteadv.dll			n/a
Decoded main payload				
21ece9af55b384ca059953582b629d042f932acb690ef6d61cb2f27f03fbbd39	n/a	192.225.226[.]123 192.225.226[.]217	53	va
dd3cdfa8425a051c3dee9c9f35a5f150a8a89f93e3becc9335b2344509bd9469	n/a	pop.playdr2[.]com mail.playdr2[.]com ns2.gamepoer7[.]com	110 25 53	n/a
139e0c4dbdf7b60320d9935cbb658ec2acc7ab9bb6e291c2b77b4483d039f064	n/a	192.225.226[.]218	443	n/a

Rshell

Sha256	Filename	C2	Loc.
Dropper EXE			
192499ad69ec23900f4c0971801e7688f9b5e1dc5d5365d3d77cb9bf14e5fd73			
947f042bd07902100dd2f72a15c37e2397d44db4974f4aeb2af709258953636f	MT_nodel.exe		ru
b1d6ba4d995061a0011cb03cd821aaa79f0a45ba2647885171d473ca1a38c098			
c3415bddc506839614cbb7186bfc6643713806de4f5b1c15445e96a644b44bea	apple.exe		
d3a50abae9ab782b293d7e06c7cd518bbcec16df867f2bdcc106dec1e75dc80b	Петербургский международный экономический форум (ПМЭФ)____2019.exe		ru
f6c4c84487bbec5959068e4a8b84e515de4695c794769c3d3080bf5c2bb63d00	info.exe		ru
6bc77fa21232460c1b0c89000e7d45fe42e7723d075b752359c28a473d8dd1fd	POCKOCMOC_installer.exe		ru
Sideloader DLL			
a99612370a8407f98746eb0bf60c72393b1b4a23f52e7d7a6896471f85e28834	siteadv.dll		
35e36627dbbcb2b6091cc5a75ab26d9e5b0d6f9764bc11eb2851e3ebd3fbfe6e	siteadv.dll		
0bac8f569df79b5201e353e1063933e52cfb7e34cd092fc441d514d3487f7771	siteadv.dll		
467979d766b7e4a804b2247bbcdde7ef2bbaf15a4497ddb454d77ced72980580	siteadv.dll		
50f035100948f72b6f03ccc02f9c6073c9060d6e9c53c563a3fdb1d0c454916e	siteadv.dll		
Main payload			
949cb5d03a7952ce24b15d6fccd44f9ed461513209ad74e6b1efae01879395b1	cc.tmp	207.148.121[.]88	
56b9648fd3ffd1bf3cb030cb64c1d983fcd1ee047bb6bd97f32edbe692fa8570	cc.tmp	207.148.121[.]88	
69863ba336156f4e559364b63a39f16e08ac3a6e3a0fa4ce11486ea16827f772	cc.tmp	207.148.121[.]88	
3ccae178d691fc95f6c52264242a39daf4c44813d835eaa051e7558b191d19ee	cc.tmp	207.148.121[.]88	
7b7a65c314125692524d588553da7f6ab3179ceb639f677ed1cefe3f1d03f36e	cc.tmp	207.148.121[.]88	

Gravy (GravityProxy)

Sha256	Filename	Loc.
Injector		
0253e700764a008b2e724e1d24718594ff8ff4b138298b5a0d79f0a42503938f		va

NBTScan

Sha256	Filename	Loc.
Netbios scanner		
7e8285c0a9c91484e56a34ebdde05fca01f846a4e626de92e64c1dd95876a96d	nbt1.exe	va

ScanLine

Sha256	Filename	Loc.
Port scanner		
eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0	sl.exe	va

WmiExec

Sha256	Filename	Loc.
Remote execution of WMI commands		
110592b76e8aced859a4cd5707abbd5e680bcff2b2c8825b562ca6e8f1aaf94f	wmi.vbs	va
cb73caaad556bc5ea480fc349a375f4a057827306bd22fe0b68450e18d4711a1	w1.vbs	va

Network indicators:

192.225.226[.]123
192.225.226[.]152
192.225.226[.]153
192.225.226[.]217
192.225.226[.]218
pop.playdr2[.]com
mail.playdr2[.]com
ns2.gamepoer7[.]com
ns9.mcafee-update[.]com
ns1.symantec-inc[.]com
lib.hostareas[.]com
host.miscrohost[.]com
mail.svrchost[.]com
host.svchosts[.]com
login.achkus[.]com
str.notepluses[.]com
mail.chin-coj[.]com
www2.edao614[.]com
103.56.55[.]76
45.192.160[.]214
139.180.139[.]176
121.127.253[.]119
207.148.121[.]88

APPENDIX 2: YARA DETECTION RULES

```
rule Sparkle
{
	meta:
		author = "Snorre Fagerland, Norton Labs"
	strings:
		$ = "X-XSS-Protection: 1; mode=block"
		$ = "Server: gws"
		$ = "a780d739c44a5d7c"
	condition:
		all of them
}
rule Server007
{
	meta:
		author = "Snorre Fagerland, Norton Labs"
	strings:
		$a1 = "http://%s:%d/ask/main"
		$b1 = "_green_ver_"
		$b2 = "_exp_ver_"

		$c1 = "sc config %s slSet\\Services\\%s%SYSTEMROOT%\\sys/v ServiceDll /t@echo off"
	condition:
		($a1 and $b1 and $b2) or $c1
}
rule P1RatLoader
{
	meta:
		author = "Snorre Fagerland, Norton Labs"
	strings:
		$ = "P1Rat_2017"
		$ = "install_and_del" wide
	condition:
		all of them
}
```

```
rule Newbounce
{

	meta:
		author = "Snorre Fagerland, Norton Labs"
	strings:
		$ = "GAEncryptfasdfafhhIlove!!@#$!@$!@$#%!"
	condition:
		all of them
}
rule Zupdax
{
	meta:
		author = "Snorre Fagerland, Norton Labs"
	strings:
		$ = "\\AdobeBak\\Proc.dat" ascii wide
		$ = "software\\XXZH" ascii wide
		$ = "%s\\updata\\connect" ascii wide
	condition:
		any of them
}
```

```
rule Kogina
{
        meta:
                author = "Snorre Fagerland, Norton Labs"
        strings:
                $ = { 48 89 5C 24 08 57 48 83 EC 20 C6 44 24 40
                01 4C 8D 41 20 48 2B D1 41 B9 20 00 00 00 42 8A
                44 02 E0 41 88 40 20 41 88 00 49 FF C0 49 FF C9
                75 EC B3 07 48 8D 79 40 48 8D 54 24 40 48 8B CF
                E8 [4] FE CB 75 EF 48 8B 5C 24 30 48 83 C4 20 5F C3  }
        condition:
                all of them
}

rule Kotibu_Gh0st
{
        meta:
                author = "Snorre Fagerland, Norton Labs"
        strings:
                $ = "QgptkagOckl" ascii
        condition:
                all of them
}


rule RShell
{

        meta:
                author = "Snorre Fagerland, NortonLifeLock Inc"
        strings:
                $="Begin gethostbyname"
                $="End gethostbyname"
                $="Software\\CLASSES\\KmpiPlayer" wide
                $="[RS5] WAIT_TIMEOUT"
        condition:
                all of them
}
```

REFERENCES

[1] C. Cimpanu, "Chinese state hackers target Hong Kong Catholic Church," 15 July 2020. [Online]. Available: https://www.zdnet.com/article/chinese-state-hackers-target-hong-kong-catholic-church/.

[2] Recorded Future, "Chinese State-Sponsored Group ‘RedDelta’ Targets the Vatican and Catholic Organizations," 28 July 2020. [Online]. Available: https://www.recordedfuture.com/reddelta-targets-catholic-organizations/.

[3] Proofpoint, "TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader," 23 November 2020. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader.

[4] Arkbird, "The #APT Mustang Panda group targets the Vatican state with lures," 14 July 2020. [Online]. Available: https://twitter.com/Arkbird_SOLG/status/1283000270151208960.

[5] Ucanews, " China, Vatican negotiate further on bishop appointments," [Online]. Available: https://www.ucanews.com/news/china-vatican-negotiate-further-on-bishop-appointments/75132# .

[6] B. Rogers, "Rome’s dangerous gamble in China," [Online]. Available: https://catholicherald.co.uk/romes-dangerous-gamble-in-china/.

[7] New York Times, "China and Vatican Reach Deal on Appointment of Bishops," [Online]. Available: https://www.nytimes.com/2018/09/22/world/asia/china-vatican-bishops.html.

[8] M. Sainsbury, "Vatican tries to reassure critics of deal with China on bishops," Ucanews.com, [Online]. Available: https://www.ucanews.com/news/vatican-tries-to-reassure-critics-of-deal-with-china-on-bishops/89768.

[9] Mitre, "Hijack Execution Flow: DLL Search Order Hijacking," [Online]. Available: https://attack.mitre.org/techniques/T1574/001/.

[10] VirusTotal, "0b4b63b13674c56d9940cc84af5de0a24f693f0f7655c4ae5f792de4f111cee1," [Online]. Available: https://www.virustotal.com/gui/file/0b4b63b13674c56d9940cc84af5de0a24f693f0f7655c4ae5f792de4f111cee1.

[11] Archive.org, "Shapeless on SWERAT forums," [Online]. Available: https://web.archive.org/web/20080724191418/http://www.swerat.com/forums/index.php?showuser=112.

[12] Bangkok Post, "Pope Francis accepts PM's invitation to visit Thailand," [Online]. Available: https://www.bangkokpost.com/learning/advanced/369531/pope-francis-accepts-pm-invitation-to-visit-thailand.

[13] AsiaNews, "Cattolici di Singapore promuovono raccolte fondi per la costruzione di un centro pastorale," [Online]. Available: http://www.asianews.it/notizie-it/Cattolici-di-Singapore-promuovono-raccolte-fondi-per-la-costruzione-di-un-centro-pastorale-31163.html.

[14] Safebit, "PlugX-т өртсөн системийг цэвэрлэх нь," Safebit, 11 2015. [Online]. Available: http://blog.safebit.mn/2015/11/plugx.html.

[15] F. Perigauld, "PlugX “v2”: meet “SController”," Airbus cybersecurity, [Online]. Available: https://airbus-cyber-security.com/plugx-v2-meet-scontroller/.

[16] C. Mercer, "JTB Breach Leaks 7.93 Million Customer Related Records," NSFocus, [Online]. Available: https://blog.nsfocusglobal.com/threats/jtb-breach-leaks-7-93-million-customer-related-records/.

[17] Team Cymru, "#totalhash," Team Cymru, [Online]. Available: https://totalhash.cymru.com/search/?ip:103.246.245.61.

[18] A. Hinchliffe and M. Harbison, "Farseer: Previously Unknown Malware Family bolsters the Chinese armoury," Palo Alto Networks, [Online]. Available: https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/.

[19] A. Hinchliffe, M. Harbison, J. Miller-Osborn and T. Lancaster, "HenBox: The Chickens Come Home to Roost," Palo Alto Networks, [Online]. Available: https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/.

[20] A. Hinchliffe, "PKPLUG: Chinese Cyber Espionage Group Attacking Southeast Asia," Palo Alto Networks, [Online]. Available: https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/.

[21] Hauri, "Hauri Security Magazine, vol 2, 2018," [Online]. Available: https://www.hauri.co.kr/security/download.php?idx=MTIx.

[22] Y. Gu, "UDP-Based Data Transfer," [Online]. Available: https://udt.sourceforge.io/.

[23] Australian Cyber Security Centre, "Manic Menagerie:Malicious activity targeting web hosting providers," Australian Cyber Security Centre, [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-04/report_manic_menagerie.pdf.

[24] CyCraft, "Taiwan Government Targeted by Multiple Cyberattacks in April 2020," CyCraft, [Online]. Available: https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-3b20cea1dc20.

[25] Blackberry Cylance, "Reaver: Mapping Connections Between Disparate Chinese APT Groups," Blackberry Cylance, [Online]. Available: https://blogs.blackberry.com/en/2019/05/reaver-mapping-connections-between-disparate-chinese-apt-groups.

[26] M. Tartare, "Operation StealthyTrident: corporate software under attack," welivesecurity.com, [Online]. Available: https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/.

[27] _re_fox, "Hadn't seen this one mentioned.," [Online]. Available: https://twitter.com/_re_fox/status/1281413534904209410.

[28] BlackBerry Cylance, "Threat Spotlight: Breaking Down FF-Rat Malware," BlackBerry Cylance, [Online]. Available: https://blogs.blackberry.com/en/2017/06/breaking-down-ff-rat-malware.

[29] J. Miller-Osborn and J. Grunzweig, "Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets," Palo Alto Networks, [Online]. Available: https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/.

[30] SecureWorks, "BRONZE PRESIDENT Targets NGOs," SecureWorks, [Online]. Available: https://www.secureworks.com/research/bronze-president-targets-ngos.

[31] McAfee, "MVISION Insights: Reddelta Threat Group," McAfee, [Online]. Available: https://kc.mcafee.com/corporate/index?page=content&id=KB93301&locale=en_US.

[32] I. Sanmillan, "Operation NightScout: Supply-chain attack targets online gaming in Asia," Welivesecurity.com, [Online]. Available: https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/.

[33] T. Q. Ngan, "ElephantRAT (Kunming version): our latest discovered RAT of Panda and the similarities with recently Smanager RAT," VinCSS, [Online]. Available: https://blog.vincss.net/2021/02/re020-elephantrat-kunming-version-our-latest-discovered-RAT-of-Panda.html.

[34] VirusTotal, "b1d6ba4d995061a0011cb03cd821aaa79f0a45ba2647885171d473ca1a38c098," VirusTotal, [Online]. Available: https://www.virustotal.com/gui/file/b1d6ba4d995061a0011cb03cd821aaa79f0a45ba2647885171d473ca1a38c098/detection.

[35] "PKPLUG: Chinese Cyber Espionage Group Attacking Southeast Asia," Palo Alto Networks, [Online]. Available: https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/.

[36] "VirusTotal," VirusTotal, [Online]. Available: https://www.virustotal.com/gui/domain/www.sunleon.com/relations.