Friend or foe? probably both.
Overview
What I’ll be going through in this presentation

1. **Introduction**: Who am I and what do I do

2. **Myanmar**: A long time victim
   - 2.1. Recent activity: politically motivated attacks
   - 2.2. An overview of recent attacks
   - 2.3. Identifying groups

3. **Mofang**
   - 3.1. History, Targets, Attribution
   - 3.2. Modus Operandi
   - 3.3. Tools
     - 3.3.1. ShimRat
     - 3.3.2. ShimRatReporter
   - 3.4. Campaigns against Myanmar
   - 3.5. Campaign overview

4. **Closing & report publication**
Perform threat intelligence analysis at keeping track of current events and gain insight into upcoming threats.

I do my part in:

• Malware analysis (reverse engineering)
• Network Forensics
• Programming
• OSINT

My focus is on espionage related cases and gain insight into the groups behind attacks, their motivation and their targets.
2. **Myanmar**: A long time victim
Myanmar... Burma?

- Became a British colony in the 19th century
- Gained independence in 1948
- Initially became a democratic nation
- Became a military dictatorship in 1962
- Military renamed Burma to Myanmar
- “Republic of the Union of Myanmar"
Government sites leveraged to target individuals and organisations using a wide variety of tools including:

- PlugX
- EvilGrab
- Trochilus RAT
- Additional ‘unknown’ malware (mostly loaders)
Recent uptick in activity is being noticed

- **Unit 42:** Evilgrabs Delivered by Watering Hole Attack on President of Myanmar’s Website  
  [Link](http://researchcenter.paloaltonetworks.com/2015/06/evilgrabs-delivered-by-watering-hole-attack-on-president-of-myansars-website/)

- **Citizenlab:** Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites  
  [Link](https://citizenlab.org/2015/10/targeted-attacks-ngo-burma/)

- **Citizenlab:** Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns  
  [Link](https://citizenlab.org/2016/04/between-hong-kong-and-burma/)

- **ASERT:** PlugX Threat Activity in Myanmar  
  [Link](http://pages.arbornetworks.com/rs/082-KNA-087/images/ASERT%20Threat%20Intelligence%20Brief%202015-05%20PlugX%20Threat%20Activity%20in%20Myanmar.pdf)

- **ASERT:** Uncovering the Seven Pointed Dagger  
We try to identify the groups or at least be able to uniquely identify an attack. We do this based on a set of information available to us from the attacks. We use (a combination of) the following ‘classifiers’:

- **Tools**
  - Custom tools
  - Publicly available tools (or widely used tools)

- **Methods of delivery**
  - Email (attachment, link to download a file)
  - Wateringhole (0day)

- **Infrastructure**
  - Type of infrastructure
  - Overlapping infrastructure
  - Domains (registrar, name pattern)
Group: GovX(?)

Tools:
- PlugX (semi-public)
- Loader (private)

Method of delivery:
- Email with attachment
- Attachment loads PlugX from a (compromised) Myanmar government website

Infrastructure:
- Subdomains on an already known domain
- Partially shared IPs from other campaigns(?)
Group: GovX(?)

PlugX download locations:
- eyangon.gov.mm/news/update.exe
- www.moi.gov.mm/mmpdd/sites/default/files/field/moigov.exe
- www.mofa.gov.mm/wp-content/plugins/mmm_list/ministry.exe

C2 infrastructure under *.websecexp.com:
- webhttps.websecexp.com
- ns.websecexp.com
- dns.websecexp.com
- usagovdns.websecexp.com
- usafbi.websecexp
Tools:
- PlugX (semi-public)

Method of delivery:
- Email with a link or attachment
- Attachment contains a packed PlugX payload

Infrastructure:
- Subdomains on an already known domain
- Partially shared IPs from other campaigns(?)
## Group: NewsX (lures)

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Packed</th>
<th>Type</th>
<th>Modified</th>
<th>CRC32</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td></td>
<td></td>
<td>File folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>president-office</td>
<td></td>
<td></td>
<td>File folder</td>
<td>12/23/2014 4:16 PM</td>
<td>030E5664</td>
</tr>
<tr>
<td>The bureaucracy’s keen young clerks.lnk</td>
<td>1,389</td>
<td>639</td>
<td>Shortcut</td>
<td>3/9/2015 2:34 PM</td>
<td>7FB648A5</td>
</tr>
</tbody>
</table>

Friend or Foe? probably both.

Myanmar: A long time victim
Friend or Foe? probably both.

Group: NewsX (lures)

2. Myanmar: A long time victim
Friend or Foe? probably both.

Myanmar: A long time victim
Friend or Foe? probably both.

Group: NewsX (lures)

The bureaucracy’s keen young clerks

For more information, please read.

Please unzip the file to your desktop.

In the old days it wasn’t easy to get to know Myanmar government officials. The system was designed to discourage too much fraternization with visiting foreigners.

This has changed rapidly and radically. In half-a-decade the bureaucracy, numbering about one million people, has shifted its priorities. Secrecy and hesitation previously trumped any enthusiasm for contact, creativity, initiative or risk-taking.

Myanmar: A long time victim
In the old days it wasn’t easy to get to know Myanmar government officials. The system was designed to discourage too much fraternization with visiting foreigners.

This has changed rapidly and radically. In half-a-decade the bureaucracy, numbering about one million people, has shifted its priorities. Secrecy and hesitation previously trumped any enthusiasm for contact, creativity, initiative or risk-taking.

For more information, please read.

Please unzip the file to your desktop.

In the old days it wasn’t easy to get to know Myanmar government officials. The system was designed to discourage too much fraternization with visiting foreigners.

This has changed rapidly and radically. In half-a-decade the bureaucracy, numbering about one million people, has shifted its priorities. Secrecy and hesitation previously trumped any enthusiasm for contact, creativity, initiative or risk-taking.
2. **Myanmar**: A long time victim

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Packed</th>
<th>Type</th>
<th>Modified</th>
<th>CRC32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kokang</td>
<td></td>
<td></td>
<td>File folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kokang Rebels</td>
<td></td>
<td></td>
<td>File folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>China Protests Burma Border Air Raid That Kills 4 Chinese.Ink</td>
<td>1,779</td>
<td>619</td>
<td>Shortcut</td>
<td>3/15/2015 5:01 PM</td>
<td>33984A3F</td>
</tr>
<tr>
<td>China sends fighter jets to Burma border after bomb kills four.doc</td>
<td>20,480</td>
<td>2,623</td>
<td>Microsoft Word 97 - 2003 Document</td>
<td>3/15/2015 5:13 PM</td>
<td>1C7BD999</td>
</tr>
<tr>
<td>Welcome to <a href="http://www.thithtoolwin.com">www.thithtoolwin.com</a></td>
<td>326,841</td>
<td>282,456</td>
<td>MS-DOS Application</td>
<td>3/15/2015 4:46 PM</td>
<td>74C00C25</td>
</tr>
</tbody>
</table>
Friend or Foe? probably both.

Myanmar: A long time victim
**Group: NewsX (lures)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Packed</th>
<th>Type</th>
<th>Modified</th>
<th>CRC32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kokang</td>
<td></td>
<td></td>
<td>File folder</td>
<td>1/8/2015 11:11 PM</td>
<td></td>
</tr>
<tr>
<td>Kokang Rebels</td>
<td></td>
<td></td>
<td>File folder</td>
<td>1/3/2015 3:44 PM</td>
<td></td>
</tr>
<tr>
<td>China Protests Burma Border Air Raid That Kills 4 Chinese.Ink</td>
<td>1,779</td>
<td>619</td>
<td>Shortcut</td>
<td>3/15/2015 5:01 PM</td>
<td>33984A3F</td>
</tr>
<tr>
<td>China sends fighter jets to Burma border after bomb kills four.doc</td>
<td>20,480</td>
<td>2,623</td>
<td>Microsoft Word 97 - 2003 Document</td>
<td>3/15/2015 5:13 PM</td>
<td>1C7BD999</td>
</tr>
<tr>
<td>Welcome to <a href="http://www.thithtoolwin.com">www.thithtoolwin.com</a></td>
<td>326,841</td>
<td>282,456</td>
<td>MS-DOS Application</td>
<td>3/15/2015 4:46 PM</td>
<td>74C00C25</td>
</tr>
</tbody>
</table>

2. **Myanmar: A long time victim**
Friend or Foe?

probably both.

Group: NewsX (lures)

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Packed</th>
<th>Type</th>
<th>Modified</th>
<th>CRC32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kokang</td>
<td></td>
<td></td>
<td>File folder</td>
<td>1/8/2015 11:11 PM</td>
<td></td>
</tr>
<tr>
<td>Kokang Rebels</td>
<td></td>
<td></td>
<td>File folder</td>
<td>1/13/2015 3:44 PM</td>
<td></td>
</tr>
<tr>
<td>China Protests Burma Border Air Raid That Kills 4 Chinese.Ink</td>
<td>1,779</td>
<td>619</td>
<td>Shortcut</td>
<td>3/15/2015 5:01 PM</td>
<td>33984A3F</td>
</tr>
<tr>
<td>China sends fighter jets to Burma border after bomb kills four.doc</td>
<td>20,480</td>
<td>2,623</td>
<td>Microsoft Word 97 - 2003 Document</td>
<td>3/15/2015 5:13 PM</td>
<td>1C7B9999</td>
</tr>
<tr>
<td>Welcome to <a href="http://www.thithtoolwin.com">www.thithtoolwin.com</a></td>
<td>326,841</td>
<td>282,456</td>
<td>MS-DOS Application</td>
<td>3/15/2015 4:46 PM</td>
<td>74C00C25</td>
</tr>
</tbody>
</table>

China sent fighter jets to its border with neighboring Burma on Saturday and lodged a diplomatic protest after it said a Burmese warplane dropped a bomb on Chinese territory, killing four people.

The incident occurred as Burma's government stepped up its fight against ethnic Chinese rebels in the country's Kokang region along China's southwestern border.

The upsurge in fighting in recent weeks has sent thousands of people fleeing across the border into China's Yunnan province.

China “strongly condemns” the incident and calls on Burma to carry out a thorough investigation, report the findings to China, punish the guilty and take steps to ensure similar events do not occur, the ministry said in a statement.

2. Myanmar: A long time victim
Friend or Foe? probably both.

Myanmar: A long time victim

China’s government stepped up its fight against ethnic Chinese region along China’s southwestern border.

The incident and calls on Burma to carry out a thorough investigation into the alleged attacks on its territory.

2. **Myanmar**: A long time victim
China protests over 'deadly Myanmar border raid'

14 March 2015 | Asia

Myanmar: A long time victim
A lot of groups re-use known tools which can make it really difficult to figure out if they are a new group or part of the same group. This is where working out a M.O can help out a lot.

While I was mapping out groups I stumbled upon a group that has been able to hide amongst all the other groups and has not been publicly known until now. The same goes for the custom malware they have been writing and using since early 2012.

This group’s approach is methodical and their modus operandi shows dedication.
Friend or Foe? probably both.

3. Mofang
Mofang

Tools:
- ShimRat (private)
- ShimRatReporter (private)
- Various loaders (private)

Method of delivery:
- Email with a link or attachment
- Attachment contains lures with embedded ShimRat or ShimRatReporter

Infrastructure:
- Specialised infrastructure per victim campaign
- Shared IPs and Domains over a ‘global campaign’
Mofang: Introduction

The name Mofang is based on the Mandarin verb 模仿 (Mófǎng), which means to imitate. Imitation, in this case imitation of a target’s infrastructure, is a defining feature of their modus operandi.

The Mofang group uses custom malware that dates back to at least February 2012.

By our estimation, the Mofang group is a group that operates out of China and is probably government- affiliated. Our research into the geopolitical and economic factors in relation to the campaigns of Mofang resulted in a hypotheses about the ‘why’ of these campaigns. The full picture, however, will probably remain unknown since there is obviously no easy insight in their actual agenda and goals.
Mofang: Attribution

Lure documents contain metadata that suggests they were created with WPS Office. This product, also known as Kingsoft Office, is a Chinese product comparable to Microsoft Office. Artifacts can be seen in document metadata. Simplified Chinese is set as the character set in many of the resources inside various malware samples.
Early versions of the ShimRat malware showed something interesting in their C2 communication protocol.
Friend or Foe?
probably both.

Mofang:

Beat him.
'Yuok Yerr' is an approximate phonetic representation of the Cantonese 郁佡, beat him or kill him.

It suggests at least passive knowledge of Cantonese on the part of the malware author.
The most compelling evidence that supports this hypothesis is the fact that the targets and campaigns known so far can be correlated to important geopolitical events and investment opportunities that align with Chinese interests.

- Companies that are involved with investment possibilities that also involve Chinese state owned organisations, become targets;

- Government agencies or companies that play a role in deciding about Chinese investments, become targets;
Friend or Foe? probably both.

Mofang: Attribution

- Government
- Military
- Critical Infrastructure
- Automotive Industry*
- Weapon Industry*

*R&D departments specifically
We have some certainty they started in 2012. No samples before 2012 and early versions had embedded project folders:

- `z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\installscript\`
- `z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\serviceapp\`
- `z:\project2012\remotecontrol\winhttpnet\cqgaen\app\installscript\`
- `z:\project2012\remotecontrol\winhttpnet\cqgaen\app\serviceapp\`
Mofang: History

Friend or Foe? probably both.

Mofang

Mofang: Modus Operandi

The Mofang group uses custom malware that dates back to at least February 2012. The two tools used in their campaigns are:

- ShimRat
- ShimRatReporter

As far as known, the Mofang group has never used exploits to infect targets, instead relying heavily on social engineering in order to successfully infect targets. The only exploits the group uses are privilege elevation exploits built into their own malware.
Mofang: Modus Operandi

The Mofang group has a distinct method of carrying out attacks using these two tools, with the goal of stealing information. In short, their method can be summarised as follows:

1. **Initial reconnaissance compromise**: an initial compromise is performed on specific employees of a targeted organisation with the aim of extracting key information about the target infrastructure to be used in stage 2. This attack is performed using ShimRatReporter.

2. **Faux infrastructure setup**: the group sets up (external) infrastructure designed to avoid attracting attention;

3. **The main compromise**: the group attacks the organisation with ShimRat.
Two custom tools created and used by the Mofang group:

**ShimRat**: their ‘main’ tool which provides control over a victim’s machine.

**ShimRatReporter**: reconnaissance tool, builds a ‘report’ and loads ShimRat
Mofang: Tools - ShimRat

Build up of two components:

- **InstallScript**: first stage, takes care of persistence
- **ServiceApp**: second stage, performs the C2 communication and executes the operator’s commands

Extended over the years:

- **Persistence**: originally only startup keys and services, Shims were added in 2015
- **Privilege elevation**: a method to bypass Windows UAC was implemented. It leverages a DLL hijacking technique on Migwiz, a publicly known bug.
In 2012 ShimRat would be send without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
In 2012 ShimRat would be sent without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
In 2012 ShimRat would be send without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
Mofang: Tools - ShimRat

In 2012 ShimRat would be send without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
In 2012 ShimRat would be send without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
In 2012 ShimRat would be sent without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
Mofang: Tools - ShimRat

In 2012 ShimRat would be send without any packaging, just social engineering through the filename. This changed in 2013, a method currently still used:
ShimRat has three methods of becoming persistent on a system:

1. Installing a registry startup key
2. Installing a service
3. Install a shim

ShimRat contains a persistence configuration block. This block specifies the persistence info used as well as the persistence mode:

1. Persistence through a service
2. Persistence through Shims

<table>
<thead>
<tr>
<th>Service description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service title</td>
</tr>
<tr>
<td>Installation folder</td>
</tr>
<tr>
<td>Injection target process</td>
</tr>
<tr>
<td>Installation mode</td>
</tr>
</tbody>
</table>
Over the years Microsoft has focussed a lot of time and energy into backward compatibility. One of the solutions to do this was the implementation of the Application Compatibility Framework ACF in short.

This framework allows small fixes to be applied on specific versions of certain applications. Essentially hotpatching applications with fixes.
Mofang: Tools - ShimRat - Shims

ShimRat manually performs the installation steps to ensure it is not listed in the installed updates sections, it installs a custom fix.

First, it copies an SDB file and the .dat and .dll to the appropriate location:

• `%WINDIR%\AppPatch\Custom\` (32 bit)
• `%WINDIR%\AppPatch\AppPatch64\Custom\` (64 bit)

Second, it registers itself in the registry:

• HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom
• HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB

It finishes by calling `SdbRegisterDatabaseEx` to register itself and `ShimFlushCache`. 
<table>
<thead>
<tr>
<th>Platform</th>
<th>x86</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Clengine_Shim</td>
</tr>
<tr>
<td>Application name</td>
<td>Clengine_Apps</td>
</tr>
<tr>
<td>Database name</td>
<td>Clengine_Database</td>
</tr>
<tr>
<td>Type of fix</td>
<td>InjectDLL</td>
</tr>
<tr>
<td>Injection target</td>
<td>svchost.exe</td>
</tr>
<tr>
<td>Injection DLL</td>
<td>elogger.dll</td>
</tr>
</tbody>
</table>
ShimRat talks to an HTTP (or HTTPS) server that is configured in the RAT.

The proxy username and password are usually configured after an initial compromise with ShimRatReporter which gathers this information.
**Mofang: Tools - ShimRatReporter**

First seen in 2014, never ‘packed’ and used in the first step of the attack planning.

It builds up a report from the victim’s machine:

- **Network information**
- **Operating system information**
- **Active processes information**
- **Browser and proxy configuration**
- **Active user sessions**
- **User accounts**
- **Installed software**
Friend or Foe? probably both.

Mofang: Myanmar
Mofang: Myanmar

Mofang has had a focus on Myanmar since their start in 2012.

Over the years the targets became more specific and at this point it paints a quite clear and interesting picture of the goal of their operations.
Mofang: Myanmar

May 2012, a command and control server gate path:

commerce.gov.mm/templates/css1/logon.php
Friend or Foe? probably both.

Mofang: Myanmar

June 2015, a ShimRat payload was staged from:

203.81.162.178/text.txt
Mofang: Myanmar

September 2015, a ShimRat payload lure was staged from: www.flymna.com/sites/photo.tar
Mofang: Myanmar

One of Mofang’s most extensive campaigns requires historical knowledge to understand the extend and reasoning behind it.

This campaigns goes back to events starting in 2009 and unfolding over the years with a lot of activity in the summer of 2015 and ending in January 2016.
In 2009 China and Myanmar signed a memorandum of understanding for China to build a seaport and a pipeline from Kyaukpyu to mainland China.

With this seaport they would save some 5,000 km and not have to pass through the strait of Malacca.
In 2009 China and Myanmar signed a memorandum of understanding for China to build a seaport and a pipeline from Kyaukpyu to mainland China.

With this seaport they would save some 5,000 km and not have to pass through the strait of Malacca.
From 2009 on Myanmar has had a large increase of foreign investments. It grew from a reported 300 million USD in 2009-2010 it grew to 20 billion in 2010-2011.

To further increase and facilitate foreign investment, the government of Myanmar established special economic zones (SEZs). These zones are supposed to encourage economic growth and foreign investments even more. These SEZs would give investors a variation of tax reliefs, 5 year tax holidays as well as longer land leases.
In 2011 Myanmar established the **Central Body for the Myanmar Special Economic Zones**, a regulatory body which would oversee foreign investments in the SEZs.

In the same year the SEZ law and Dawei law were also passed, establishing a set of three SEZs in Myanmar. The current SEZs under development in Myanmar are:

- Dawei SEZ
- Thilawa SEZ
- Kyaukphyu SEZ
Friend or Foe? probably both.

Mofang:
Mofang: Myanmar

Myanmar started a consulting tender for the **Kyaukphyu SEZ** in 2013. To pick a consortium that would become the advisor for the Kyaukphyu SEZ and oversee operations and decisions on certain investments.

In late September 2013 this tender closed and in early March 2014 the results were presented. A consortium led by the **CPG Corporation**, a company originating from Singapore, was the winner and would become the SEZ consultant. One of the other consortia was lead by the **CITIC** group.
Friend or Foe? probably both.

Mofang: Myanmar

In 2014 there was another tender, this time to set up infrastructure in the SEZ. This tender closed in November 2014 and results would be put out early 2015.

The date of the publication of the tender outcome passed but no information was published. In late June the Myanmar government still had not put out any word who would win infrastructure investments for the SEZ. One of the contenders for this tender was China’s CITIC group.
At this point Mofang had acquired their target: CPG Corporation
Spear phishing attacks started in June 2015 with a really unique lure. In order to display the characters of the Burmese language additional software is usually installed. This software makes it possible to give proper input in Burmese. These special fonts that were installed are called ‘Zawgyi’ fonts.
Mofang: Myanmar - CPG Corporation

ShimRatReporter was send named as ‘AlphaZawgyl_font.exe’. It was configured to send out its report to:

library.cpgcorp.org/links/images/file/blanks.php

Additionally later samples were configured to download ShimRat from either two locations:

library.cpgcorp.org/links/images/blanks.jpg
secure2.sophosrv.com/en-us/support/blanks.jpg
ShimRat samples in this campaign were configured to connect to:

secure2.sophosrv.com/en-us/support/ms-cache_check.php
The actual publication of the outcome of the infrastructure tender was postponed until the start of 2016. Early 2016 the results came:

China’s CITIC group had won the tender

This allowed China to continue building upon their gas and oil infrastructure as well as the seaport.
Friend or Foe? probably both.

Mofang: India

Every year the Indian government holds an event called the **MSME DEFEXPO**.

This event allows MSMEs to show their current and new capabilities in the defense and aerospace technology to various government agencies.

Over the years, its exhibitors have been a continuing target for the Mofang Group.
Mofang: India

Spear phishing the **exhibitors** of the **MSME DEFEXPO 2013**
Mofang: India

Spear phishing the exhibitors of the MSME DEFEXPO 2013

Command and control server: store.outlook-microsoft.net
Mofang: India / United States

Spear phishing government employees attending the “essentials of 21st century electronic warface” course

Command and control server: store.outlook-microsoft.net
Mofang: India

Land, Naval & Internal Security Systems Exhibition
06th - 09th February 2014, Pragati Maidan, New Delhi

Spear phishing the exhibitors of the MSME DEFEXPO 2014
Command and control server: images.defexpoindia14.com
Friend or Foe? probably both.

Mofang: India

How about MSME DEFEXPO 2015, 2016?

We cannot confirm any cases but Mofang’s specialisation in 2014 says enough.
While Mofang has really specific targets for which they setup infrastructure as part of their MO they don't always do this. There is also something we call the ‘global campaign’:

- Attacks aimed at individuals & organisations without ‘specialising’
- C2 infrastructure mimics services from Microsoft and Google
<table>
<thead>
<tr>
<th>Mofang: global campaign</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ie.update-windows-microsoft.com</td>
<td>store.outlook-microsoft.com</td>
</tr>
<tr>
<td>mail.upgoogle.com</td>
<td>support.outlook-microsoft.com</td>
</tr>
<tr>
<td>windws-microsoft.com</td>
<td>help.outlook-microsoft.com</td>
</tr>
<tr>
<td>account.google.com.gmgoogle.com</td>
<td>oem.outlook-microsoft.com</td>
</tr>
</tbody>
</table>
In September 2015 the Mofang group setup a new type of lure we had never seen them do before.
Mofang: some latest activity

Friend or Foe? probably both.
Mofang: some latest activity

<table>
<thead>
<tr>
<th>Domain</th>
<th>Created</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>citrixmeeting.com</td>
<td>2005-04-13</td>
<td></td>
</tr>
</tbody>
</table>
Mofang: some latest activity

<table>
<thead>
<tr>
<th>Domain</th>
<th>Created</th>
<th>Expires</th>
</tr>
</thead>
</table>
Mofang: some latest activity

<table>
<thead>
<tr>
<th>Domain</th>
<th>Created</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2015-07-27</td>
<td>2016-07-27</td>
</tr>
</tbody>
</table>
Mofang: some latest activity

A package containing ShimRat was located at:

http://www.citrixmeeting.com/download/livechat.exe

It dropped ShimRat and a new antivirus module we had never seen before. It was also from a vendor we hadn’t seen them abuse before:

<table>
<thead>
<tr>
<th>Application name</th>
<th>Norton Identity Safe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version (product specific)</td>
<td>2015.2.1.5</td>
</tr>
<tr>
<td>Hijacked DLL</td>
<td>msvcr110.dll</td>
</tr>
<tr>
<td>First seen used</td>
<td>2015-09-07</td>
</tr>
<tr>
<td>MD5</td>
<td>1f330f00510866522f14790398a5be59</td>
</tr>
</tbody>
</table>
Mofang: some latest activity

ShimRat was configured with a pseudo global campaign domain:

api.officeonlinetool.com
Conclusion

- Active since early 2012
- Two custom tools:
  - ShimRat
  - ShimRatReporter
- International attack profile
- Information & IP stealing
- Most likely PRC state affiliated
Conclusion

- Active since early **2012**

- Two custom tools:
  - ShimRat
  - ShimRatReporter

- **International** attack profile

- **Information & IP** stealing

- Most likely **PRC** state affiliated
Conclusion

- Active since early 2012
- Two custom tools:
  - ShimRat
  - ShimRatReporter
- International attack profile
- Information & IP stealing
- Most likely PRC state affiliated
Conclusion

- Active since early 2012
- Two custom tools:
  - ShimRat
  - ShimRatReporter
- International attack profile
- Information & IP stealing
- Most likely PRC state affiliated
Conclusion

- Active since early 2012

- Two custom tools:
  - ShimRat
  - ShimRatReporter

- International attack profile

- Information & IP stealing

- Most likely PRC state affiliated
Conclusion

- Active since early 2012
- Two custom tools:
  - ShimRat
  - ShimRatReporter
- International attack profile
- Information & IP stealing
- Most likely PRC state affiliated
Mofang
A politically motivated information stealing adversary

- History
- Campaign details
- Malware analysis
- Host based IOCs & rules
- Network based IOCs & rules

Full report available at: http://f0x.nl/mofang