



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**



Yonathan Klijnsma

Senior Threat Intelligence Analyst

Perform threat intelligence analysis at  **FOX IT** 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

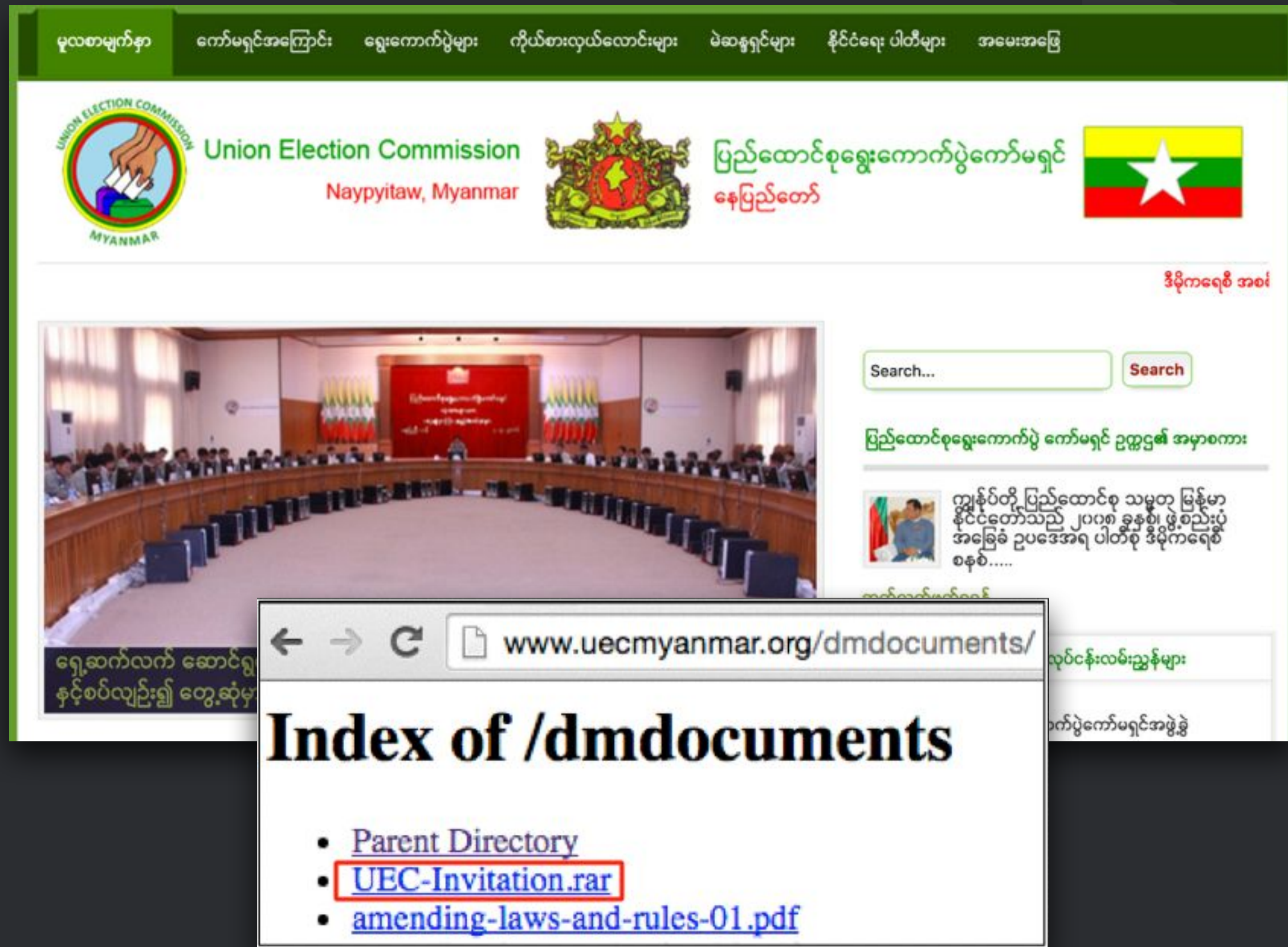


Myanmar... Burma?

- 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"



Political change



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:** Evilgrab Delivered by Watering Hole Attack on President of Myanmar's Website
<http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/>
- **Citizenlab:** Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites
<https://citizenlab.org/2015/10/targeted-attacks-ngo-burma/>
- **Citizenlab:** Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns
<https://citizenlab.org/2016/04/between-hong-kong-and-burma/>
- **ASERT:** PlugX Threat Activity in Myanmar
<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
<https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Pointed-Dagger.pdf>



'Groups'

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.com



Group: NewsX

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)



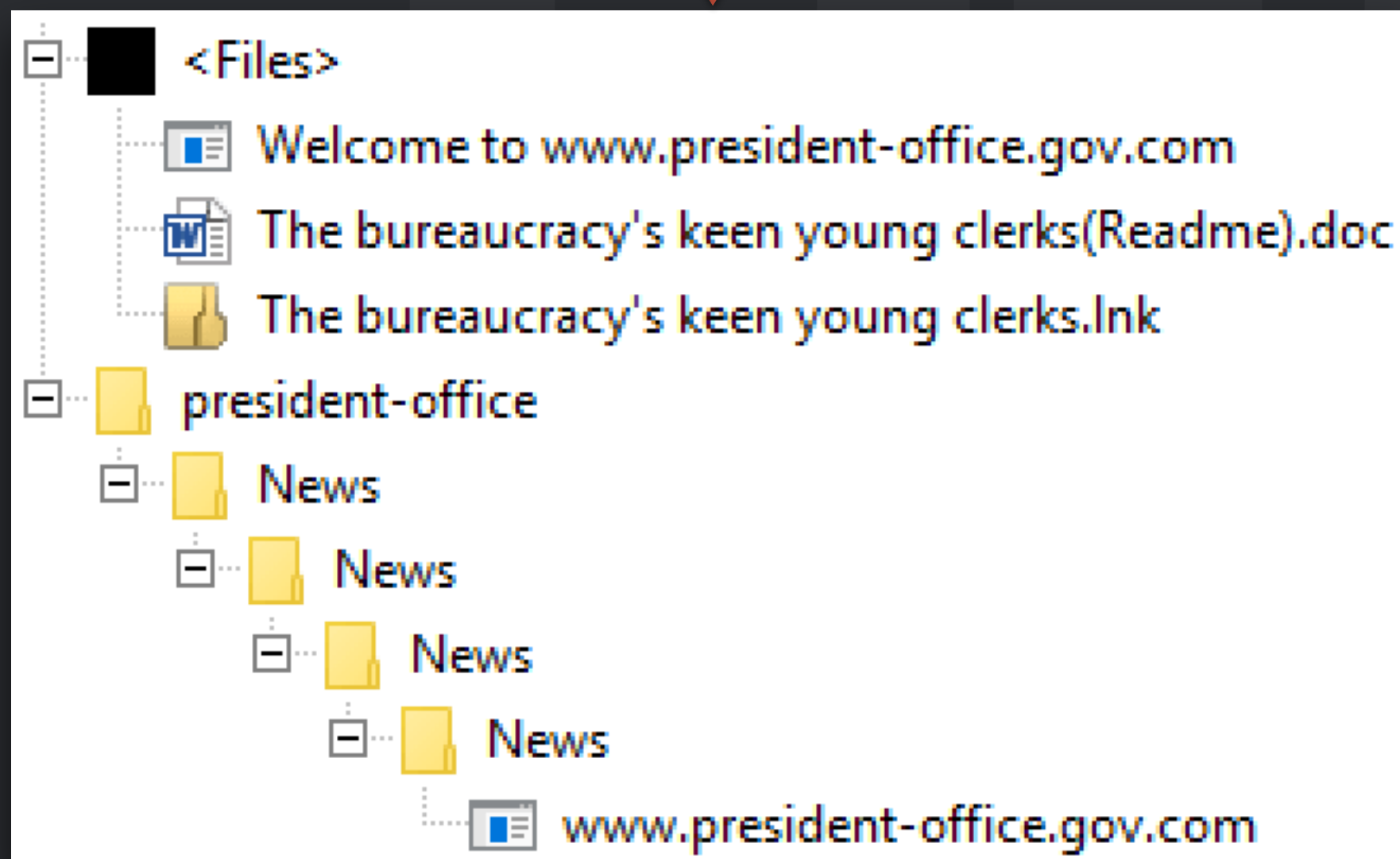
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
president-office			File folder	12/23/2014 4:16 PM	
The bureaucracy's keen young clerks(Readme).doc	25,600	5,365	Microsoft Word 97 - 2003 Document	3/9/2015 2:38 PM	030E5664
The bureaucracy's keen young clerks.lnk	1,389	639	Shortcut	3/9/2015 2:34 PM	7FB64BA5
Welcome to www.president-office.gov.com	335,883	287,547	MS-DOS Application	3/4/2015 5:59 PM	BF61AE18



Group: NewsX (lures)



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
president-office			File folder	12/23/2014 4:16 PM	
The bureaucracy's keen young clerks(Readme).doc	25,600	5,365	Microsoft Word 97 - 2003 Document	3/9/2015 2:38 PM	030E5664
The bureaucracy's keen young clerks.lnk	1,389	639	Shortcut	3/9/2015 2:34 PM	7FB64BA5
Welcome to www.president-office.gov.com	335,883	287,547	MS-DOS Application	3/4/2015 5:59 PM	BF61AE18



Group: NewsX (lures)



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
president-office			File folder	12/23/2014 4:16 PM	
The bureaucracy's keen young clerks(Readme).doc	25,600	5,365	Microsoft Word 97 - 2003 Document	3/9/2015 2:38 PM	030E5664
The bureaucracy's keen young clerks.lnk	1,389	639	Shortcut	3/9/2015 2:34 PM	7FB64BA5
Welcome to www.president-office.gov.com	335,883	287,547	MS-DOS Application	3/4/2015 5:59 PM	BF61AE18



<Files>

- Welcome to www.president-office.gov.com
- The bureaucracy's keen young clerks(Readme).doc
- The bureaucracy's keen young clerks.lnk
- president-office
 - News
 - News
 - News
 - News
 - www.president-office.gov.com



Group: NewsX (lures)



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
president-office			File folder	12/23/2014 4:16 PM	
The bureaucracy's keen young clerks(Readme).doc	25,600	5,365	Microsoft Word 97 - 2003 Document	3/9/2015 2:38 PM	030E5664
The bureaucracy's keen young clerks.lnk	1,389	639	Shortcut	3/9/2015 2:34 PM	7FB64BA5
Welcome to www.president-office.gov.com	335,883	287,547	MS-DOS Application	3/4/2015 5:59 PM	BF61AE18



<Files>

- Welcome to www.president-office.gov.com
- The bureaucracy's keen young clerks(Readme).doc
- The bureaucracy's keen young clerks.lnk
- president-office
 - News
 - News
 - News
 - News
 - www.president-office.gov.com

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.



Group: NewsX (lures)



News Business Lifestyle Development Election 2015

Home » News » Opinion » The bureaucracy's keen young clerks

The bureaucracy's keen young clerks

By Nicholas Farrelly

On Monday, 2 March 2015

Facebook Tweet 0 0 0



Photo: Hong Sar/Mizzima

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.

	Size	Packed	Type	Modified	CRC32
			File folder		
			File folder	12/23/2014 4:16 PM	
oc	25,600	5,365	Microsoft Word 97 - 2003 Document	3/9/2015 2:38 PM	030E5664
	1,389	639	Shortcut	3/9/2015 2:34 PM	7FB64BA5
	335,883	287,547	MS-DOS Application	3/4/2015 5:59 PM	BF61AE18

The bureaucracy's keen young clerks

For more information, please read.

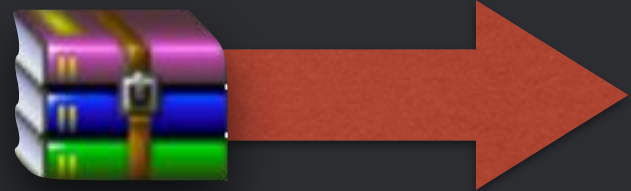
Please unzip the file to your desktop.

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.



Group: NewsX (lures)



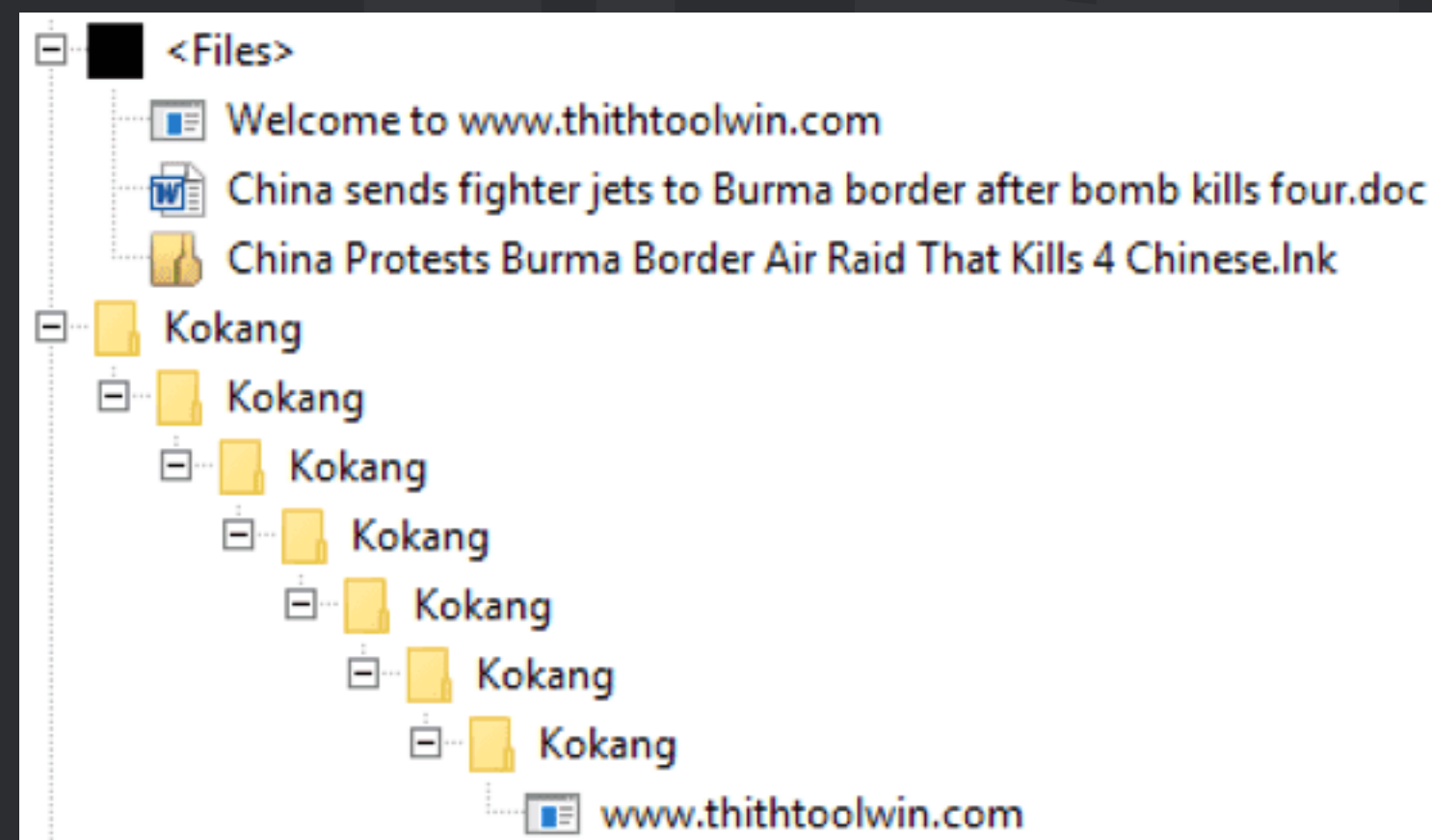
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Kokang			File folder	1/8/2015 11:11 PM	
Kokang Rebels			File folder	1/13/2015 3:44 PM	
China Protests Burma Border Air Raid That Kills 4 Chinese.lnk	1,779	619	Shortcut	3/15/2015 5:01 PM	33984A3F
China sends fighter jets to Burma border after bomb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



Group: NewsX (lures)



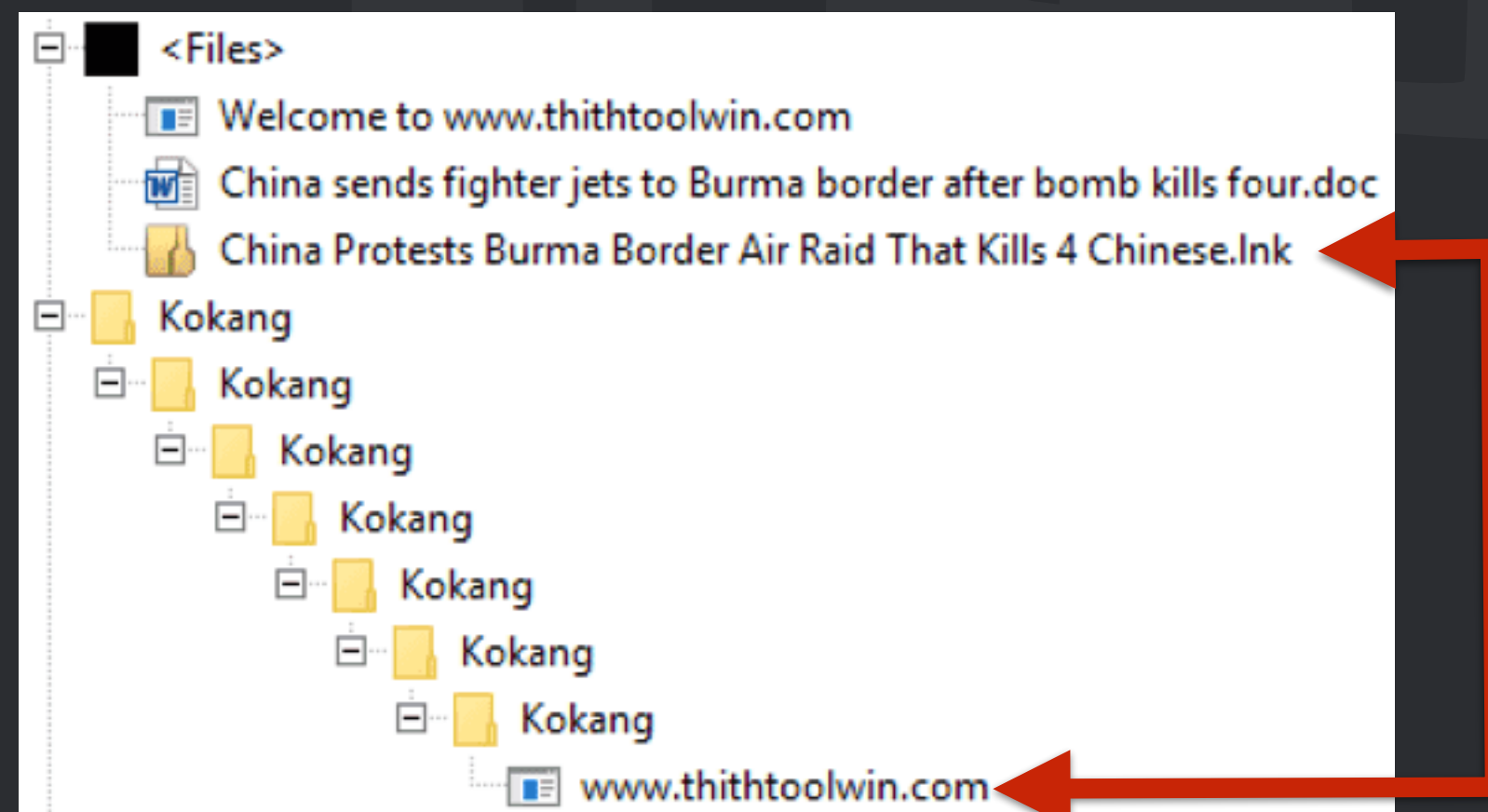
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Kokang			File folder	1/8/2015 11:11 PM	
Kokang Rebels			File folder	1/13/2015 3:44 PM	
China Protests Burma Border Air Raid That Kills 4 Chinese.Ink	1,779	619	Shortcut	3/15/2015 5:01 PM	33984A3F
China sends fighter jets to Burma border after bomb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



Group: NewsX (lures)



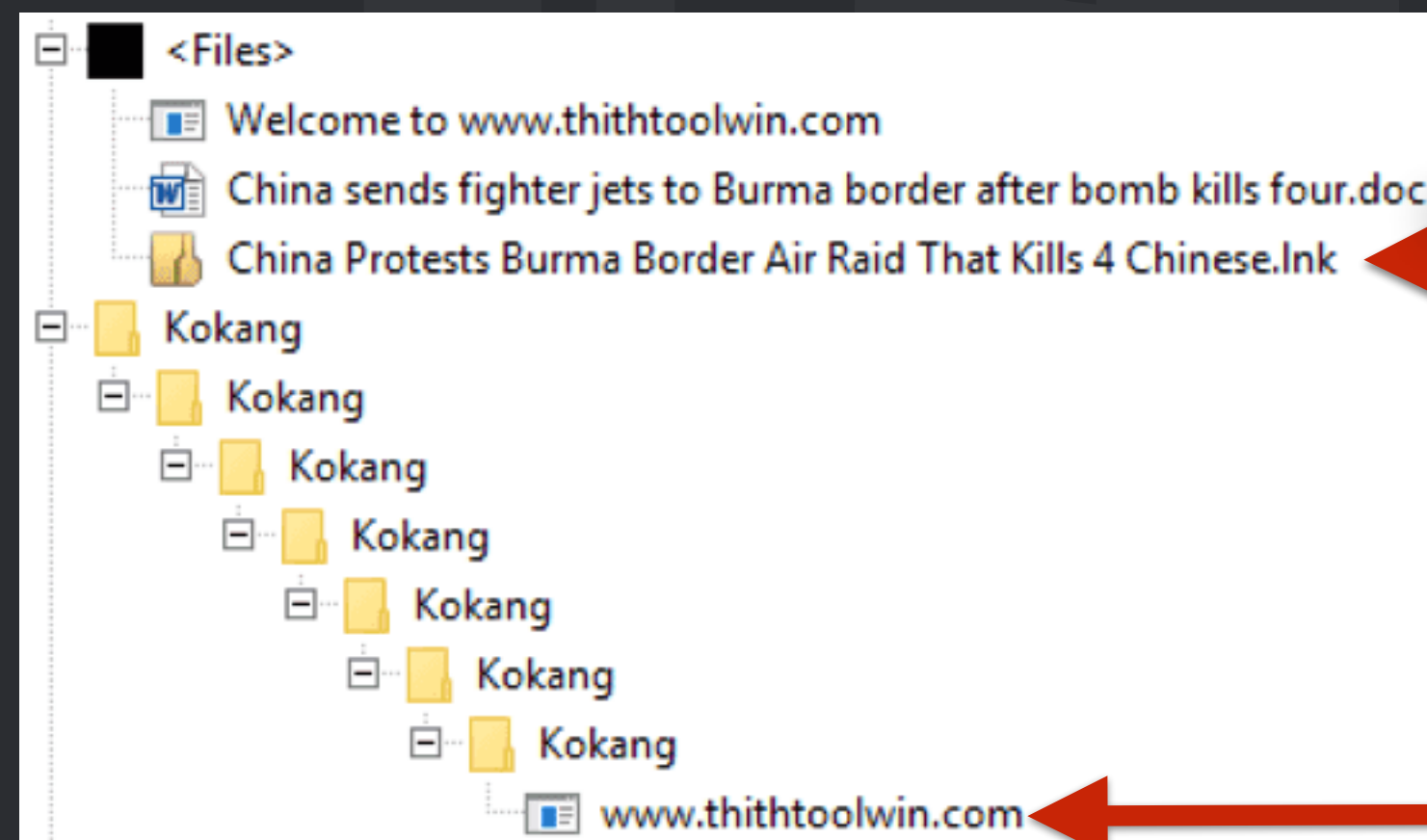
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Kokang			File folder	1/8/2015 11:11 PM	
Kokang Rebels			File folder	1/13/2015 3:44 PM	
China Protests Burma Border Air Raid That Kills 4 Chinese.Ink	1,779	619	Shortcut	3/15/2015 5:01 PM	33984A3F
China sends fighter jets to Burma border after bomb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



Group: NewsX (lures)



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



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.



Group: NewsX (lures)

[နေ့စဉ်သတင်း](#)
[ကျန်းမာရေး](#)
[သတင်းစာ နှင့် ကျန်းမာရေး](#)
[အားကစား](#)
[နည်းပညာ ဒီဂျစ်တယ်](#)
[နာမည်ကြီး ပုဂ္ဂိုလ်များ](#)
[ဗဟုသုတ](#)
[ENGLISH](#)
[ဆက်သွယ်ရန်](#)



 သစ်ထူးလွင် - နေ့စဉ်ပြန်မာသတင်း

[Home](#)
[ပြည်တွင်းသတင်း](#)
[နိုင်ငံတကာ သတင်း](#)
[ဆောင်းပါး](#)
[ပညာရေး](#)
[မူခင်း](#)
[Voice of facebook](#)
[အခြားကဏ္ဍ](#)

MYOPENADS

ခေါင်းလောင်းစာကို ယူနက်စကို-ကမ္ဘာ့မှတ်တမ်း အမွေအနှစ်စာရင်း တင်သွင်း

11 May 2016 20:25(+0630) (25 မိနစ် ခန့်က)



ဟံသာဝတီဆင်ဖြူရှင်ဘုရင့်နောင်မင်းတရားကြီးက ပုဂံရွှေစည်းခုံ ဘုရားတွင် လှူဒါန်းခဲ့သည့် ခေါင်းလောင်းစာကို ယူနက်စကို-ကမ္ဘာ့မှတ်တမ်း အမွေအနှစ်စာရင်း တင်သွင်းခြင်း ပုဂံရွှေစည်းခုံဘုရားမှ ဘုရင့်နောင်ခေါင်းလောင်းတွင် ရေးထိုးထားသော ကမ္ဘာ့မှတ်တမ်းဟု ဟံသာဝတီ ဆင်ဖြူရှင် ဘုရင့်နောင်မင်း တရားကြီး ၏ ဆောင်ရွက်ချက်များကို ဖော်ပြသော ပါဠိ၊ မွန်၊ မြန်မာ၊ သုံးဘာသာဖြင့်...

[သတင်းအပြည့်အစုံဖတ်ရန် »](#)

ADVERTISEMENT

Name	Size	Backup	Type	Modified	CRC32
				1/8/2015 11:11 PM	
				1/13/2015 3:44 PM	
				3/15/2015 5:01 PM	33984A3F
2003 Document				3/15/2015 5:13 PM	1C7BD999
				3/15/2015 4:46 PM	74C00C25

border with neighboring Burma on Saturday and lodged a complaint with the Chinese government that a Burmese warplane dropped a bomb on Chinese territory, causing civilian casualties.

China's government stepped up its fight against ethnic Chinese separatists in the region along China's southwestern border.

The incident has sent thousands of people fleeing across the border into China.

The incident and calls on Burma to carry out a thorough investigation and report the results to China, punish the guilty and take steps to ensure similar incidents do not recur, he said in a statement.



Group: NewsX (lures)

နေ့စဉ်သတင်း ကျန်းမာရေး သတင်းစာ နှင့် ကုန်ပစ္စည်း အားကစား နည်းပညာ ဒီဂျစ်တယ် နာမည်ကြီး ပုဂ္ဂိုလ်များ ဗဟု


THITHTOOLWIN
သစ်ထူးလွင် - နေ့စဉ်ပြန်မာသတင်း

Home ပြည်တွင်းသတင်း နိုင်ငံတကာ သတင်း ဆောင်းပါး ပညာရေး

MYOPENADS

ခေါင်းလောင်းစာကို ယူနက်စကို-ကမ္ဘာ့မှတ်တမ်း အဖွဲ့က တင်သွင်း

11 May 2016 20:25(+0630) (25 မိနစ် ခန့်က)



ဟံသာဝတီဆင်ဖြူရှင်ဘုရင့်နောင်မင်းတရားရဲ့ ခုံ ဘုရားတွင် လှူဒါန်းခဲ့သည့် ခေါင်းလောင်းစာ ကမ္ဘာ့မှတ်တမ်း အဖွဲ့အနစ်စာရင်း တင်သွင်း ခုံဘုရားမှ ဘုရင့်နောင်ခေါင်းလောင်းတွင် ရေ ကမ္ဘာ့မှတ်တမ်းဟာ ဟံသာဝတီ ဆင်ဖြူရှင် ဘုရားကြီး ၏ ဆောင်ရွက်ချက်များကို ဖော်ပြပေးမာ၊ သုံးဘာသာဖြင့်...

သတင်းအပြည့်အစုံဖတ်ရန် »

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & A

Asia | China | India

China protests over 'deadly Myanmar border raid'

🕒 14 March 2015 | Asia



Groups

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.



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.

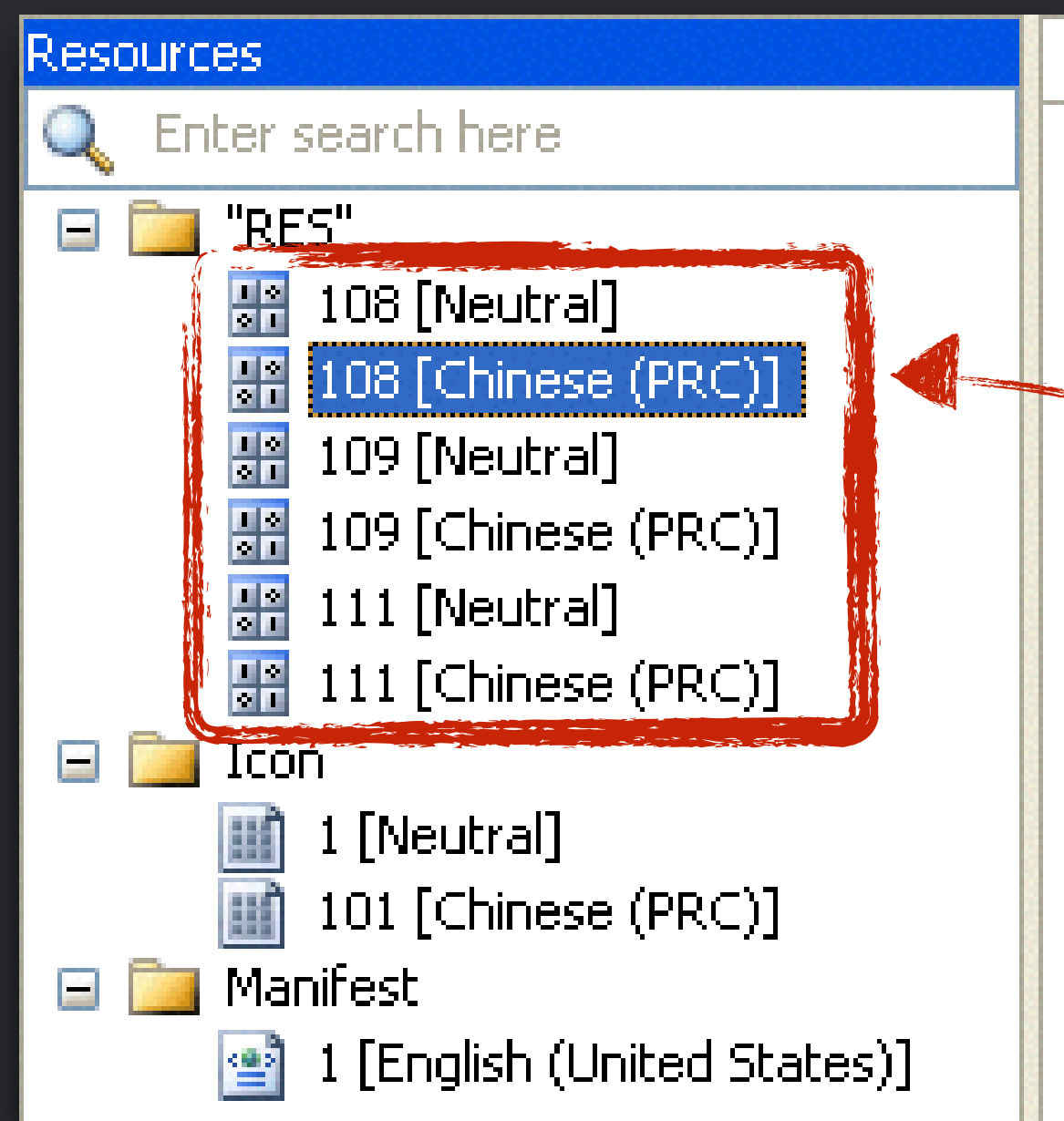
The Mofang group uses custom malware that dates back to at least February 2012.

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



Properties:

Name	Value
KSOProductBuildVer	2052-8.1.0.2998

Simplified Chinese is set as the character set in many of the resources inside various malware samples.



Mofang: Attribution

Early versions of the ShimRat malware showed something interesting in their C2 communication protocol.

```
POST /js/js/js.php HTTP/1.1
User-Agent: Asynchronous WinHTTP/1.0
Host: update.nfkllyuisyahooapis.com
Content-Length: 145
Connection: Keep-Alive
```

2012

```
Yuok$
$004B766C217B736C6A171FCF04D3A9785D15...user5...2.1.461...
Microsoft Windows XP Professional Service Pack 3 (build 2600)YuokHTTP/1.1
200 OK
Date: Sun, 04 Nov 2012 03:19:34 GMT
Server: Apache
X-Powered-By: PHP/5.2.10
Content-Length: 4
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Yerr


```
POST /_vti_log/log.php HTTP/1.1
User-Agent: IE8.0
Host: energysavingpro.ca
Content-Length: 108
Connection: Keep-Alive
```

2013

```
Data$00. ....superman.0.0.01.1=Microsoft Wi
Service Pack 3 (Build2600)DataHTTP/1.1 200 OK
Date: Thu, 31 Jan 2013 23:30:36 GMT
Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0
mod_auth_pgsq/2.0.3
X-Powered-By: PHP/5.2.17
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

```
4
Data
0
```



A man in a dark tuxedo and bow tie is shown from the chest up, looking slightly to his left with a surprised or concerned expression. He is in a dimly lit room with blue ambient lighting and strings of warm white lights in the background. Another person is partially visible in the background to the left.

郁佢，郁佢！
Beat him.

Mofang: Attribution

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

It suggests at least passive knowledge of Cantonese on the part of the malware author.

```
POST /js/js/js.php HTTP/1.1
User-Agent: Asynchronous WinHTTP/1.0
Host: update.nfkllyuisyahooapis.com
Content-Length: 145
Connection: Keep-Alive
```

2012

```
Yuok$
$004B766C217B736C6A171FCF04D3A9785D15...user5...2.1.461...
Microsoft Windows XP Professional Service Pack 3 (build 2600)YuokHTTP/1.1
200 OK
Date: Sun, 04 Nov 2012 03:19:34 GMT
Server: Apache
X-Powered-By: PHP/5.2.10
Content-Length: 4
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Yerr
```



Mofang: Attribution

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;



Mofang: Attribution



Mofang: History

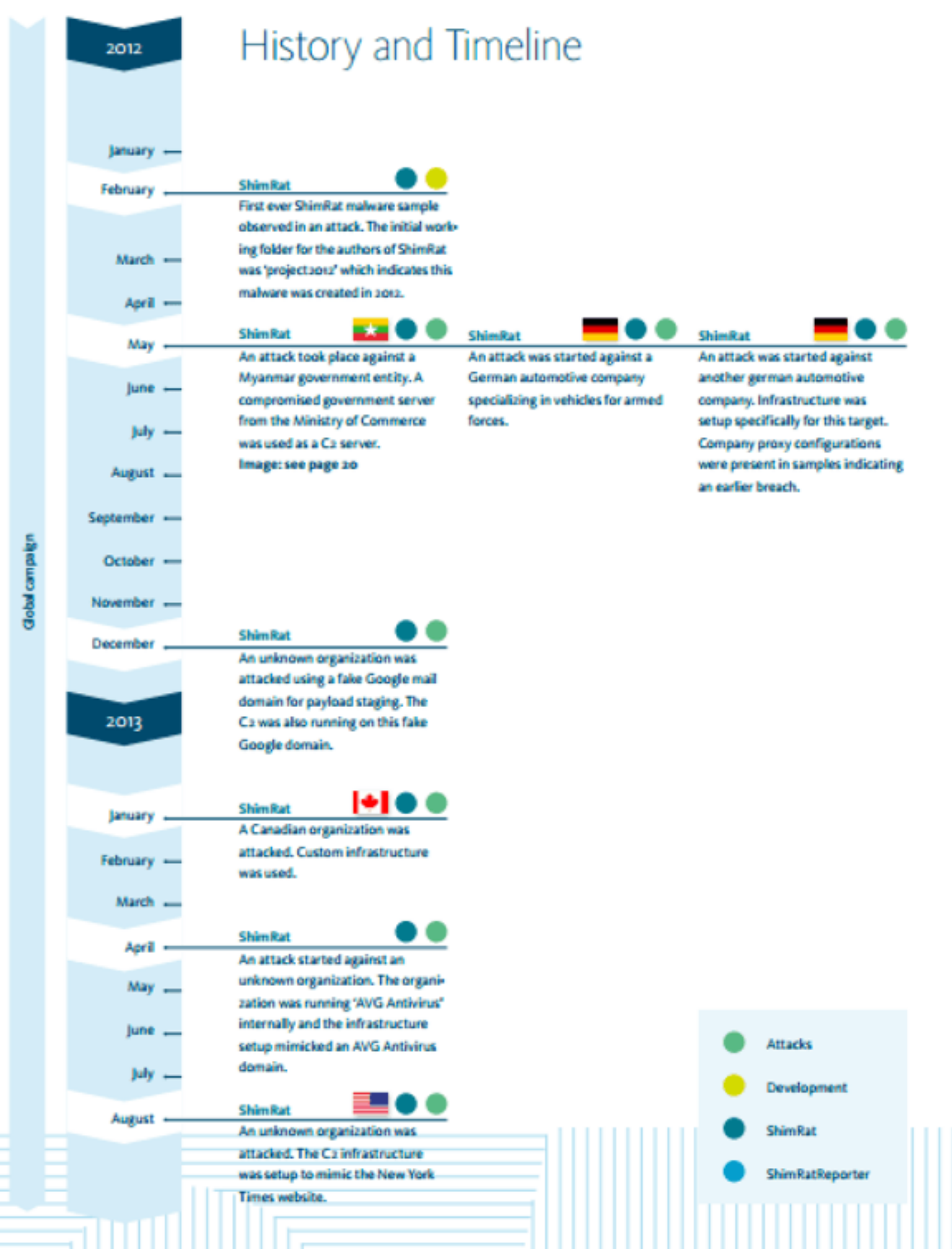
We have some certainty they started in 2012. No samples before 2012 and early versions had embedded project folders:

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

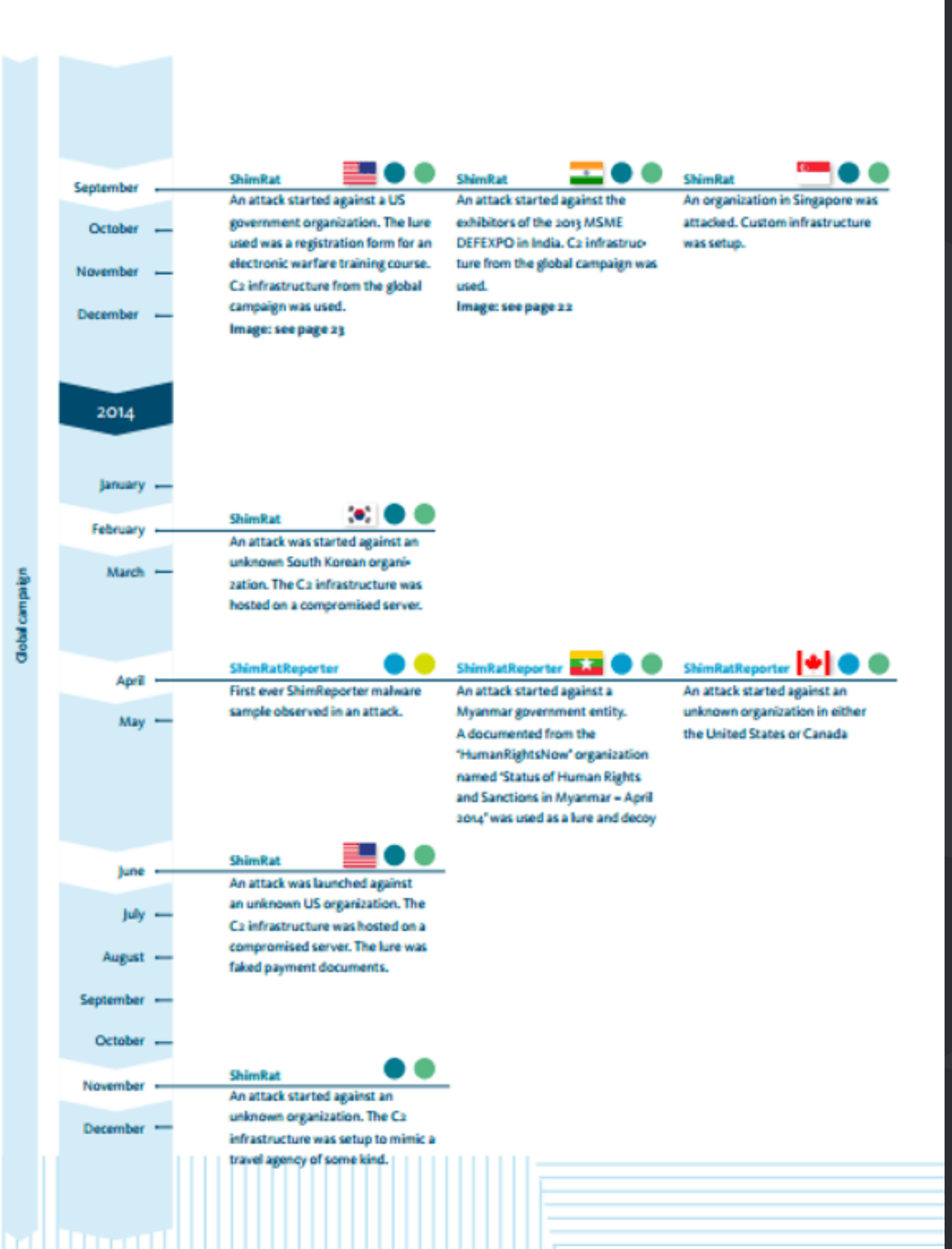


Mofang: History

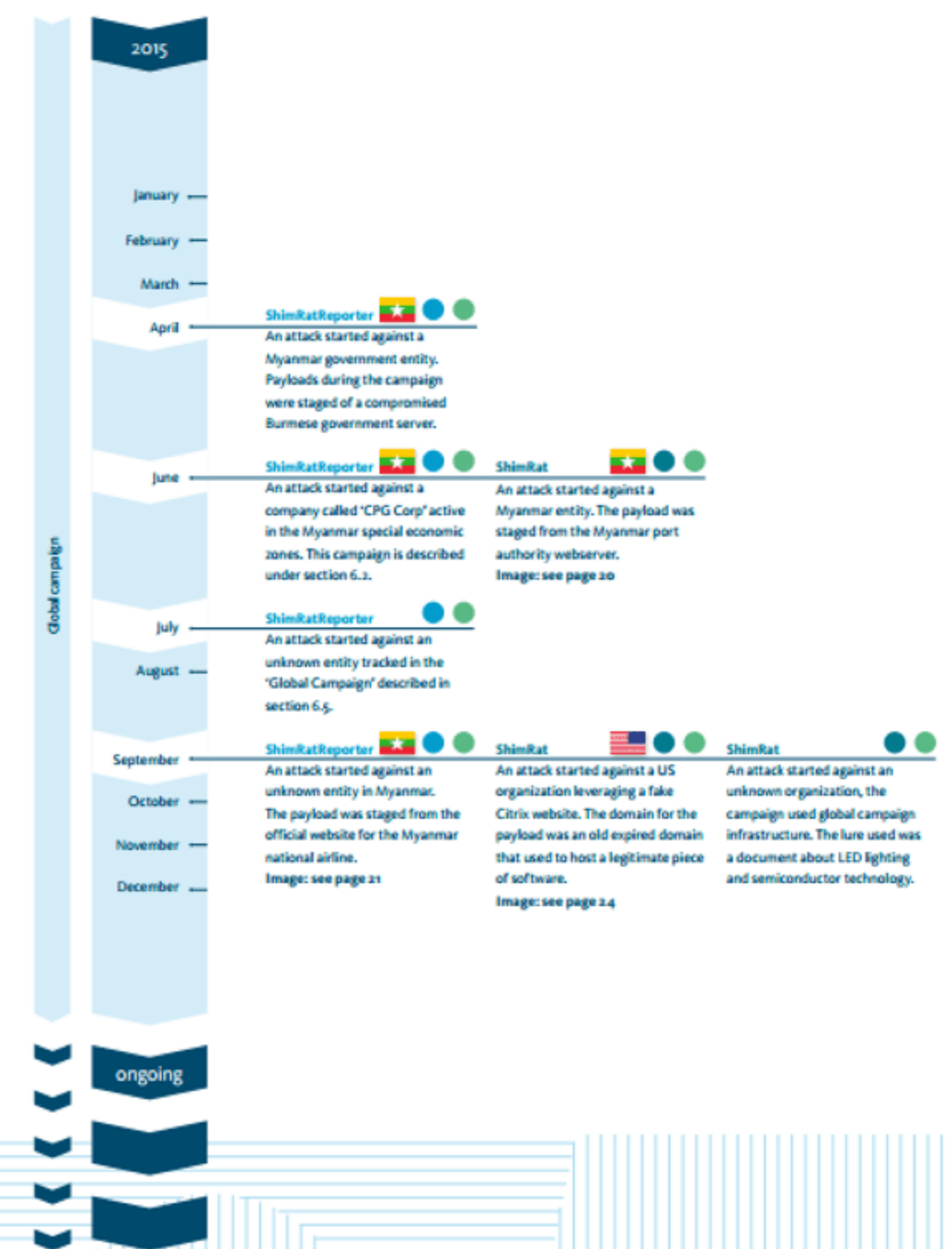
History and Timeline



14 | Mofang | A politically motivated information stealing adversary | May 2016 | 15



14 | Mofang | A politically motivated information stealing adversary | May 2016



14 | Mofang | A politically motivated information stealing adversary | May 2016 | 17



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.



Mofang: Tools

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.



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 stil used:



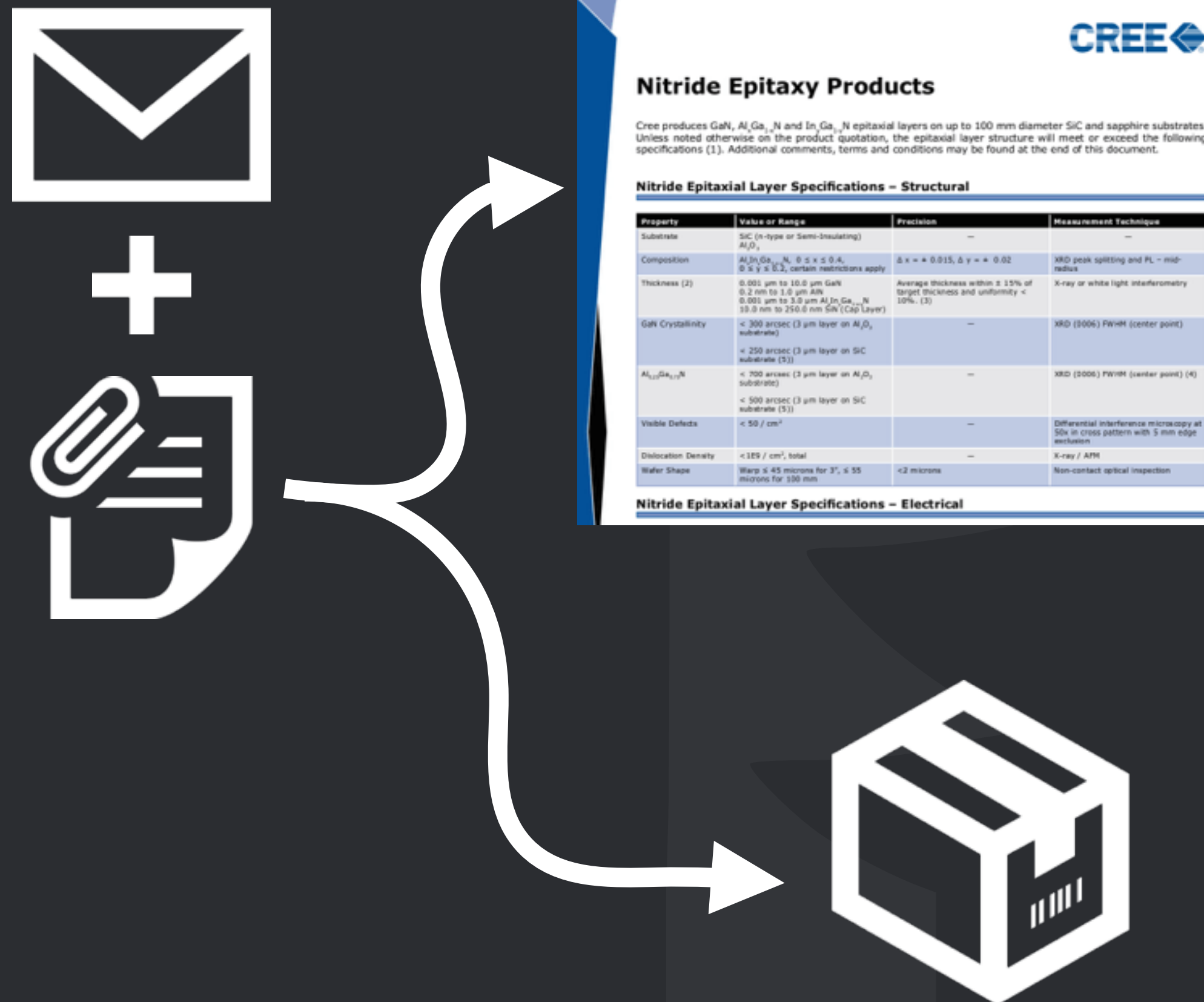
Mofang: Tools - ShimRat

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



CREE

Nitride Epitaxy Products

Cree produces GaN, Al_xGa_{1-x}N and In_xGa_{1-x}N epitaxial layers on up to 100 mm diameter SiC and sapphire substrates. Unless noted otherwise on the product quotation, the epitaxial layer structure will meet or exceed the following specifications (1). Additional comments, terms and conditions may be found at the end of this document.

Nitride Epitaxial Layer Specifications – Structural

Property	Value or Range	Precision	Measurement Technique
Substrate	SiC (n-type or Semi-insulating) Al ₂ O ₃	—	—
Composition	Al _x In _{1-x} Ga _{1-x} N, 0 ≤ x ≤ 0.4, 0 ≤ y ≤ 0.2, carbon impurities apply	Δx = ± 0.015, Δy = ± 0.02	XRD peak splitting and PL - mid-band
Thickness (2)	0.001 μm to 10.0 μm GaN 0.2 nm to 1.0 μm AlN 0.001 μm to 2.0 μm Al _x In _{1-x} Ga _{1-x} N 10.0 nm to 250.0 nm SiN (Cap Layer)	Average thickness within ± 15% of target thickness and uniformity < 10% (3)	X-ray or white light interferometry
GaN Crystallinity	< 300 arcsec (3 μm layer on Al ₂ O ₃ substrate) < 250 arcsec (3 μm layer on SiC substrate (5))	—	XRD (006) FWHM (center point)
Al _x In _y Ga _{1-x-y} N	< 700 arcsec (3 μm layer on Al ₂ O ₃ substrate) < 500 arcsec (3 μm layer on SiC substrate (5))	—	XRD (2006) FWHM (center point) (4)
Visible Defects	< 50 / cm ²	—	Differential interference microscopy at exclusion
Dislocation Density	< 1E5 / cm ² , total	—	X-ray / AFM
Wafer Shape	Warp ≤ 45 microns for 3", ≤ 55 microns for 350 mm	< 2 microns	Non-contact optical inspection

Nitride Epitaxial Layer Specifications – Electrical



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 stil used:



CREE

Nitride Epitaxy Products

Cree produces GaN, Al_xGa_{1-x}N and In_xGa_{1-x}N epitaxial layers on up to 100 mm diameter SiC and sapphire substrates. Unless noted otherwise on the product quotation, the epitaxial layer structure will meet or exceed the following specifications (1). Additional comments, terms and conditions may be found at the end of this document.

Nitride Epitaxial Layer Specifications – Structural

Property	Value or Range	Precision	Measurement Technique
Substrate	SiC (n-type or Semi-insulating) Al ₂ O ₃	—	—
Composition	Al _x In _y Ga _{1-x-y} N, 0 ≤ x ≤ 0.4, 0 ≤ y ≤ 0.2, carbon impurities apply	Δx = ± 0.015, Δy = ± 0.02	XRD peak splitting and PL - mid-band
Thickness (2)	0.001 μm to 10.0 μm GaN 0.2 nm to 1.0 μm AlN 0.001 μm to 2.0 μm Al _x In _y Ga _{1-x-y} N 10.0 nm to 250.0 nm SiN (Cap Layer)	Average thickness within ± 15% of target thickness and uniformity < 10% (3)	X-ray or white light interferometry
GaN Crystallinity	< 300 arcsec (3 μm layer on Al ₂ O ₃ substrate) < 250 arcsec (3 μm layer on SiC substrate (5))	—	XRD (006) FWHM (center point)
Al _x In _y Ga _{1-x-y} N	< 700 arcsec (3 μm layer on Al ₂ O ₃ substrate) < 500 arcsec (3 μm layer on SiC substrate (5))	—	XRD (206) FWHM (center point) (4)
Visible Defects	< 50 / cm ²	—	Differential interference microscopy at exclusion
Dislocation Density	< 1E5 / cm ² , total	—	X-ray / AFM
Wafer Shape	Warp ≤ 45 microns for 3", ≤ 35 microns for 350 mm	< 2 microns	Non-contact optical inspection

Nitride Epitaxial Layer Specifications – Electrical

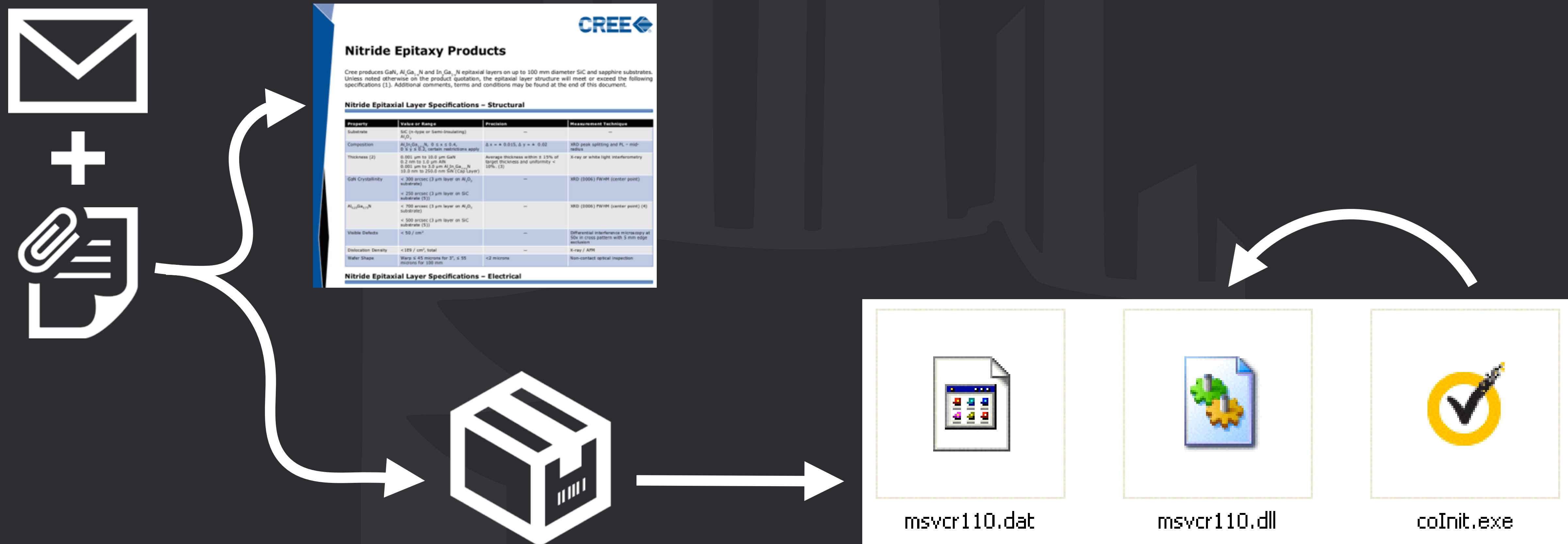


msvcr110.dat msvcr110.dll coInit.exe



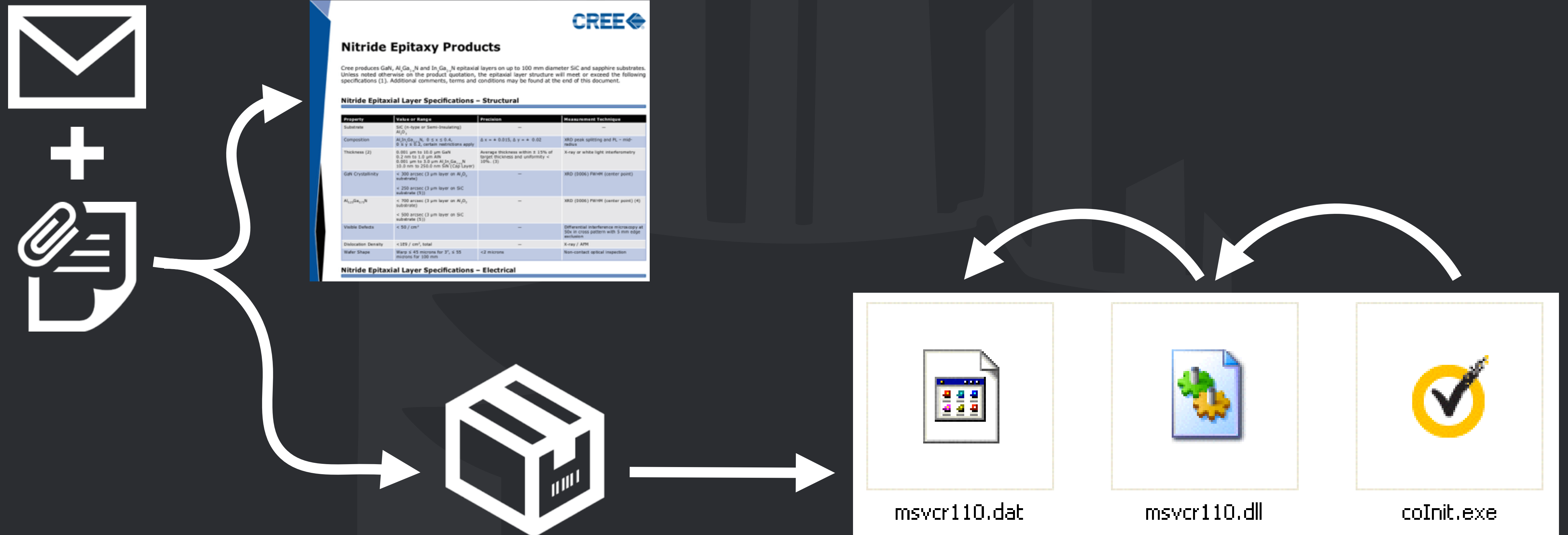
Mofang: Tools - ShimRat

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



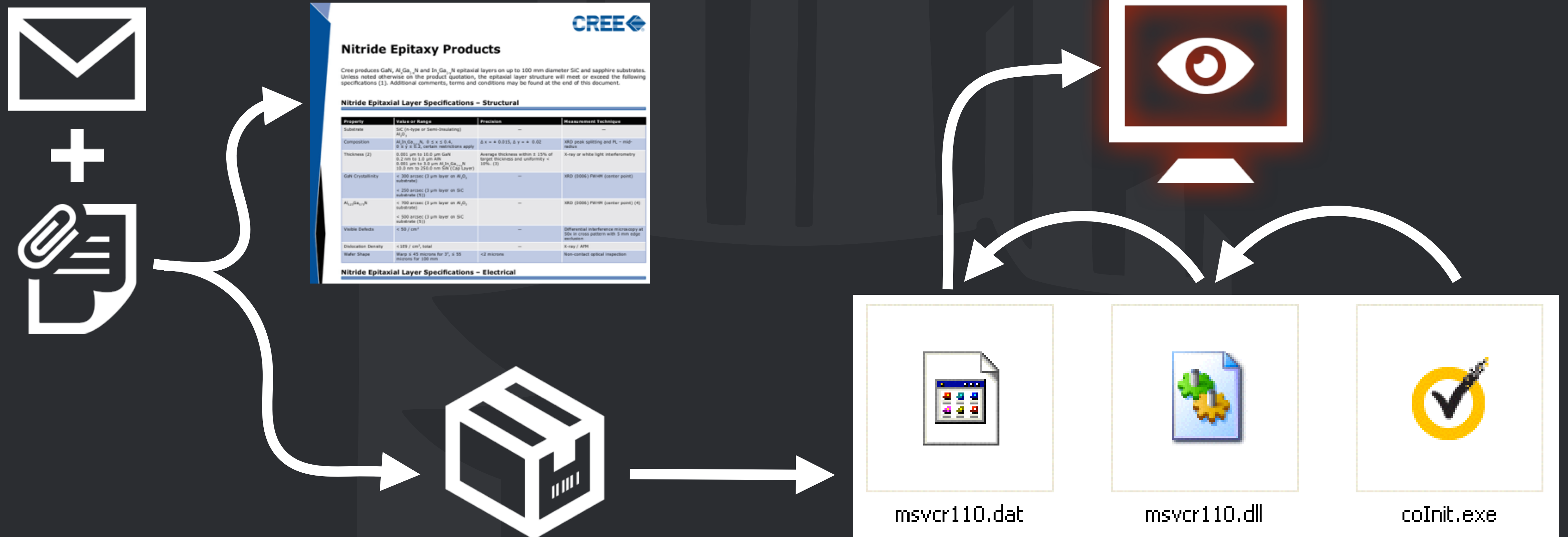
Mofang: Tools - ShimRat

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



Mofang: Tools - ShimRat

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

Service description

Service title

Installation folder

Installation filename

Injection target process

Installation mode



Mofang: Tools - ShimRat - Shims

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`.



Mofang: Tools - ShimRat - Shims

Platform	x86
Name	Clengine_Shim
Application name	Clengine_Apps
Database name	Clengine_Database
Type of fix	InjectDLL
Injection target	svchost.exe
Injection DLL	elogger.dll



Mofang: Tools - ShimRat

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.

Primary C2 location

Secondary C2 location

Campaign ID

C2 server password

Proxy

Proxy username

Proxy password



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**



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:

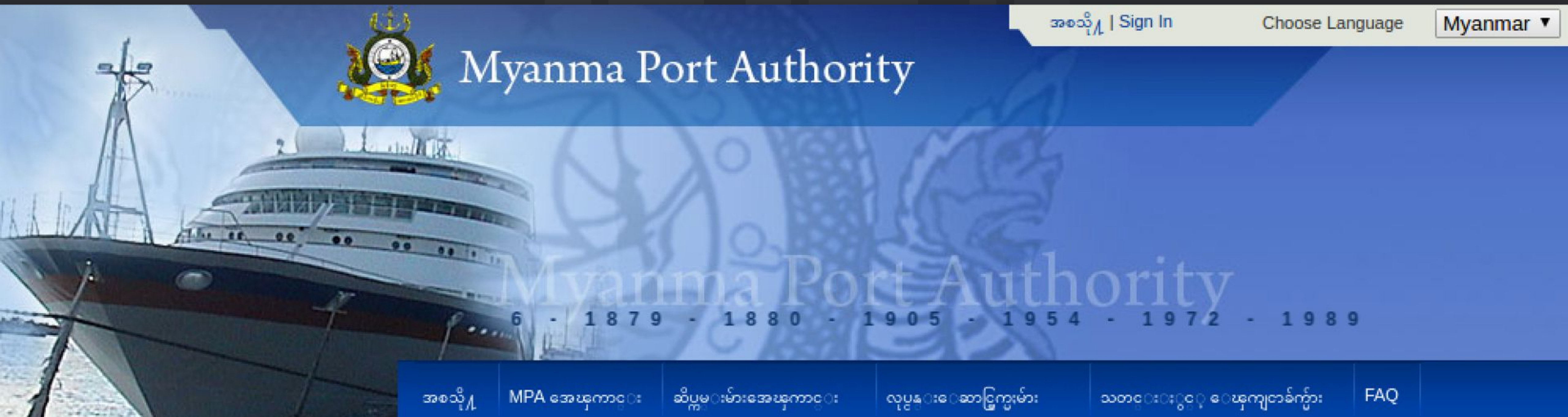
commerce.gov.mm/templates/css1/logon.php



Mofang: Myanmar

June 2015, a ShimRat payload was staged from:

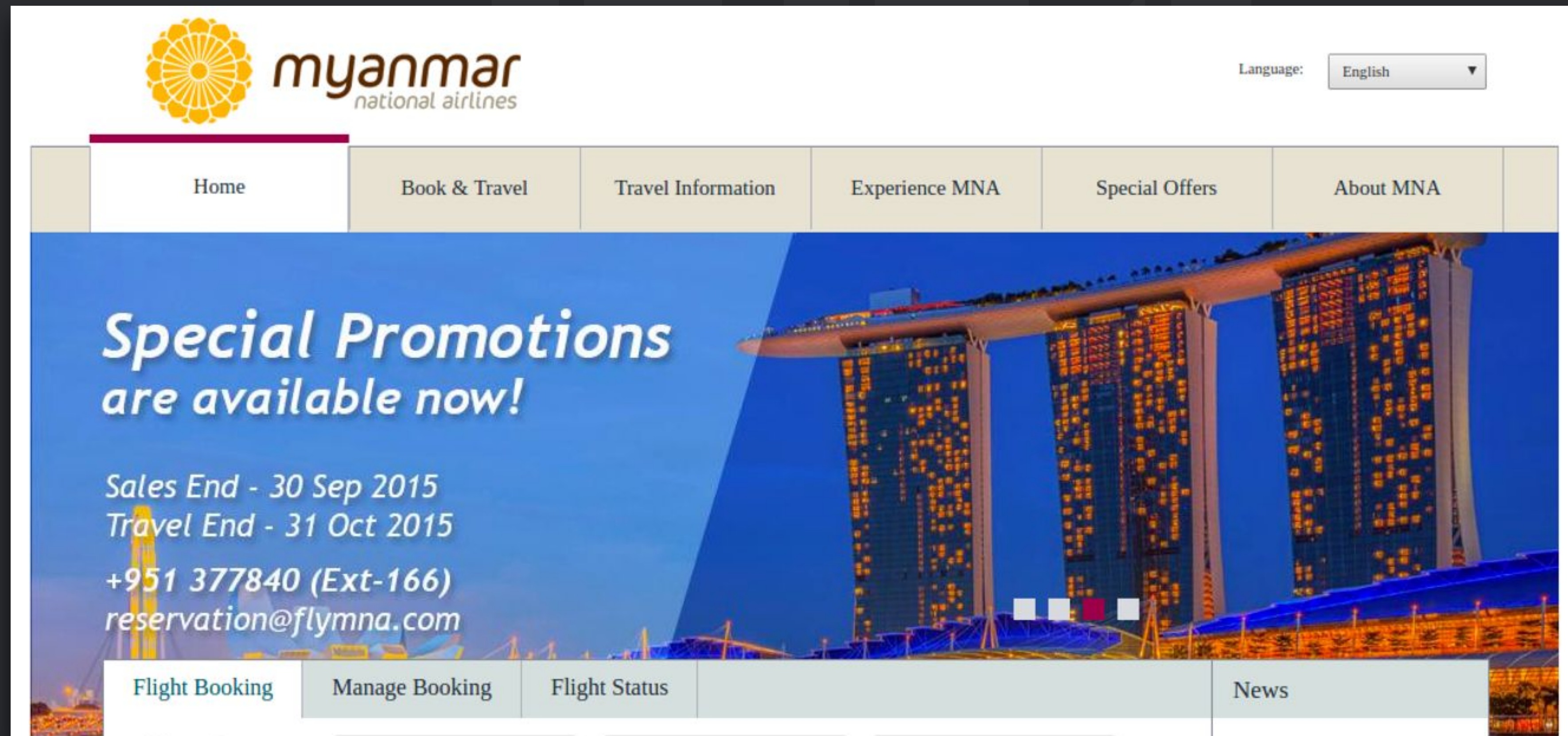
203.81.162.178/text.txt



Mofang: Myanmar

September 2015, a ShimRat payload lure was staged from:

www.flymna.com/sites/photo.tar



The screenshot shows the Myanmar National Airlines website. At the top left is the logo, a yellow sunburst icon next to the text "myanmar national airlines". To the right is a language dropdown menu set to "English". Below the logo is a navigation bar with links: Home, Book & Travel, Travel Information, Experience MNA, Special Offers, and About MNA. The main content area features a large blue banner with the text "Special Promotions are available now!". Below this, it states "Sales End - 30 Sep 2015" and "Travel End - 31 Oct 2015". Contact information includes the phone number "+951 377840 (Ext-166)" and the email "reservation@flymna.com". At the bottom of the banner are four small colored squares (white, white, red, white). Below the banner is another navigation bar with links: Flight Booking, Manage Booking, Flight Status, and News.



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.



Mofang: Myanmar

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.

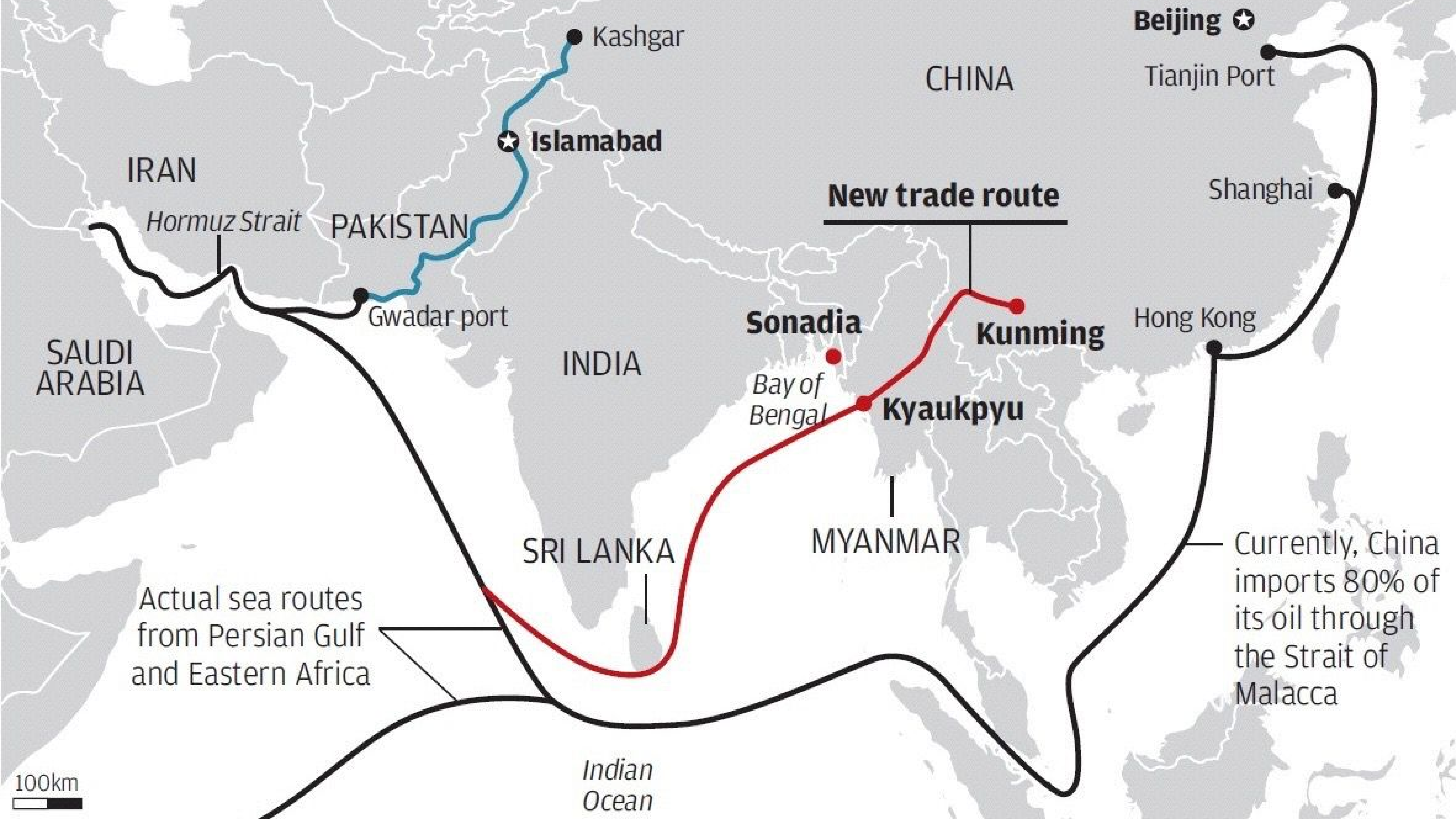


Mofang: Myanmar

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.





Beijing ★

Tianjin Port

CHINA

Shanghai

New trade route

Hong Kong

Kunming

Sonadia

Bay of Bengal

Kyaukpyu

INDIA

MYANMAR

SRI LANKA

PAKISTAN

IRAN

SAUDI ARABIA

Hormuz Strait

Gwadar port

Kashgar

★ Islamabad

Actual sea routes from Persian Gulf and Eastern Africa

Currently, China imports 80% of its oil through the Strait of Malacca

Indian Ocean

100km

Mofang: Myanmar

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.



Mofang: Myanmar

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**



Kyauk Phyu SEZ ●



MYANMAR

Thilawa SEZ ●

THAILAND

Dawei SEZ ●



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**.



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**.



Mofang: Myanmar

At this point Mofang had acquired their target: **CPG Corporation**



Mofang: Myanmar - CPG Corporation

Spear phishing attacks started in June 2015 with a really unique lure.

မြန်မာအခက်ခဲရာ

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



Mofang: Myanmar - CPG Corporation

ShimRat samples in this campaign were configured to connect to:

secure2.sophosrv.com/en-us/support/ms-cache_check.php



Mofang: Myanmar - CPG Corporation

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.



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.

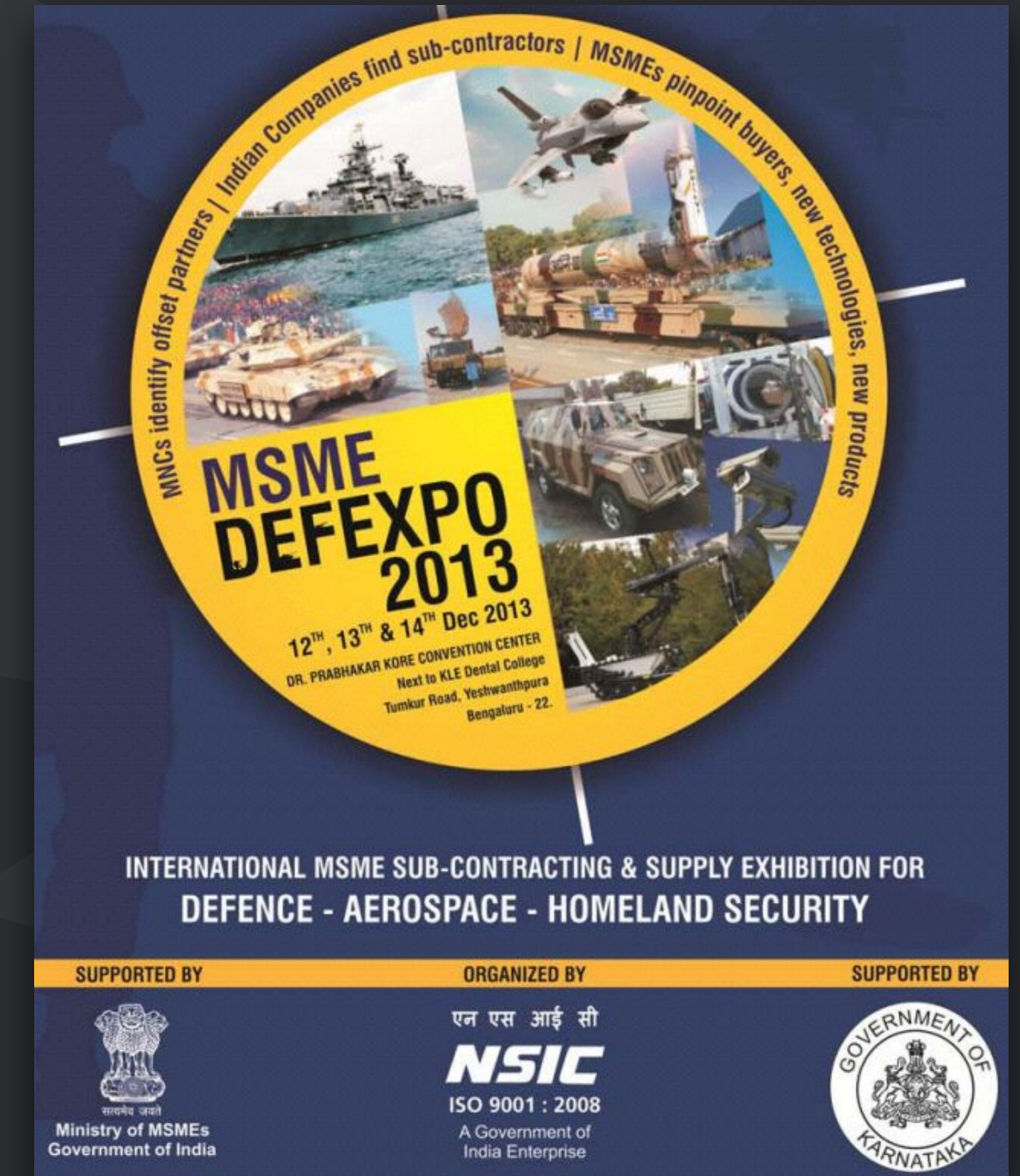
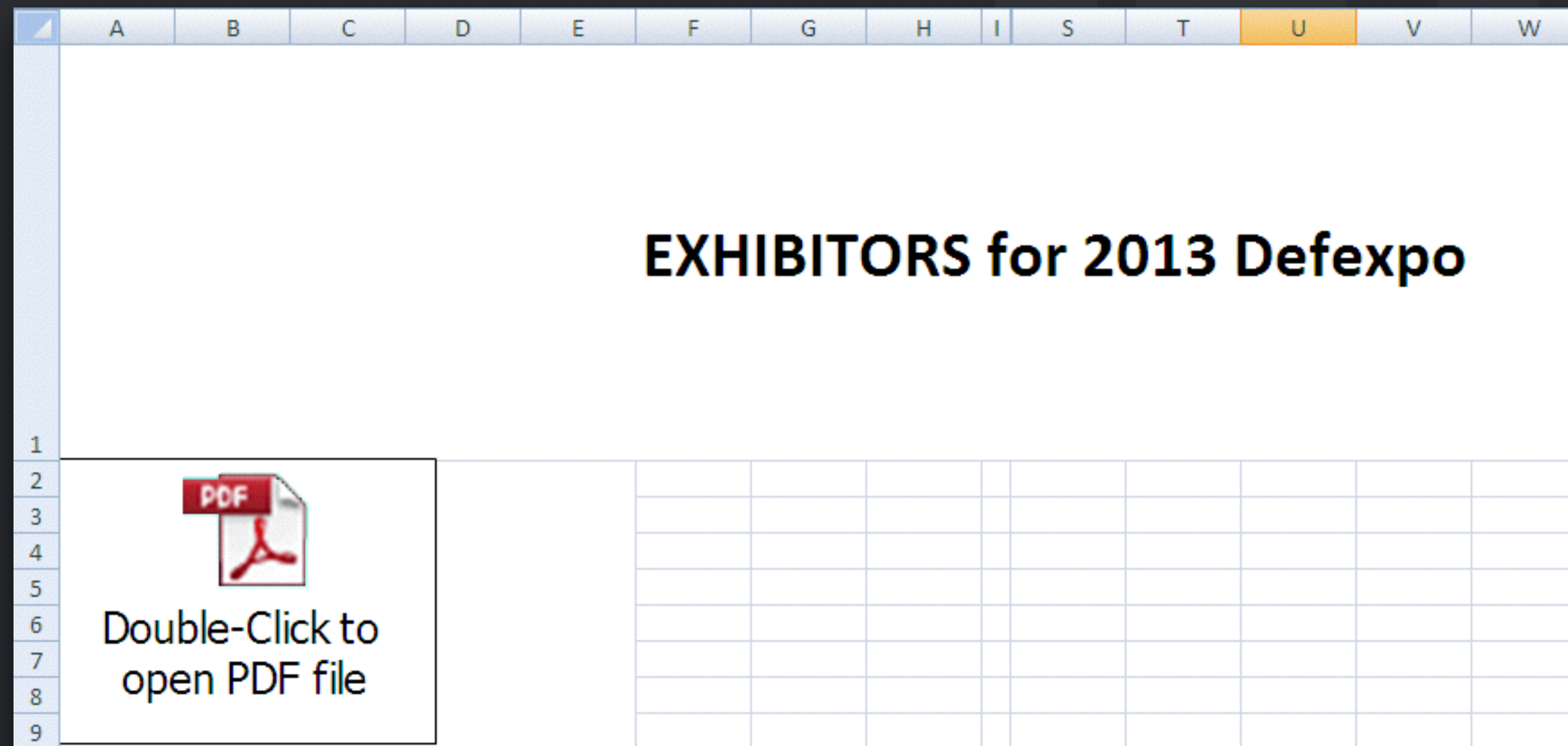


The poster for MSME DEFEXPO 2013 is circular with a yellow border. The text around the border reads: "MNCs identify offset partners | Indian Companies find sub-contractors | MSMEs pinpoint buyers, new technologies, new products". The center of the poster features a collage of images including a ship, a jet, a tank, and a truck. The main text in the center reads: "MSME DEFEXPO 2013", "12TH, 13TH & 14TH Dec 2013", "DR. PRABHAKAR KORE CONVENTION CENTER", "Next to KLE Dental College", "Tumkur Road, Yeshwanthpura", "Bengaluru - 22". Below the circular graphic, the text reads: "INTERNATIONAL MSME SUB-CONTRACTING & SUPPLY EXHIBITION FOR DEFENCE - AEROSPACE - HOMELAND SECURITY". At the bottom, there are three sections: "SUPPORTED BY" with the Ministry of MSMEs Government of India logo, "ORGANIZED BY" with the NSIC logo (एन एस आई सी, ISO 9001 : 2008, A Government of India Enterprise), and "SUPPORTED BY" with the Government of Karnataka logo.



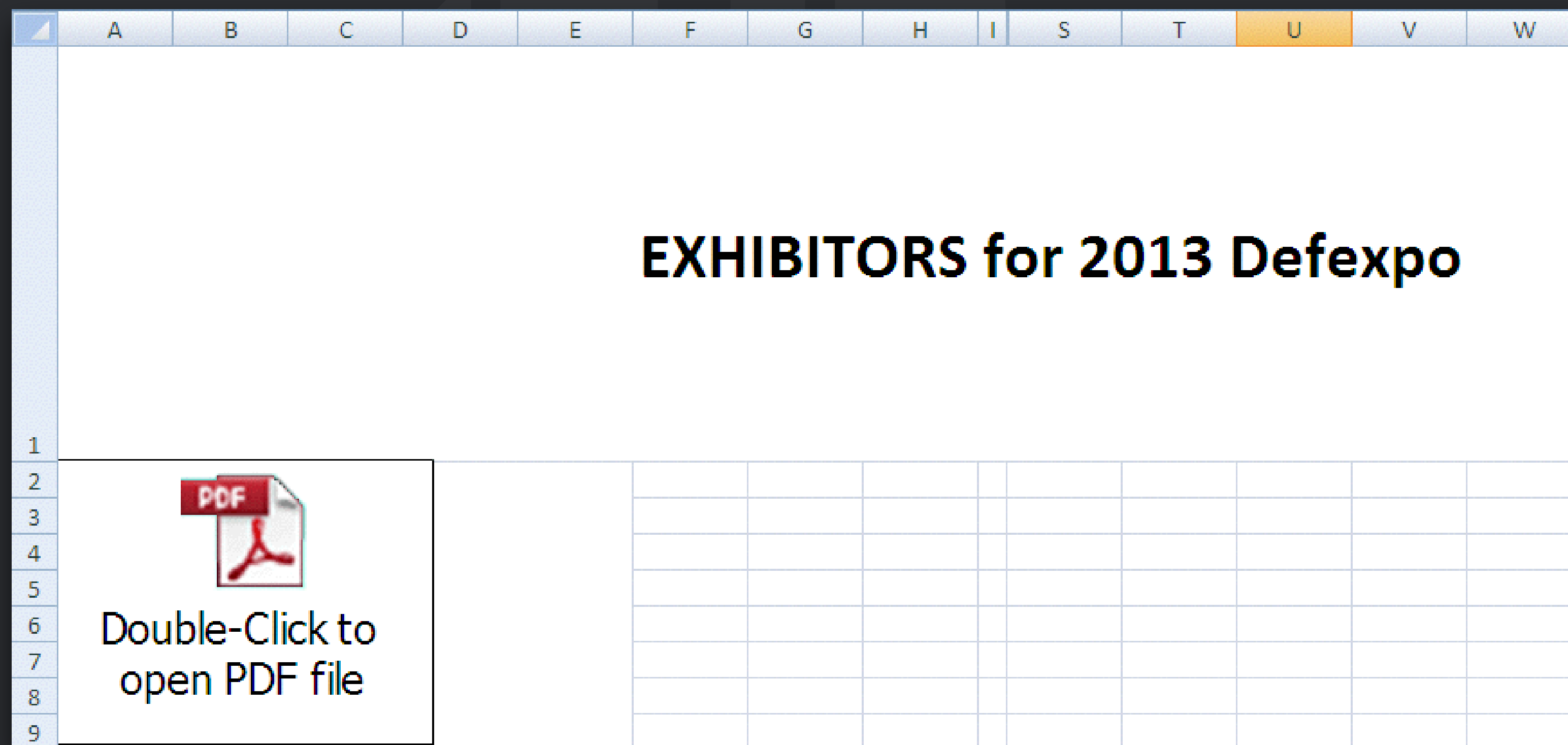
Mofang: India

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 warfare**” course



ESSENTIALS OF 21st CENTURY ELECTRONIC WARFARE COURSE
Registration Form
September 24 – 27, 2013 | AOC Headquarters – Alexandria, Virginia

Attendee Information (please print clearly or type)

AOC Member Number _____ Rank _____ or Dr. Mr. Mrs. Ms.

First Name _____ MI _____ Last Name _____

Badge Name _____ Title _____

Organization _____

Organization Complete Address _____

Email _____

Telephone Number (_____) _____ Fax Number (_____) _____

How did you first hear about this course? Brochure JED Internet AOC Email Word of Mouth Defense News Other

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



Mofang: India

The screenshot shows the top banner of the defexpo 14 India website. On the left is the 'defexpo 14 INDIA' logo. In the center is the State Emblem of India with the motto 'सत्यमेव जयते' and the text 'Ministry of Defence Government of India'. On the right is the logo of the Defence Exhibition Organisation with the text 'Defence Exhibition Organisation Ministry of Defence Government of India'. Below these is the main title 'Land, Naval & Internal Security Systems Exhibition' and the dates '06th - 09th February 2014, Pragati Maidan, New Delhi'. A navigation menu on the left lists 'Home', 'About Us', 'Exhibitions', 'Contact Us', and 'Enquiry'. The main content area features a large image of a military helicopter and a tank. A semi-transparent text box is overlaid on the image.

defexpo 14 INDIA

सत्यमेव जयते
Ministry of Defence
Government of India

Defence Exhibition Organisation
Ministry of Defence
Government of India

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

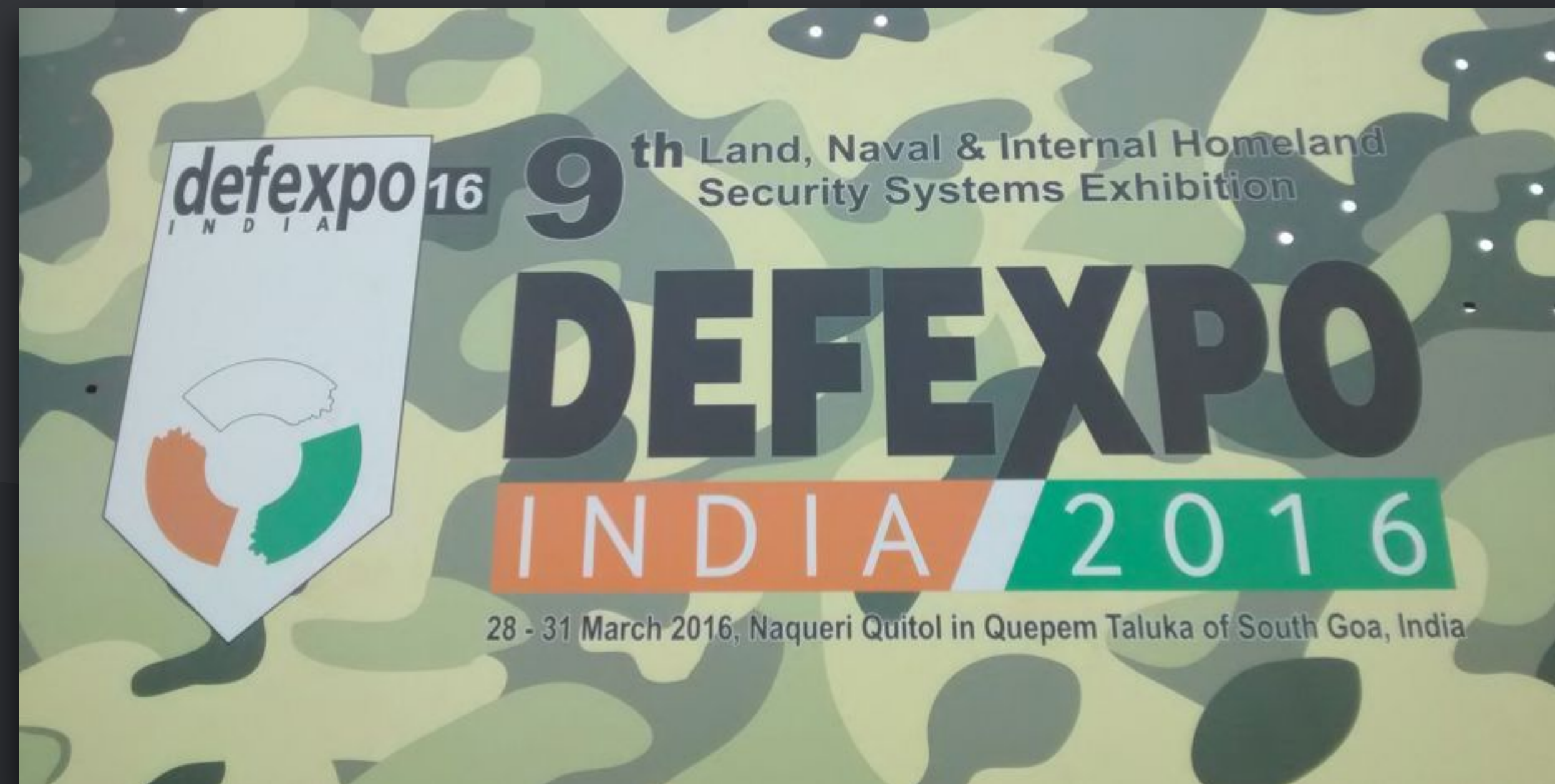
- ▶ Home
- ▶ About Us
- ▶ Exhibitions
- ▶ Contact Us
- ▶ Enquiry

Spear phishing the **exhibitors** of the **MSME DEFEXPO 2014**
Command and control server: **images.defexpoindia14.com**



Mofang: India

How about MSME DEFEXPO 2015, 2016 ?



We cannot confirm any cases but Mofang's specialisation in 2014 says enough.



Mofang: global campaign

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



Mofang: global campaign

ie.update-windows-microsoft.com

store.outlook-microsoft.com

mail.upgoogle.com

support.outlook-microsoft.com

windws-microsoft.com

help.outlook-microsoft.com

account.google.com.gmgoogle.com

oem.outlook-microsoft.com



Mofang: some latest activity

In September 2015 the Mofang group setup a new type of lure we had never seen them do before.



Mofang: some latest activity



CITRIX®

GoToMeeting



Mofang: some latest activity



Domain	Created	Expires
citrixmeeting.com	2005-04-13	



Mofang: some latest activity



CITRIX
GoToMeeting

Domain	Created	Expires
citrixmeeting.com	2005-04-13	2015-04-13



Mofang: some latest activity



CITRIX®
GoToMeeting

Domain	Created	Expires
citrixmeeting.com	2005-04-13	2015-04-13
	2015-07-27	2016-07-27



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:

Application name	Norton Identity Safe
Version (product specific)	2015.2.1.5
Hijacked DLL	msvcr110.dll
First seen used	2015-09-07
MD5	1f330f00510866522f14790398a5be59



Mofang: some latest activity

ShimRat was configured with a pseudo global campaign domain:

api.officelinetool.com

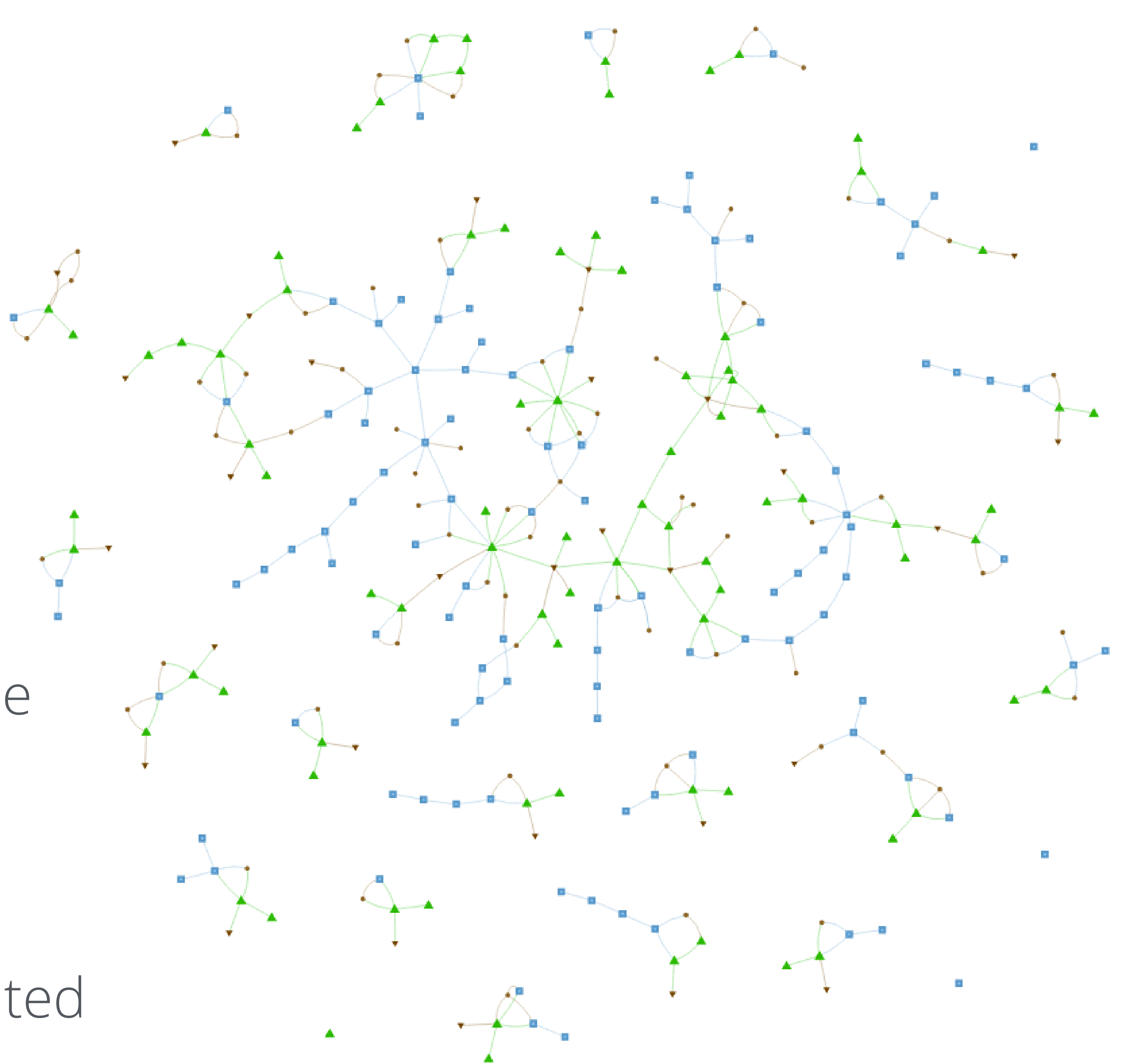


Conclusion

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

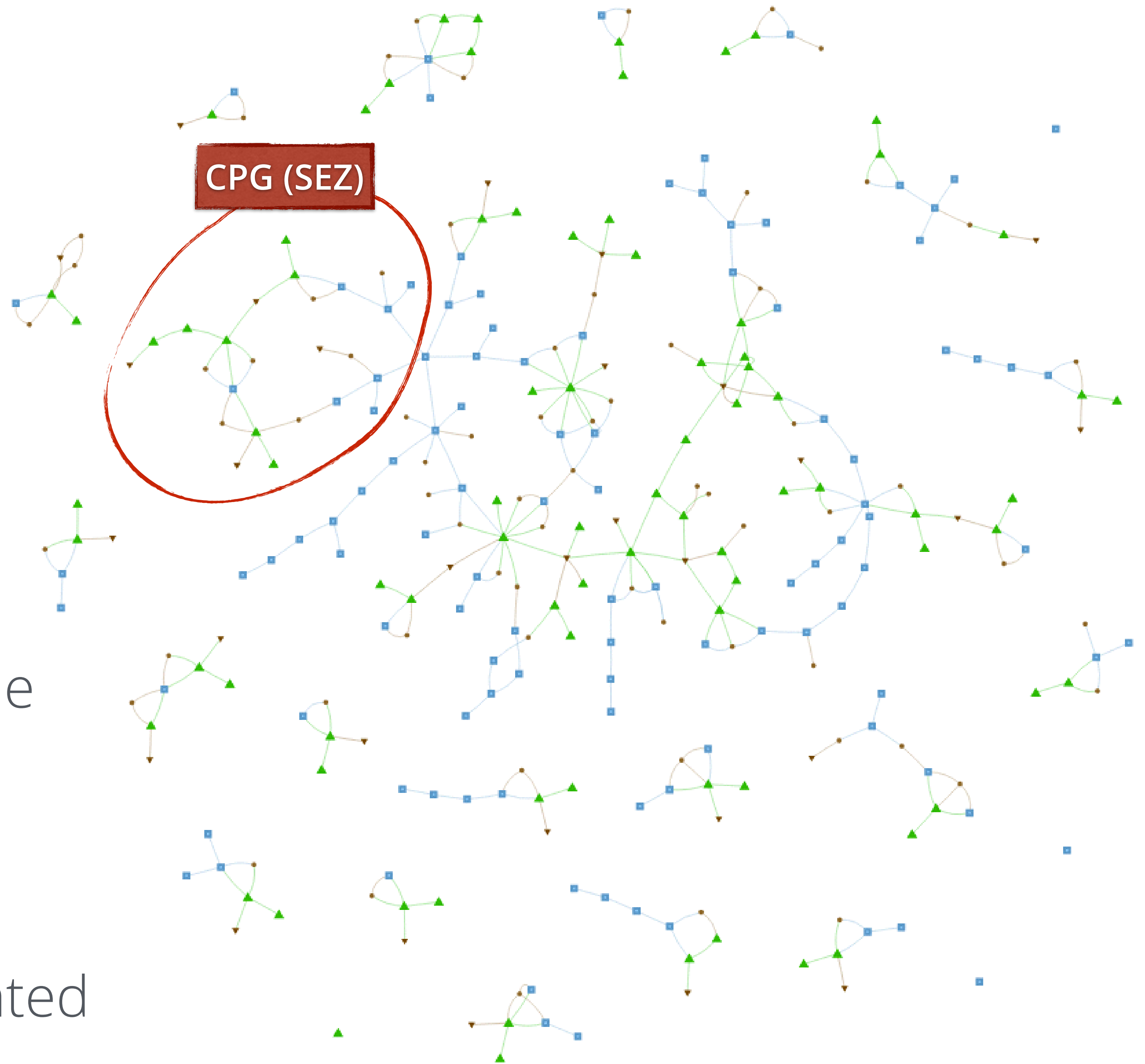
Conclusion

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



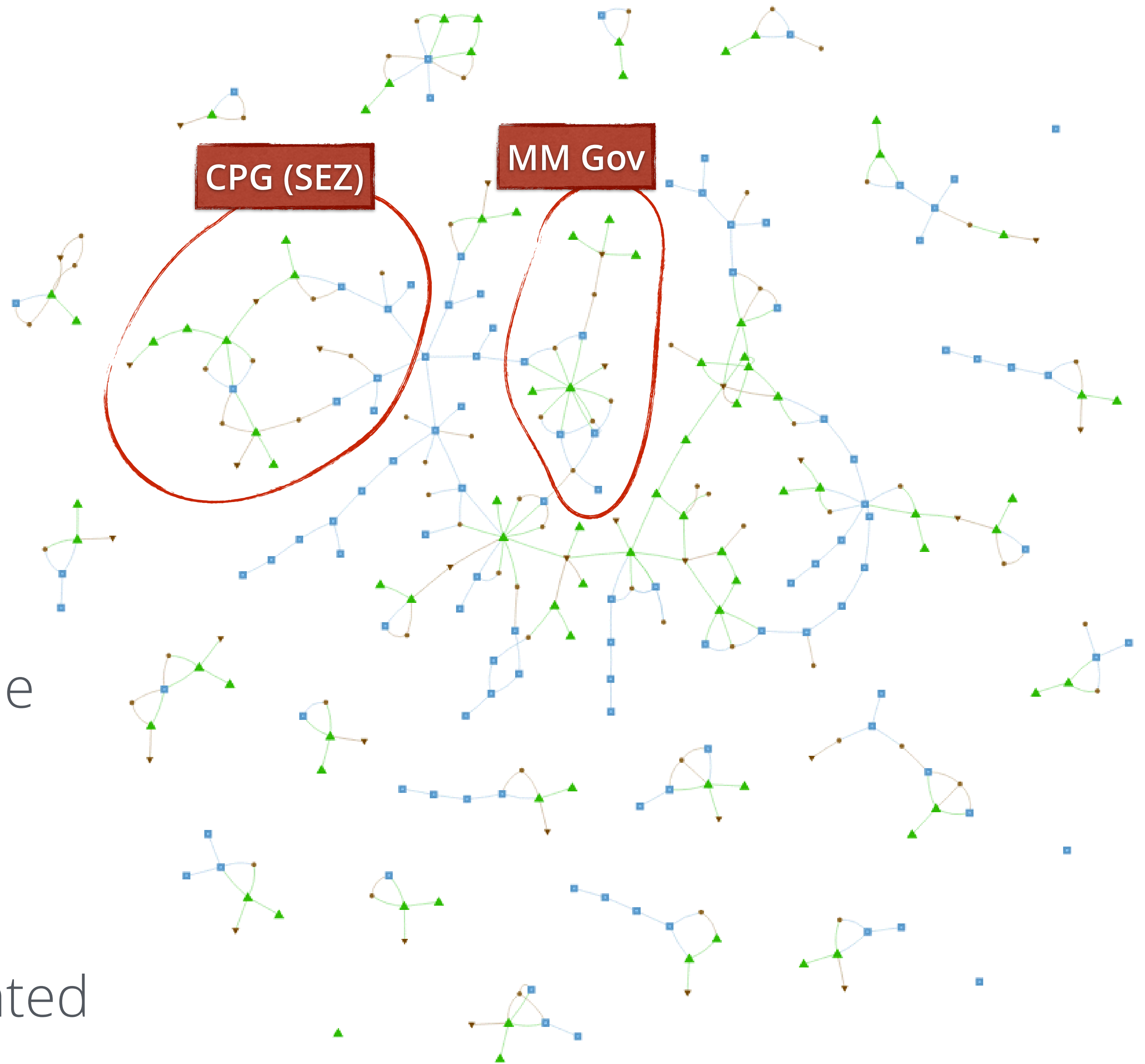
Conclusion

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



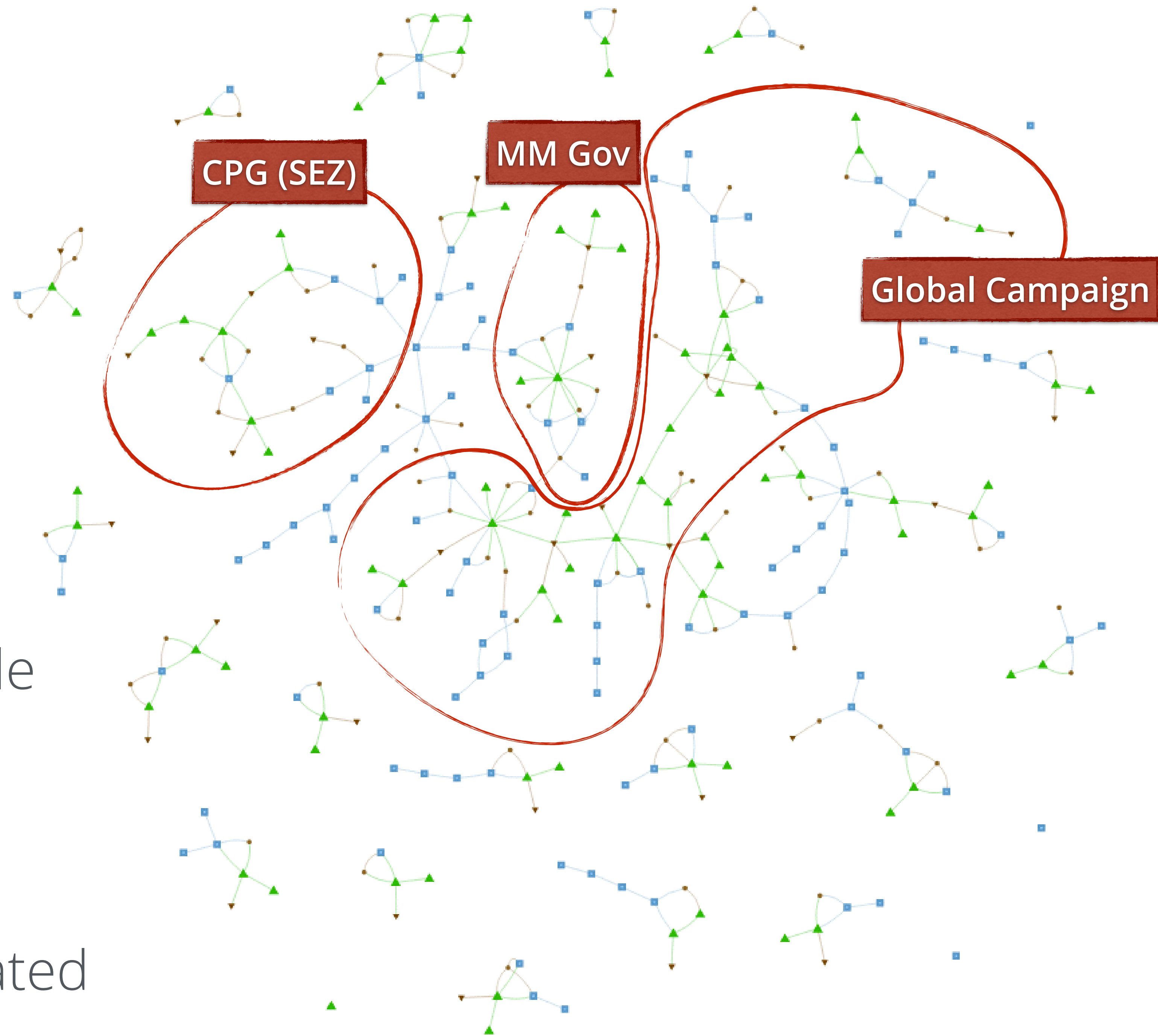
Conclusion

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



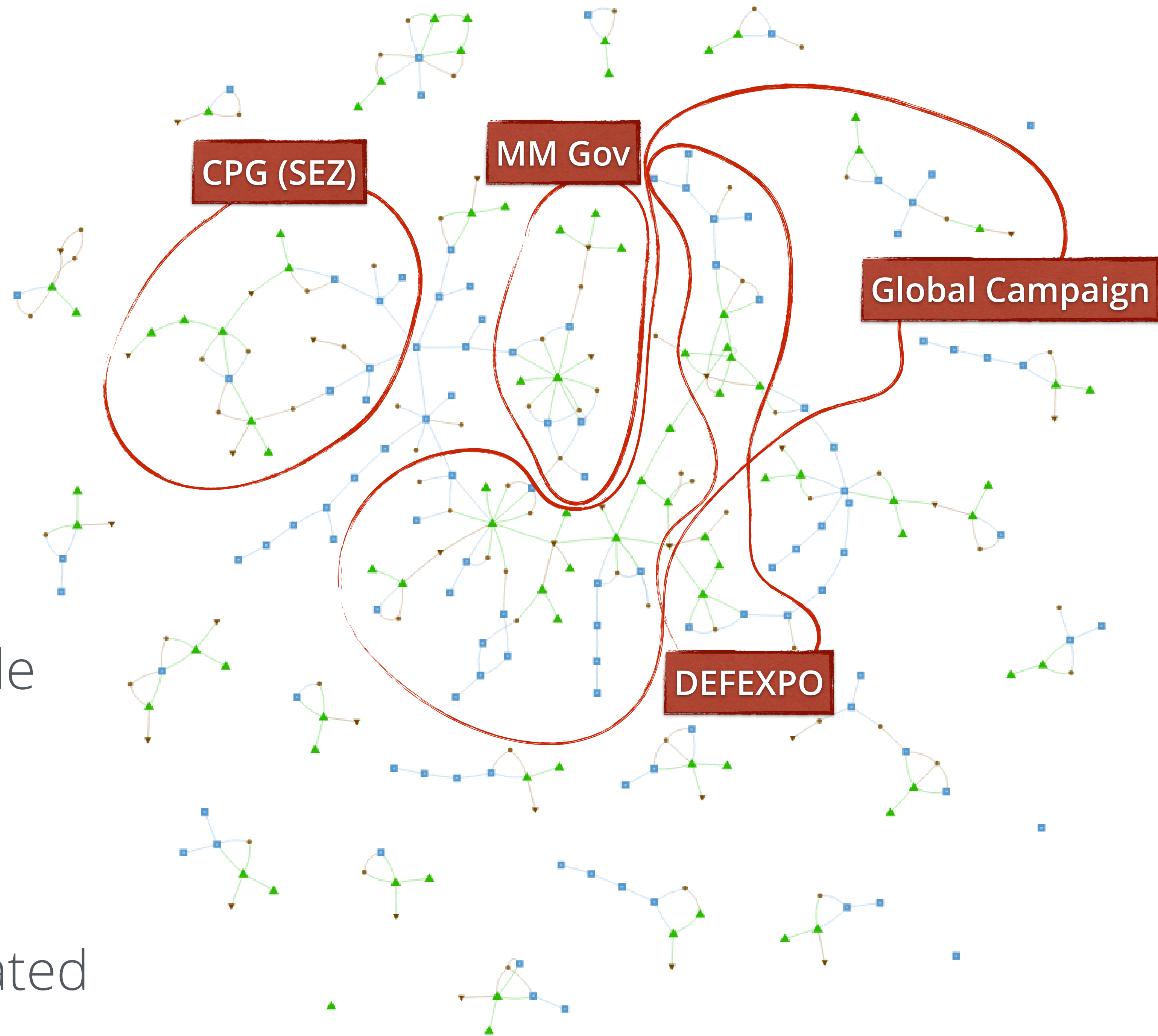
Conclusion

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



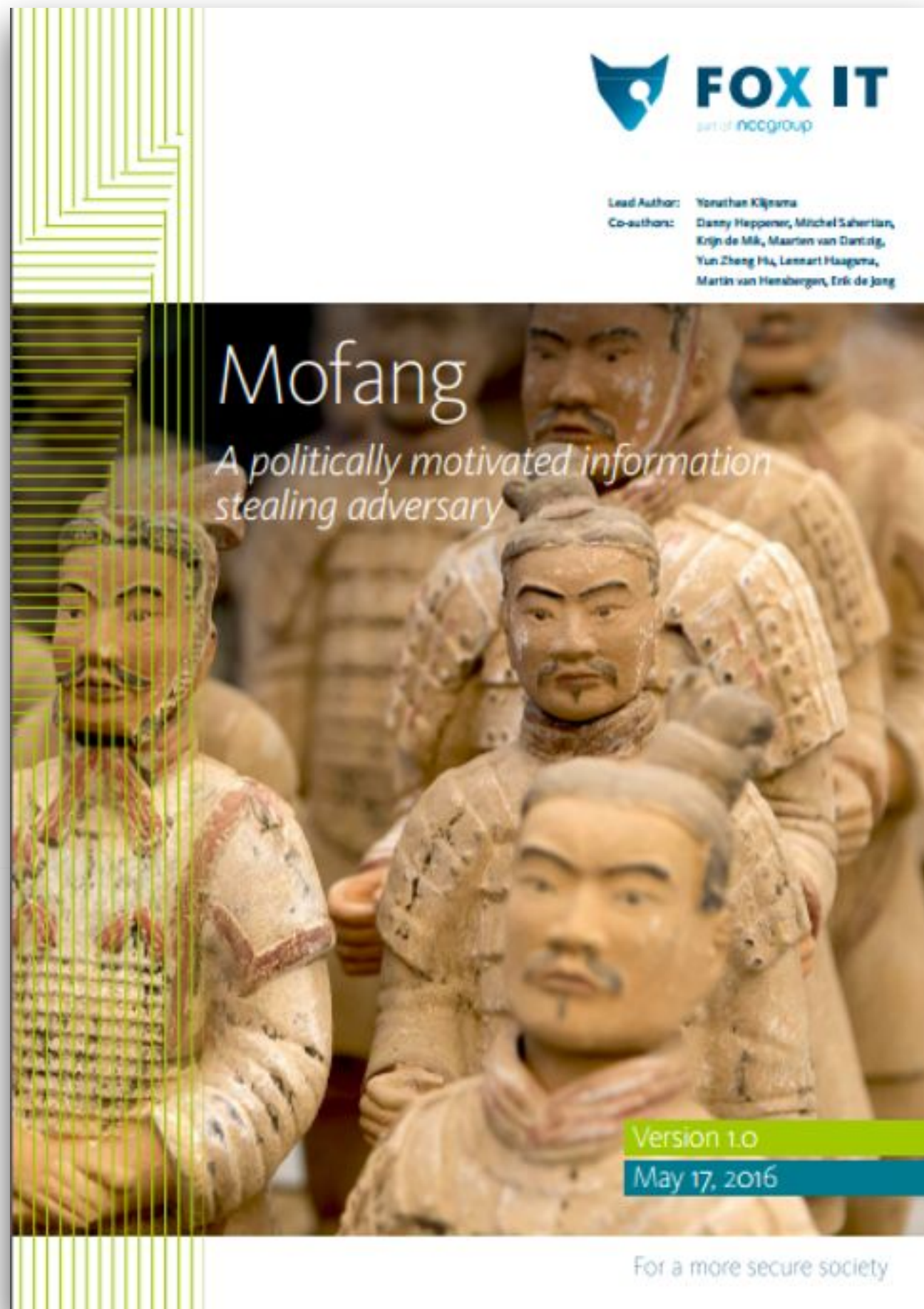
Conclusion

- 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>

