



---

## Contents

- 1 The Shifu Banking Trojan
  - 1 About Shifu
  - 2 High Level Features
  - 2 Principal Trojan Capabilities
  - 7 Communication Schemes
  - 9 Configuration
  - 10 Fraud M.O.
  - 14 Current Targets
  - 14 Likely Origins
  - 15 Protecting Banks Against Shifu Attacks
  - 15 About IBM Security Trusteer Solutions
  - 15 Contributors
- 

# Meet Shifu

*Masterful New Banking Trojan Targeting Japan and UK banks Version 1.0 September 2015*

## The Shifu Banking Trojan

### About Shifu

A brand new advanced banking Trojan discovered in the wild has been named “Shifu” by IBM X-Force research, after the Japanese word for ‘thief’. The malware appears to have been active since as early as April 2015; it was unearthed by IBM Security anti-fraud products through continuous protection of customer endpoints all over the world.

Due to the capabilities Shifu presents, it is considered a highly sophisticated banking Trojan. Our analysis reveals that some of this malware’s features and modules were borrowed from other banking Trojans leaked source codes, including Shiz, Gozi, Zeus and Dridex, making it a power-patchwork of sorts.

This report brings forward X-Force’s research and findings concerning Shifu, including information about its attack methods which are almost entirely focused on UK and Japanese banks at this time. This report is designed to better the detection of Shifu and help banks provide better protection for their customers.



## Shifu's High Level Features

The Shifu Trojan may be a new beast, but its inner workings are not entirely unfamiliar. The malware relies on a few tried and true Trojan mechanisms from other infamous crimeware codes. It appears Shifu's internal makeup was composed by savvy developers who are quite familiar with other banking malware, dressing Shifu with select features from the more nefarious of the bunch.

Some examples for those similarities are:

- **Domain Generation Algorithm:** Shifu uses the Shiz Trojan's DGA. The exposed algorithm itself is easy to find online, and the developers behind Shifu have elected to use it for the generation of random domain names for covert botnet communications.
- **Theft from Bank Apps:** Theft of passwords, authentication token files, user certificate keys, and sensitive data from Java applets is one of Shifu's principal mechanisms. This type of modus operandi is familiar from Corcow and Shiz's codes. Both Trojans used these mechanisms to target the banking applications of Russian and Ukraine-based banks. Shifu, too, targets Russian banks as part of its target list in addition to UK and Japanese banks.
- **Anti-Sec:** Shifu's string obfuscation and anti-research techniques were taken from Zeus VM (in its Chtonik/Maple variation), including anti-VM, and the disabling of security tools and sandboxes.
- **Stealth:** Part of Shifu's stealth techniques are unique to the Gozi/ISFB Trojan, and Shifu uses Gozi's exact same command execution scheme to hide itself in the Windows file system.
- **Config:** The Shifu Trojan is operated with a configuration file written in XML format; not a common format for Trojans, and similar to the Dridex Trojan's configuration (Dridex is a Bugat offspring).
- **Wipe System Restore:** Shifu wipes the local system restore point on infected machines in a similar way to the [Conficker worm](#), which was popular in 2009.

The following are the modules built in to the initial Shifu malware even before it communicates with its C&C server:

- Anti-Research, VM, and sandbox tools
- Browser hooking and web-inject parser
- Keylogger
- Screenshot grabber
- Certificate grabber
- Endpoint classification and monitoring applications of interest
- RAT and bot control module

In addition to these 'built-in' modules, Shifu calls home and downloads auxiliary capabilities from its Command and Control server (C&C) after the installation. Interestingly, the download of any other modules is done selectively and per conditions defined by the botmaster, or on-demand (manual).

## Shifu's Principal Trojan Capabilities


For a banking Trojan to be defined as 'advanced', it would typically need to possess a variety of real time theft mechanisms and more than one way to control infected endpoints, including user-grade takeover via RDP/VNC. Shifu appears to come with quite a few bells and whistles in that regard.

This Trojan steals a large variety of information that victims use for authentication purposes, covering different sorts of authentication. For example—it keylogs passwords, grabs credentials users key into HTTP form data, steals private certificates, and scrapes external authentication tokens used by some banking applications, on top of using web injection to manipulate users into divulging further critical information. These elements enable Shifu's operators to use confidential user credentials and take over bank accounts held with a large variety of financial service providers.

## Avoiding Security

First and foremost, and much like other advanced malware, Shifu deploys anti-security mechanisms to keep itself protected and avoid security roadblocks. The Trojan begins by verifying that it is not running on a virtual machine or in a sandbox environment. Next, it runs a scan of all running processes on the infected PC and disables a list of security products, including AVG, ESET, and PhishWall, and also looks for security research tools that may be running on that endpoint.

Shifu then deletes the user's local system restore snapshots so that they won't be able to restore the endpoint to a time when the malware was not on it.



```
01D00B52  _DeleteAllSRSnapshots proc near
01D00B52  push    ebp
01D00B53  mov     ebp, esp
01D00B55  push    esi
01D00B56  push    10h
01D00B58  pop     eax
01D00B59  call    j_chkstk
01D00B5E  mov     eax, esp
01D00B60  test    eax, eax
01D00B62  jz      short loc_1D00B75
```

Figure 1. Shifu deletes all system restore snapshots

## Web Browser Hooking and Manipulation

In order to control what victims see on bank web pages and enable itself to grab all outgoing HTTP form data, Shifu hooks all the popular browsers: IE, Chrome, Firefox, Opera, and Maxthon. To inject into these browsers, Shifu relies on URL triggers in its configuration file, selectively activating web-injections adapted to the target entity. In Shifu's case, all the current targets are banks.

## Remote Access and Endpoint Takeover

The Shifu Trojan possesses remote administration capabilities (RAT), enabling it to send commands to the infected endpoint, specifically to upload and download files. The botmaster likely downloads malware and configuration updates and uploads stolen files from the endpoint using this feature.

On top of its RAT-type commands, Shifu has a VNC module for remote desktop sharing. This feature is known from other banking Trojans, like Citadel for example, that use a VNC connection to the infected PC in order to initiate transactions directly from the infected device. By doing so, they can bypass fraud protections that are based on device fingerprints, IP addresses, or any other element that relies on trusting the user's device(s).

## Trigger-Based Information Stealing

Shifu steals different authentication elements and data from infected PCs based on triggers set up in its configuration file. Some examples appear below:

- **Key strokes:** Keylogging – Shifu implements a keylogger on the infected PC that collects keystrokes and writes them into a file with details of the application they were grabbed from.
- **Screenshots:** To steal real time information on what the user is doing on their PC, Shifu can take screen captures on demand, going into action according to the website or application the user has topmost on their desktop. In many cases, Trojans use this feature to grab passwords entered on a virtual keyboard.
- **Certificates:** Shifu possesses a certificate grabber designed to scan the certificate store on the endpoint, steal and forward the user's private certificates to the attacker.
- **Cookies:** The malware wipes all the cookies from the infected endpoint to make the browser acquire new ones, and then steal them on the fly.

## Special Handling for Point of Sale

Shifu does not skip a beat and checks if the endpoint it has landed on is perhaps operated as a point of sale (POS). If so, it can be of value to its operators for stealing payment card data.

To check whether the endpoint is a POS, the malware searches the machine for the string pos.exe. If it finds that string, Shifu has a RAM-scraper ready to deploy. RAM-scraping is the top method for siphoning credit and debit cards' track 1 and track 2 data, used in major breaches like the Target breach.

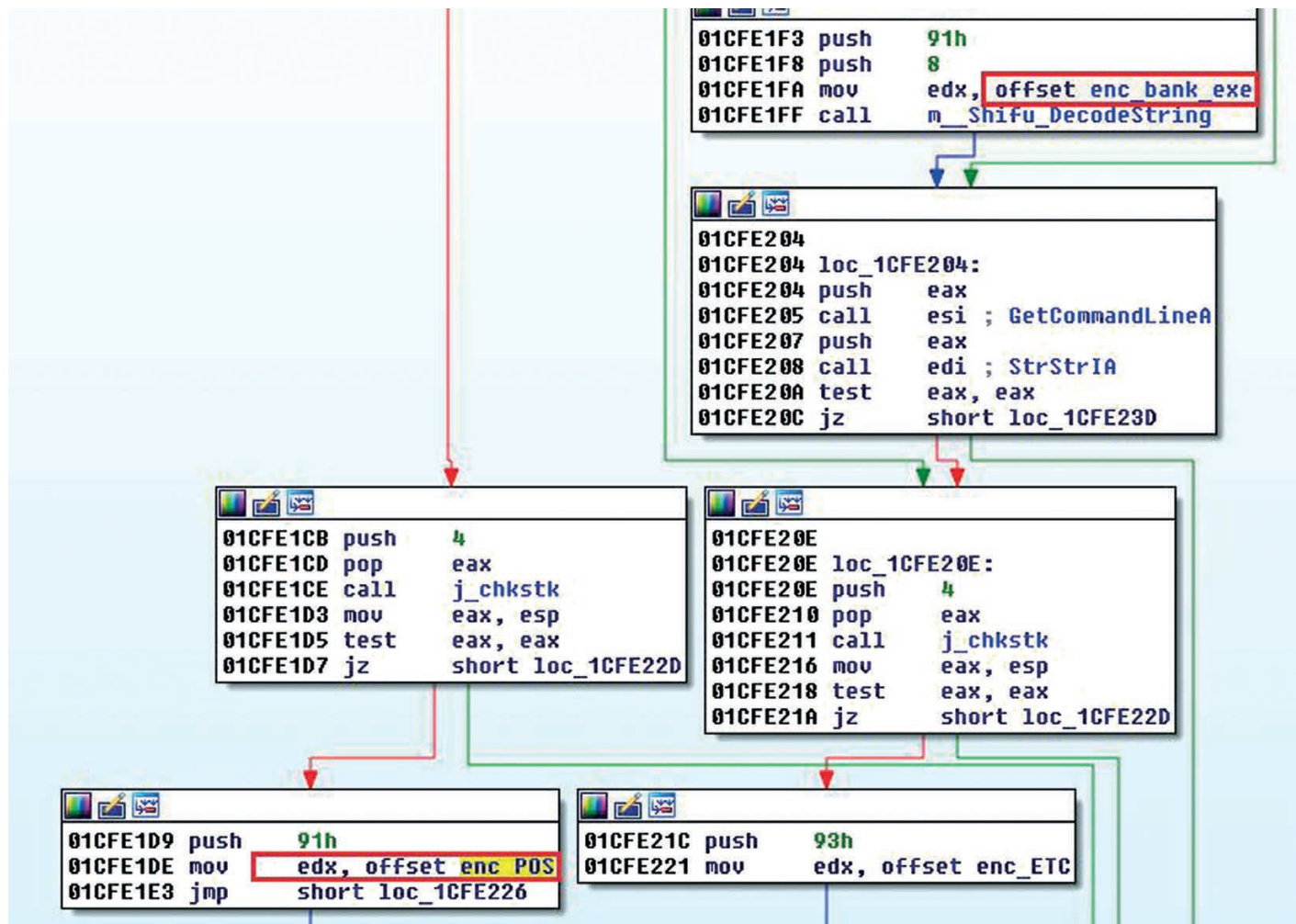


Figure 2. Shifu scans for executable files named POS or bank

## Exfiltrating Data from Smartcards

Shifu appears to be shooting in all directions and grabbing information from a number of sources. Another feature in Shifu enables it to steal the contents of smartcards attached to the infected endpoint.

For each new injected process on the endpoint, shifu checks for connected smartcard readers. If a smartcard is present, Shifu parses its content and in some cases it also attempts to copy and exfiltrate data from the card reader.

## Crypto-Currency Wallet Stealing

Crypto-Currency stealer – Shifu searches the endpoint for Bitcoin and Litecoin wallets, looking for Administrator\litecoin\wallet.dat files. Taking over wallets can enable Shifu to steal the coins they have amassed for their owners.

## Attack Electronic Banking Platforms

While web-injections are a common Trojan capability, very few Trojans target banking platforms. Such attack type is known from older malware like Shiz that targeted banking platforms used by Russian banks. Shifu has a similar aim on Java applet-based platforms where it hooks the Java processes and scans for .tok files. What Shifu is after in this case, are tokens used as short term authorizations for external authentication schemes.

Shifu also steals digital signature credentials used by business banking applications to authenticate customers, particularly in Japan, Germany, Austria, Italy, and Russia.

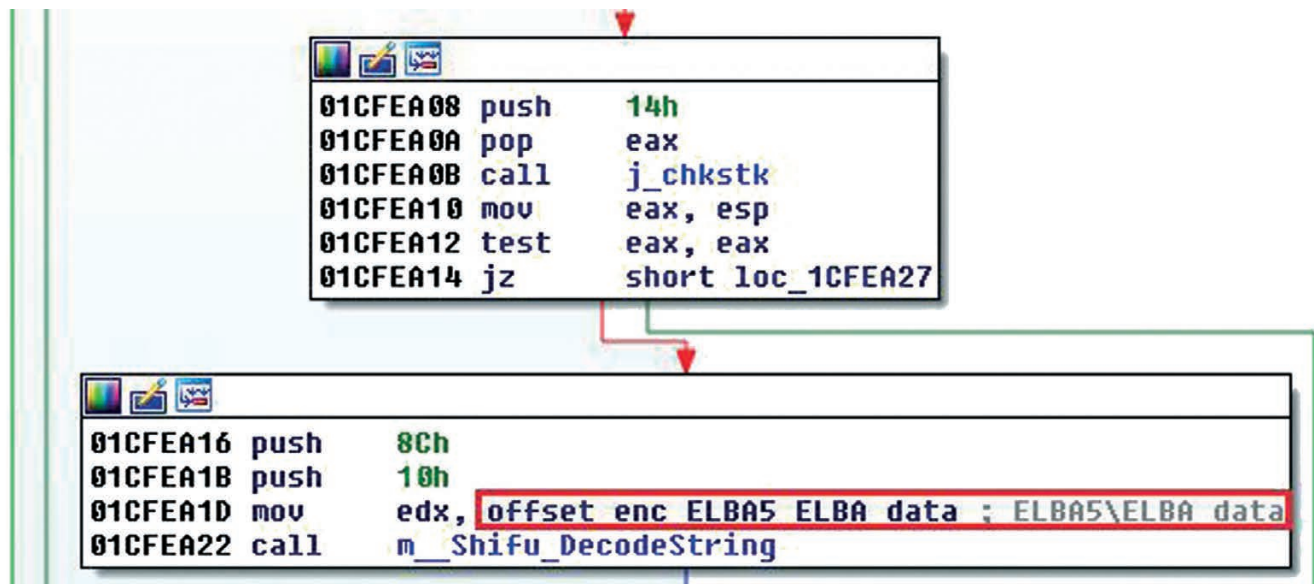


Figure 3. Shifu scans for specific bank application folders

The benefit of targeting banking application, rather than specific websites, is to make attacks more generic in the sense that they will fit more targets. If the malware's developer finds a way to compromise an application/platform in one case, it will likely work the same on other banks using that platform.

In that sense, it is not surprising that Shifu wants to cover as many potential victims as possible with one broad stroke. Malware like Dyre and Dridex are also known for building their configuration files to target regular expression strings common to popular banking applications.

In its current configurations, Shifu targets the following platforms:

[MultiCash](#) and MultiCash@Sign – An electronic banking platform that serves large corporations for the purpose of e-banking across the globe. MultiCash serves customers all across Europe. Shifu hunts for access credentials to the MultiCash@Sign plugin banks enable their major customers to use.

[Elba5](#) – Electronic banking platform vendor serving the Austrian market. Shifu hunts for Elba data that may be found on the infected machine.

[HBP Hypo Office Banking](#) – a platform that serves enterprise clients for the purpose of e-banking via multiple bank accounts. HBP serves the Austria market. Shifu hunts for HBP customer profile data.

## Keeping Intruders Out

Once Shifu has landed on a newly infected machine, it wants to keep all other uninvited malware out of the game. This concept is not new: the SpyEye malware author already implemented it with his “[Kill Zeus](#)” command in 2010. But Shifu goes the extra mile to make sure that no other malware at all lands on the computer.

Shifu monitors the processes of a list of applications that interact with the Internet on a regular basis:

- iexplore.exe
- opera.exe
- firefox.exe
- chrome.exe
- maxthon.exe
- java.exe
- javaw.exe
- plugin-container.exe
- acrobat.exe
- acrod32.exe

The Trojan hooks the [URLDownloadToFile](#) function, which is used for simply downloading code from the Internet and saving it as a file on the computer. This way, Shifu keeps close watch on the incoming files the endpoint receives, looking out for competition in the shape of common malicious file characteristics:

- Files coming from non-secured connections (HTTP)
- Executables
- Unsigned



As soon as a file of that sort comes in, Shifu copies it to the local disk and names it “`infected.exe`”. It then exfiltrates it to its master’s C&C server. Shifu also spoofs a reply to the operating system which is trying to run the downloaded file, with: “Out of Memory” (OOM).

This feature serves to keep Shifu exclusive on the machines it infects.

Moreover, sending malware files to its operator on a regular basis allows Shifu to keep tabs on the competition and find out when other cybercriminals are attacking in the same geographical turfs.

### Download More Malware

Shifu can work as a downloader for other malware, which it is able to pull from any Internet source. The Trojan downloads an executable file to a temporary folder. It then calls a `process create` API function, and launches the executable.

### Endpoint Event Log

Endpoint Tracker – Shifu tracks and logs all the events that take place on the infected endpoint, and reports them to the botmaster on demand. Although it may not be the only reason, it is possible that since the malware is in active development, the developer has set up this tracking to better understand what happens on the endpoint when the malware is blocked or runs into any issue.

### Shifu's Communication Schemes

After its first live ping to the C&C server, Shifu monitors the user’s activity and sends data/files to the command and control according to its configuration.

Shifu communicates over HTTPS secured connections. It uses a self-signed certificate using generic details:

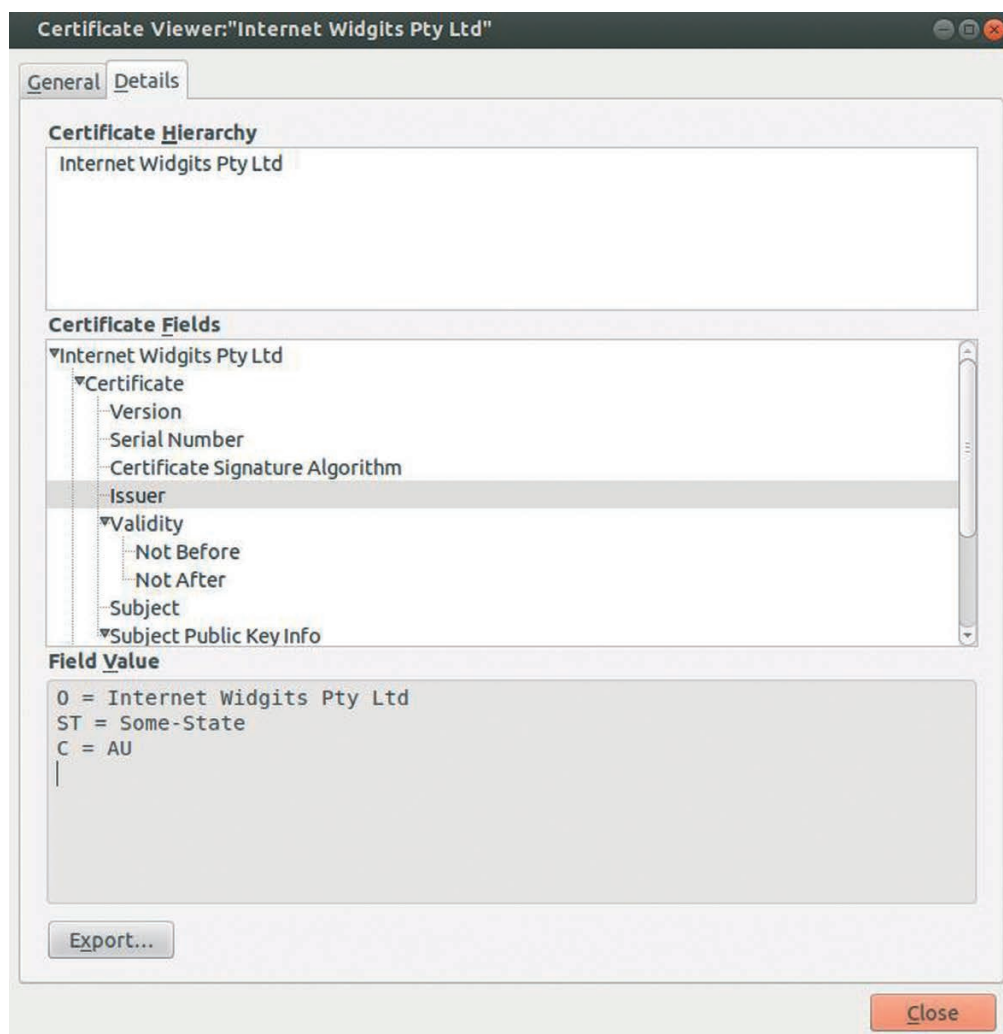


Figure 4. Shifu's self-signed SSL certificate



“Internet Widgits Pty Ltd” is a generic entity name; it is used by other malware, like [Dyre](#) for example. That sort of self-signed certificate can be created for free, with OpenSSL. Legitimate entities would normally use a certificate signed by a trusted Certification Authority.

The first call home transmission contains information about the endpoint, sent in a set template:

```
botid=%s&ver=%s.%u&up=%u&os=%u&lname=%s&d&tok  
en=%d&cn=%s&av=%s&dmn=%s
```

The endpoint details Shifu collects and sends to the C&C server are:

Parameter	Information collected
ver	Malware's bot version
up	OS uptime since last reboot
os	Endpoints operating system version
lname	Local time on the infected endpoint: GMT + X
av	Name of Anti-Virus installed on the endpoint

Some of Shifu's known bot commands are:

Parameter	Information collected
!inject	Activate web injections
!update	Update malware version
!load	Load and execute external binary
!kill_os	Download and launch a module to kill the operating system
!wipe_cookies	Erase the user's cookies
!docfind	Search the local file system

Shifu operates a C&C server for the malware's updates and commands, and three additional communications resources for the configuration and web injections.

Bots are instructed to communicate with Shifu's servers using its DGA.

### Shifu's Configuration

Shifu operates with a malware configuration of the same functionality as other banking Trojans. Its configuration's structure, written in XML, closely resembles the Dridex Trojan's configuration.

Shifu's developer has encrypted the information in the config file, including its C&C addresses and the web injections. Moreover, the Trojan reaches out to a remote server to request the corresponding injection.

### On the Fly Injection Fetching

Reminiscent of another advanced banking malware, Dyre, Shifu conceals its web-injections and does not show them in the configuration file. Instead, it fetches them in real time from a remote server. But this is where its resemblance to other Trojans end. To call on the correct injection at the right time, Shifu's developers have created an interesting round-robin resolution to a local PHP server opened on the infected machine.

### Deobfuscation via Local PHP Server

When a new endpoint is infected by Shifu, the malware downloads and deploys an archived file folder on that PC that turns it into a LocalHTTPserver. This local Apache server is then used for decrypting web injections, host, and receive injected JavaScript from a remote Shifu server.

To implement this real time fetching, Shifu accesses a remote web-injects server. Wanting to keep that server's address concealed, the server's name as it appears in the configuration is not decipherable and seems bogus at a first glance.

For example, the string below is supposed to be the web address of Shifu's remote server, sent to the browser to resolve:

```
https://secure.12345a6786238571814517665722e6  
2123a.moz.bankName/?c=script&v=1&r="  
bank-injection-token
```

In reality, the request is obfuscated. Instead of going to the web browser as-is, Shifu's requests first go to the local PHP server. The server has HEXtoString function instructions to interpret the request, fix it, and then send the real one off to the browser in its proper form.

```
https://shifuremote.server/?c=script&v=1&b=  
USER!WIN8X86SP2!E12ABC34&r="bank-injection-  
token
```

The part in the request that notes "bank-injection-token" is used by the remote web-injects server to discern which attack script it should return, according to the request's parameters. Each infected endpoint can thus receive a different injection adapted to the banking website used.

Resembling Dyre's methods, Shifu's injections are selective and change according to the targeted entity. In some cases it replaces the bank's entire page with a fake replica designed to harvest the data Shifu's operators are after. In other cases, the

Trojan displays social engineering content on the page, using JavaScript injections, to ask victims for additional authentication elements it will need for a subsequent fraudulent transaction, such as PII, or one time passwords.

Shifu, like other high-grade Trojans of its level, further operates a transaction automation system (ATS) which streamlines fraudulent transactions in an automated manner, pre-programmed by its operators.

ATS panels have a dashboard interface that allows fraudsters to initiate and streamline illicit transactions directly from the panel, essentially controlling compromised accounts from one central. ATS panels are not a new concept and have been available in the underground for over six years now both as a commodity and in SaaS mode.

### Shifu's Fraud M.O.

The Shifu Trojan's extensive theft capabilities and data acquisition techniques enable its operators to use different fraud methods against banking customers.

The main financial fraud methods Shifu uses in the wild are based on certificate grabbing and web injections. Some details on each scenario appear below.

### Fraud via Certificate Theft

In this first method, Shifu targets banks and banking applications that authenticate users based on a digital certificate the user holds on their endpoint. With that certificate, the user does not typically need to use additional authentication credentials and the endpoint is considered trusted. Shifu steals that certificate and accesses the victim's account, able to then carry out fraudulent transactions.

In other cases, Shifu resets the certificate's password and renews the digital signature.

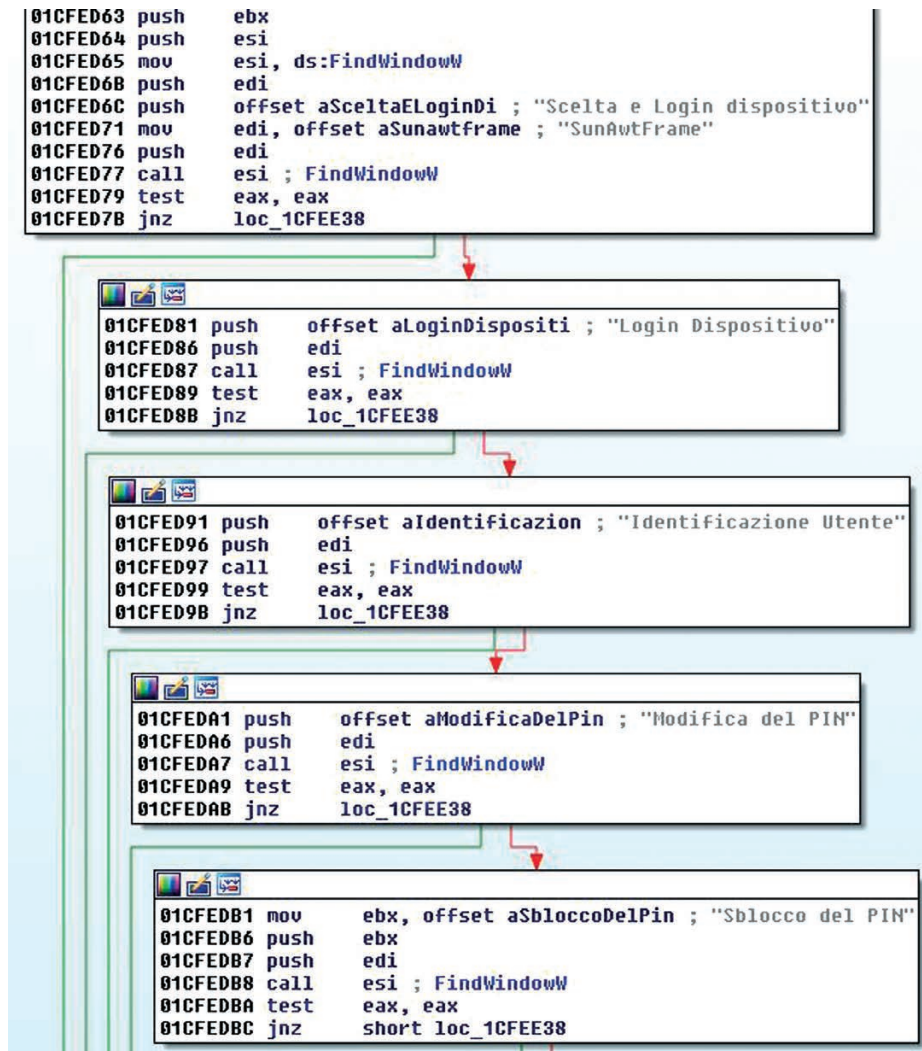


Figure 5. Shifu hunts certificate credentials to reset their PIN code

## Fraud via Web Injections

In its more popular fraud method, Shifu manipulates what users see on the bank's page to ask for and obtain victims' login credentials, as well as any other authentication elements needed. The fraudster then follows up with an illicit transaction from the victim's device, using VNC. In other cases the fraud originates from another device the fraudster controls.

Shifu begins by disabling some security solutions, like the PhishWall browser extension, and AVG and ESET AV if those are installed on the machine. It then proceeds with its malicious activity.

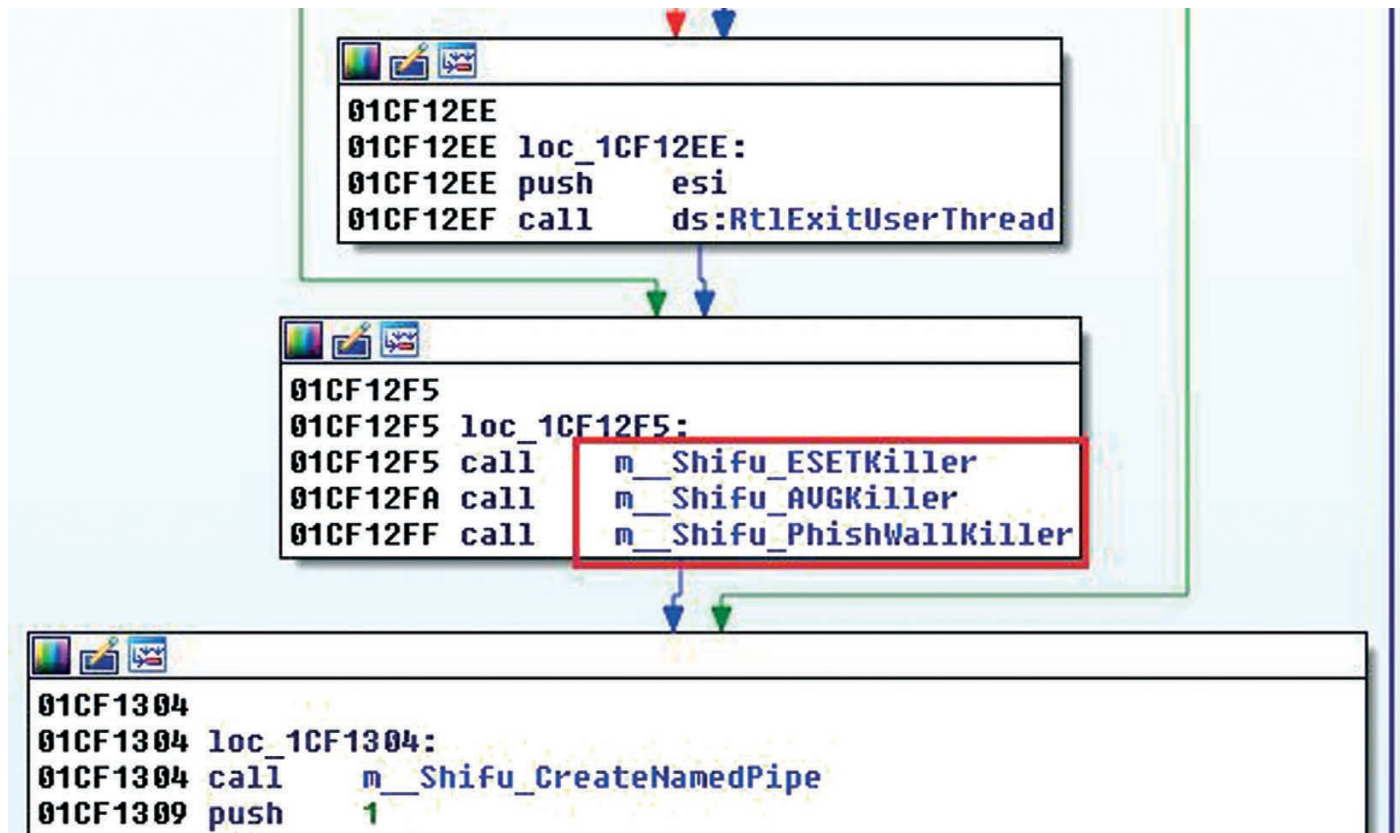


Figure 6. Shifu disables special security extensions in the browser

Unlike most Trojans, which vastly use Zeus' injection mechanism, Shifu's web injections are a proprietary creation coded by its developer; rather indicative of the developer's capabilities and his desire to write his own code.

On top of its custom injection mechanism, Shifu has the proper infrastructure in place to use Zeus-like injections. This makes it more versatile and customizable to use on different bank websites.

To steal credentials, Shifu begins by grabbing HTTP forms before the actual login takes place. It sends the data to the C&C and the banking session proceeds normally.

In some cases, depending on the bank being targeted, Shifu may need more details from the account holder. It will then alter the online banking page using JavaScript to insert questions or data fields that the victim will be tricked into filling. Shifu replaces the entire page according to the amounts of data it plans on harvesting.

Once the victim is tricked into divulging their confidential information and authentication tokens to Shifu, the fraudster operating in the background uses the details in fraudulent transactions.

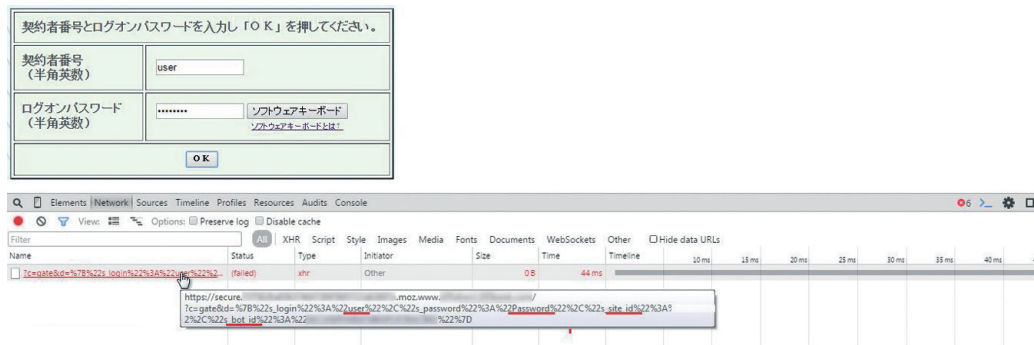


Figure 7. Shifu parameters for credential interception

### Shifu's Current Targets

- Financial institutions in the UK
- Financial institutes in Japan
- Financial institutes across Europe

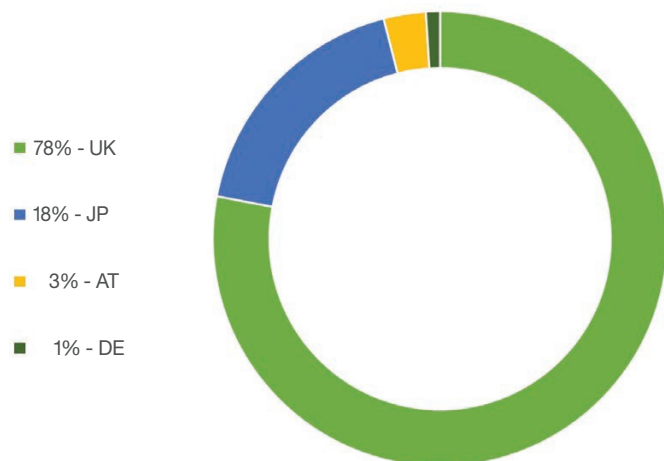


Figure 8. Shifu Trigger Distribution per Target Country  
(Source: IBM Security)

According to Shifu's URL trigger list, it presently targets 18 major UK banks, and 14 major Japanese banks. According to IBM Security data, while Japan was initially the only geography where banks are under active attacks by Shifu, the situation shifted in late September 2015, adding UK banks to the list of the attacked geographies.

Beyond its bank-specific attacks, Shifu also targets electronic banking platforms that serve banks across Europe, with specific aims for vendors that operate in Austria, Germany, and Italy.

### Shifu's Likely Origins

Following analysis of Shifu's scripts, our researchers found comments written in Russian. Shifu's developers could be either Russian speakers or native to countries in the former Soviet Union. It is also possible that the actual authors are obfuscating their true origin, throwing researchers off by implicating an allegedly common source of cybercrime.

Some specific strings found during analysis of Shifu are not written in Cyrillic letters, but have meanings in Russian. For example:

BUH – References the word “accounting” in Russian

KASSA – “Cashbox” in Russian

FINOTDEL – Corporate slang for the “Accounting Dept”.

ROSPIL – Russian government most prominent opposition party.

Shifu's servers are located in different countries, with domains hosted on IP addresses alongside a plethora of .ru domains that may or may not be linked to the same gang.

## Protecting Banks Against Shifu Attacks

### Trusteer Customers – Current Protection Status

#### IBM® Security Trusteer Rapport®

**IBM Security Trusteer Pinpoint™ Malware Detection**  
(PPMD detects Shifu, malware ID: 71, with Active detection).

#### IBM Security Trusteer Pinpoint Criminal Detection

#### IBM Security Trusteer Apex™ Advanced Malware Protection

All versions are updated in real time and detect this Shifu malware variant, as well as ATO and transactions initiated from Shifu-infected machines, providing protection against its malicious activity. Please note that Shifu is a highly reactive project at this time and its developers are working constantly to continue evolving the malware's evasion and attack techniques.

### About IBM Security Trusteer Solutions

With IBM Security Trusteer® solutions, financial organizations gain access to a real-time malware intelligence network that provides insight into fraudster techniques and capabilities. This global threat intelligence serves as the foundation for IBM Security Trusteer automated threat protection capabilities, and is used by IBM Security experts to help develop and deliver new protections for organizations like yours.

At IBM, a research and development (R&D) team of security experts scrutinizes threat intelligence as it arrives from a variety of sources including from Trusteer-protected endpoints as well as underground venues. IBM Security Trusteer solutions use this intelligence to deliver flexible protection layers that can be rapidly configured and updated by IBM R&D staff. As a result, as soon as new threats emerge or mutate, new protections are automatically deployed back into Trusteer software without any intervention by bank security staff and without any noticeable impact to banking customers.

If you have any questions, contact our Enterprise Support team at: [enterprise.support@trusteer.ibm.com](mailto:enterprise.support@trusteer.ibm.com)

### Contributors

We would like to thank the following individuals for their contribution to the publication of this research paper.

Contributor	Title
Denis Laskov	Information Security & Malware Researcher, IBM Security Trusteer
Ilya Kolmanovich	Information Security Threat Engineer, IBM Security Trusteer
Limor S. Kessem	Sr. Cybersecurity Evangelist, IBM Security



## For more information

To learn more about IBM Security Trusteer, please contact your IBM representative or IBM Business Partner, or visit the following website: [ibm.com/Security/services](http://ibm.com/Security/services)

If you have any questions, contact our Enterprise Support team at: [enterprise.support@trusteer.ibm.com](mailto:enterprise.support@trusteer.ibm.com)

IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. For credit-qualified clients we can customize a financing solution to suit your business and development requirements, enable effective cash management, and improve your total cost of ownership. For more information, visit: [ibm.com/financing](http://ibm.com/financing)

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



© Copyright IBM Corporation 2015

Security  
Route 100  
Somers, NY 10589

Produced in the United States of America  
September 2015

IBM, the IBM logo, ibm.com, Microsoft, Trusteer Rapport, Trusteer Pinpoint, Trusteer Apex, and Security Trusteer trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.



Please Recycle