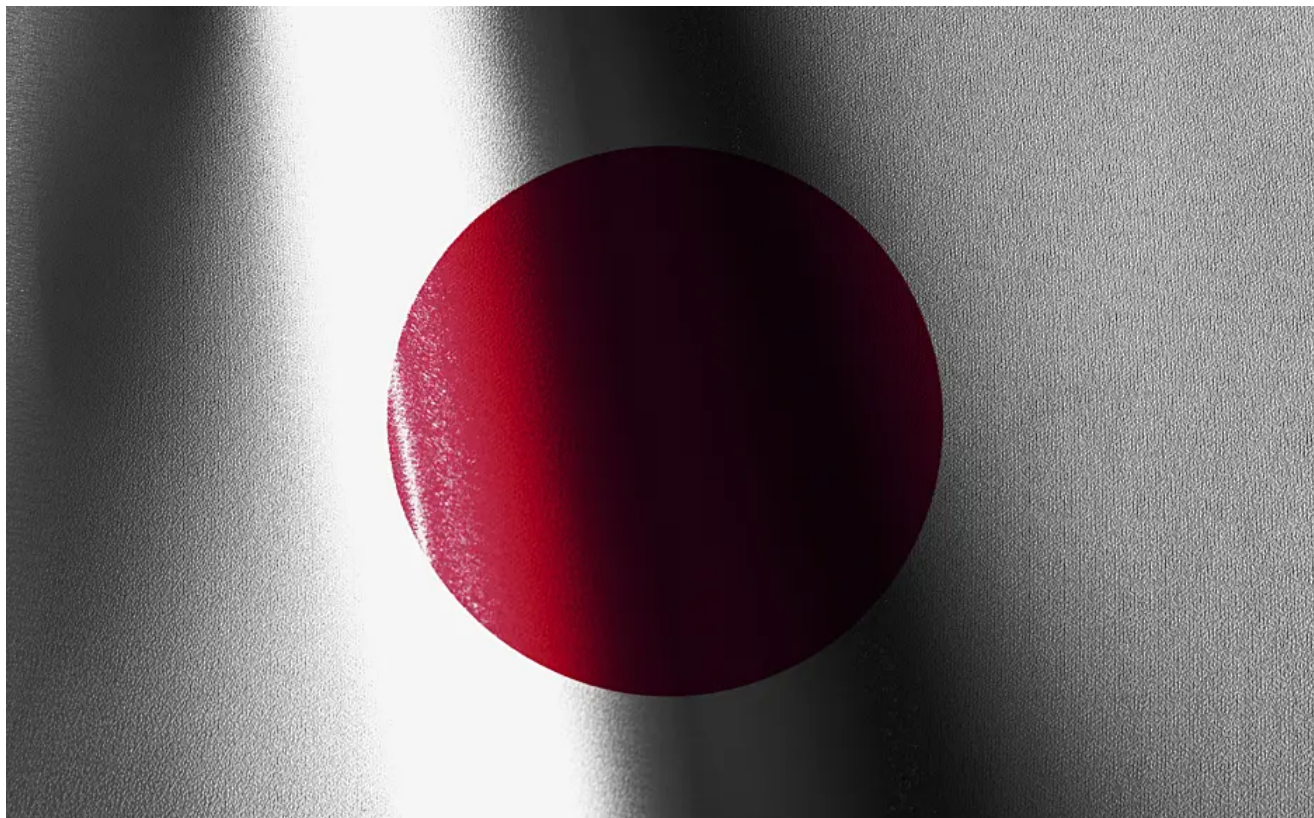


# 'Masterful' New Banking Trojan Is Attacking 14 Japanese Banks

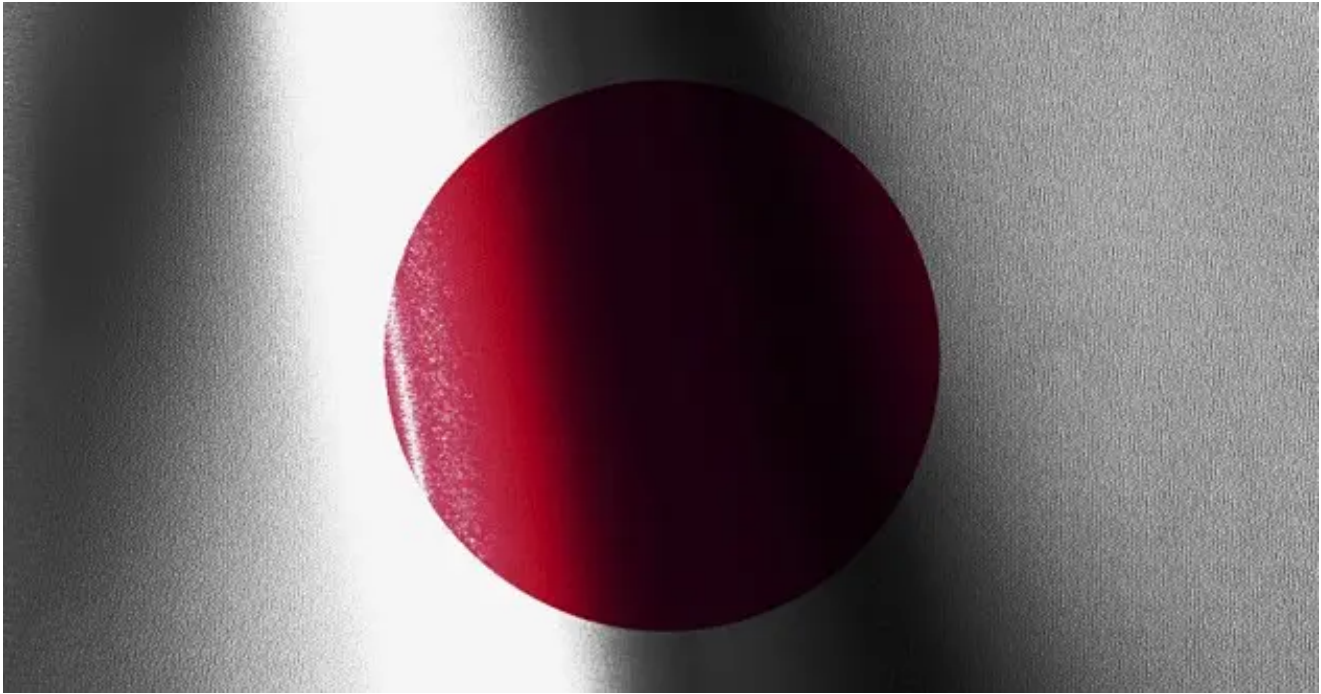
 [securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/](https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/)

August 31, 2015



[Home](#) &nbsp; [Advanced Threats](#)

Shifu: 'Masterful' New Banking Trojan Is Attacking 14 Japanese Banks



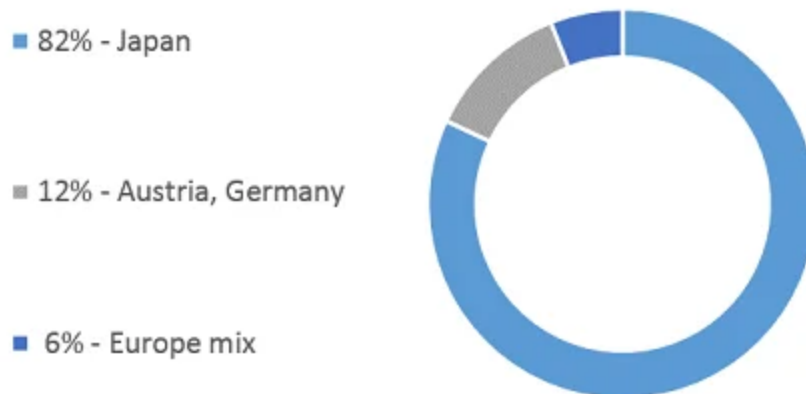
Advanced Threats August 31, 2015

By Limor Kessem co-authored by Ilya Kolmanovich , Denis Laskov 7 min read

A brand-new advanced banking Trojan discovered in the wild has been named “Shifu” by IBM Security X-Force, 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 antifraud platforms through continuous protection of customer endpoints all over the world.

Shifu currently targets 14 Japanese banks and select electronic banking platforms used across Europe; however, at this time, only Japan is seeing active attacks.

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.



## Cybercrime’s New Familiar Face

---

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 that 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 of those similarities are:

**Domain Generation Algorithm (DGA):** 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's and Shiz's codes. Both Trojans used these mechanisms to target the banking applications of Russia- and Ukraine-based banks. Shifu, too, targets Russian banks as part of its target list in addition to 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.

On the less technical side, Shifu communicates via secure connection that uses a self-signed certificate, just like the one used by the Dyre Trojan.

Shifu comes with basic built-in capabilities, which are supplemented by additional modules once it contacts its command-and-control (C&C) server.

The initial package comes with features like:

- Anti-research, anti-VM and anti-sandbox tools;
- Browser hooking and webinject parser;

- Keylogger;
- Screenshot grabber;
- Certificate grabber;
- Endpoint classification, monitoring applications of interest;
- Remote-access tool (RAT) and bot-control modules.

## **Out to Get It All**

---

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 that users key into HTTP form data, steals private certificates and scrapes external authentication tokens used by some banking applications. 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.

Shifu scans, parses and exfiltrates data from smartcards if they are attached to a smartcard reader on the endpoint, and searches cryptocurrency wallets to steal from the infected victim.

## **Are You a Point of Sale?**

---

Beyond their interest in defrauding bank accounts, Shifu's operators target payment card data. The malware scans infected endpoints for strings that may indicate it has landed on a point-of-sale (POS) endpoint, and if that sort of string is found on the machine, Shifu deploys a RAM-scraping plugin to collect payment card data. 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.

## **Electronic Banking Platforms Join the Hit List**

---

While webinjections are a common Trojan capability, very few Trojans target banking platforms. Such an 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.

Moreover, Shifu looks for digital signature credentials issued by certification authorities to business banking users, particularly in Italy. By resetting the PIN on the certificate, Shifu's operators can impersonate the victim in fraudulent banking operations that authenticate users based on their valid digital signature.

Targeting banking applications rather than specific websites provides the benefit of making 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.

## Local Deobfuscation Server Hides Injection C&C

---

Reminiscent of another advanced banking malware — like Dyre — Shifu conceals its webinjections 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.

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 webinjections, hosting and receiving injected JavaScript from a remote Shifu server.

To implement this real-time fetching, Shifu accesses a remote webinjects server, the address of which it strives to keep concealed. The server's name as it appears in the configuration is not decipherable and seems bogus at first glance. In reality, the request is obfuscated, and instead of going to the Web browser as is, Shifu's requests first go to the local PHP server for deobfuscation. The local 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.

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.

## Intruders: Back Off!

---

Shifu's operators appear to have no intention of sharing the spoils with anyone outside their gang. Once Shifu has landed on a newly infected machine, it activates an antivirus-type feature designed to keep all other malware out of the game by stopping the installation of suspicious files.

Shifu monitors the processes of a list of applications that interact with the Internet on a regular basis, it hooks the `URLDownloadToFile` function and keeps close watch on the incoming files the endpoint receives. Files that may harbor malware will be stopped if they:

- Come from unsecured connections (HTTP);
- Are executables;

- Are unsigned.

As soon as a file of that sort is downloaded by the Web browser, 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 trying to run the downloaded file with an “Out of Memory” message.

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.

This is the first time we are seeing malware build “rules” for suspicious files in order to make sure that the endpoint it’s on remains in its exclusive control from the moment of infection. If the endpoint is already infected with other malware, Shifu does not find and delete other malware; but by stopping new files from coming in, it can prevent malware from receiving version and configuration updates, potentially cutting its ties with other botmasters.

## Shifu’s Likely Origins

---

So who put the masterful Shifu together? 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 department”;
- **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.

## More to Come

---

Shifu is a complex and interesting new malware. At this time, the malware is actively attacking banks in Japan, but it has the potential — and a target list in place — to spread. Its main fraud methods are based on credential grabbing, webinjections and certificate theft. Having been built with code base from other crimeware families, Shifu is also protecting its infected turf against other malware, shutting out the competition from its spoils.

IBM Security X-Force has issued a complete report on Shifu and will release it in the coming week. Stay tuned for additional information both here on Security Intelligence and on IBM X-Force Exchange.

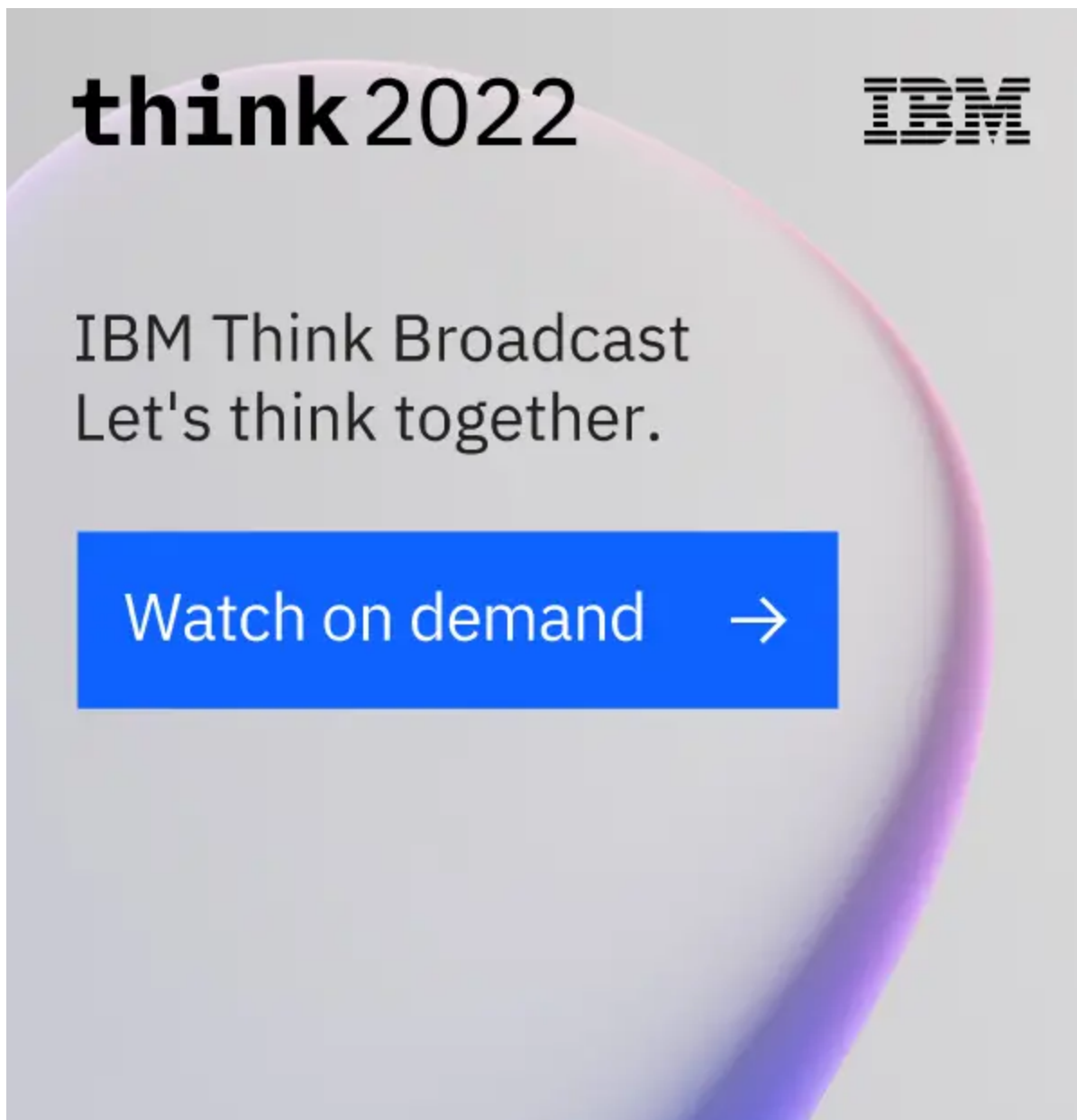
Shifu sample MD5 [b9bc3f1b2aace824482c10ffa422f78b](#) is presently detected as a generic malware by 19 of 56 (34 percent) antivirus engines, according to VirusTotal and IBM X-Force Exchange as of Aug. 27, 2015.

[Read the white paper: Accelerating growth and digital adoption with seamless identity trust](#)

[Limor Kessem](#)

Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...

A promotional graphic for IBM Think 2022. The background is a light gray with a large, curved, purple-to-pink gradient shape on the right side. In the top left, the text "think 2022" is written in a bold, lowercase sans-serif font. In the top right, the IBM logo is displayed in its classic eight-stripe font. Below the "think 2022" text, the words "IBM Think Broadcast" and "Let's think together." are stacked in a clean, sans-serif font. At the bottom, a blue rectangular button contains the text "Watch on demand" in white, followed by a white right-pointing arrow.

**think 2022** **IBM**

IBM Think Broadcast  
Let's think together.

Watch on demand →

