
Bigstock

# Organized Cybercrime Big in Japan: URLZone Now on the Scene

**BY LIMOR KESSEM** • FEBRUARY 1, 2016

**Categories:** Threat Intelligence, IBM X-Force, Malware



Four months after an organized cybercrime group started using the sophisticated Shifu Trojan against Japanese banks, IBM X-Force researchers reported on a second gang setting its sights on Japanese customers with the help of the Rovnix Trojan. Now, not a month later, a third well-known cybercrime group has moved to attack 14 major Japanese banks: The URLZone team.

In what's marking a definite trend in cybercrime migration, the move of this third organized group to attack banks in Japan is a clear indication of an evolving fraud

infrastructure in the country.

## Why Target Japan?

Why are these organized crime groups spreading to Japan? In most cases of malware migration, cybercriminal groups with adequate resources are looking for easier money, less security and an element of surprise. They may be counting on all these factors to see more success in their attacks, especially as they target the less-aware Japanese customers who are not as experienced with encountering cybercrime as their Western counterparts.

Japan has enjoyed some protection from most cybercrime for many years because of its linguistic specificity. While fraudsters were easily able to translate texts into English, even if imperfect or lacking, the same task was trickier when it came to Japanese. Another aspect that kept most cybercriminal factions out of Japan is the likely lack of a local infrastructure for Web fraud, which would require money mule recruitment in Japanese and local rogues to help criminals understand the banking and payment systems.

Tools and building contacts in Japan would cost cybercriminals time and money; this is often an investment they could not or did not wish to afford. The smaller Trojan-operating factions from Eastern Europe typically attack locales in which they already have resources and may not invest in building tools and a localized team for fraud in a unique language zone such as Japan.

With organized crime in the pictures, the grace period for Japan has ended. Although other malware such as Tsukuba did target banks in the country, it was not until the launch of Shifu attacks that it became obvious Japan was in trouble. When it comes to organized cybercrime, Shifu's operators laid the foundations for what came next.

## One Size Fits All?

Why would a Trojan like Shifu pave the way for other attackers? According to information from actual attack campaigns, IBM X-Force researchers noted that organized cybercrime gangs share resources and buy tools from one another or from the same black-hat vendors.

Once Shifu's group had the infection scheme set up to attack in Japanese, as well as webinjections and localized knowledge about banks in the country, much of the work

was already done for other gangs who could now invest in entering the new turf. Unfortunately, cybercrime is a thriving business, and gangs are out there to make money, sometimes in furtive collaborations with one another.

Take, for example, the Rovnix Trojan. When this malware began attacking in Japan in December 2015, it unsurprisingly opted to infected users with email spam and not its usual malvertising or drive-by downloads. This is the same way Shifu infected victims in Japan.

There are other similarities beyond using emails in Japanese. Rovnix's developers seemed to draw on Shifu's existing attack schemes and webinjections, perhaps by analyzing them and then applying some additional elements. These tactics are not a rarity: In October 2015, IBM X-Force researchers noted that Dridex was emulating some of Shifu's attacks in the U.K., and Shifu was using the same webinjections deployed by Neverquest.



## URLZone Gets in the Zone

In January 2016, the URLZone gang officially joined the roster of attackers targeting Japanese banks. This evolution happened within a matter of two weeks from the Rovnix case. Again, the same infection method was selected: email spam containing a poisoned attachment. The malware itself is considered sophisticated and complex, but the current target list and webinjection set appear basic and may have been developed or bought from a specialized black-hat vendor.

Since the URLZone group is coming into Japan after other gangs have already set up shop in the country, it is very likely they would be able to rely on mule accounts and trusted rogue agents to work with locally.

## About URLZone

URLZone, a banking Trojan also known as Bebloh and Shiotob, was first detected in the wild in 2009 when it was attacking German banks. Right from the start, this banking Trojan was considered to be one of the most advanced due to special techniques to conceal malicious activity from both users and researchers, Wired reported. For

example, after robbing accounts of almost their entire balance, URLZone uses HTML injections to replace the balance and hide the transaction line from the victim's online banking account view.

Moreover, to hide its mule account list from researchers, the malware would validate each infected machine to ensure it is indeed part of its botnet and only then provide a mule account for the illicit transactions it carries out. If the infected machines did not pass the test, URLZone's command-and-control (C&C) server would send back unrelated bank account numbers to keep researchers and banks confused. This capability was rather unique to URLZone and considered one of its more interesting tricks.

While currently there are two separate versions of URLZone in the wild, the Trojan is reported to have always been the property of a closed cybercrime group that uses it to defraud the customers of European banks, according to Threatpost.

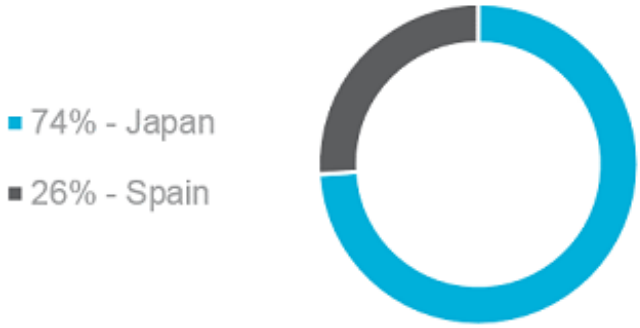
In 2009, using the LuckySploit exploit kit to infect victims, URLZone managed to rob banks of more than $500,000 in less than a month. From 2009 to 2013, URLZone was used in what was considered low-volume campaigns because it would typically target banks only in Germanic countries. In 2013, the Trojan saw a version upgrade that included the addition of evasion techniques, anti-VM features and a persistence mechanism.

Between 2013 and 2015, this Trojan and the gang that operates it continued to be active in low volumes and, for most of 2015, fell nearly silent.

The situation changed in August 2015, when IBM X-Force researchers discovered a new version upgrade for URLZone. Changes to the malware updated its evasion techniques to avoid research tools. The Trojan was also fitted with a new configuration file designed to target banking customers in the U.K., Italy, Poland and Croatia.

URLZone has seen increased activity since August 2015 both in terms of attacks and code updates. In December 2015 it began attacking banks in Spain, and in January 2016 it received an upgrade to target Japanese banks.

The new URLZone configuration continues to attack banks in Spain, although to a lesser extent in terms of the number of brands targeted.



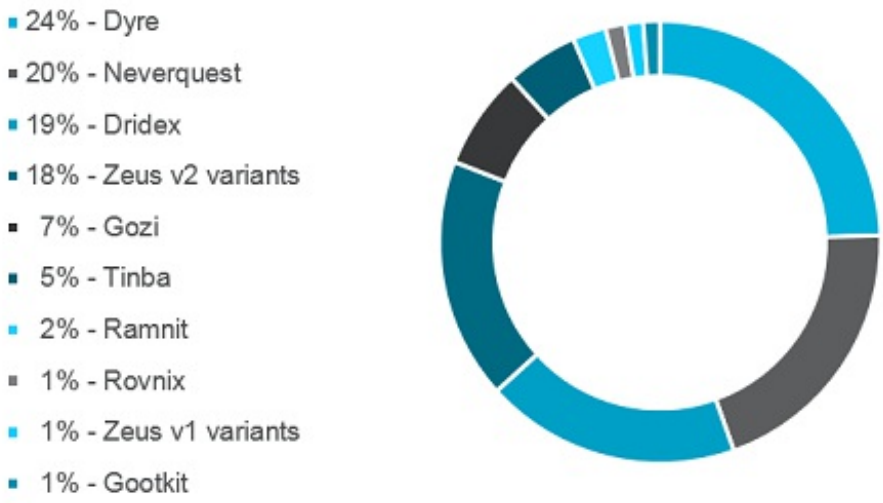

The top features that enable URLZone to defraud online banking customers include:

- Customer credentials theft;
- Screenshot grabber;
- Webinjections for social engineering and hiding account balances;
- Use of a transaction orchestration panel;
- Use of a domain generation algorithm (DGA) as a fallback for the botnet's communications;
- Encrypted C&C communications;
- Encrypted webinjection configuration file; and
- Elaborate security and research evasion features.

# Global Perspective

In terms of URLZone's ranking on the global malware list this year, IBM Security data showed that this malware has not yet cracked the top 10. So far, URLZone's global reach is limited because it usually attacks in one or two countries at a time.

The chart below shows the top offenders on the financial malware roster from January 2015 to January 2016.




# Detecting and Fighting URLZone Attacks

IBM Security X-Force has worked with customers to study and stop URLZone attacks and can be of help to banks that wish to learn more about this high-risk threat. To help stop threats like URLZone, banks and service providers can use adaptive solutions to detect infections and protect customer endpoints when malware migrates or finds new focus in the organization's region.

On the bank's side, fighting evolving threats — such as URLZone's attacks — is made easier with the right malware detection solutions. With protection layers designed to address the ever-changing threat landscape, financial organizations can benefit from malware intelligence that provides real-time insight into fraudster techniques and capabilities.

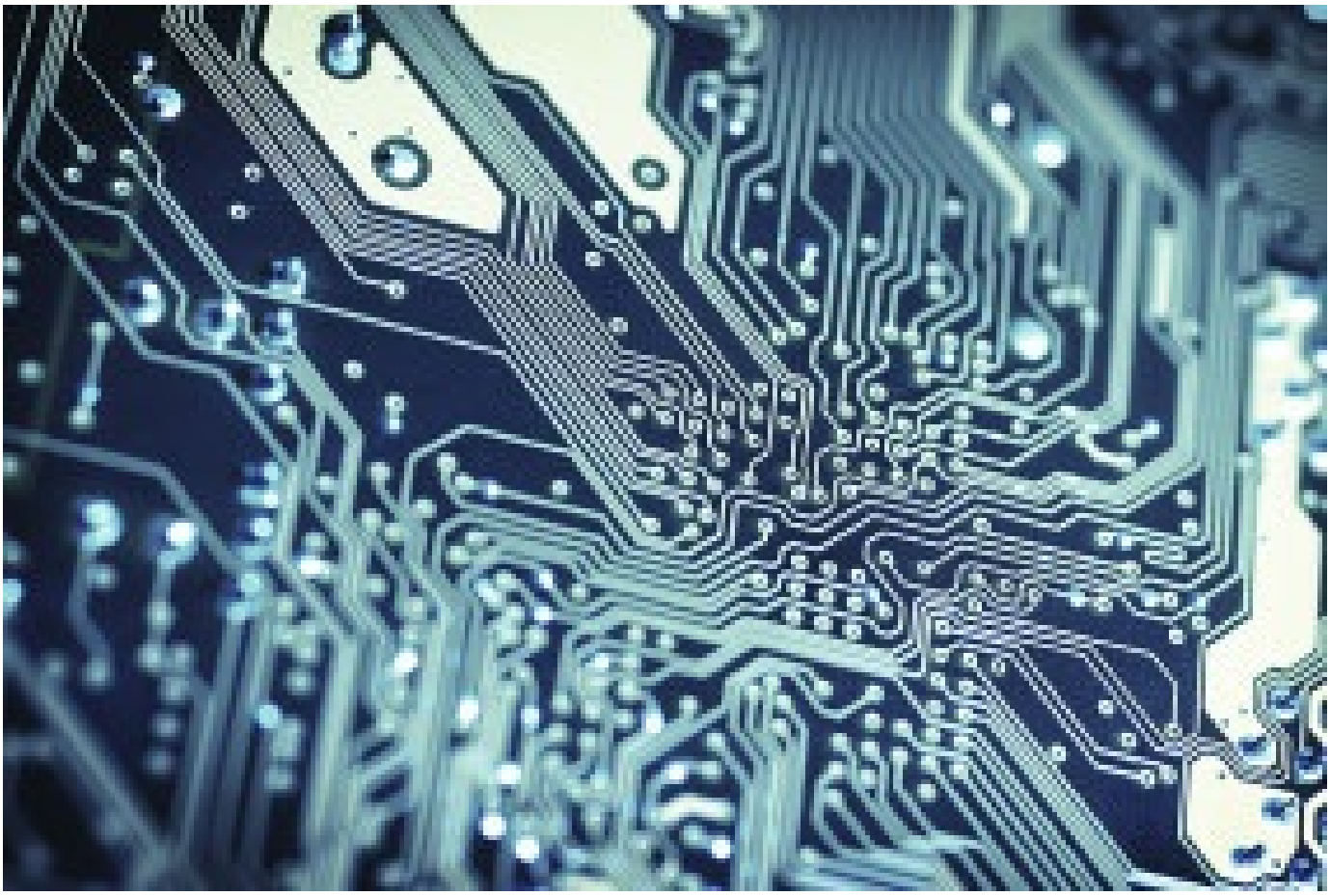
Sample MD5 analyzed by IBM X-Force researchers: b24dec9f053f8e3ff698aea4e4eb4ccd.

**Topics:** IBM X-Force Security Research, Advanced Threats, Malware, Threat Intelligence, Online Banking, Trojan, Banking Trojan, X-Force, Banking Industry, Shifu, Rovnix, URLZone

IBM X-Force Security Research in the Spotlight at InterConnect 2016


The InfoSecond, Nov. 16–20: Hacking Contests and Millennials, 2015 Security Lessons and

More!



Factorization Machines: A New Way of Looking at Machine Learning

**Security Intelligence RSS Feed**

**Subscribe+**

IBM SECURITY NAMED A LEADER IN 2015 GARTNER MAGIC QUADRANT FOR INTRUSION PREVENTION SYSTEMS

MORE IN THIS TOPIC:

The Boy Who Cried Mobile Malware

***By Jonathan Dale***

Dyre Straights: Group Behind the Dyre Trojan Busted in Moscow?

***By Limor Kessem***

Organized Cybercrime Big in Japan: URLZone Now on the Scene

***By Limor Kessem***

Malware: Bigger and Badder Than Ever

***By Security Intelligence Staff***

Dridex Launches Dyre-Like Attacks in UK, Intensifies Focus on Business Accounts

***By Limor Kessem***

FEATURED MEDIA:


## Infographic + Report: State of Application Security

JANUARY 12, 2016

UPCOMING WEBINARS:

### Is Your Security Staff Addressing the Top 3 Data Protection Challenges Today?

FEBRUARY 17, 2016

### Don’t be an IT Dinosaur. Accelerate your Cloud Evolution.

FEBRUARY 17, 2016

### Empower Mobile Users with Secure Corporate Access using APM and EMM

FEBRUARY 17, 2016