

MUST READ USB Killer 2.0 - How to easily burn a PC with a USB device

The rise of the Japanese Cybercrime Underground

October 13, 2015 By [Pierluigi Paganini](#)



Researchers at Trend Micro have issued a new report on the Japanese Cybercrime Underground, a growing criminal community with his characteristics.

Cybercrime underground is a growing and prolific industry that knows no crisis as demonstrated by the numerous reports issued by principal security companies and law enforcement.

In the past we have analyzed criminal most prolific criminal underground, [Russian](#), [Chinese](#) and [Brazilian](#) communities have been dissected by the experts at Trend Micro that provided detailed information on the criminal activities in these ecosystems and the offer of the principal criminal rings.

Now Researchers at Trend Micro's Forward Looking Threat Research team have issued a new report on the Japan's Cybercrime Underground, a criminal online community that is growing in a significant way despite it has a still highly stealthy underground economy.



According to the Japan's National Police Agency cybercriminal activities until March 2015 increased 40% over the previous year. On June 2015, the Japan's Pension Service suffered a significant data breach that exposed more than one million users' records.

We have discovered that Russian underground is specialized in hacking and payment card frauds, the Chinese cybercrime underground is specialized in mobile frauds meanwhile the Brazilian underground is more focused on Banking malware.

What about the Japan's Cybercrime Underground?

The researchers consider Japan cybercriminal rings still newbies, due to the nation's strict criminal laws Japanese criminals don't write malware due to due to the severe penalties against such activities.

The experts noticed that Japanese Cybercrime Underground is very active in the illegal buying and selling of [counterfeit passports](#), drugs, weapons, [stolen credit card data](#), phone number databases, hacking advice and child pornography.

Despite the victims of the Japanese cyber criminals are mainly located in the country, the increasing interest in DDoS tools/services and [ransomware](#) would indicate that the actors are looking beyond national borders to expand their gains.

Japanese players in the criminal underground exploit secured bulletin boards, virtual PO boxes and secret jargon. The principal payment methods are Amazon gift cards and Sony PlayStation Store codes. In one case the experts discovered a Japanese BBS called Tor 2 Channel displaying in homepage a warning that it had been seized by the FBI, Europol, and the US Department of Homeland Security Immigration and Customs Enforcement. In reality the BBS is active and users can access it by clicking on one of the national flag icons on that page.

"They're building a greater foundation for gilded thieves in Japan," says Tom Kellermann, chief cybersecurity officer for Trend Micro. "These cybercrime forums operate under heavier security than do many of their counterparts in other nations, he says. "Other [nations' cybercriminals] are starting to retrofit operational security. You're seeing them [Japanese cybercriminals] build it from the ground up," "Their number one focus is stealth, remaining covert in their operations and obfuscating their activities."

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | **elligence** Laws
Laws and regulations | Malware | Mobile | Data Breach | Security |
Social Networks | Reports | EXTENDED COOKIE POLICY | Contact me | **EXTENDED COOKIE PO**

According to Trend Micro, the Japanese banks are a privileged target for cyber criminals, numerous banking malware hit the customers of Japanese financial institutions last year. The last in order of time is [Shifu](#), a new sophisticated malware that has been used to target the customers of more than a dozen Japanese banks.



Japan was one of the countries that suffered the greatest number of attacks based on the [Angler exploit kit](#). On September 2015, 3,000 High-Profile Japanese [websites were hit](#) by a Massive [Malvertising](#) Campaign.

Threat actors mainly use [watering hole](#) attacks to infect victims' machines.

What about the future?

The experts have no doubts, bad actors in the Japan's criminal underground will start the development of their own malware.

"There's far too much talent" for them to not create their own tools, said Kellermann. "This is in line with the cultural manifestation of a lot of people in a society disaffected with the government."

Pierluigi Paganini**(Security Affairs – Japanese criminal underground, malware)**Share it please ...        **Share this:** Email  Twitter  Print  LinkedIn  Facebook  More [Angler exploit kit](#) [criminal underground](#) [Hacking](#) [Japan](#) [malware](#) [watering hole](#)
 [Breaking News](#) [Cyber Crime](#) [Hacking](#) [Malware](#) [Reports](#)**SHARE ON**

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Accept](#) [Read More](#)



Pierluigi Paganini is Chief Information Security Officer at bit4id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

MORE S**MEF – /****Paymen**

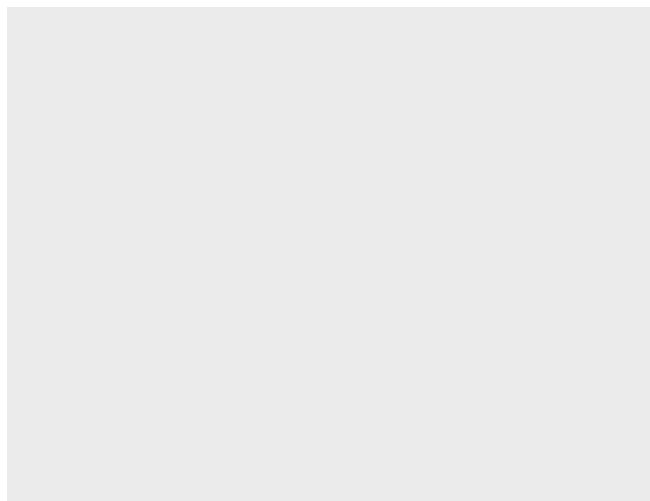
The CEN
ANTIFRA
Italian M
released



PREVIOUS ARTICLE

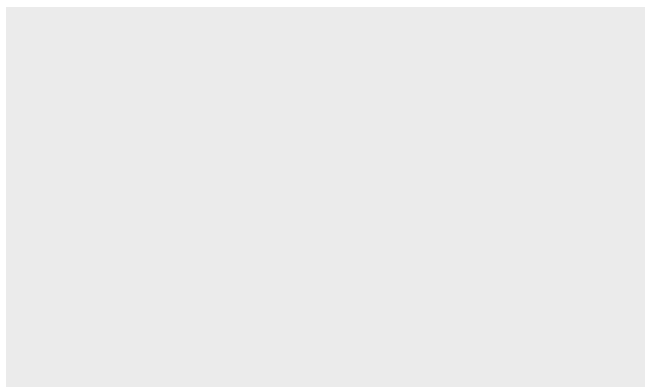
[MEF – Annual Report 2015 - Payment
card frauds](#)

YOU MIGHT ALSO LIKE



[NSA SHARKSEER program aims to detect
and mitigate malware Zero-Day](#)

October 13, 2015 By [Pierluigi Paganini](#)



[US Ports – Cyber attacks can cause the
release of dangerous chemicals](#)

October 12, 2015 By [Pierluigi Paganini](#)

Promote your solution on Security Affairs



Copyright Security Affairs by Pierluigi Paganini - All Right Reserved.