Rent the infamous AlienSpy backdoor is now quite easy

February 9, 2016 By Pierluigi Paganini

Security experts at Kaspersky have spotted in the wild a new variant of AlienSpy RAT Family openly offered with a model of malware-as-a-service.

Today we will speak about a case of malware-as-a-service, in the specific case the threat is a remote access trojan, aka RAT, that could be used to gain control over multiple platforms, including Windows, Linux, Mac OS X, and Android.

The RAT belongs to a family of Java malware that exists since 2013 and that recently is offered for sale as a “commercial” backdoor-as-a-service. It is known as AlienSpy or Adawind, and security experts spotted it in an attack on an employee of a Singapore bank.

In April 2015, experts at Fidelis discovered that variants of the AlienSpy remote access trojan (RAT)

backdoor mechanism.

AlienSpy implements the typical features of other RATs plus further features, including the ability to capture webcam sessions, to steal browser credentials, to use the victim's microphone to record environment conversations, to access files and to provide a remote desktop control.

AlienSpy uses plugins to implement the above capabilities and experts have dozens of different plugins.

AlienSpy botnet was destroyed in 2015 when the experts identified the command and control infrastructure and neutralized it.

Security experts at Kaspersky have spotted a new variant of the malware that has been modified and offered as a service in the criminal underground. Researchers at Kaspersky observed more than 150 attack campaigns relying on the new variant of AlienSpy, bad actors in the wild targeted more than 60,000 individuals.

[it] is open for service again to customers ranging from Nigerian scam operators to possible nation-state actors. Ars has confirmed that the service is offered openly through a website on the public Internet." states Ars.

The analysis of subscribers to the malware-as-a-service revealed that the majority of clients come from the US, Canada, Russia, and Turkey.

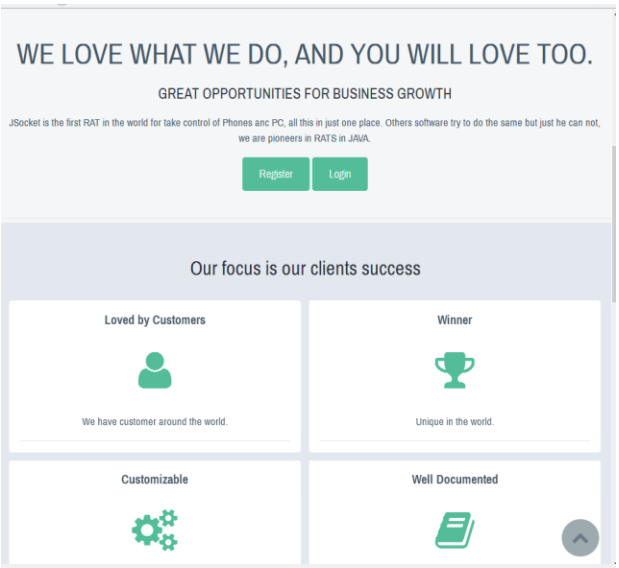

Image from Ars post

The new variant of AlienSpy is dubbed JSocket and jRat and is available for rent on the Internet at prices ranging from $30 for one month to $200 for an unlimited version.

According to the researcher Vitaly Kamluk who analyzed the threat, the operator behind the service's author is a native Spanish speaker, likely Mexican.

The new variant of AlienSpy, aka JSocket and jRat, is widely adopted in scam scheme, particularly the Nigerian e-mail-based scam campaigns targeting bank customers.

Pierluigi Paganini

(Security Affairs – AlienSpy, malware-as-a-service)

Pierluigi Paganini

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”.

PREVIOUS ARTICLE

Carbanak cybergang is back and it is not alone

NEXT ARTICLE

Are you searching for a Facebook Hacking Tool? Be careful!

- +Pierluigi Paganini

  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) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

[redacted]

1. Best Antivirus Software 

2. Remove Antivirus Scan 

3. Cheap Laptops Online 

4. Cell Phone Reviews 

5. Top 10 Cell Phones 

6. Password Management Software 

7. Computer Repair Services 

8. Protect Your Privacy 

Back to top