Poseidon Group, a single actor behind a long series of attacks

February 11, 2016 By Pierluigi Paganini

Experts at Kaspersky Lab have linked a series of cyber attacks started in 2001 to a single threat actor called the Poseidon Group.

Experts at Kaspersky Lab have identified a single threat actor behind a long-known campaign of cyberattacks financially motivated.

The group of hackers identified by Kaspersky dubbed Poseidon Group attempts to extort money to corporate victims.

The researchers believe the group has been active since 2001, the hackers developed malicious code to infect systems that use English and Portuguese settings.

"During the latter part of 2015, Kaspersky researchers from GReAT *(Global Research and Analysis Team) got hold of the missing pieces of an intricate puzzle that points to the dawn of the first*

sample found points to 2001" Kaspersky wrote in a post .

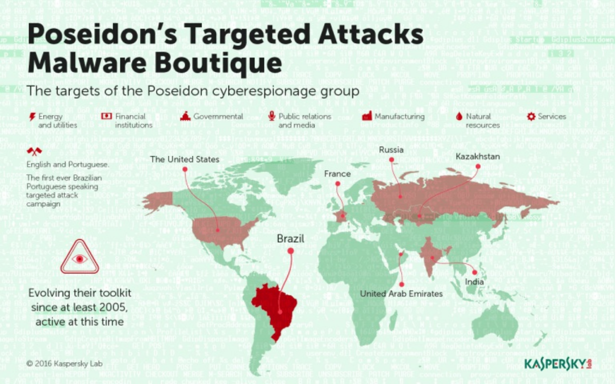
The attackers spread the malware through spear-phishing emails, the messages include malicious office documents as an attachment. Once the□ malware compromises a system in the target network, it tries to map its topology searching for sensitive data to exfiltrate.□

In order to map the network and make lateral movements, the malware searches for all administrator accounts on both the local machine and the network.

The Poseidon group not only steal data from victims, it tries to use the information gathered to blackmail victims into contracting the hacking crew.

"The information exfiltrated is then leveraged by a□ company front to blackmail victim companies into contracting the Poseidon Group as a security firm,'□ continues Kaspersky. " Even when contracted, the Poseidon Group may continue its infection or initiate another infection at a later time, persisting on the network to continue data collection beyond its contractual obligation."

Experts at Kaspersky revealed that at least 35 companies have been targeted by the Poseidon Group, including organizations in banking, government, telecommunications, manufacturing and energy, and media industries.


Poseidon's Targeted Attacks
Malware Boutique
The targets of the Poseidon cyberespionage group
Energy and utilities
Financial institutions
Governmental
Public relations and media
Manufacturing
Natural resources
Services
English and Portuguese.
The first ever Brazilian Portuguese speaking targeted attack campaign
The United States
Russia
Kazakhstan
France
Brazil
United Arab Emirates
India
Evolving their toolkit since at least 2005, active at this time
© 2016 Kaspersky Lab
KASPERSKY

This the first time that a security firm link the□ Poseidon Group's attacks to a single threat actor.

"We noticed that several security companies and enthusiasts had unwittingly reported on fragments of

Poseidon's campaigns over the years. However, nobody noticed that these fragments actually belonged to the same threat actor." states the report from Kaspersky

"By carefully collecting all the evidence and then reconstructing the attacker's timeline, we found that it was actually a single group operating since at least 2005, and possible earlier, and still active on the market,"

Kaspersky informed victims of the attacks and disclosed the indicators of compromise to allow firms to identify the threat.□

Pierluigi Paganini

(Security Affairs – Poseidon Group, cybercrime)

Share it please ...

SHARE ON

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

SAP fixed a flaw in xMII that could open the door to nation-state hackers

NEXT ARTICLE

Million CISCO ASA Firewalls potentially vulnerable to attacks

- +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".

Back to top ^