PROMETHIUM and NEODYMIUM APTs used same Zero-Day to Target Turkish citizens

December 16, 2016 By Pierluigi Paganini

Microsoft discovered two distinct APT groups, PROMETHIUM and NEODYMIUM, that exploited the same Flash Player zero-day flaw on same targets.

Security researchers have discovered two distinct APT groups, PROMETHIUM and NEODYMIUM, that exploited the same Flash Player zero-day vulnerability (CVE-2016-4117) in cyber espionage campaigns on Turkish citizens living in Turkey and various other European countries. Both groups exploited the flaw before its public disclosure and against the same type of targets.

We have already read about the activities of the PROMETHIUM APT group in a report published by Kaspersky Lab that named it StrongPity. In October, Kaspersky published a report on cyber espionage activities conducted by StrongPity APT that most targeted Italians and Belgians with watering holes attacks.

The experts noticed many similarities in the operation of both groups, a circumstance that suggests a possible link between them. The ATP groups used different infrastructure and malware, but there are some similarities that indicate a possible connection at a higher organizational level.

The flaw was patched by Adobe on May 12, but according to the experts from the firm Recorded Future published a report on the most common vulnerabilities used by threat actors in the exploit kits.

The PROMETHIUM APT has been active since at least 2012, the hackers used instant messaging applications as the attack vector and shared malicious links that pointed to documents to exploit the CVE-2016-4117 vulnerabilities. Microsoft observed that the attacker used a specific strain of malware dubbed Truvasys that was designed to compromise target devices with Turkish locale settings.

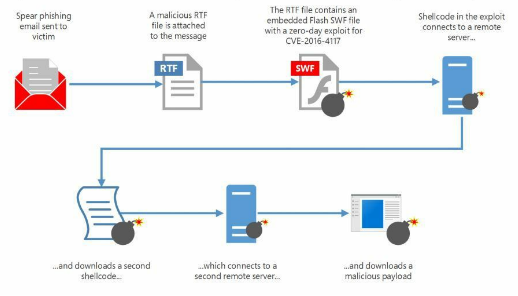
"The attack itself began with certain individuals receiving links in instant messenger clients. These links led to malicious documents that invoked exploit code and eventually executed a piece of malware called Truvasys *on unsuspecting victims' computers" states the Microsoft Security Intelligence Report.*

The PROMETHIUM APT also used another malware dubbed Myntor in targeted attacks.

The NEODYMIUM also exploited the CVE-2016-4117 flaw in targeted attacks in May via spear-phishing messages. This second APT leveraged a backdoor, dubbed *Wingbird*, that shows many similarities with surveillance software FinFisher.

"NEODYMIUM used a backdoor detected by Windows Defender as Wingbird, whose characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicates that it is typically used to attack individuals and individual computers instead of networks" continues the Report.

Figure 13. The NEODYMIUM attack chain shows how the exploit CVE-2016-4117 was used to infect target individuals' computers


Spear phishing email sent to victim
A malicious RTF file is attached to the message
RTF
The RTF file contains an embedded Flash SWF file with a zero-day exploit for CVE-2016-4117
SWF
Shellcode in the exploit connects to a remote server...
...and downloads a second shellcode...
...which connects to a second remote server...
...and downloads a malicious payload

The vast majority of the NEODYMIUM victims was located in Turkey (80%), but several infections were also detected in the U.S., Germany and the U.K.

Let me suggest reading the Microsoft Security Intelligence Report to have more details on PROMETHIUM and NEODYMIUM, including indicators of compromise (IoC).

Pierluigi Paganini

(Security Affairs – NEODYMIUM APT, PROMETHIUM APT)

Share this...

APT | cyber espionage | Hacking | malware | NEODYMIUM | PROMETHIUM | StrongPity

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 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
More than 8,800 WordPress Plugins out of 44,705 are flawed

NEXT ARTICLE
Cryptolulz666 continues targeting Government websites with DDoS

YOU MIGHT ALSO LIKE

Trend Micro addresses two issues exploited by hackers in the wild
March 18, 2020 By Pierluigi Paganini

TrueFire Guitar tutoring website was hacked, financial data might have been exposed
March 18, 2020 By Pierluigi Paganini