Featured news

Cyber crooks opt for APT method for delivering malware

Posted on 03.09.2015

Delivering malware without it being flagged by users and security solutions is one of the biggest challenges malware peddlers face. Luckily for them, if they don't know how, they can outsource that task to more knowledgeable and/or resourseful malicious actors.

Or, they can use a malware construction kit that allows them to package the malware into a payload that will (hopfully) foil all defenses.

One of these kits is Microsoft Word Intruder (MWI), which has been recently analyzed by SophosLabs researcher Gabor Szappanos.

"MWI generates Rich Text Format (RTF) documents that exploit multiple vulnerabilities in Microsoft Word," he explained.

"The latest versions support multiple vulnerabilities within the same document. Each of the vulnerabilities has its own exploit block; these blocks are stored sequentially in the RTF document. This gives a higher chance of success, because a victim who has forgotten any one of the needed patches is therefore at risk."

Since May 2013, when it first appeared and used an exploit for only one vulnerability, the toolkit has been used by a variety of attackers.

Sold on underground markets, the kit became so popular that, in early 2014, security researchers noted that it was used more and more by run-of-the-mill cyber crooks who were simply after money. Prior to that, exploited documents were used almost exclusively by APT players.

MWI's creator, who is believed to be Russian and who goes by the online handle "Objekt", worried about this increased popularity as it meant that, in time, the exploits it uses and the documents it creates will be flagged by more and more security solutions.

So he tried to do some damage control, and instructed paying customers to use the kit only for low volume, targeted attacks.

And they seem to have complied. According to Sophos, the samples they collected contain mostly money-stealing Trojans, commercial password stealers, and RATs, and the kit remained largely unknown to the general public until 2015.

"It seems that its primary users are money-making cybercriminals aiming for smaller, less obvious, malware campaigns," says Szappanos, pointing out that some cybergangs (Sophos follows a dozen) obviously discovered that sometimes less can be more.

For more technical details about the kit, download the paper here.

APT cybercrime malware

Spotlight

1 2 3 4 5

Best practices for ensuring compliance in the age of cloud computing

Here are the major considerations organizations should incorporate into their compliance programs, as well as pitfalls that can be avoided to ensure businesses stay compliant while using cloud computing.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address

Daily digest

Receive a daily digest of the latest security news.

Email @ Address

DON'T MISS
Thu, Sep 3rd

- **Persistent cyber spies try to impersonate security researchers**
- **Vulnerable gambling apps put corporate data at risk**
- **Best practices for compliance in the age of cloud computing**
- **95% of websites in 10 new TLDs are suspicious**
- **0-days found in widely used Belkin router, fixes still unavailable**

Back to TOP