Wild Neutron, Butterfly, Sphinx Moth

APT group: Wild Neutron, Butterfly, Sphinx Moth

Names	Wild Neutron *(Kaspersky)* Butterfly *(Symantec)* Morpho *(Symantec)* Sphinx Moth *(Kudeslski)* The Postal Group *(CERT Polska)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2013
Description	(Symantec) A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks. Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target. This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases and is instead focused on high-level corporate information. Butterfly may be selling this information to the highest bidder or may be operating as hackers for hire. Stolen information could also be used for insider-trading purposes.
Observed	Sectors: Financial, Healthcare, IT and Bitcoin-related companies, Investment companies, Real estate, lawyers and individual users.

	Countries: Algeria, Australia, Austria, Canada, France, Germany, Kazakhstan, Palestine, Poland, Russia, Slovenia, Spain, Switzerland, UAE, UK, USA.	
Tools used	HesperBot, JripBot and many 0-days vulnerabilities.	
Operations performed	Jan 2013	Attack on Twitter <https://blog.twitter.com/official/en_us/a/2013/keeping-our-users-secure.html>
	Feb 2013	Attack on Facebook <https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766>
	Feb 2013	Attack on Apple <https://www.reuters.com/article/us-apple-hackers/exclusive-apple-macs-hit-by-hackers-who-targeted-facebook-idUSBRE91I10920130219>
	Feb 2013	Attack on Microsoft <https://blogs.technet.microsoft.com/msrc/2013/02/22/recent-cyberattacks/>
Information	<https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks> <https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/> <https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
