**The first major attacks**

During 2013, Apple, Facebook, Microsoft, and Twitter were compromised. Researchers at Symantec took special note after discovering all four attacks used the same modus operandi -- attack the company website used by mobile-app developers via OSX.Pintsized (a Mac OS X back door) and/or Backdoor.Jiripbot (a Windows back door).

Additional reasons why the Butterfly group has captured Symantec's interest are:

* Even though Butterfly has been around since 2012, not much information has been made public about the group.
* Attacks on desired targets are quick and well executed.
* Butterfly attackers have on occasion cleaned up or abandoned a successful break-in, almost as if that particular attack was a mistake.
* An abrupt lull in activity occurred near the end of 2013, and then just as abruptly, attacks started again in late 2014.

Speaking to the group's success, [a Symantec employee wrote in a July 8, 2015 blog](http://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks) that, "Symantec has to date discovered 49 different organizations in more than 20 countries that have been attacked by Butterfly. Over time, a picture has emerged of a cybercrime gang systematically targeting large corporations to steal confidential data."

## ****Attack tactics****

The Butterfly attackers have an impressive suite of custom-built malware tools, though the old standbys -- OSX.Pintsized and Backdoor.Jiripbot -- are often used to gain access. To garner that kind of success, the group's coders tweak the two pieces of malcode as needed for each attack.

Once access is gained, the attackers find and compromise email servers. "Once the attackers have this access, they presumably then eavesdrop on email conversations and may have been in a position to potentially insert fraudulent emails as well," surmised the Symantec researchers.

Content-management servers are another popular Butterfly target. "These systems are used for indexing and storing a company's various documents and other digital assets," mention the researchers. "Such servers would not contain source code, but rather legal documents, internal policies, training documents, product descriptions, and financial records."

When any data of interest is found, the installed malware will send it to the Butterfly group's servers for review and then put it up for sale. "This is a group that has the discipline and organizational skills of a nation state, but they've pointed it towards out and out crime," Kevin Haley, director of security response at Symantec told [Yahoo News](https://ca.news.yahoo.com/no-one-suspects-the-butterfly--new-hacker-group-is-infiltrating-the-world-s-largest-corporations-215938448.html).

**Impressive counterintelligence capabilities**

The Symantec researchers are impressed with the Butterfly group's counterintelligence capabilities. "The Butterfly attackers use a number of anti-forensics techniques to prevent detection and presumably hinder an investigation into their activity when discovered," state the researchers. "The group's malware and other files are securely deleted using either the GNU Shred tool, which overwrites a file's contents as well as deleting the index from the file allocation table, or the shred functionality written into a custom tool."

Additional steps taken by Butterfly's attackers include:

* modifying event logs to remove any evidence of the attackers' activity;
* using bogus names and email addresses when registering domains for Command and Control (C&C) servers (also, no reusing names and email addresses); and
* using Bitcoins to pay hosting providers to host their C&C servers.

**Additional information**

The Symantec report's appendix includes a repository of Butterfly information, keys, malware signatures, hashes, and C&C server details for those who want to configure IDS/IPS systems.

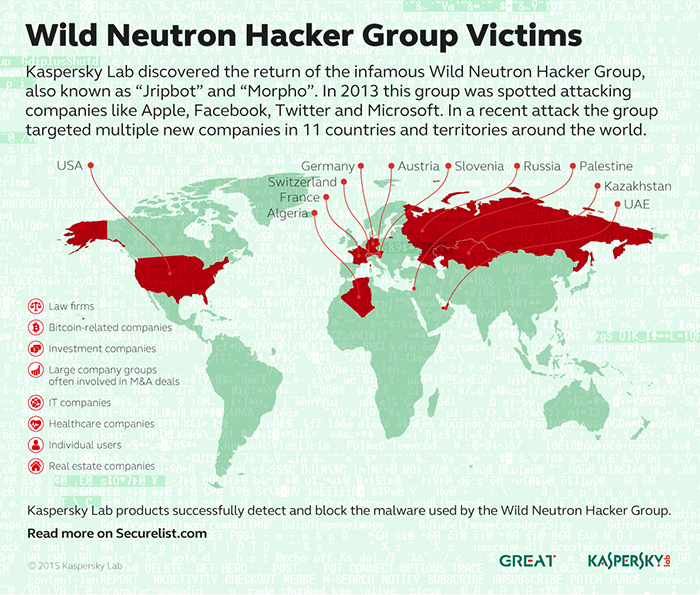
**In 2013, a hacker group known to Kaspersky Lab as “Wild Neutron” (and which is also known as “Jripbot” and “Morpho”) attacked several high profile companies including Apple, Facebook, Twitter and Microsoft. After the incident was widely publicized, the threat actor went dark for almost a year. In late 2013 and early 2014, the attacks resumed and have continued in 2015**.

The actor uses a stolen valid code verification certificate and an unknown Flash Player exploit to infect companies and private users around the world and steal sensitive business information.

Kaspersky Lab researchers were able to identify targets of Wild Neutron in 11 countries and territories, including France, Russia, Switzerland, Germany, Austria, Palestine, Slovenia, Kazakhstan, UAE, Algeria and the United States. They include:

* Law firms
* Bitcoin-related companies
* Investment companies
* Groups of large companies often involved in M&A deals
* IT companies
* Healthcare companies
* Real estate companies
* Individual users

The focus of the attacks suggests that this is not a nation-state sponsored actor. However, the use of zero-days, multi-platform malware as well as other techniques makes Kaspersky Lab researchers believe it’s a powerful entity engaged in espionage, possibly for economic reasons.



### The attack

The initial infection vector of the recent attacks is still unknown, although there are clear indications that victims are exploited by a kit that leverages an unknown Flash Player exploit through compromised websites. The exploit delivers a malware dropper package to the victim.

In the attacks observed by Kaspersky Lab researchers, the dropper was signed with a legitimate code verification certificate. The use of certificates allows malware to avoid detection by some protection solutions. The certificate used in the Wild Neutron attacks appears to be stolen from a popular manufacturer of consumer electronics. The certificate is now being revoked.

After getting in the system, the dropper installs the main backdoor.

In terms of functionality, the main backdoor is no different to many other Remote Access Tools (RATs). What really stands out is the attacker’s care in hiding the command and control server (C&C) address and its ability to recover from a C&C shutdown. The command and control server is an important part of the malicious infrastructure as it serves as a “homebase” for the malware deployed on victims’ machines. Special measures built into the malware help the attackers to protect the infrastructure from any possible C&C-takedowns.

### Mysterious origin

The origin of the attackers remains a mystery. In some of the samples, the encrypted configuration includes the string “La revedere” (“Good bye” in Romanian) to mark the end of the C&C communication. In addition to that, Kaspersky Lab researchers have found another non-English string which is the Latin transcription of the Russian word “Успешно” ("uspeshno" -> "successfully").

“Wild Neutron is a skilled and quite versatile group. Active since 2011, it has been using at least one zero-day exploit, custom malware and tools for Windows and OS X. Even though in the past it has attacked some of the most prominent companies in the world, it has managed to keep a relatively low profile via solid operational security which has so far eluded most attribution efforts. The group’s targeting of major IT companies, spyware developers (FlexiSPY), jihadist forums (the “Ansar Al-Mujahideen English Forum”) and Bitcoin companies indicate a flexible yet unusual mindset and interests,” - said Costin Raiu, Director Global Research and Analysis Team at Kaspersky Lab.

Kaspersky Lab products successfully detect and block the malware used by the Wild Neutron threat actor with the following detection names:

Trojan.Win32.WildNeutron.gen,   
Trojan.Win32.WildNeutron.\*,   
Trojan.Win32.JripBot.\*,   
Trojan.Win32.Generic

To learn more about the Wild Neutron hacker group, please read the blog post available at [Securelist.com](https://securelist.com/blog/research/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/).

How GReAT works: <http://youtu.be/FzPYGRO9LsA>

More information about the Wild Neutron attribution is available to Kaspersky Intelligence Services customers. Contact: [intelreports@kaspersky.com](https://www.kaspersky.com/intelreports@kaspersky.com)