Crouching Yeti (Energetic Bear) Malware

kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat

January 13, 2021

VIRUS DEFINITION

Virus Type: Malware / Advanced Persistent Threat (APT)

What is it?

Crouching Yeti is a threat involved in several advanced persistent threat (APT) campaigns that have been active going back to at least the end of 2010.

The Primary targeted sectors for this threat include:

- Industrial/machinery
- Manufacturing
- Pharmaceutical
- Construction
- Education
- Information technology

After detailed research, it was determined that the largest number of victims we identified fall into the industrial/machinery building sector, which is a good indication that this is a sector of special interest.

The Crouching Yeti threat relayed on three methods to infect the victims, Spear-phishing e-mails using PDF documents embedded with an Adobe Flash exploit (CVE-2011-0611)

- Trojanized software installers
- Waterhole attacks using a variety of re-used exploits

Threat Details

Crouching Yeti is hardly a sophisticated campaign. For example, the attackers used no zero-day exploits, only exploits that are widely available on the Internet. But that didn't prevent the campaign from staying under the radar for several years.

The total number of known victims is over 2800 worldwide, out of which Kaspersky Lab researchers were able to identify 101 organizations. This list of victims seems to indicate Crouching Yeti's interest in strategic targets, but it also shows an interest of the group in many other not-so-obvious institutions.

Kaspersky Lab's experts believe they might be collateral victims, but it might also be reasonable to redefine Crouching Yeti not only as a highly targeted campaign in a very specific area of interest, but also as a broad surveillance campaign with interests in different sectors.

How do I know if I'm infected by Crouching Yeti

The best way to determine if you've been a victim of Crouching Yeti if to identify if there has been an intrusion. Threat identification can be done with a strong antivirus product such as Kaspersky Anti-Virus.

Kaspersky Lab products will detect the malware involved in the Crouching Yeti campaign with the following threat definitions:

- Trojan.Win32.Sysmain.xxx
- Trojan.Win32.Havex.xxx
- Trojan.Win32.ddex.xxx
- Backdoor.MSIL.ClientX.xxx
- Trojan.Win32.Karagany.xxx
- Trojan-Spy.Win32.HavexOPC.xxx
- Trojan-Spy.Win32.HavexNk2.xxx
- Trojan-Dropper.Win32.HavexDrop.xxx
- Trojan-Spy.Win32.HavexNetscan.xxx
- Trojan-Spy.Win32.HavexSysinfo.xxx

How can I protect myself against Crouching Yeti

- Keep all your software up to date. None of the exploits used by Crouching Yeti threats were zero day exploit attacks, the majority of the infections could have been prevented by using up-to-date third party software.
- Install and keep your security solution updated to prevent virus infections.
- Education is an important part of security, especially regarding the spear phishing emails.

Kaspersky
Crouching Yeti is a threat involved in several advanced persistent threat (APT) campaigns that have been active going back to at least the end of 2010.