Kontakt pro média:
David Řeháček
drehacek@checkpoint.com
Mobil: +420 603 536 812

Petr Cícha
petr.cicha@colin.cz
Mobil: +420 603 193 245

Check Point odhalil celosvětovou kyberšpionážní kampaň pravděpodobně napojenou na libanonskou politickou skupinu

PRAHA, 31. března 2015 - Check Point Software Technologies Ltd. (Nasdaq: CHKP), největší celosvětový dodavatel čistě bezpečnostních řešení, dnes vydal podrobnou zprávu o dlouhodobě aktivní útočné skupině, která pravděpodobně pochází z Libanonu a má politické vazby.

Experti z bezpečnostního týmu Check Point Malware and Vulnerability Research Group odhalili útočnou kampaň s názvem Volatile Cedar, která využívá upravený malware s krycím názvem Explosive. Kampaň probíhá od začátku roku 2012 a útočníci úspěšně pronikli do velkého počtu vytipovaných organizací z celého světa, což jim umožnilo monitorovat aktivity obětí a krást data.

Doposud napadené organizace, které je možné potvrdit, zahrnují dodavatele obranných řešení, telekomunikační a mediální společnosti, ale také například vzdělávací instituce. Ze stylu a provedení útoků a souvisejících následků vyplývá, že motivy útočníků nejsou finanční, ale cílem je krádež citlivých informací.

Klíčová zjištění:

- Volatile Cedar je přesně cílená a dobře řízená kampaň. Cíle jsou pečlivě vybírány a šíření infekce je omezeno na minimum, aby byly splněny cíle útočníků, ale přitom nedošlo k odhalení škodlivého kódu.
- První aktivita nějaké verze malwaru Explosive pochází z listopadu 2012. Postupně vznikaly další verze tohoto škodlivého kódu.
- Typické pro tuto útočnou skupinu je, že na začátku je napaden veřejný webový servery a k útoku je využito automatické i manuální vyhledávání zranitelností.
- Jakmile útočník získá kontrolu nad serverem, může jej použít k prozkoumání, identifikování a útokům na další cíle, které se nachází hlouběji ve vnitřní síti. Check Point odhalil manuální on-line hackování i automatizované USB mechanismy využívané pro infikování.

„Volatile Cedar je velmi zajímavá malwarová kampaň. Byla úspěšně aktivní a neodhalená velmi dlouhou dobu, detekci se vyhýbala pomocí dobře plánovaných a pečlivě řízených operací, které neustále monitorovaly činnost obětí a rychle reagovaly na detekci incidentů," říká Dan Wiley, vedoucí týmu Incident Response & Threat Intelligence ve společnosti Check Point Software Technologies. „Vidíme jednu z tváří cílených útoků budoucnosti. Malware, který tiše sleduje síť, krade data a může se rychle přizpůsobit a změnit, pokud je detekován antivirovým systémem. Je nejvyšší čas, aby se organizace začaly o zabezpečení svých sítí zajímat ještě aktivněji."

Zákazníci společnosti Check Point jsou chráněni před útoky typu Volatile Cedar prostřednictvím signatur na bezpečnostních bladech, blady s technologií ThreatCloud identifikovaly každou variantu malwaru Explosive. Organizace se mohou chránit před útoky, jako je Volatile Cedar, pomocí chytré bezpečnostní infrastruktury, která zahrnuje správnou firewallovou segmentaci, IPS, ochranu proti botům, pravidelné aktualizace a záplatování a konfiguraci ovládání aplikací.

Více informací a celou zprávu Volatile Cedar najdete na stránce:
http://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

Bezpečnostní divize Threat Intelligence & Research společnosti Check Point pravidelně odhaluje a analyzuje útoky, zranitelnosti a narušení bezpečnosti a vyvíjí ochranu potřebnou k zabezpečení zákazníků. Pro více informací o dalších průzkumech společnosti Check Point navštivte stránky: http://www.checkpoint.com/threatcloud-central/.

Sledujte Check Point online:
Twitter: www.twitter.com/checkpointsw a www.twitter.com/CheckPointCzech
Facebook: www.facebook.com/checkpointsoftware
YouTube: www.youtube.com/user/CPGlobal

O společnosti Check Point Software Technologies
Check Point Software Technologies Ltd. (www.checkpoint.com) je největší celosvětový dodavatel čistě bezpečnostních řešení. Chrání zákazníky před kyberútoky prostřednictvím unikátních řešení, která nabízí bezkonkurenční úspěšnost zachycení malwaru a jiných typů útoků. Check Point nabízí kompletní bezpečnostní architekturu, která chrání vše od podnikových sítí až po mobilní zařízení, a navíc Check Point poskytuje i nejkomplexnější a nejintuitivnější správu zabezpečení. Check Point chrání více než 100 000 organizací všech velikostí. Ve společnosti Check Point zabezpečujeme budoucnost.