Háborús Játékok

Varga-Perke Bálint
OSCP, GWAPT
ITBN 2012 Útmutató IT-biztonsági szakértője
Silent Signal Kft.

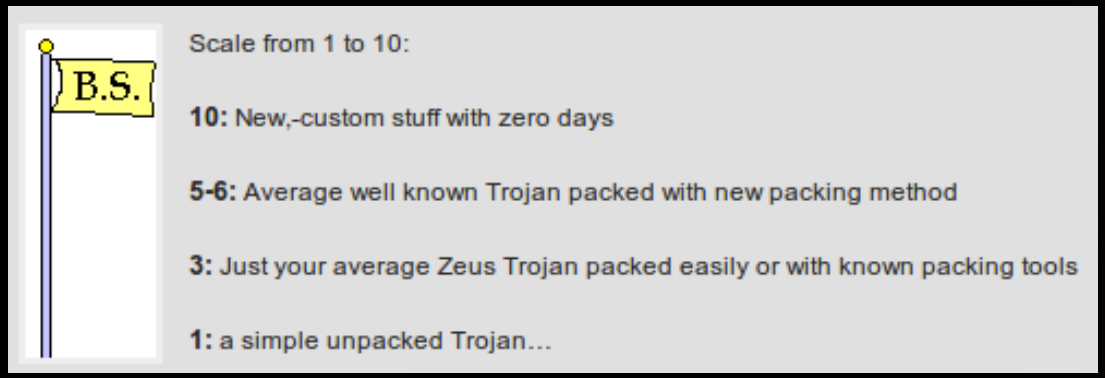
Advanced Persistent Threat

- Kifinomult támadások
- Hosszú ideig észrevétlen támadói jelenlét
- Menetrend:
  1. Spear phishing / Stratégiai website kompromittáció
  2. Kliens sérülékenység kihasználása
  3. Trójai telepítés
  4. Mindebből senki nem vesz észre semmit
  5. Profit

Advanced?

"Emerging 'Stack Pivoting' Exploits Bypass Common Security" – Li-Szőr, Intel-McAfee

- Return-Oriented-Programming - < 2008
- Stack Pivoting - < 2010
- ROP-only shellcode - < 2010



Advanced?

"Emerging 'Stack Pivoting' Exploits Bypass Common Security" – Li-Szőr, Intel-McAfee

- Return-Oriented-Programming - < 2008
- Stack Pivoting - < 2010
- ROP-only shellcode - < 2010

"We were out of our league, in our own game" – Mikko Hypponen, F-Secure

0-day-ek?

CVE-2011-0263

- Kutatás időtartama: Tesztkörnyezet installálás + 10 perc
- Bejelentés a ZDI-nek: 2010-03-10
- Jelzés a gyártónak: 2010-09-14
- Gyártói javítás: 2011-01-11
- Javítás telepítése: ???

10 hónap

0-day-ek?

CVE-2011-0263

- Kutatás időtartama: Tesztkörnyezet installálás + 10 perc
- Bejelentés a ZDI-nek: 2010-03-10
- Jelzés a gyártónak: 2010-09-14
- Gyártói javítás: 2011-01-11
- Javítás telepítése: ???

10 hónap

A 0-day információ a piacon rendelkezésre áll!

0-day-ek?

CVE-2011-0263

- Kutatás időtartama: Tesztkörnyezet installálás + 10 perc
- Bejelentés a ZDI-nek: 2010-03-10
- Jelzés a gyártónak: 2010-09-14
- Gyártói javítás: 2011-01-11
- Javítás telepítése: ???

10 hónap

A 0-day információ a piacon rendelkezésre áll!

A 0-day információ nem feltétel!

Advanced?

Két és fél évet kapott a Marriottot zsaroló magyar hacker

MTI | **[origo]** | 2012. 02. 03., 21:06 | Utolsó módosítás: 2012. 02. 04., 9:33 | 1 komment

Címkék: USA, Maryland, hacker, kékfény, zsarolás, számítógépes biztonság, külföldi bünügyek

Ez a cikk 1 éve frissült utoljára. A benne szereplő információk a megjelenés idején pontosak voltak, de mára elavultak lehetnek.

Tweet | tumblr | Ajánlom | Recommend

Egy magyar férfi még 2010-ben törte föl a Marriott International számítógépes rendszerét, és munkát kért azért cserébe, hogy ne tegye közzé a cég bizalmas adatait.

Jogerősen két és fél év szabadságvesztéssel sújtotta a Baltimore-i Szövetségi Kerületi Bíróság pénteken azt a magyar hackert, aki 2010-ben feltörte a Marriott International számítógépes rendszerét, és azzal zsarolta meg a szállodaláncot, hogy ha nem hajlandó őt alkalmazni, közzéteszi bizalmas adatait.

Útmutatás

A "kifinomult támadás" nem az államok monopóliuma

Szabályozás?

Eszköztár

Lockheed-Martin: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

TODO?

- Tudatosítás
  - Felhasználó
  - Üzemeltető
  - Management
- Védelmi fókusz kiterjesztése a munkaállomásokra
  - Miből építkezhetünk?
  - Hogyan építkezzünk?
- Audit erősítése – Mindenki gyanús
- Visszacsatoláson alapuló incidenskezelési stratégia kidolgozása
- A puding próbája az evés!

Köszönöm megtisztelő figyelmüket!

Facebook

vpbalint@silentsignal.hu

web

e-mail

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Hivatkozások

- http://blog.trailofbits.com/2013/05/13/elderwood-and-the-department-of-labor-hack/
- http://blog.phishme.com/2013/03/defining-a-sophisticated-attack/
- http://blogs.mcafee.com/mcafee-labs/emerging-stack-pivoting-exploits-bypass-common-security
- http://www.origo.hu/nagyvilag/20120203-ket-es-fel-evet-kapott-a-marriottot-zsarolo-magyar-hacker.html
- http://www.zerodayinitiative.com/advisories/ZDI-11-005/
- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- https://www.youtube.com/watch?v=X2M9nmqP6n0
- https://www.youtube.com/watch?v=vBQET68HHSg
- http://www.wired.com/threatlevel/2012/06/internet-security-fail/
- http://buhera.blog.hu
- https://www.youtube.com/watch?v=SFGDzHAeTrE :)