Filter online threats off your network

Životní cyklus malwaru

1 Infekce

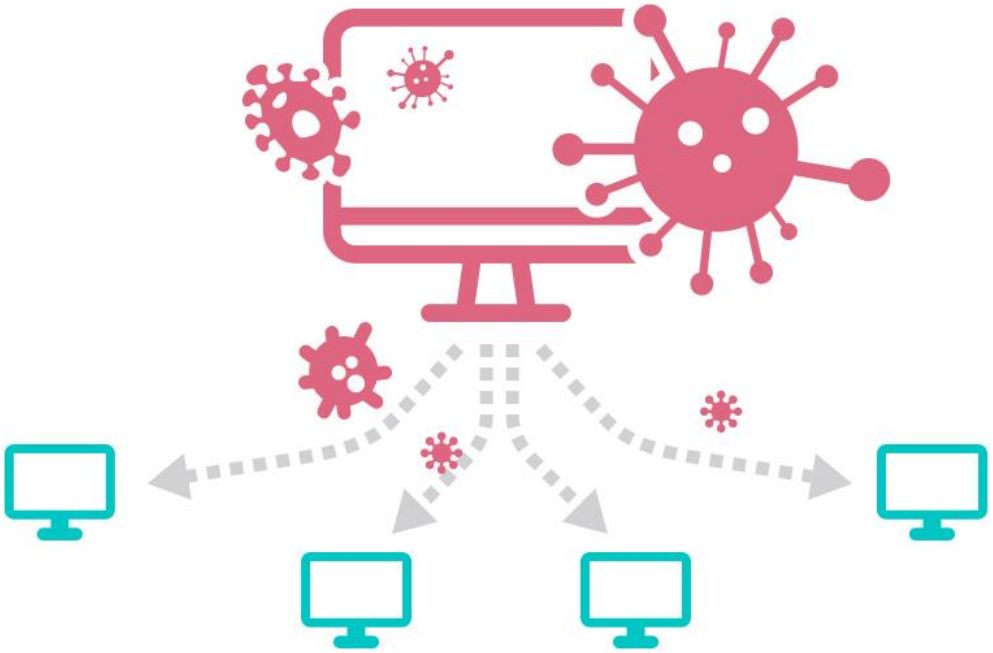
- Emailem rozesílaný downloader
- Infekce nebo exploit hostovaný na webu

2 Instrukce od C&C

- Malware vyčkává s aktivitou až do prvních instrukcí od C&C serveru
- Útočník se snaží C&C server udržet naživu co nejdéle

3 Aktivita malwaru

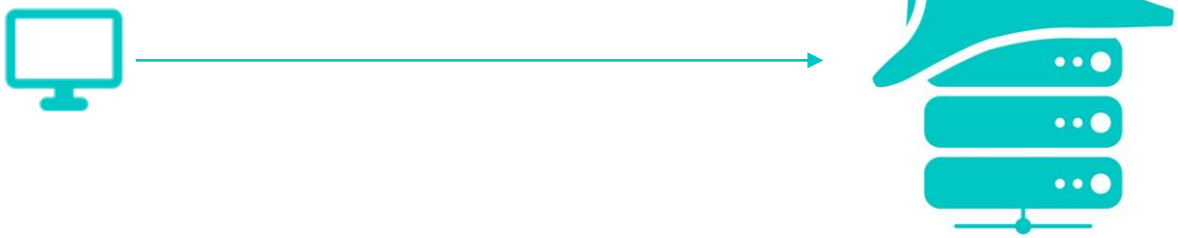
- Rozesílání spamu
- DDoS útoky
- Těžba kryptoměn
- Bruteforcing online služeb
- Keylogging
- Šifrovaná dat a vydírání



Domain Generation Algorithm (DGA)

- Mechanismus, jak mohou infikované stroje kontaktovat C&C server
- Infikovaný stroj si generuje náhodné domény např. na základě aktuálního data
- Útočník některé z domén koupí
- Příklady domén:
  - http://osint.bambenekconsulting.com/feeds/dga-feed.txt

xqmwkms.com
gaeqkhd.com
ejxqfzs.com
yfwqjxo.com
lzcxzes.com
wzmwqza.com
yxcqodq.com
zrqrcxu.com
twzyxej.com
xuqnqtg.com



xqmwkms.com
gaeqkhd.com
ejxqfzs.com
yfwqjxo.com
lzcxzes.com
wzmwqza.com
yxcqodq.com
zrqrcxu.com
twzyxej.com
xuqnqtg.com

Workshop

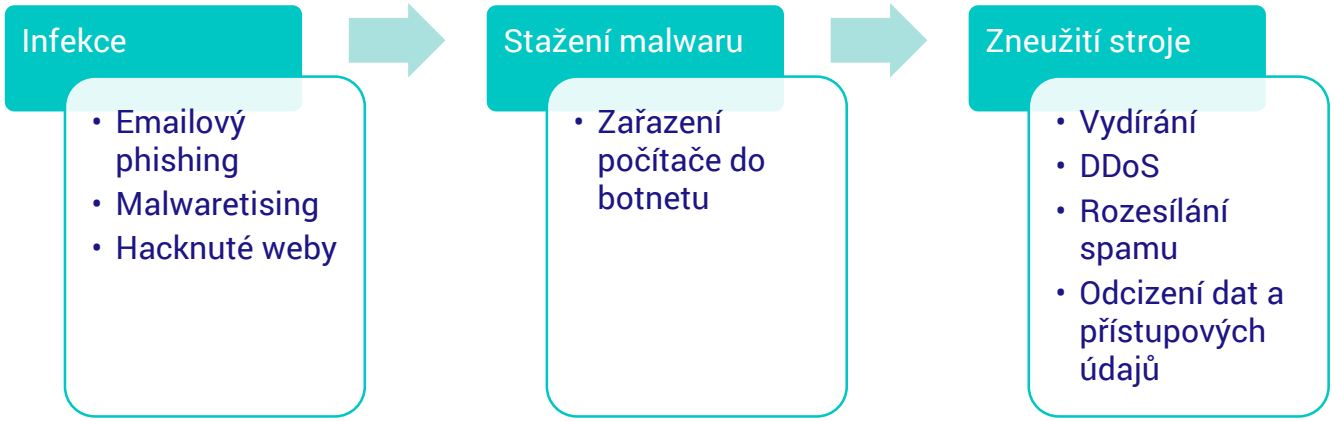
whalebone

Životní cyklus malwaru

whalebone

Příklad útoku na uživatele

Postup útoku



Použité nástroje

Spam botnet

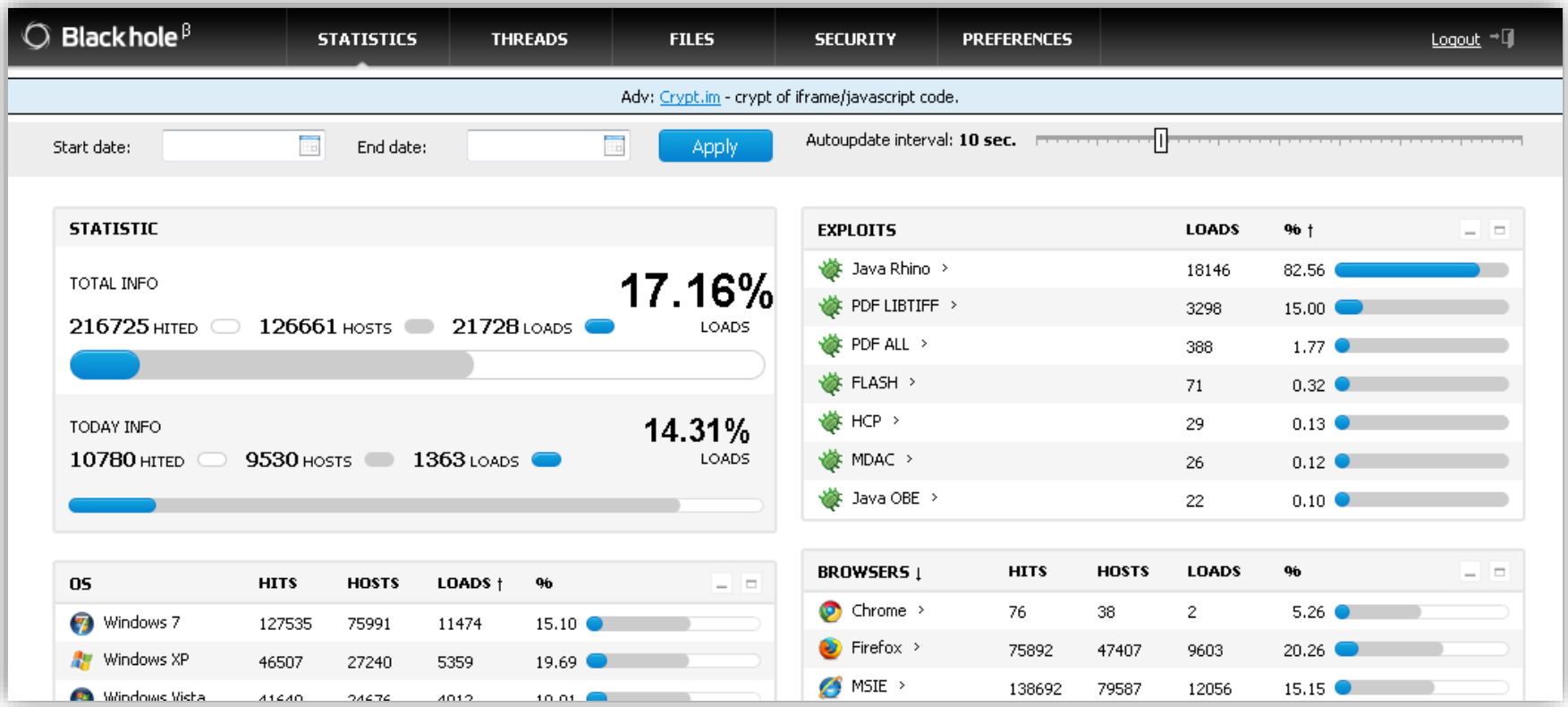
$10 - $500 za million emailů

Ceny se liší podle spolehlivosti doručení a možností customizace spam kampaně

Offering	Price
Cheap email spamming service	US$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US$50-500 per 50,000-1,000,000 emails
SMS spamming service	US$3-150 per 100-10,000 text messages
ICQ spamming service	US$3-20 per 50,000-1,000,000 messages
1-hour ICQ flooding service	US$2
24-hour ICQ flooding service	US$30
Email flooding service	US$3 for 1,000 emails
1-hour call flooding service (i.e., typically takes call center services down)	US$2-5
1-day call flooding service	US$20-50
1-week call flooding service	US$100
SMS flooding service	US$15 for 1,000 text messages
Vkontante.ru account database	US$5-10 for 500 accounts
Mail.ru address database	US$1.30-19.47 per 100-5,000 addresses
Yandex.ru address database	US$7-500 per 1,000-100,000 addresses
Skype SMS spamming tool	US$40
Email spamming and flooding tool	US$30

Trend Micro Incorporated Research Paper (2012)
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Exploit Kit - rozhraní



Brian Krebs, Crimevertising: Selling Into the Malware Channel (2012)
http://krebsonsecurity.com/2012/02/crimevertising-selling-into-the-malware-channel/

Exploit Kit

Katrin	$25/day	2011
Robopak	$150/week or $500/month	2011
Blackhole (v1.1.0)	$1,500	2011
Blackhole (v1.2.1)	$700/three months or $1,500/year	2011
Bleeding Life (v3.0)	$1,000	2011
Phoenix (v3.0)	$2,200/single domain	2011
Phoenix (v3.0)	$2,700/multi-threaded domain	2011
Eleonore (v1.6.3a)	$2,000	2011
Eleonore (v1.6.4)	$2,000	2011
Eleonore (v1.6.2)	$2,500-$3,000	2012
Phoenix (v2.3.12)	$2,200 / domain	2012
Styx sploit pack rental	$3,000 / month	2012
Exploit kits that employ botnets	up to $10,000	2012
CritXPack	$400/week	2012
Phoenix (v3.1.15)	$1,000-$1,500	2012
NucSoft	$1,500	2012
Blackhole—hosting (+ crypter + payload + sourcecode)	$200/week or $500/month	2013
Whitehole	$200–$1,800 rent	2013
Blackhole—license	$700/three months or $1,500/year	2013
Cool (+ crypter + payload)	$10,000/month	2013
Gpack	$1,000–$2,000	2013
Mmpack	$1,000–$2,000	2013
Icepack	$1,000–$2,000	2013
Eleonore	$1,000–$2,000	2013
Sweet Orange	$450/week or $1,800/month	2013
Whitehole	$200–600/week or $600–1,800/month, depending on traffic	2013

SOURCES: Clarke, 2013a; Fossi et al., 2011; Fortinet, 2012; Goncharov, 2012; Kafeine, 2013a; Krebs, 2013a; M86 Security Labs, 2010; Martinez, 2007; McAfee Labs, 2011; O'Harrow, 2012; Paget, 2010b, 2012; Parkour, 2014.

RAND (National Security Research Division), Markets for Cybercrime Tools and Stolen Data (2014)
https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Exploit Kit

- Kompletní Angler exploit kit včetně zdrojového kódu
  - $20-30k
- Pronájem Angler Exploit kitu na měsíc
  - $500
  - Jsou dokumentovány případy, kdy se platí pay-per-infection

Exploit Kits as a Service – How Automation Is Changing the Face of Cyber Crime
https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime

Malware

- Botnet setup (consulting)
  - $400
- Banking Trojan
  - $386
- Remote Access Tool (RAT)
  - 20$ - 50$
- Packers/crypters
  - $50 - $150
    - Aegis
    - Sheikh Crypter
    - xProtect

http://resources.infosecinstitute.com/cyber-criminal-ecosystems-in-the-deep-web/
http://resources.infosecinstitute.com/wp-content/uploads/Secureworks-Underground-Hacking-Report.pdf

Sečteno, podtrženo

Položka	Cena (USD)
Spam	500
Exploit kit	1500
Botnet	400
Packer	100
Suma	**2500**

Odfiltrujte hrozby ze své sítě

Robert Šefr
robert.sefr@whalebone.io
+420 608 737 930
https://whalebone.io

whalebone