TREND MICRO

Securing Your Web World



Realidade das BotNets Atuais

Ranieri Romera

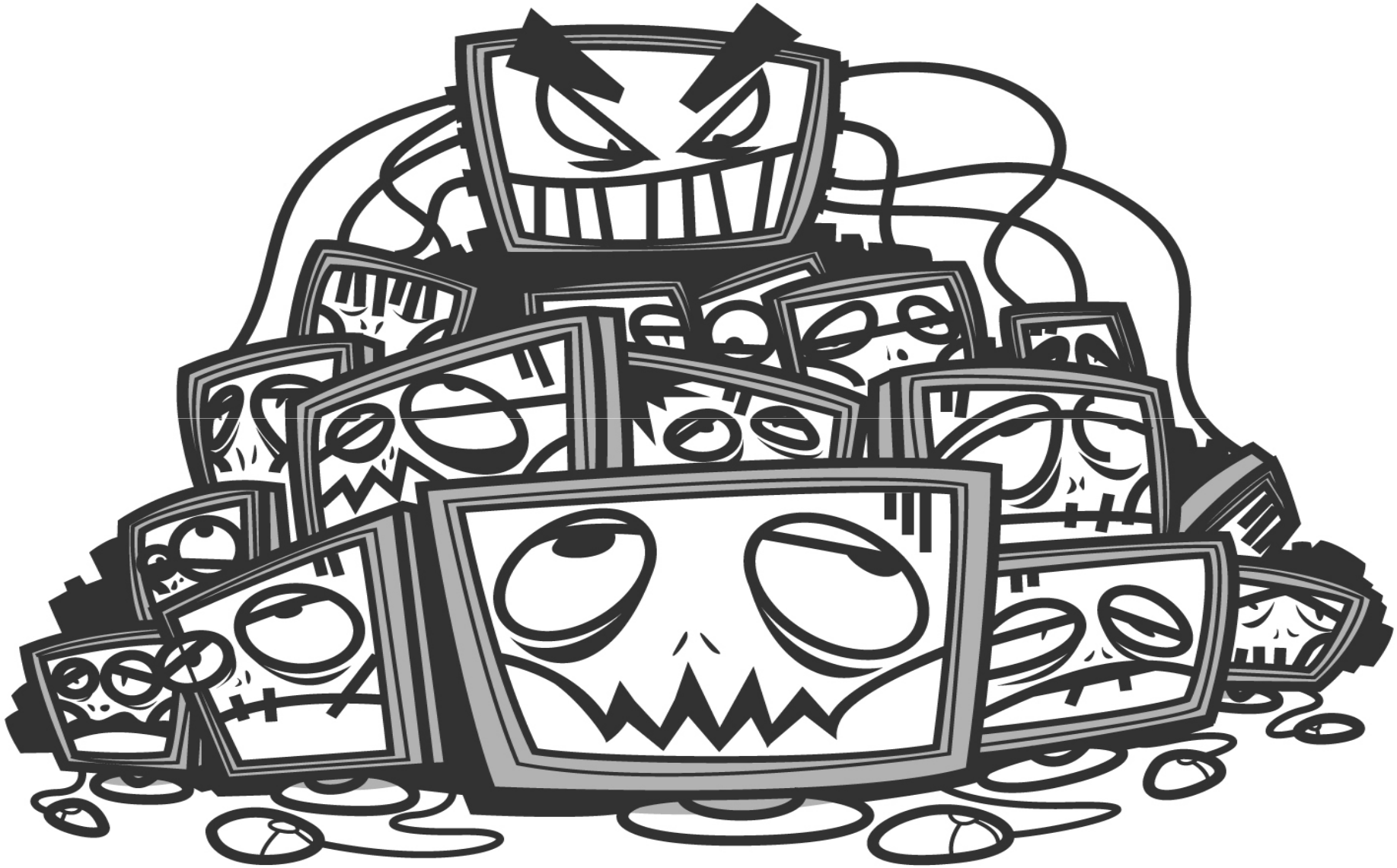
H2HC

Nov/2010

Agenda

- Algumas definições
- Fatos
- Principais BotNets
- Mecanismos de defesas das BotNets
- BotNet no ringue
  - O Mau fazendo o Bem
  - O Bom fazendo o Mal
- Tendências
- Perguntas

Algumas Definições

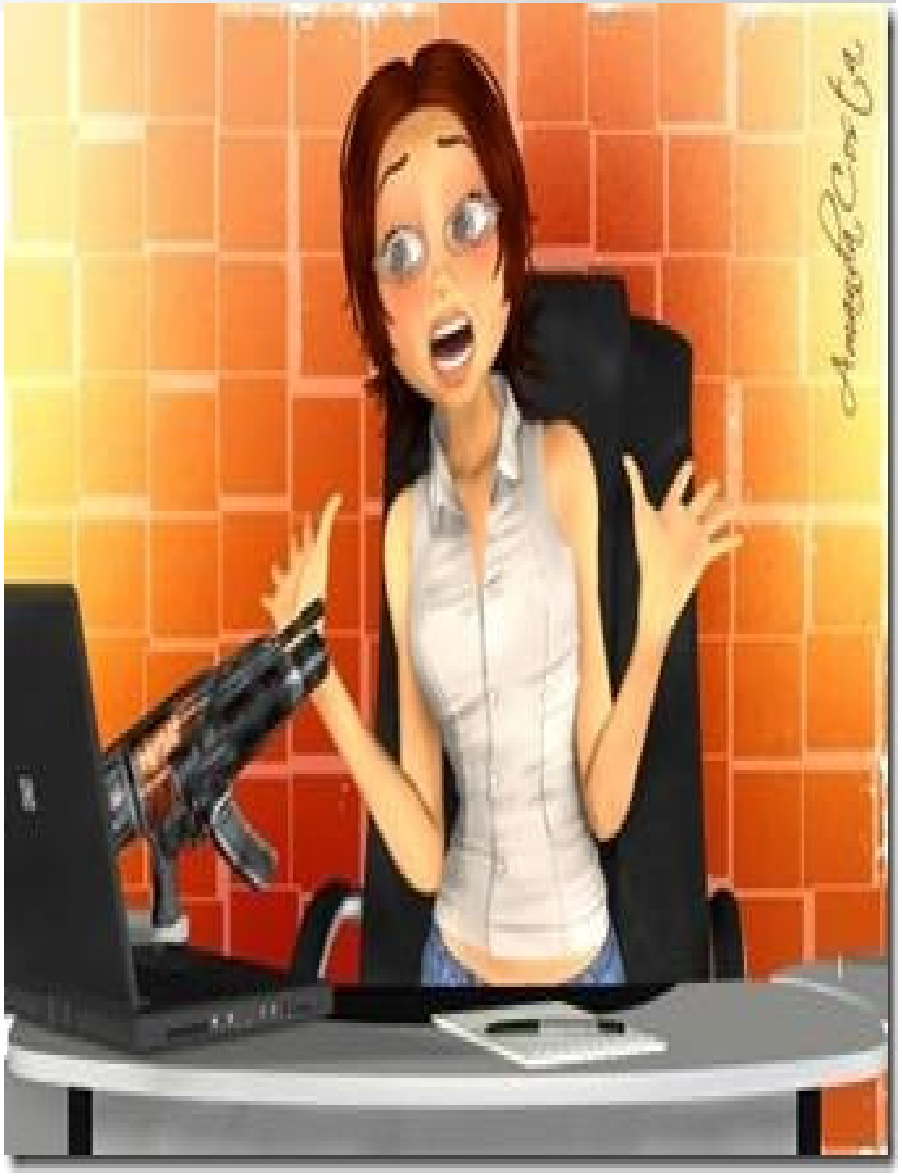


Algumas Definições - Nomenclatura

- **BotMaster**
- **Bot / Zumbi**
- **C&C / Canal de controle**
- **BotNet**

Alguma Definições – Principais Usos

- Roubo de senhas
- Roubo de dados financeiros
- Envio de SPAM
- Instalação de softwares
- DOS/DDOS
- Publicidade
- ETC!!!



Fatos (malware)

Questão	Passado	Presente
Motivação	Por brincadeira; POC; Pelo conhecimento.	Principalmente pelo dinheiro
Capacidades	Destrutivas; Que chamavam a atenção;	Tentam não chamar a atenção; Tudo o que já falamos e mais o que o desenvolvedor pensar/fazer.

Fatos

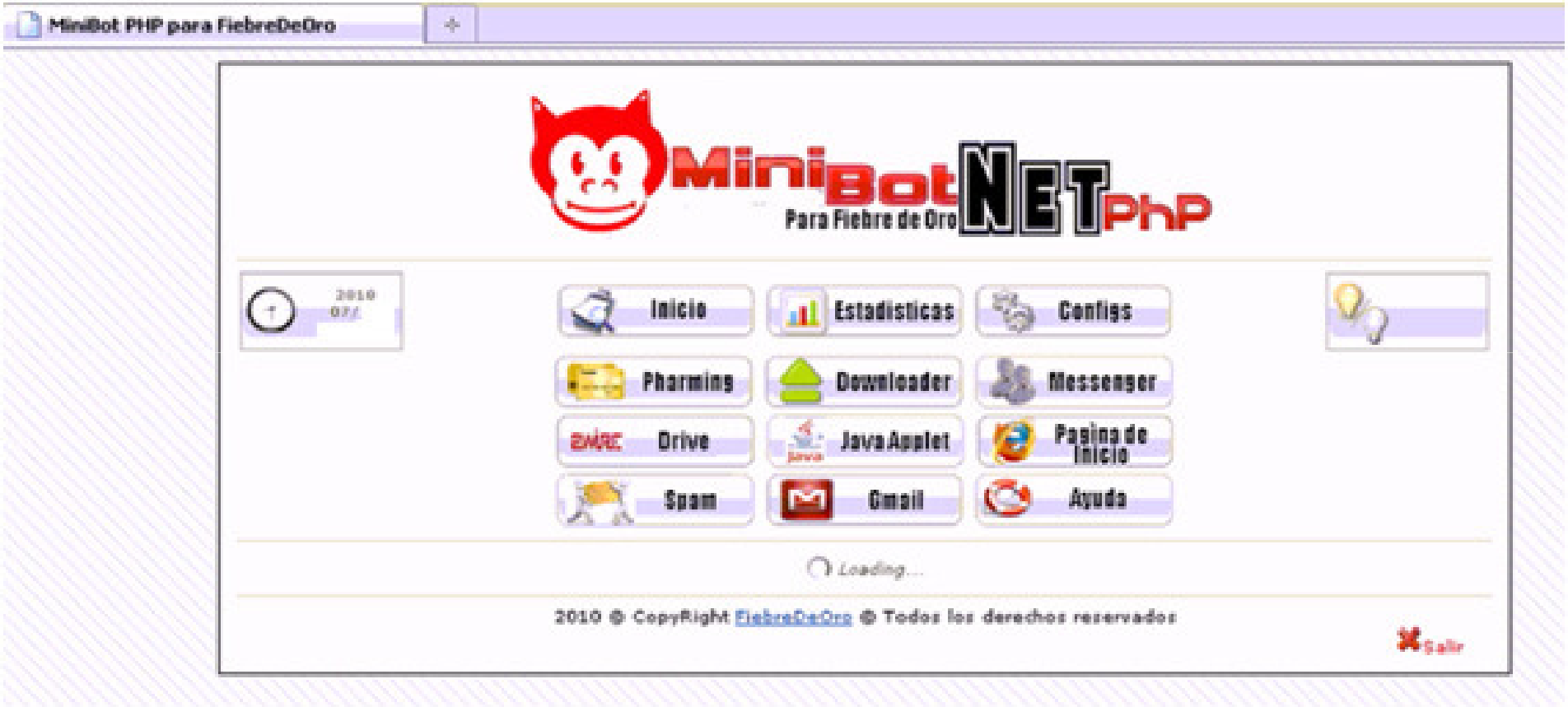
- Em 2007 as previsões diziam que 2008 seria o ano das BotNets.
  - Porém pouco se ouviu falar, em 2008, sobre ações de BotNets;
- No final de 2008 é descoberto o Conficker
  - Conficker infectou milhões de maquinas pelo mundo;
  - FUD – muitos boatos e duvidas sobre o malware;
    - Qual a intenção do autor? Quem é o autor?
    - Um worm apenas? Ou um worm e botnet?
    - Em determinadas data iria gerar o caos!!!
    - Recompensa de US 250k para quem entregar o autor!!!
    - Se era apenas um worm por que fazia atualizações constantes? Apenas novos exploits? Apenas mutações no código para dificultar a detecção?
    - As senhas descobertas eram repassadas?

Principais BotNets (atuais)

- FakeAV
  - Principal uso para roubo de dados financeiros;
- Zeus
  - Kit expansível que pode ser utilizada para múltiplos propósitos;
- SpyEyes
  - Kit expansivél que pode ser utilizada para múltiplos propósitos;

SpyEye C&C Padrão

SpyEye C&C – Com módulos



SpyEye C&C – Com módulos (2)

Principais BotNets (atuais)

- FakeAV
  - Principal uso para roubo de dados financeiros;
- Zeus
  - Kit expansível que pode ser utilizada para múltiplos propósitos;
- SpyEyes
  - Kit expansivél que pode ser utilizada para múltiplos propósitos;
- Koobface
  - BotNet que se propaga por mensagem dentro de redes sociais;
  - Possui múltiplos módulos que afetam a resolução de nomes, resultado de pesquisas online, informações do usuário logado, número de série dos produtos instalados, módulos de propagação via redes sociais, módulo para “quebra” de captcha e até mesmo um módulo de AD.
- Qakbot
  - Bot para roubo de senhas, que teoricamente no Q3 havia cessado suas operações, porém no Q4 voltou a aparecer.

Mecanismos de defesa

➔ Muitos kits fazem atualizações de seu arquivos de configuração (que em geral são criptografados);

Mecanismos de defesa

Historical information

ConfigURL History

Changedate	Host	ConfigURL	Hash
2010-11-19	193.104.146.49	193.104.146.49/n/bin/config.bin	d5d706eb9f50cf1268405bebf03a80af
2010-11-18	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4
2010-11-12	193.104.146.49	193.104.146.49/n/bin/config.bin	08c635f56e4fa935781cff5819d7c645
2010-11-11	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4
2010-11-11	193.104.146.49	193.104.146.49/n/bin/config.bin	24af01f77a796bfa22b06cb1df844d02
2010-11-11	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4
2010-11-11	193.104.146.49	193.104.146.49/n/bin/config.bin	19e322db0757d27654f2f2bec41bc4d6
2010-11-10	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4
2010-10-25	193.104.146.49	193.104.146.49/n/bin/config.bin	43192477342bd0498c63953554aeeb43
2010-10-24	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4
2010-10-23	193.104.146.49	193.104.146.49/n/bin/config.bin	ba7b74010a95e1ac7da725f84757f3fb
2010-10-23	193.104.146.49	193.104.146.49/n/bin/config.bin	a99dafe8e9c51cf09d15e4764749baa4

# of rows: **12**

Mecanismos de defesa

ZeuS ConfigURLs on this C&C

Dateadded	ZeuS ConfigURL	Status	V	Builder	Filesize	MD5 hash	HTTP Status
2010-11-24	currencyis.com/22oct_bir.cpm	online	2	n/a	3'869	655d6d1dd61341128c20a851785ee3be	200
2010-11-24	currencyis.com/22oct_dmi.cpm	online	2	2.0.7.0	7'080	ed3bd158147147d91d6724769f1a8a88	200
2010-11-24	currencyis.com/22oct_den.cpm	online	2	2.0.7.0	7'078	afb3719a4ca655791d2f509db17ff78d	200
2010-11-24	currencyis.com/14oct_usa.cpm	online	2	2.0.7.0	6'948	563b37f61056e87652f85e1b453cedfe	200
2010-11-24	currencyis.com/22oct_pac.cpm	online	2	2.0.7.0	7'080	5e9d73959e89726c4cebae2c9ddc8a8e	200
2010-11-24	currencyis.com/22oct_ic3.cpm	online	2	n/a	1'116	f9ecdbc54f6a7b099c0268035f84392f	200

Mecanismos de defesa

- ➔ Muitos kits fazem atualizações de seu arquivos de configuração (que em geral são criptografados);
- ➔ Os C&C mudam de endereço IP;

Mecanismos de defesa

Domain History

Changedate	Host	IP address	AS number	AS name	Country
2010-11-27	hq.livelongdieoldandreborn.cc	94.23.16.147	16276	OVH OVH	
2010-11-26	hq.livelongdieoldandreborn.cc	77.246.145.81	29182	ISPSYSTEM-AS ISPsystem Autonomous System	
2010-11-26	hq.livelongdieoldandreborn.cc		0		-
2010-11-25	hq.livelongdieoldandreborn.cc	219.147.255.39	17897	CHINATELECOM-HLJ-AS-AP asn for Heilongjiang Provincial Net of CT	
2010-11-25	hq.livelongdieoldandreborn.cc	77.246.145.81	29182	ISPSYSTEM-AS ISPsystem Autonomous System	

# of rows: **5**

Mecanismos de defesa

- ➔ Fazer atualizações de seu arquivos de configuração (que em geral são criptografados);
- ➔ Os C&C mudam de endereço IP;
- ➔ Distribuição de novos clientes da bot;

Mecanismos de defesa

BinaryURL History

Changedate	Host	BinaryURL	Hash
2010-11-27	for-advanced-cfg1.com	for-advanced-cfg1.com/monte-karlo/us.exe	04966c92954176339d796ebac55bfaeb
2010-11-27	for-advanced-cfg1.com	for-advanced-cfg1.com/abudabi/uk.exe	484c914bb51a43d0f930e9b131b0f7b8
2010-11-27	for-advanced-cfg1.com	for-advanced-cfg1.com/abudabi/uk.exe	a5c417f9fa84ff8136f06321940e655b
2010-11-25	for-advanced-cfg1.com	for-advanced-cfg1.com/monte-karlo/us.exe	611adf9caec8bf9b248bf679d680d5a4
2010-11-25	for-advanced-cfg1.com	for-advanced-cfg1.com/abudabi/uk.exe	0738aaaf5fb77f13ac0413c1641670ce

# of rows: **5**

Mecanismos de defesa

- ➔ Fazer atualizações de seu arquivos de configuração (que em geral são criptografados);
- ➔ Os C&C mudam de endereço IP;
- ➔ Distribuição de novos clientes da bot;
- ➔ Domain Generation Algorithm (DGA);

Mecanismos de defesa


```
suffix = ["anj", "ebf", "arm", "pra", "aym", "unj",
          "ulj", "uag", "esp", "kot", "onv", "edc"]
def generate_daily_domain():
    t = GetLocalTime()
    p = 8
    return generate_domain(t, p)

def scramble_date(t, p):
    return (((t.month ^ t.day) + t.day) * p) +
            t.day + t.year

def generate_domain(t, p):
    if t.year < 2007:
        t.year = 2007
    s = scramble_date(t, p)
    c1 = (((t.year >> 2) & 0x3fc0) + s) % 25 + 'a'
    c2 = (t.month + s) % 10 + 'a'
    c3 = ((t.year & 0xff) + s) % 25 + 'a'
    if t.day * 2 < '0' || t.day * 2 > '9':
        c4 = (t.day * 2) % 25 + 'a'
    else:
        c4 = t.day % 10 + '1'
    return c1 + 'h' + c2 + c3 + 'x' + c4 +
           suffix[t.month - 1]
```

Mecanismos de defesa

- ➔ Fazer atualizações de seu arquivos de configuração (que em geral são criptografados);
- ➔ Os C&C mudam de endereço IP;
- ➔ Distribuição de novos clientes da bot;
- ➔ Domain Generation Algorithm (DGA);
- ➔ Blacklist para acesso ao C&C;

Mecanismos de defesa

- ➔ Fazer atualizações de seu arquivos de configuração (que em geral são criptografados);
- ➔ Os C&C mudam de endereço IP;
- ➔ Distribuição de novos clientes da bot;
- ➔ Domain Generation Algorithm (DGA);
- ➔ Blacklist para acesso ao C&C;
- ➔ Além das defesas triviais (compactação do PE; códido do C&C muitas vezes seguro)

BotNet no Ringue

O Mau fazendo o Bem

➔ Uma das funcionalidades do SpyEye é remover o Zeus, caso ele esteja instalado na maquina que o SpyEye está tentando infectar;

O Mau fazendo o Bem


```
#include <windows.h>
#pragma warning(disable : 4005) // macro redefinition
#include <ntdll.h>
#pragma warning(default : 4005)
#include <shlwapi.h>
#include <shlobj.h>
void GetZeusInfo(ULONG dwArg, PCHAR lpOut, DWORD dwOutLn, PCHAR lpMutex, DWORD dwMutexLn)
{
    PSYSTEM_HANDLE_INFORMATION shi = 0;
    NTSTATUS Status = 0;
    ULONG len = 0x2000;
    POBJECT_NAME_INFORMATION obn = 0;
    HANDLE proc = 0, thandle = 0, hFile = 0;
    BOOLEAN enable = FALSE;
    UCHAR name[300] = {0};
    ULONG temp = 0, rw = 0;
    do
    {
        shi = (PSYSTEM_HANDLE_INFORMATION)malloc(len);
        if (shi == 0)
            10
        {
            return;
        }
    Status = NtQuerySystemInformation(SystemHandleInformation, shi, len, NULL);
    if (Status == STATUS_INFO_LENGTH_MISMATCH)
    {
        free(shi);
        len *= 2;
    }
    else
        if (NT_ERROR(Status))
```

O Bem fazendo o Mal

➔ Policia Alemã envia arquivo em uma BotNet BredoLAB, para avisar os usuários que eles estão infectados!!!

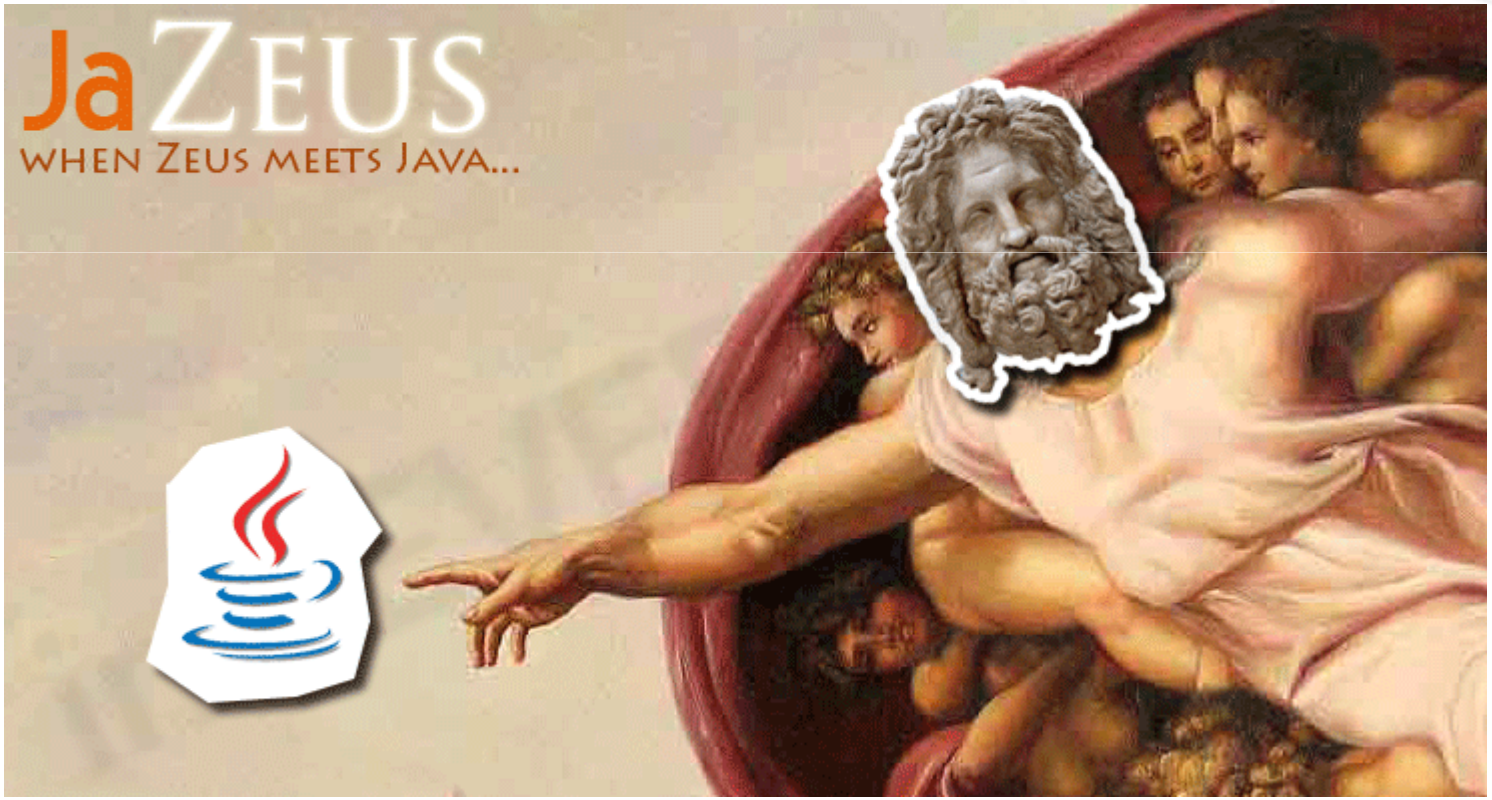
➔ http://www.bestspywareremovalblog.com/tag/crime-unit/

Tendências

- Malwares feitos em Java
  - Multiplataforma
  - Já há casos registrados para KoobFace e Zeus

Tendências

- Malwares feitos em Java
  - Multiplataforma
  - Já há casos registrados para KoobFace e Zeus



Tendências

- Malwares feitos em Java
  - Multiplataforma
  - Já há casos registrados para KoobFace e Zeus
- As BotNets não podem ser detidas, teremos de conviver com elas;
- Novas BotNets surgiram com muito mais poder de fogo;
- BotNets utilizarão cada vez mais exploits e zero days;
- As botnets ampliarão seus vetores de ataque;
- Uma possível fusão entre códigos de diferentes botnets;

Perguntas

Thank you.

Danke.

Salamat.

Go raibh maith agat.

Dank u.

Gracias.

Merci.

Спасибо

شكرا

謝謝

ありがとう

Obrigado.