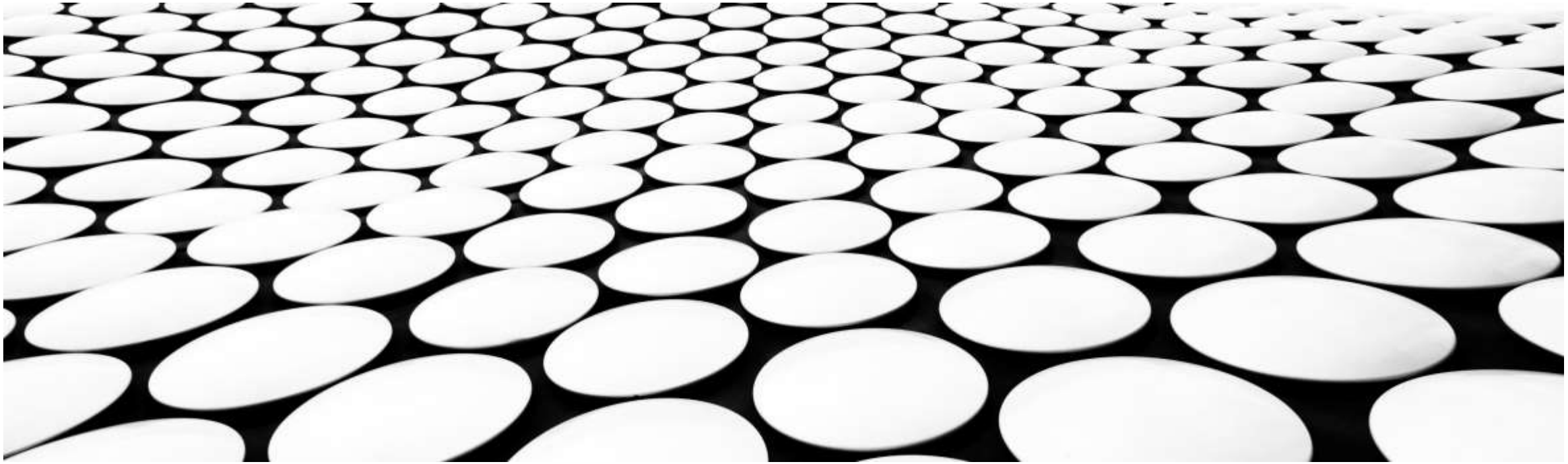
RANSOMWARE
O NOVO DESAFIO DOS ATAQUES DO FUTURO

MARCELO CAIADO, M.SC.

CISSP, GCFA, GCIH, GSLC, CCO, CCPA, CHFI, CTIA, CEI, CCFC, CRC



AVISO LEGAL

Todas as opiniões apresentadas aqui são exclusivas do orador, apenas para fins ilustrativos, e são pessoais e não representam as de pessoas, instituições ou organizações com as quais o apresentador possa estar associado em capacidade profissional ou pessoal, a menos que explicitamente declarado. Quaisquer opiniões ou pontos de vista não são recomendações técnicas e nem jurídicas, e não têm a intenção de difamar qualquer religião, grupo étnico, clube, organização, empresa ou indivíduo.

MARCELO CAIADO

- Mestre em Ciência da Computação (UnB)
- Pós-graduado em Gestão Pública (FGV)
- Perito em TIC / MPU (desde 1997)
- Cyber Forensics Analyst / BlackBerry (2008/2010)
- Professor (INSPER, IDESP, IPOG e WB)
- Coautor dos livros Cyber Risk e Técnicas Avançadas de Investigação
- http://dfir.com.br/

O INÍCIO

Dezembro de 1989

EDITORIAL

AIDS Information Version 2.0

On various d...

... Credit

... *usiness World* who

... acted Jim Bates, a member of the

... *itution of Analysts & Programmers*, and asked him to undertake a disassembly of the disk. Jim, a regular contributor and editorial advisor to the *Virus Bulletin*, proceeded to conduct a most thorough and painstaking analysis of the AIDS Information disk. In the course of his investigations he produced both a reliable removal

also been a number of totally inaccurate, unjustified and false accusations levelled against entirely innocent organisations and individuals.

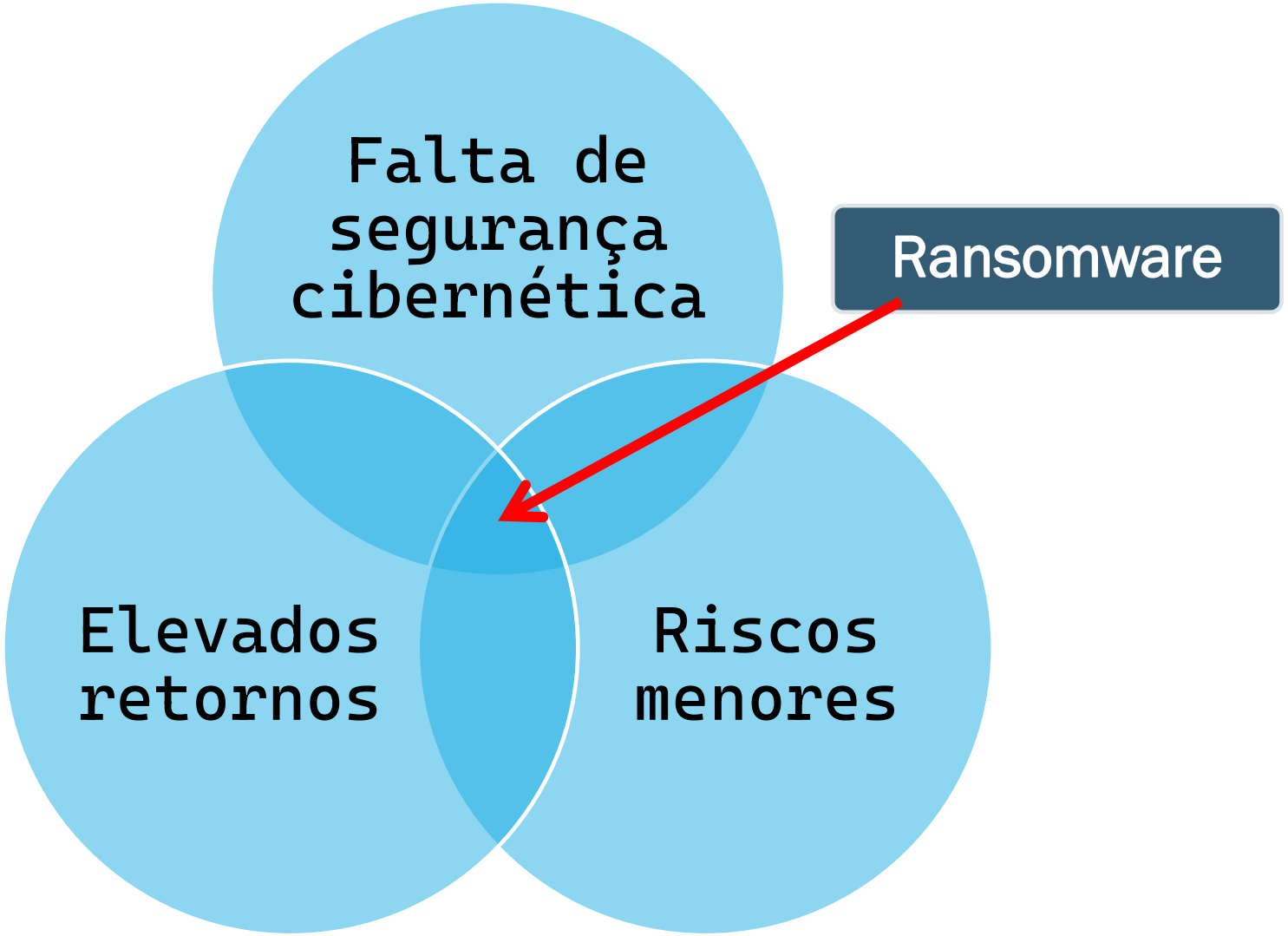
... utory lessons have been learned. Unsolicited ... vill, in the future, be treated with extreme caution ... t is extraordinary that controls to prevent use of ... disks failed, or never existed, in so many ... It is also worth pointing out that virus specific ... iseless for tackling unknown threats. Only ... ng programs revealed the corruption of the ... BAT caused by the AIDS disk. Finally, ... ould take note that they are vulnerable to the ... mailing lists and a reassessment of list ... many companies and list brokers may be

... was, perhaps, inevitable that the profiteers would exploit the situation. Some individuals and companies were quick to offer "AIDS clearing" and "AIDS protection" services - at a price - to affected users. Many of these offers were made based on the flimsiest knowledge and sometimes without any analysis whatsoever! Conversely, the national UK newspapers showed welcome restraint in reporting this incident. Fortunately the tabloids seem to have 'missed the boat' on this one. Anyone who saw the *Daily Star's* Britain on the Blink' Datacrime exclusive on

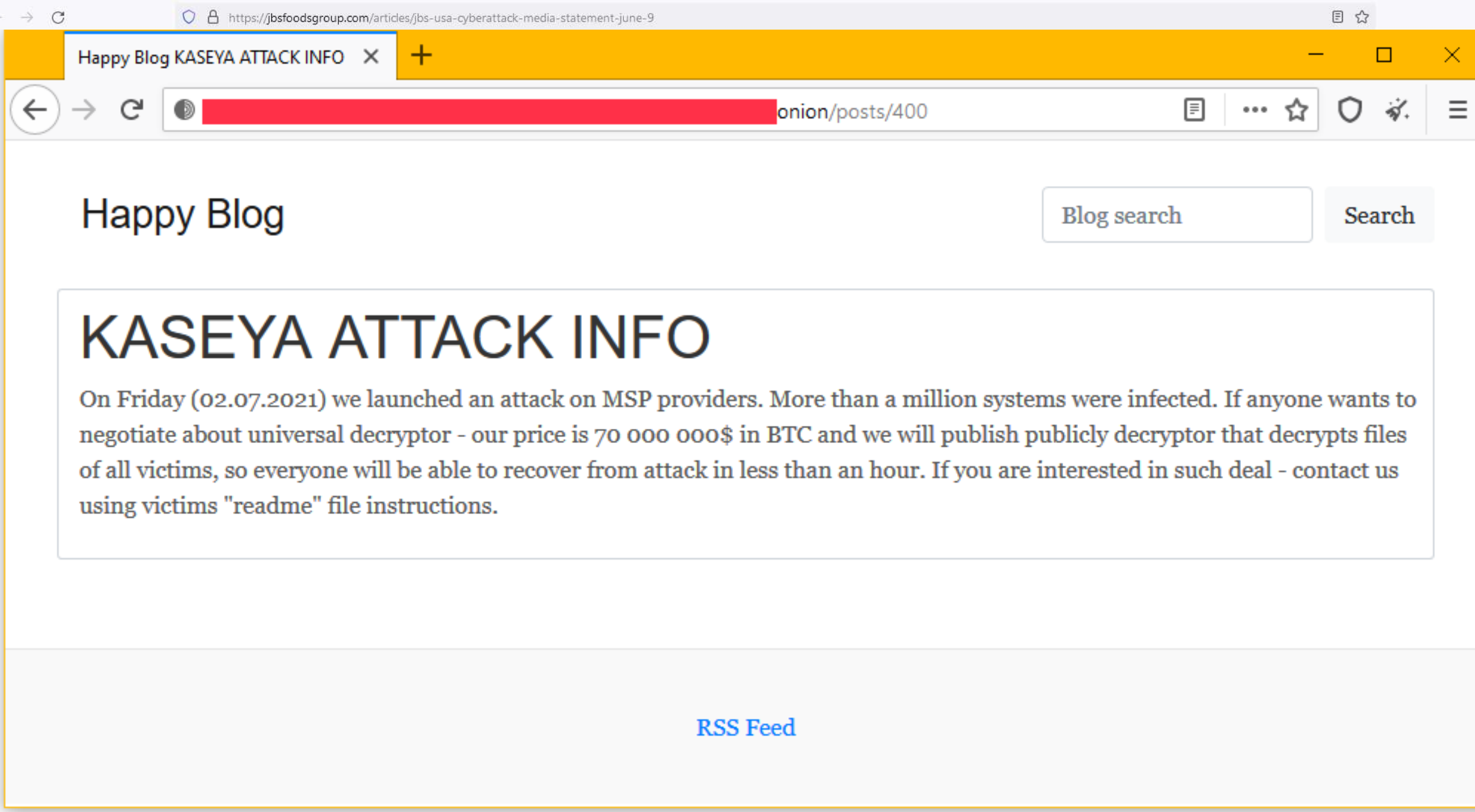
"Concluída a configuração do arquivo na unidade C: o programa imprime uma fatura de pagamento pelo 'aluguel' deste software para uma caixa postal no Panamá."

Fonte: Virus Bulletin, January 1990

CRIME ORGANIZADO




.. 2009.2.27 DEFENSE CHIEF LIFTS BAN ON PICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE PENTAGON WILL ALLOW THE PRESS TO PHOTOGRAPH THE FLAG-DRAPED COFFINS OF AMERICA
09.2.27 U.S., PAKISTAN AND AFGHANISTAN TO HOLD REGULAR TALKS: THE PLAN WAS ANNOUNCED AFTER THREE DAYS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSTRI
IVE AT A JEWISH COMMUNITY CENTER IN CARACAS, BUT NOBODY WAS HURT IN THE BLAST. 2009.2.27 WORLD BRIEFING THE AMERICAS: VENEZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS
SE TOWN OF MALAKAL KILLED AT LEAST 14 CIVILIANS AND SCORES OF F... 2009.2.27 IRAQ HANDS DEATH PENALTY TO 28 CULTISTS FOR ATTACKS: A MESSIANIC SHIITE FRINGE GROUP HAS TAKEN
S EARLY AS 1.5 MILLION YEARS AGO AN ANCESTRAL SPECIES HAD ALREADY EVOLVED THE FEET AND WALKING GAIT OF MODERN HUMANS. 2009.2.27 MALBORK JOURNAL: FACING GERMAN SUFFERIN
N A TURKISH AIRLINES JET CRASH-LANDED ON WEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID 2009.2.27 U.S. WILL GIVE QAEDA SUSPECT A CIVILIAN TRIAL: THE CH
OLVED THE FEET AND WALKING GAIT OF MODERN HUMANS. 2009.2.27 WORLD BRIEFING THE AMERICAS: VENEZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS THREW AN EXPLOSIVE AT A JEWIS
CE IT HARDER FOR IRAQ TO PAY FOR SERVICES AND COULD AFFECT U.S. PLANS FOR WITHDRAWAL. 2009.2.27 DEFENSE CHIEF LIFTS BAN ON PICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE
PRO-SHARIF DEMONSTRATIONS SPREAD ACROSS PUNJAB: THOUSANDS OF SUPPORTERS OF THE OPPOSITION LEADER NAWAZ SHARIF PROTESTED THE SUPREME COURT 2009.2.27 BOOK CASTS HARS
ONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2009.2.27 IRAQ HANDS DEATH PENALTY TO 28 CULTISTS FOR ATTACKS: A MESSIANIC SHIITE FRINGE GROUP HAS TAKEN AIM AT SHIITE PILGRIMS A
LP. GUARDSMEN IN THE WEST BANK ARE TRAINING TO ENFORCE LAW AND ORDER. 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DE
LIFTS BAN ON PICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE PENTAGON WILL ALLOW THE PRESS TO PHOTOGRAPH THE FLAG-DRAPED COFFINS OF AMERICA 2009.2.27 U.S., PAKISTAN AN
HE SCOPE OF THE AMER... 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE SCOPE OF THE HOLOCAUST WAS NOT SUFFICIE
TRALIA 2009.2.27 IN SOUTHEAST ASIA, THE UNEMPLOYED RETURN HOME: AS A MEETING OF THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS BEGINS, THE REGION IS EXPECTING AN EXODUS OF WO
S APOLOGIZED FOR REMARKS IN WHICH HE DENIED THE... 2009.2.27 WORLD BRIEFING AFRICA: SUDAN: 14 CIVILIANS DIE DURING FIGHTING: TWO DAYS OF CLASHES BETWEEN LOCAL GOVERNMENT
2009.2.27 CHINA SAYS U.S. DISTORTS FACTS IN REPORT ON RIGHTS: THE STATE DEPARTMENT SEES 2009.2.27 IRAQ WITHDRAWAL PLAN GAINS G.O.P. SUPPORT: PRESIDENT OBAMA IS TO AN
MORE THAN $11 MILLION OF INTERNATIONAL DONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2009.2.27 WORLD BRIEFING EUROPE: THE NETHERLANDS: VICTIMS: THE NINE PEOPLE WHO DIED
SRI LANKA: EDITOR ACCUSED IN ATTACK: THE POLICE ARRESTED THE EDITOR OF A TAMIL-LANGUAGE NEWSPAPER DURING A FUNERAL IN COLOMBO, THE CAPITAL, ACCUSING HIM OF AIDING A REBEL
NETHERLANDS: VICTIMS: THE NINE PEOPLE WHO DIED WHEN A TURKISH AIRLINES JET CRASH-LANDED ON WEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID. 2009.2.2
USTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BUSHFIRES IN AUSTRALIA 2009.2.27 FIREFIGHTERS CONTAIN NEW AUSTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BU
FOUND IN BANGLADESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY CONTAINING AROUND 30 BODIES. AN OFFICIAL SAID.
HARIF DEMONSTRATIONS SPREAD ACROSS PUNJAB: THOUSANDS OF SUPPORTERS OF THE OPPOSITION LEADER NAWAZ SHARIF PROTESTED THE SUPREME COURT 2009.2.27 U.S. WILL GIVE QAEDA SU
BAKILI MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN $11 MILLION OF INTERNATIONAL DONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2009.2.27 WORLD BRIEFING ASIA: S
YS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSTRIKES IN PAKISTAN, AND THE SCOPE OF THE AMER... 2009.2.27 FIREFIGHTERS CONTAIN NEW AUSTRALIAN BUSHFIRES
RIEFING THE AMERICAS: VENEZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS THREW AN EXPLOSIVE AT A JEWISH COMMUNITY CENTER IN CARACAS, BUT NOBODY WAS HURT IN THE BLAST. 2
U.S. DISTORTS FACTS IN REPORT ON RIGHTS: THE STATE DEPARTMENT SEES 2009.2.27 MASS GRAVE FOUND IN BANGLADESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDE
RIEFING UNITED NATIONS: IRANIAN REBUKES U.S. COUNTERPART: A PASSING REMARK FROM THE NEW AMERICAN AMBASSADOR TO THE UNITED NATIONS, SUSAN RICE, PROMPTED A REBUKE FROM HE
HE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY CONTAINING AROUND 30 BODIES. AN OFFICIAL SAID. 2009.2.27 WORLD BRIEFING EUROPE: THE NETHERL
GRAVE IN POLAND HAS REVEALED THAT AN UNDERSTANDING OF CIVILIAN SUFFERING IN FORMER GERMAN TERRITORIES IS STARTING... 2009.2.27 WORLD BRIEFING ASIA: SRI LANKA: EDITOR ACCU
A MASS GRAVE ON FRIDAY CONTAINING AROUND 30 BODIES. AN OFFICIAL SAID. 2009.2.27 CHINA FAILS TO HALT SALE OF LOOTED RELICS AT PARIS AUCTION: TWO BRONZE HEADS ORIGINALLY LOO
RLYSTS SAY ETHNIC DIVISIONS ARE ESCALATING INTO A CRISIS THAT COULD PUT THE DAYTON ACCORDS OF 1995, WHICH ENDED A SAVAGE WAR THAT KILLED MORE THAN 1... 2009.2.20 FALLING RE
ERS CONTAIN NEW AUSTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BUSHFIRES IN AUSTRALIA 2009.2.27 U.S., PAKISTAN AND AFGHANISTAN TO HOLD REGULAR TALKS: THE PLAN WA
OUNCED AFTER THREE DAYS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSTRIKES IN PAKISTAN, AND THE SCOPE OF THE AMER... 2009.2.27 DEBT TESTS CANADIAN ME
ISSIONS AFTER FIERCE PROTESTS AND A FAILED LEGAL CHALLENG... 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE SC
ESS TO PHOTOGRAPH THE FLAG-DRAPED COFFINS OF AMERICA 2009.2.27 U.S. HELPS PALESTINIANS BUILD FORCE FOR SECURITY: WITH AMERICAN HELP, GUARDSMEN IN THE WEST BANK ARE TRAI
ANCIAL CRISIS AND FALLING OIL PRICES WILL MAKE IT HARDER FOR IRAQ TO PAY FOR SERVICES AND COULD AFFECT U.S. PLANS FOR WITHDRAWAL. 2009.2.27 WORLD BRIEFING ASIA: KAZAKHSTA
ACING BANKRUPTCY. 2009.2.27 CHINA SAYS U.S. DISTORTS FACTS IN REPORT ON RIGHTS: THE STATE DEPARTMENT SEES 2009.2.27 PRO-SHARIF DEMONSTRATIONS SPREAD ACROSS PUNJAB: T
NEWSPAPER DURING A FUNERAL IN COLOMBO, THE CAPITAL, ACCUSING HIM OF AIDING A REBEL AIR ATTACK THERE... 2009.2.27 IRAQ HANDS DEATH PENALTY TO 28 CULTISTS FOR ATTACKS: A MES
I MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN $11 MILLION OF INTERNATIONAL DONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2009.2.27 PALESTINIAN RIVALS ANNOUNCE
A CIVILIAN TRIAL: THE CHARGES WOULD MOVE THE CASE OF THE ONLY ENEMY COMBATANT TO BE HELD ON U.S. SOIL, ALI SALEH KAHLAH AL-MARRI, INTO A CIVILIAN CRIMINAL COURT. 2009.2.27
S, DUTCH OFFICIALS SAID. 2009.2.27 MASS GRAVE FOUND IN BANGLADESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY
COPE OF THE HOLOCAUST WAS NOT SUFFICIENT. 2009.2.27 IN SOUTHEAST ASIA, THE UNEMPLOYED RETURN HOME: AS A MEETING OF THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS BEGINS, T
NITY CENTER IN CARACAS, BUT NOBODY WAS HURT IN THE BLAST. 2009.2.27 DEBT TESTS CANADIAN MEDIA COMPANY: CANWEST GLOBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON I
T, A COLOMBIAN POLITICIAN, IS DEPICTED AS SELFISH AND HAUGHTY IN A MEMOIR BY FELLOW HOSTAGES HELD WITH HER. 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT
F MODERN HUMANS. 2009.2.27 IRAQ HANDS DEATH PENALTY TO 28 CULTISTS FOR ATTACKS: A MESSIANIC SHIITE FRINGE GROUP HAS TAKEN AIM AT SHIITE PILGRIMS AND FOUGHT AMERICAN AND IR
09.2.27 BISHOP OFFERS APOLOGY FOR HOLOCAUST REMARKS: BISHOP RICHARD WILLIAMSON, WHOSE RECENT REHABILITATION BY POPE BENEDICT XVI PROVOKED GLOBAL OUTRAGE, HAS APOLOGIZE
BEGINS, THE REGION IS EXPECTING AN EXODUS OF WORKERS TO RETURN TO THE FAMILY FARM AS A RESU... 2009.2.27 CHINA FAILS TO HALT SALE OF LOOTED RELICS AT PARIS AUCTION: TWO BRI
.27 FIREFIGHTERS CONTAIN NEW AUSTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BUSHFIRES IN AUSTRALIA 2009.2.27 CHINA FAILS TO HALT SALE OF LOOTED RELICS AT PARIS AU
SU... 2009.2.27 U.S., PAKISTAN AND AFGHANISTAN TO HOLD REGULAR TALKS: THE PLAN WAS ANNOUNCED AFTER THREE DAYS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICA
IONS RISE IN FRAGILE BOSNIA AS COUNTRY: ANALYSTS SAY ETHNIC DIVISIONS ARE ESCALATING INTO A CRISIS THAT COULD PUT THE DAYTON ACCORDS OF 1995, WHICH ENDED A SAVAGE WAR THAT
DSMEN IN THE WEST BANK ARE TRAINING TO ENFORCE LAW AND ORDER. 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE
HER. 2009.2.27 WORLD BRIEFING AFRICA: MALAWI: FORMER PRESIDENT IS ARRESTED FORMER PRESIDENT BAKILI MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN $11 MILLION
MILAN MILUTINOVIC, WAS ACQUITTED. 2009.2.27 IRAQ WITHDRAWAL PLAN GAINS G.O.P. SUPPORT: PRESIDENT OBAMA IS TO ANNOUNCE THAT HE WOULD PULL COMBAT FORCES OUT BY AUGUST 20
IS DEPICTED AS SELFISH AND HAUGHTY IN A MEMOIR BY FELLOW HOSTAGES HELD WITH HER. 2009.2.27 MALBORK JOURNAL: FACING GERMAN SUFFERING, AND NOT LOOKING AWAY: THE DISCOVER
DS: VICTIMS: THE NINE PEOPLE WHO DIED WHEN A TURKISH AIRLINES JET CRASH-LANDED ON WEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID. 2009.2.27 PRO-SHARI
RI, INTO A CIVILIAN CRIMINAL COURT. 2009.2.27 DEBT TESTS CANADIAN MEDIA COMPANY: CANWEST GLOBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON ITS CRUSHING DEBT LOAD AND P
ERN FOOT IN PREHUMANS: FOSSIL FOOTPRINTS SHOW THAT AS EARLY AS 1.5 MILLION YEARS AGO AN ANCESTRAL SPECIES HAD ALREADY EVOLVED THE FEET AND WALKING GAIT OF MODERN HUMANS
THE FORMER SERB PRESIDENT, MILAN MILUTINOVIC, WAS ACQUITTED. 2009.2.27 PRINTS SHOW A MODERN FOOT IN PREHUMANS: FOSSIL FOOTPRINTS SHOW THAT AS EARLY AS 1.5 MILLION YEARS A
TO A CIVILIAN CRIMINAL COURT. 2009.2.27 MASS GRAVE FOUND IN BANGLADESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRI
.. 2009.2.27 DEBT TESTS CANADIAN MEDIA COMPANY: CANWEST GLOBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON ITS CRUSHING DEBT LOAD AND POSSIBLY FACING BANKRUPTCY. 200

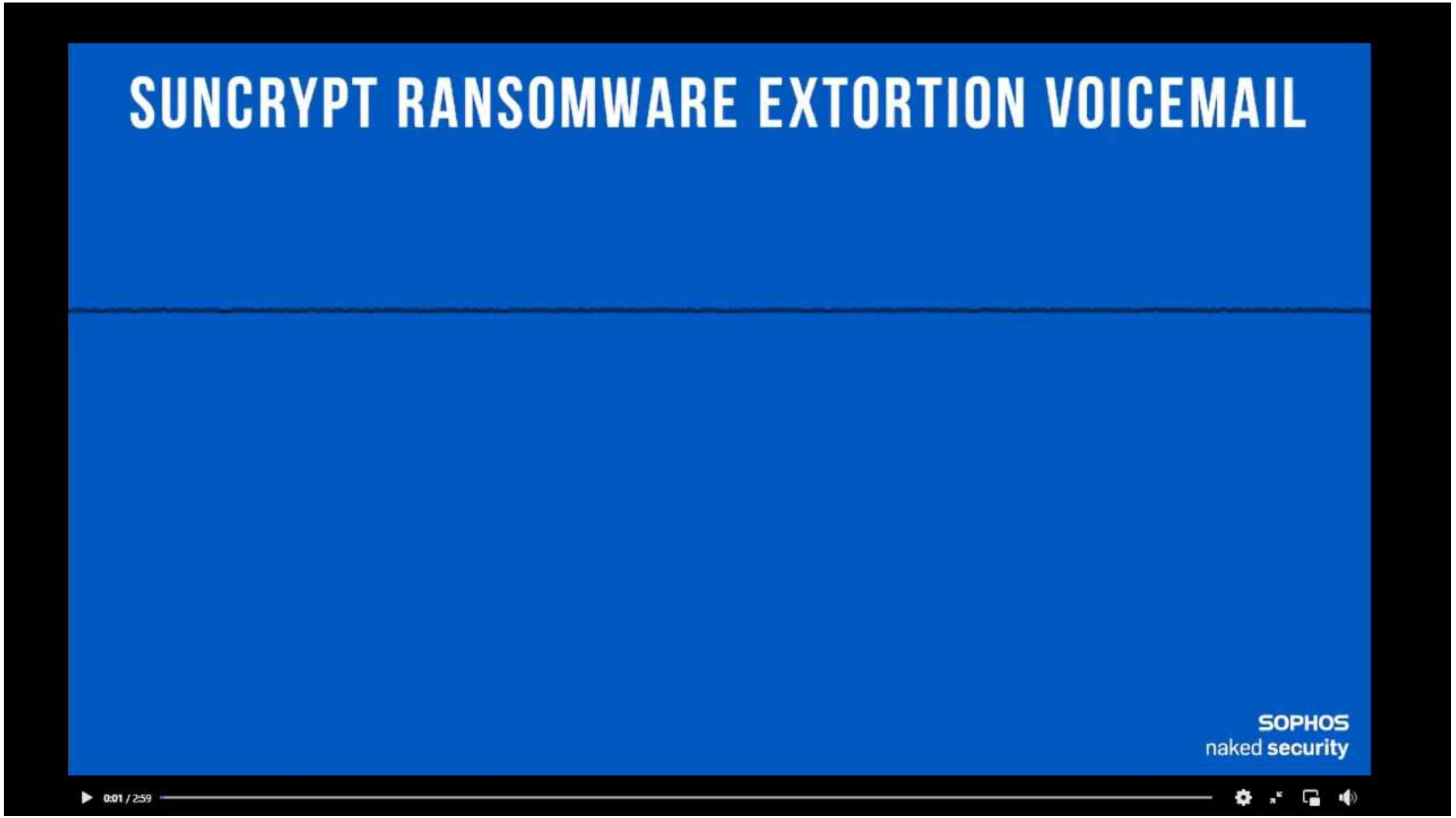


to quickly resolve the issues resulting from the attack was due to its cybersecurity protocols, redundant systems and

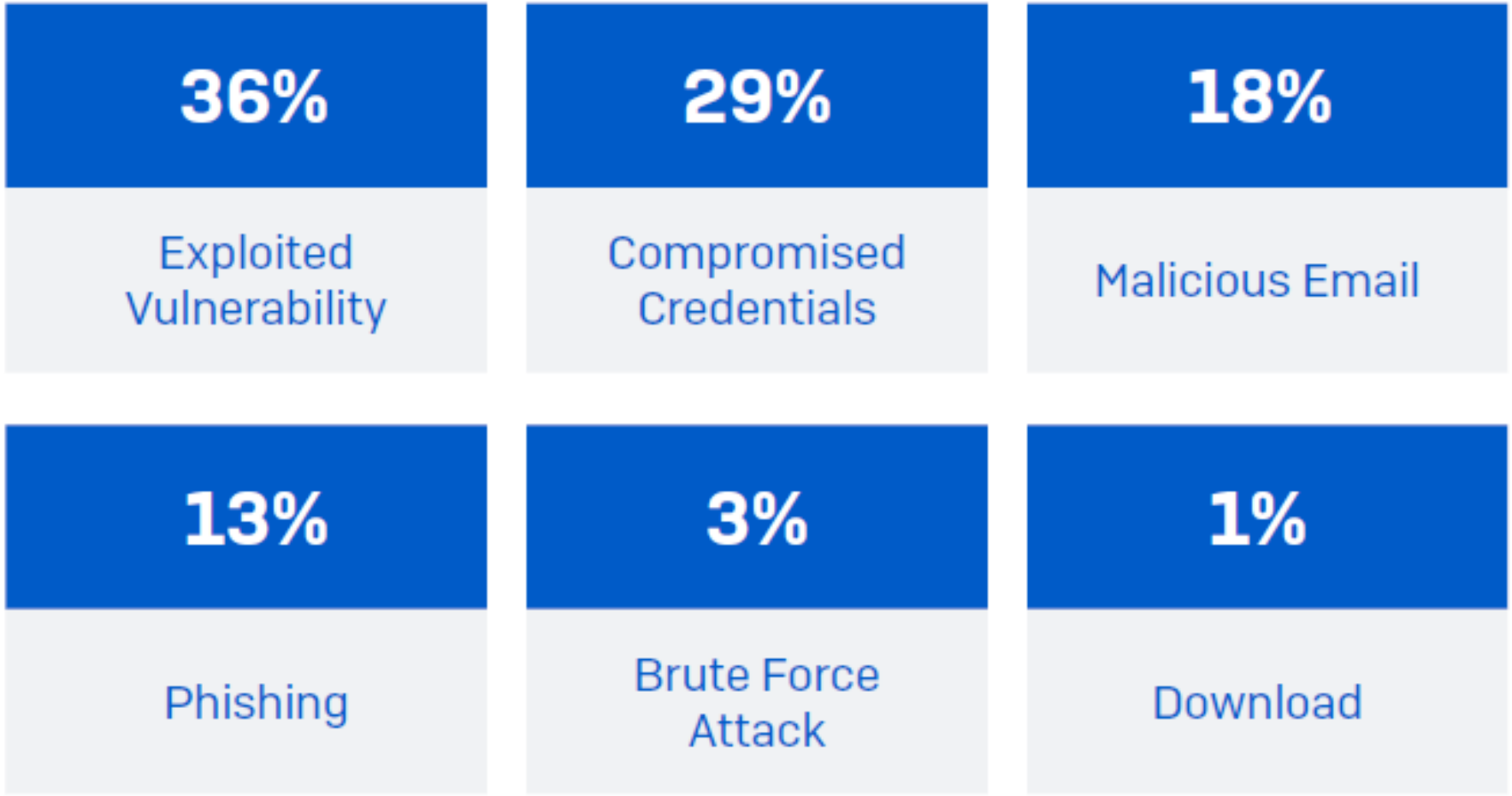
GRUPOS DE RANSOMWARE

Fonte: https://www.ransom-db.com/ransomware-groups em 01/10/2023

No.	Group Name	Description	Last Incident \ Victim	Victim Count	Last Seen	Icon
1	LockBit 3.0	Read more	palaciodosleiloes.com.br (2023-09-30-00:27)	2128	Online	
2	Conti	Read more	Alliance Steel (2022-06-07-19:37)	807	Offline	
3	Alphav (BlackCat)	Read more	Baumschlager Hutter Partners - Business Information (2023-07-16-17:41)	549	Online	
4	CL0P	Read more	SMWLLC.COM (2023-09-15-00:41)	514	Online	
5	Pysa (Mespinoza)	Read more	Chr Solutions (2021-12-06)	309	Offline	
6	BlackBasta	Read more	Raleigh Housing Authority (2023-08-21-14:08)	301	Online	
7	REvil Sodinokibi	Read more	kusd.edu (2022-11-28-21:39)	297	Offline	


SUNCRYPT RANSOMWARE EXTORTION VOICEMAIL
SOPHOS
naked security
0:01 / 2:59

UMA EXTORSÃO, DUAS EXTORSÕES, TRÊS EXTORSÕES...



THE STATE OF RANSOMWARE 2023

Fonte: Sophos.com

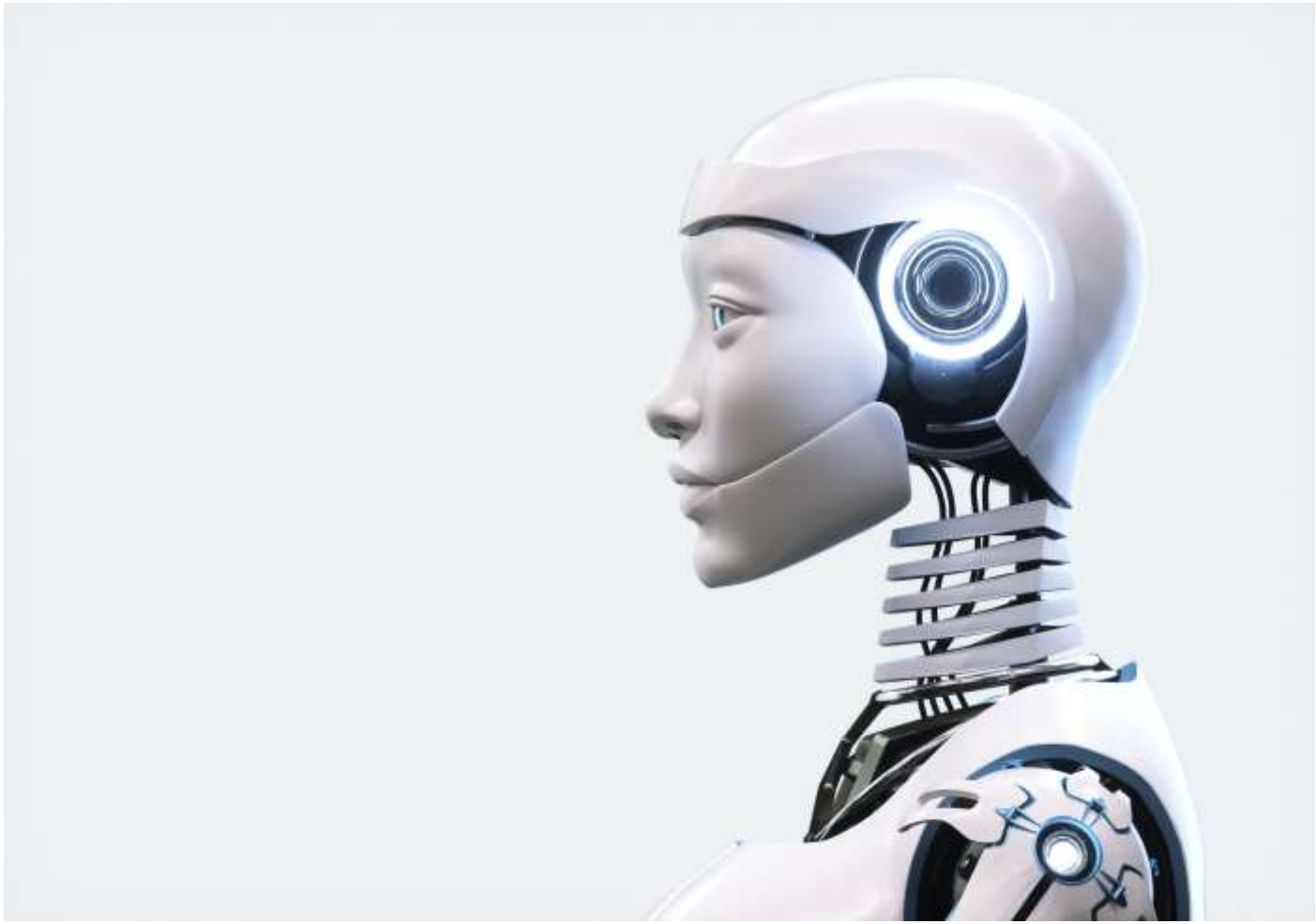
PREVENÇÃO (USUÁRIO)

- Conscientização
- Segurança de rede e de dispositivos
- Backup

PREVENÇÃO – CONSCIENTIZAÇÃO

- Observe e sempre fique atento a ataques de engenharia social
- Antes de clicar em um link curto: use complementos que permitam visualizar o link de destino
- Mensagens de conhecidos nem sempre são confiáveis
- Redes de Wi-Fi públicas são perigosas
- USB de origem duvidosa jamais deve ser utilizado/inserido no computador. Cuidado também onde conecta seu dispositivo

PREVENÇÃO – SEGURANÇA DE REDE E DE DISPOSITIVOS



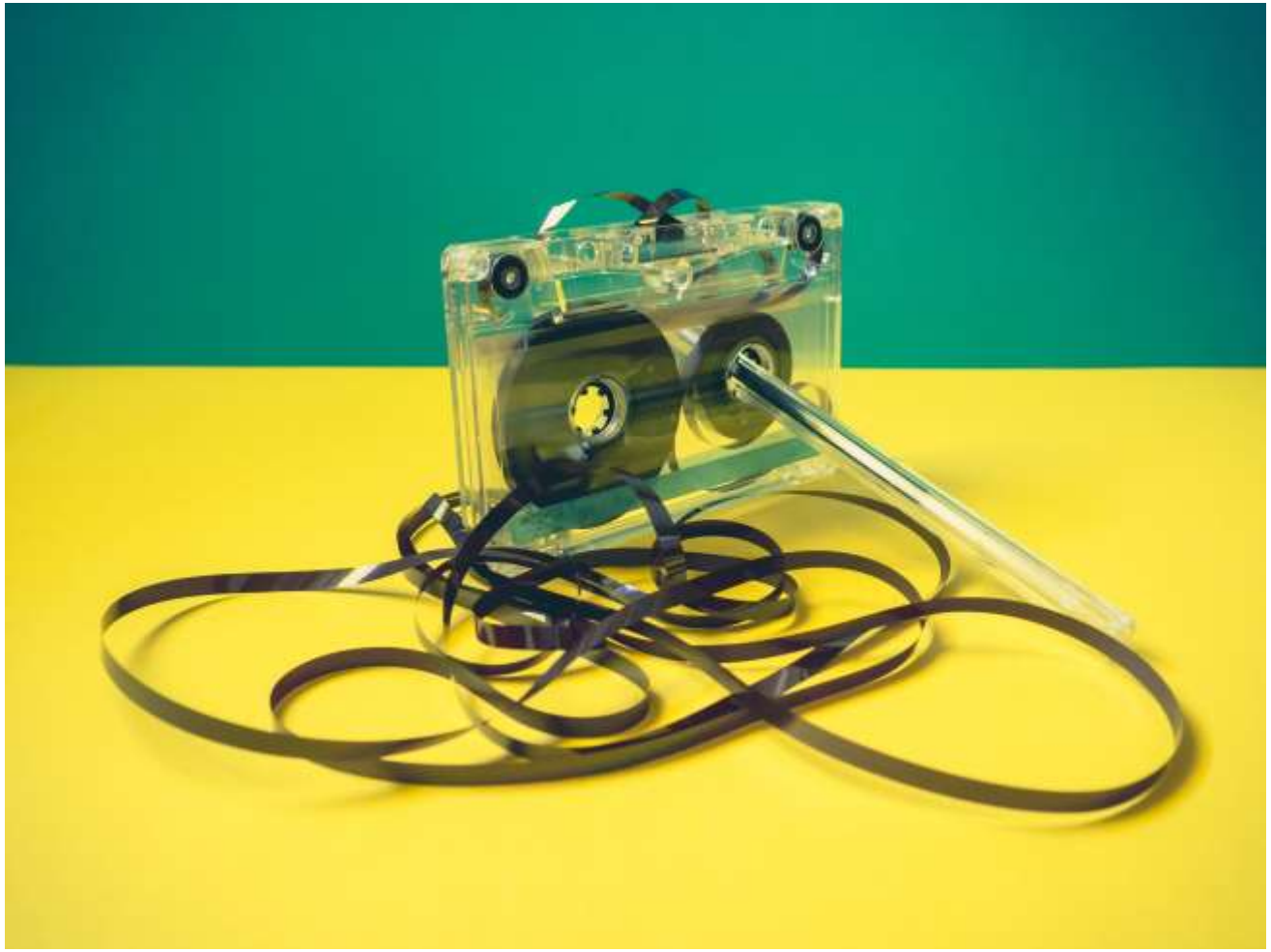
PREVENÇÃO – SEGURANÇA DE REDE E DE DISPOSITIVOS (1/2)

- Tenha sempre as versões mais recentes dos programas
- Remova os programas que não usa mais
- Configure a atualização automática dos programas:
- Cheque periodicamente por novas atualizações usando as opções disponíveis nos programas

PREVENÇÃO – SEGURANÇA DE REDE E DE DISPOSITIVOS (2/2)

- Use apenas programas originais
- Instale um antivírus (antimalware)
- Cuidado extra ao instalar aplicativos de terceiros
- Use a conta de administrador do sistema apenas quando necessário

PREVENÇÃO - BACKUP



PREVENÇÃO – BACKUP (1/2)

Mantenha os backups atualizados e em local seguro

Criptografe os dados sensíveis

Faça cópias redundantes com diferentes estratégias

PREVENÇÃO – BACKUP (2/2)

- Configure-os para serem realizados automaticamente
- Mantenha-os desconectados do seu sistema
- Teste-os periodicamente

E O FUTURO?

"O ransomware é um grande negócio, possibilitado por **redes inseguras** que permitem aos criminosos obter acesso às redes, em primeiro lugar, e por **criptomoedas** que permitem pagamentos que os governos não podem interditar. O ransomware tornou-se o modelo de negócio do crime cibernético mais lucrativo e, **até resolvermos esses dois problemas, isso não vai mudar**".
Bruce Schneier, maio de 2021

CONTATO

https://www.linkedin.com/in/caiado

http://dfir.com.br/