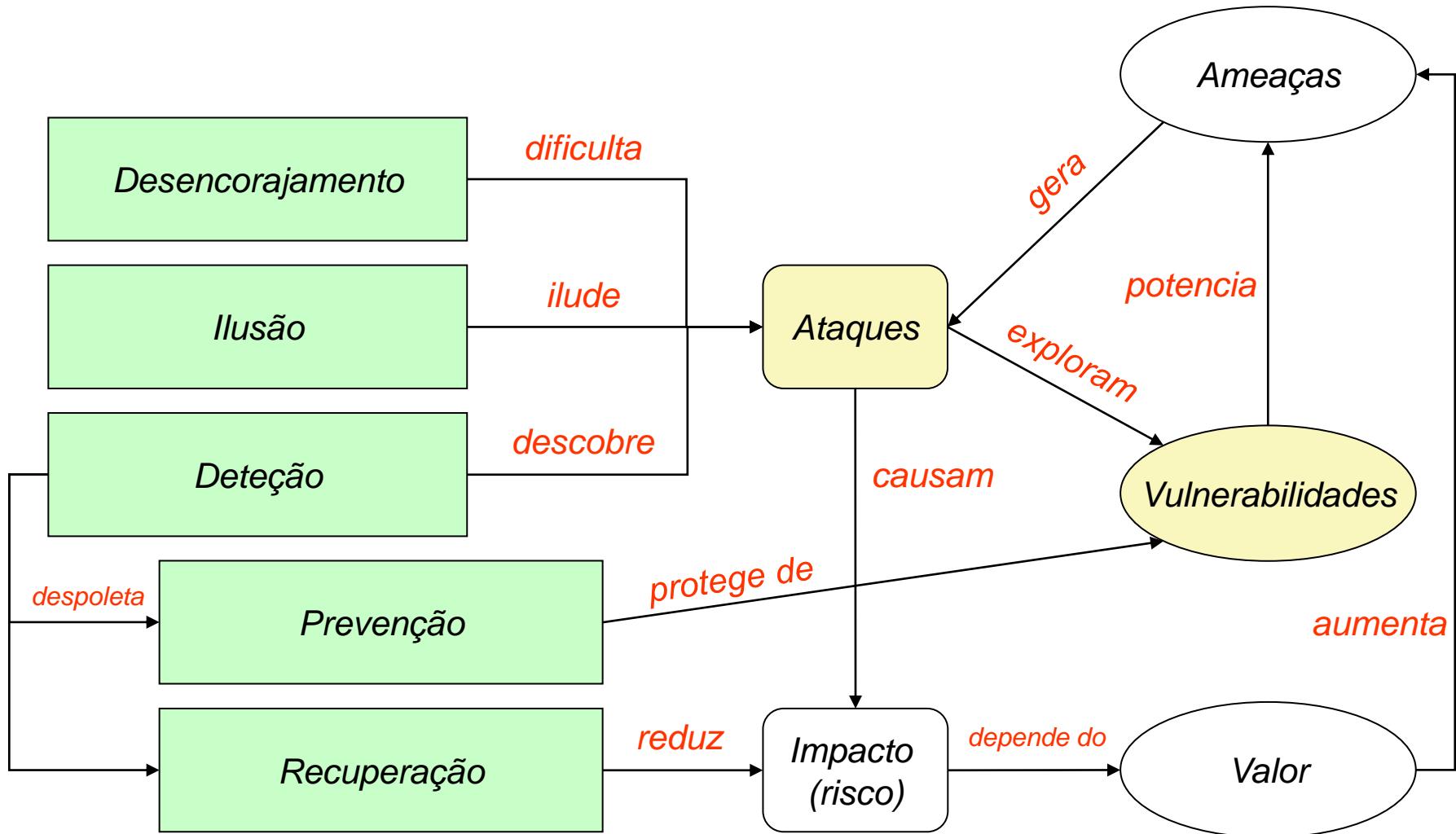


Vulnerabilidades

Segurança da Informação



Medidas (e algumas ferramentas)

*plat. formas m̄o seguras
asortas para aprender
com ataques*

• Desencorajamento

- Punição
 - Restrições legais
 - Provas forenses
- Barreiras de Segurança
 - Firewalls
 - Autenticação
 - Comunicação Segura
 - Sandboxing

• Deteção

- Sistemas de Deteção de Intrusões
 - ex: Snort, Zeek, Suricata
- Auditorias
- Análise Forense

• Ilusão

- Honeypots /Honeynets
- Acompanhamento Forense

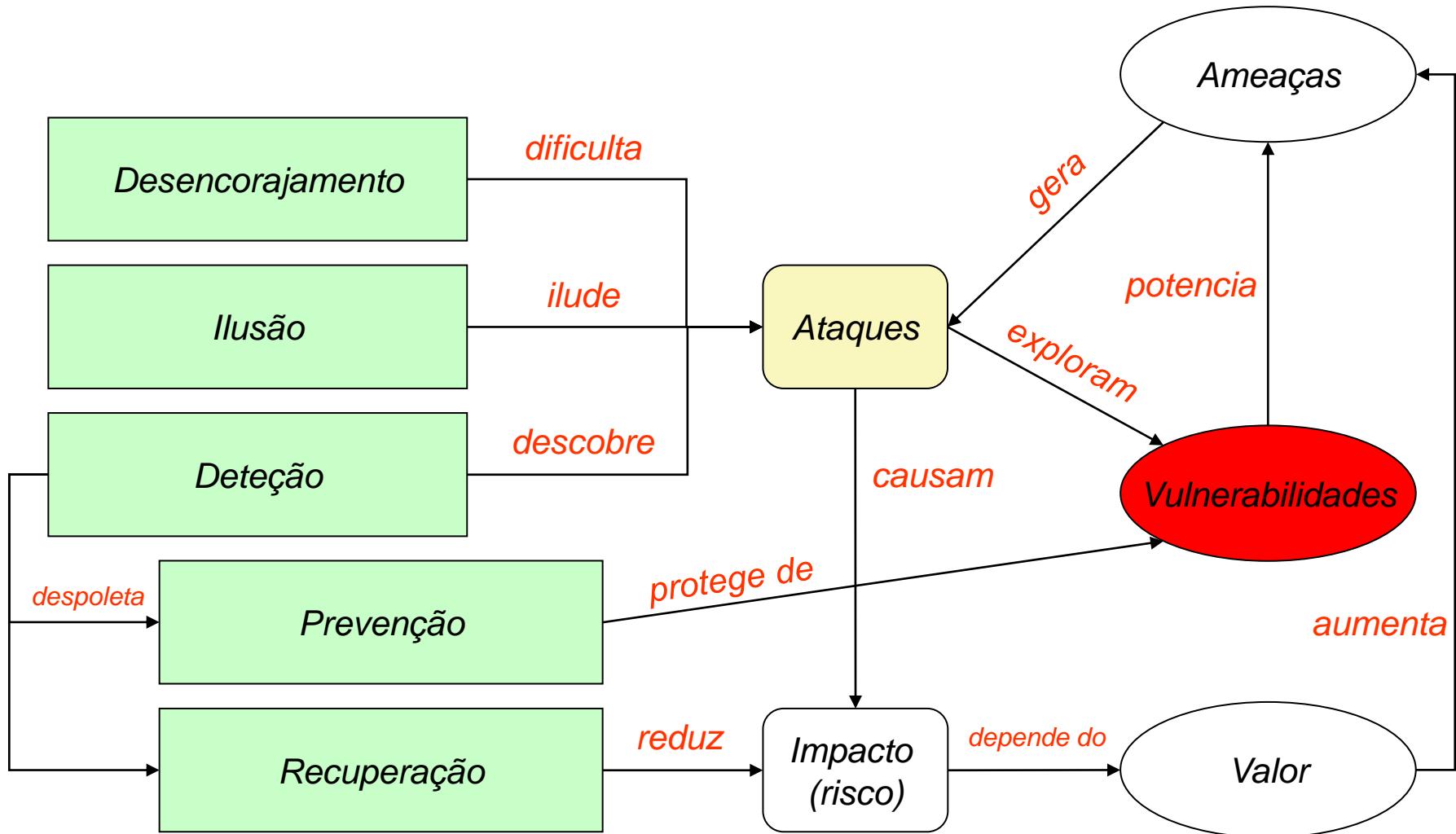
• Prevenção

- Políticas restritivas
 - ex: privilégio mínimo
- Deteção de vulnerabilidades
 - ex: OpenVAS, metasploit
- Correção de Vulnerabilidades
 - ex: atualizações regulares

• Recuperação

- Backups
- Sistemas redundantes
- Recuperação forense

Segurança da Informação



Vulnerabilidade

Erro no software que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede

- **Um erro só é uma vulnerabilidade se permitir que o atacante viole uma política de segurança**
 - Exclui políticas de segurança “abertas” onde todos os utentes são de confiança ou onde não se considera a existência de riscos para o sistema
- **Um vulnerabilidade é um estado de um sistema que permite:**
 - que um atacante execute comandos em nome de terceiros
 - que um atacante aceda a dados ultrapassando as restrições de acesso
 - que o atacante se apresente como outrem
 - que o atacante negue a prestação de serviços

Exposição

Problema de configuração de um sistema ou um erro no software que permitem aceder a informação ou capacidades que podem auxiliar um atacante

- **Não permite comprometer diretamente um Sistema/rede**
 - Mas é uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável
- **Uma exposição é um estado de um sistema que:**
 - permite que um atacante realize recolhas de informação
 - permite a um atacante esconder as suas atividades
 - Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
 - É um ponto de entrada comum para atacantes obterem acesso
 - É considerado problemático por uma política de segurança razoável

Prontidão (Security Readiness)

- **Medidas de Desencorajamento, Ilusão e Detecção** endereçam maioritariamente vulnerabilidades conhecidas
 - Tentativas de reconhecimento (ex: Port Scanning)
 - Ataques genéricos (ex: Interceção de redes)
 - Ataques específicos (ex: Buffer Overflows)
- **Medidas de Prevenção** endereçam vulnerabilidades conhecidas e desconhecidas
 - Vulnerabilidades genéricas
 - ex: reação a respostas mal formadas (protocol scrubbers)
 - ex: ataques furtivos (normalização para formatos canónicos)
 - Vulnerabilidades específicas
 - ex: erro de particular de software (testes e validação)

Prontidão (Security Readiness)

A aplicação das medidas requer conhecimento específico

- **Vulnerabilidades conhecidas**

- Problema, forma de exploração, impacto, etc.

source: [flickr](#)

- **Padrões de atividade dos ataques**

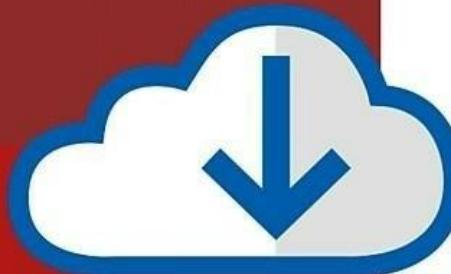
- Modus operandi
- Assinaturas de ataques

- **Padrões anormais de atividade**

- Anormal é o oposto de normal...
 - ... mas o que é que é normal?
- Difícil de definir em ambientes heterogéneos



1
DEVICE



1 Year Subscription
Abonnement d'un an

Includes Antivirus Security
Comprend la protection
antivirus

100%

GUARANTEE / GARANTIE
DE PROTECTION COMPLÈTE*

Viruses removed or your money back
Éradication des virus garantie ou argent remis

Always updated to the latest version
Une protection toujours dotée de la version la plus récente



Internet Connection Required
Connexion Internet requise

Prontidão (Security Readiness)

- As ameaças em redes de computadores são diferentes de outros tipos de ameaças
 - Os ataques podem ser lançados em qual hora, de qualquer local
 - Podem ser facilmente coordenados
 - Ex. Distributed Denial of Service attacks (DDoS)
 - Possuem um baixo custo de execução
 - Podem ser automatizados
 - São rápidos
- Portanto, requerem uma capacidade permanente (24x7) de reação a ataques:
 - Equipas de especialistas em segurança
 - Alertas de ataque na hora
 - Teste e avaliação dos níveis de segurança existentes
 - Procedimentos de reação expeditos

CVE: Common Vulnerabilities and Exposures

- **Dicionário público de vulnerabilidades e exposições**
 - Para gestão de vulnerabilidades
 - Para gestão de correções (patches)
 - Para alarmística de vulnerabilidades
 - Para deteção de intrusões
- **Utiliza identificadores comuns para um mesmo CVE**
 - Permite a troca de informações entre produtos de segurança
 - Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços
- **Detalhes de um CVE podem ser privados**
 - Parte do processo de divulgação responsável: **espera-se que o fornecedor crie uma correção**

CVE-ID**CVE-2015-1538**[Learn more at National Vulnerability Database \(NVD\)](#)[• CVSS Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#) • [CPE Information](#)**Description**

Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:76052
- [URL:http://www.securityfocus.com/bid/76052](http://www.securityfocus.com/bid/76052)
- [CONFIRM:http://www.huawei.com/en/psirt/security-advisories/hw-448928](http://www.huawei.com/en/psirt/security-advisories/hw-448928)
- [CONFIRM:http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm](http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm)
- [CONFIRM:https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398](https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398)
- EXPLOIT-DB:38124
- [URL:https://www.exploit-db.com/exploits/38124/](https://www.exploit-db.com/exploits/38124/)
- [MISC:http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html](http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html)
- MLIST:[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)
- [URL:https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fl6RQM/yzJvoTVrIQAJ](https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fl6RQM/yzJvoTVrIQAJ)
- SECTRACK:1033094
- [URL:http://www.securitytracker.com/id/1033094](http://www.securitytracker.com/id/1033094)

Assigning CNA

MITRE Corporation

Date Entry Created**20150206**

Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)**Comments (Legacy)****Proposed (Legacy)**

N/A

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: You can also search by reference using the [CVE Reference Maps](#).**For More Information:** [CVE Request Web Form](#) (select "Other" from dropdown)

CVE: Identificadores

Aka CVE names, CVE numbers, CVE-IDs, or CVEs

- **Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List**
 - Estados possíveis: "candidate" ou "entry"
 - **Candidate:** sob revisão para inclusão na CVE List
 - **Entry:** aceite na CVE List
- **Formato**
 - Identificador numérico CVE (CVE-Ano-Índice)
 - Estado (candidate ou entry)
 - Descrição sumária da vulnerabilidade ou exposição
 - Referências para informação adicional

Benefícios dos CVEs

Fornece uma linguagem comum para referir problemas

- **Facilita a partilha de dados entre**
 - Sistemas de deteção de intrusões
 - Ferramentas de aferição
 - Bases de dados de vulnerabilidades
 - Investigadores
 - Equipas de resposta a incidentes
- **Permite melhorar as ferramentas de segurança**
 - Maior abrangência, facilidade de comparação, interoperabilidade
 - Sistemas de alarme e reporte
- **Fomenta a inovação**
 - Local primordial para discutir conteúdos críticos das BDs

CVEs e Ataques



- **Ataques podem usar várias vulnerabilidades**
 - Um CVE para cada vulnerabilidade em todos os sistemas
- **Exemplo: Stagefright (Android, video em mensagens MMS)**
 - CVE-2015-1538, P0006, Google Stagefright 'stsc' MP4 Atom Integer Overflow Remote Code Execution
 - CVE-2015-1538, P0004, Google Stagefright 'ctts' MP4 Atom Integer Overflow Remote Code Execution
 - CVE-2015-1538, P0004, Google Stagefright 'stts' MP4 Atom Integer Overflow Remote Code Execution
 - CVE-2015-1538, P0004, Google Stagefright 'stss' MP4 Atom Integer Overflow Remote Code Execution
 - CVE-2015-1539, P0007, Google Stagefright 'esds' MP4 Atom Integer Underflow Remote Code Execution
 - CVE-2015-3827, P0008, Google Stagefright 'covr' MP4 Atom Integer Underflow Remote Code Execution
 - CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
 - CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
 - CVE-2015-3824, P0011, Google Stagefright 'tx3g' MP4 Atom Integer Overflow Remote Code Execution
 - CVE-2015-3829, P0012, Google Stagefright 'covr' MP4 Atom Integer Overflow Remote Code Execution

Deteção de Vulnerabilidades

- **Ferramentas podem detetar vulnerabilidades**
 - Exploram vulnerabilidades conhecidas
 - Testam padrões de vulnerabilidades
 - ex. buffer overflow, SQL injection, XSS, etc.
- **Ferramentas podem replicar ataques conhecidos**
 - Utilizam exploits conhecidos para vulnerabilidades conhecidas
 - ex: MS Samba v1 utilizado no WannaCry
 - Permitem implementar correções mais rapidamente
- **Vitais para aferir a robustez das aplicações e sistemas em operação**
 - Serviço frequentemente contratado

Deteção de Vulnerabilidades

- **Podem ser aplicadas a:**

- Código desenvolvido (análise estática)
 - OWASP LAPS+, RIPS, Veracode, ...
- Aplicação a executar (análise dinâmica)
 - Valgrind, Rational, AppScan, GCC, ...
- Externamente como um sistema remoto
 - OpenVAS, Metasploit, ...

- **Não devem ser aplicadas cegamente a sistemas em produção!**

- Potencial perda/corrupção de dados
- Potencial negação de serviço
- Potencial ato ilegal

CWE: Common Weakness Enumeration

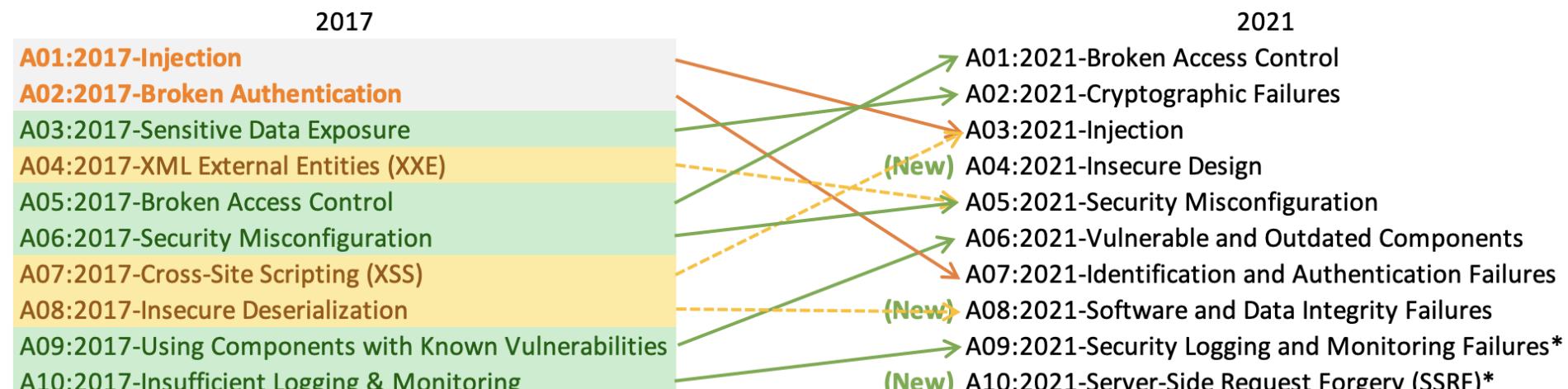
- Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança mais comuns
 - De programas, do seu desenho ou da arquitetura de sistemas
 - Cada CWE representa um tipo de vulnerabilidade
 - Gerida pela MITRE Corporation
 - Esta lista fornece uma definição pormenorizada de cada CWE
- Os CWEs são catalogados segundo uma estrutura hierárquica
 - CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidade
 - Podem ter vários CWEs filhos associados
 - CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
 - Com menos ou sem CWEs filhos

CWE != CVE

Vulnerability sources – OWASP Top 10 (Web)

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulns.
10. Insufficient logging and monitoring

Tipos de Vulnerabilidades – OWASP Top 10



CWE-348: Use of Less Trusted Source

The software has two different sources of the same data or information, but it uses the source that has less support for verification, is less trusted, or is less resistant to attack.

- Details at: <https://cwe.mitre.org/data/definitions/348.html>
 - Describes pattern, provides examples, provides list of related CVEs

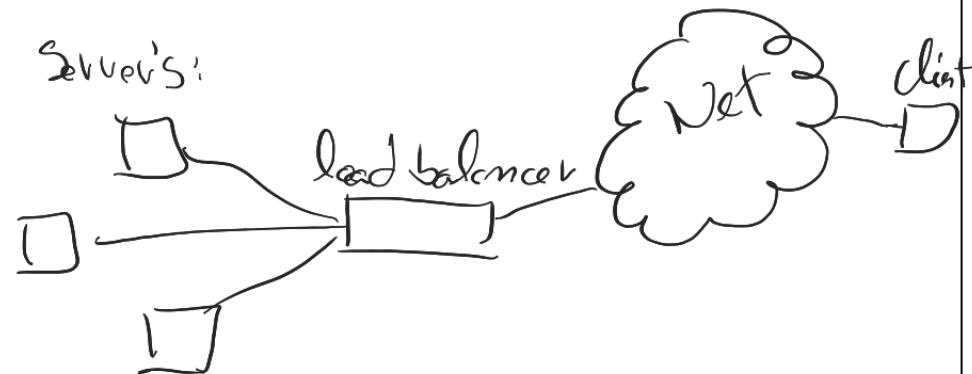
CWE-348: Use of Less Trusted Source

```
$requestingIP = '0.0.0.0';
if (array_key_exists('HTTP_X_FORWARDED_FOR', $_SERVER)) {
    $requestingIP = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else{
    $requestingIP = $_SERVER['REMOTE_ADDR'];
}

if(in_array($requestingIP,$ipAllowlist)){
    generatePage();
    return;
}
else{
    echo "You are not authorized to view this page";
}
```

Definido pelo servidor Web
Ou pelo cliente

Definido pelo servidor Web



Análise Estática (com Sonarcloud)

Reliability [Measures](#)

1.7k E

 Bugs ?

started 11 months ago

Security [Measures](#)

244 E

 Vulnerabilities ?

312

 Security Hotspots ?

Maintainability [Measures](#)

271d A

 Debt ?

15k

 Code Smells ?

Duplications [Measures](#)



3.2%

Duplications ?

2.5k

Duplicated Blocks ?

Análise Estática (com Sonarcloud)

The screenshot shows the SonarCloud interface displaying static analysis results for a WordPress plugin. The left sidebar contains navigation links for Status, Security Category (OWASP A...), SonarSource, OWASP Top 10 (A1 - INJECTION), SANS Top 25, and CWE, along with a search bar for CWEs. The main content area lists four issues found in different files:

- wp-admin/includes/plugin.php**:
 - Change this code to not use user-controlled data in include statements. [Why is this an issue?](#) (11 months ago, L1882, 0 tags)
 - Vulnerability: Blocker (Open, Not assigned, 30min effort, Comment)
- wp-admin/plugin-editor.php**:
 - Change this code to not construct the path from user-controlled data. [Why is this an issue?](#) (11 months ago, L71, 0 tags)
 - Vulnerability: Blocker (Open, Not assigned, 30min effort, Comment)
- wp-content/plugins/wpDiscuz/options/class.WpdiscuzOptions.php**:
 - Change this code to not construct the path from user-controlled data. [Why is this an issue?](#) (11 months ago, L353, 0 tags)
 - Vulnerability: Blocker (Open, Not assigned, 30min effort, Comment)
- wp-includes/functions.php**:
 - Change this code to not construct the path from user-controlled data. [Why is this an issue?](#) (11 months ago, L4838, 0 tags)
 - Vulnerability: Blocker (Open, Not assigned, 30min effort, Comment)

At the bottom, it says "4 of 4 shown".

Gestão de Vulnerabilidades

- **Durante o ciclo de desenvolvimento, como bugs**
 - Podem ser geridos por equipa de segurança ou de desenvolvimento
- **Quando o software é público, vulnerabilidades são geridas globalmente**
 - Para todos as aplicações disponíveis
- **Gestão pública permite um maior foco**
 - Discussão centrada numa aplicação específica
 - Ex: uma biblioteca específica, usada em vários sistemas
 - Admins podem rapidamente testar os seus sistemas, melhorando a segurança
 - ... Atacantes também ficam a saber melhor como atacar sistemas

Gestão de Vulnerabilidades

- Vulnerabilidades também são geridas de forma privada
 - Constituem arsenais para ataques a alvos no futuro
 - Códigos de ataque (Exploits) podem ser vistos como munições
- Conhecimento sobre exploits é comercializado
 - Preços de 0 a 2-3M€ (ou mais?) através de compras diretas
 - Ofertas públicas até 2.5M€ para programas de procura de erros (Google, Zerodium)
 - 2.5M€: 1 click Android exploit
 - 2M€: 1 click iPhone exploit
 - 1.5M€: WhatsApp ou iMessage exploit
 - ~2K por um XSS no HackerOne (existem regtos de \$1M de pagamento)
- ...e trocados de forma privada a preços desconhecidos
 - Companhias privadas, crime organizado, APTs...

CVE-2020-1472 @ MITRE

Informação Básica sobre o CVE

Refere outros trackers e páginas com informação

Páginas de fabricantes

Páginas de distribuições

Mailing lists

The screenshot shows a web browser displaying the MITRE CVE database. The URL in the address bar is cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472. The page header includes the CVE logo and navigation links for CVE List, CNAs, WGs, News & Blog, Board, and About. A sidebar on the right is titled "NVD" with links to CVSS Scores and CPE Info. The main content area shows the details for CVE-2020-1472, including its ID, a brief description of the vulnerability (an elevation of privilege), and a list of references from various sources like CERT, Synology, and Microsoft.

CVE-ID
CVE-2020-1472 [Learn more at National Vulnerability Database \(NVD\)](#)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CERT-VN:VU#490028
- [URL:https://www.kb.cert.org/vuls/id/490028](https://www.kb.cert.org/vuls/id/490028)
- CONFIRM:https://www.synology.com/security/advisory/Synology_SA_20_21
- MISC:<http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html>
- MISC:<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>
- URL:<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>
- MLIST:[oss-security] 20200917 Samba and CVE-2020-1472 ("Zerologon")
- URL:<http://www.openwall.com/lists/oss-security/2020/09/17/2>
- UBUNTU:USN-4510-1
- URL:<https://usn.ubuntu.com/4510-1/>
- UBUNTU:USN-4510-2
- URL:<https://usn.ubuntu.com/4510-2/>

CVE-2020-1472@NVD

Informação Básica sobre o CVE

Uma pequena análise

Uma pontuação de criticalidade (CVSS)

The CVE Severity Score

Ligações a outras páginas

NVD - CVE-2020-1472

nvd.nist.gov/vuln/detail/CVE-2020-1472#vulnCurrentDescriptionTitle

CVE-2020-1472 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

[View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD NIST: NVD Base Score: 10.0 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/H:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html	

QUICK INFO

CVE Dictionary Entry: CVE-2020-1472
NVD Published Date: 08/17/2020
NVD Last Modified: 09/21/2020
Source: MITRE

CVE-2020-1472 @ Microsoft (Vendor)

Mais detalhe sobre o problema, como aparece, como pode ser resolvido

Informação para staff sobre atualizações

Informação sobre a existência de exploits públicos

Cada fornecedor usa um formato próprio, com níveis de detalhe muito variados.

The screenshot shows a Microsoft Edge browser window displaying the security advisory for CVE-2020-1472. The URL is portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472. The page title is "CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability". It includes sections for "Security Vulnerability", "Published: 08/11/2020 | Last Updated : 08/11/2020", and "MITRE CVE-2020-1472". The main content describes the vulnerability as an elevation of privilege issue related to the Netlogon protocol. It mentions that Microsoft is addressing the vulnerability in a phased two-part rollout. A sidebar titled "On this page" lists links to "Executive Summary", "Exploitability Assessment", "Security Updates", "Mitigations", "Workarounds", "FAQ", "Acknowledgements", "Disclaimer", and "Revisions". At the bottom, there's a "Exploitability Assessment" section with a table comparing publicly disclosed information across different software releases.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

Security Updates CVSS Score

CVE-2020-1472 @ Em outros locais

**Profissionais (ou não)
criam provas de
conceito para explorar
o problema**

**Podem ser usados para
validar se um Sistema
é vulnerável**

**Comunidade ad-hoc e
muito dinâmica**

The screenshot shows a GitHub repository page for 'VoidSec/CVE-2020-1472: Exploit'. The repository has 4 stars, 97 forks, and 21 contributors. It contains 1 branch and 0 tags. The 'Code' tab is selected, showing a list of files: README.md, research/exploit, .gitignore, README.md, cve-2020-1472-exploit.py, nRPC.py, reinstall_original_pw.py, and requirements.txt. The README.md file contains the following content:

```
CVE-2020-1472

Checker & Exploit Code for CVE-2020-1472 aka Zerologon

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

NOTE: It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to
```

The repository also includes sections for About, Releases, Packages, and Languages.

Gestão de vulnerabilidades

- Tarefa não é simples
- Exploits nem sempre são conhecidos
- Impato e valor podem ser sub-estimados
- Informação antiga pode levar a um falso sentido de segurança
- Comunidade é muito dinâmica
 - Defensores que podem testar diretamente
 - Atacantes que podem incorporar vulnerabilidades

+View Analysis Description

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD NIST: NVD Base Score: 10.0 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A



CVE-2020-1472

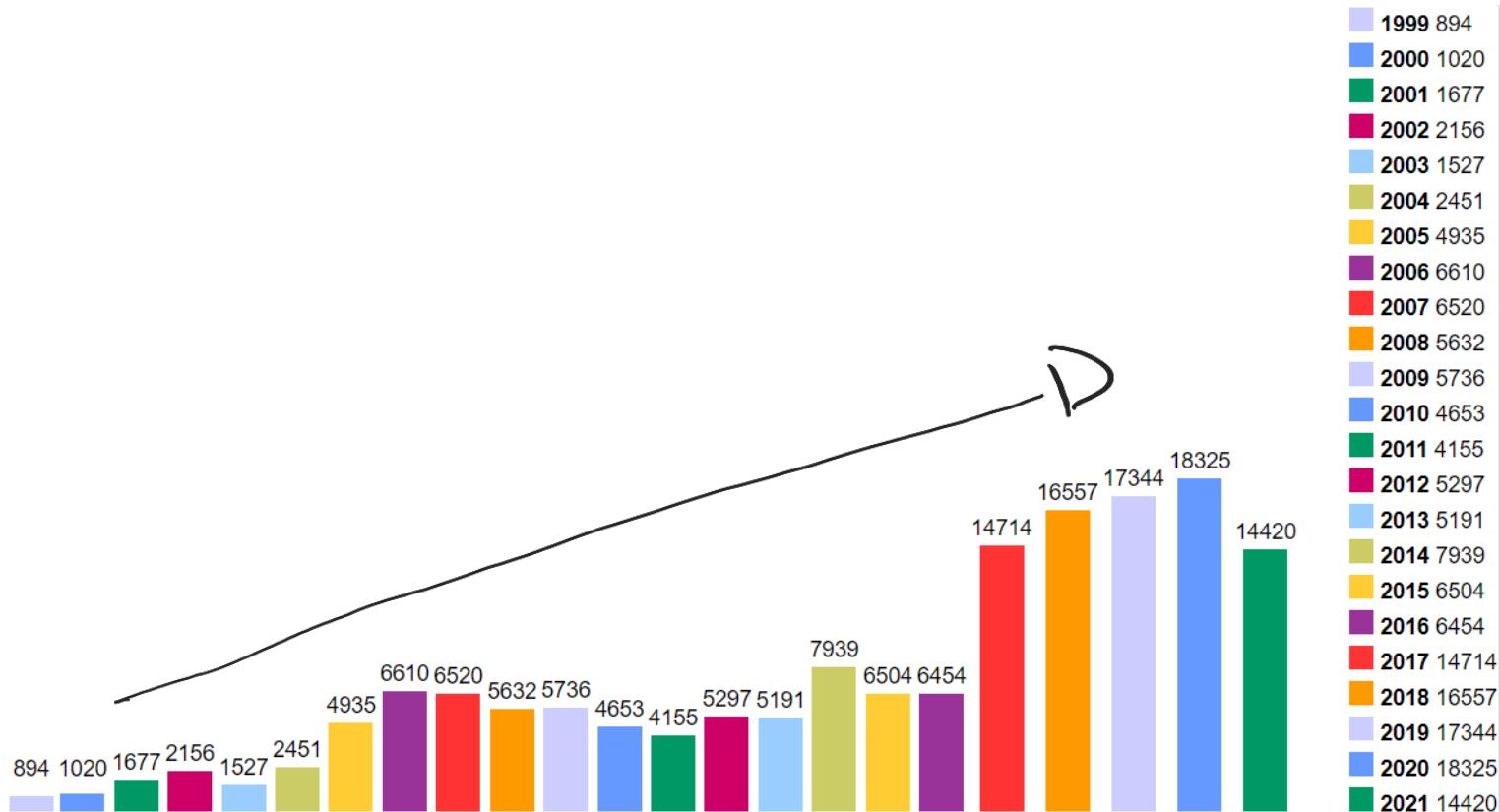
Checker & Exploit Code for CVE-2020-1472 aka Zerologon

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

NOTE: It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to



CVE por ano – cvedetails.com (as of Sep 2021)



Ataques de dia Zero (0 day)

- Ataque que usa vulnerabilidades que são
 - Desconhecidas de terceiros
 - Não comunicadas ao fornecedor de software
- Ocorre no dia zero do conhecimento dessas vulnerabilidades
 - Para as quais não existe correção (ou não está aplicada)
- Um ataque “0 day” pode existir por meses/anos
 - Conhecido para atacantes mas não para utilizadores
 - Parte frequente de arsenais de ataques informáticos
 - Comercializados em mercados específicos

ShadowBrokers

- **Background:** Atores estatais possuem arsenal para explorar vulnerabilidades desconhecidas do público
 - Parte integrante das suas atividades, por muitos anos e nunca reveladas
- **Agosto 2016:** Shadowbrokers publicam um grande quantidade de ferramentas deste atores
 - Usando canais públicos: Twitter, Github, PasteBin, Medium
 - Apresentam outras ferramentas: fazem um leilão, fazem uma venda de Black Friday, etc...
 - Objetivo: vender ferramentas que exploram 0 days a quem pagar mais
- **Março 2017:** Microsoft lança atualizações para várias versões de Windows
 - mas não lança para o W7, W8, XP e Server 2003
 - poderá ter existido dica de investigadores ou atores estatais
 - gravidade da atualização não é realçada

ShadowBrokers

- **Abril 2017: ETERNALBLUE libertada ao público num dos pacotes**
 - Explora vulnerabilidade no MS Windows SMB v1 (Remote Code Execution)
- **Maio 2017: WannaCry ransomware**
 - Utiliza 2 exploits libertados pelos SB (ETERNALBLUE é o 1º)
 - Impacto: Cifra ficheiros, afeta > 300K dispositivos
 - Pede resgate de \$300-\$600 para obtenção da chave de decifra
- **Maio 2017: EternalRocks ransomware**
 - Utiliza 7 exploits libertados pelos SB (ETERNALBLUE é o 1º)
 - Impacto: Pânico apenas. Autor desativa ataque
- **Junho 2017: NotPetya ransomware**
 - Variante que utiliza ETERNALBLUE e cifra ficheiros
 - Pede resgate de \$300 (mas não é possível decifrar ficheiros)
 - Alvo: Infraestruturas críticas, bancos, jornais na Ucrânia e Rússia (outros tb afetados)
 - Impacto: Ficheiros perdidos, >\$10B de danos

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
`1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX`
2. Send your Bitcoin wallet ID and personal installation key to e-mail: `womsmith123456@posteo.net`. Your personal installation key:
`X86GcZ-7PRNBE-3MNFMp-z88UnG-uF5nhF-4wzxwZ-XdNrr6-FYG89D-xk4rNz-9`



Sobrevivência

Como se sobrevive a uma ataque do dia zero?

Como se reage a uma ataque do dia zero massivo?

• Diversidade poderá ser uma solução ...

- Mas a produção, distribuição e atualização de software vai no sentido contrário!

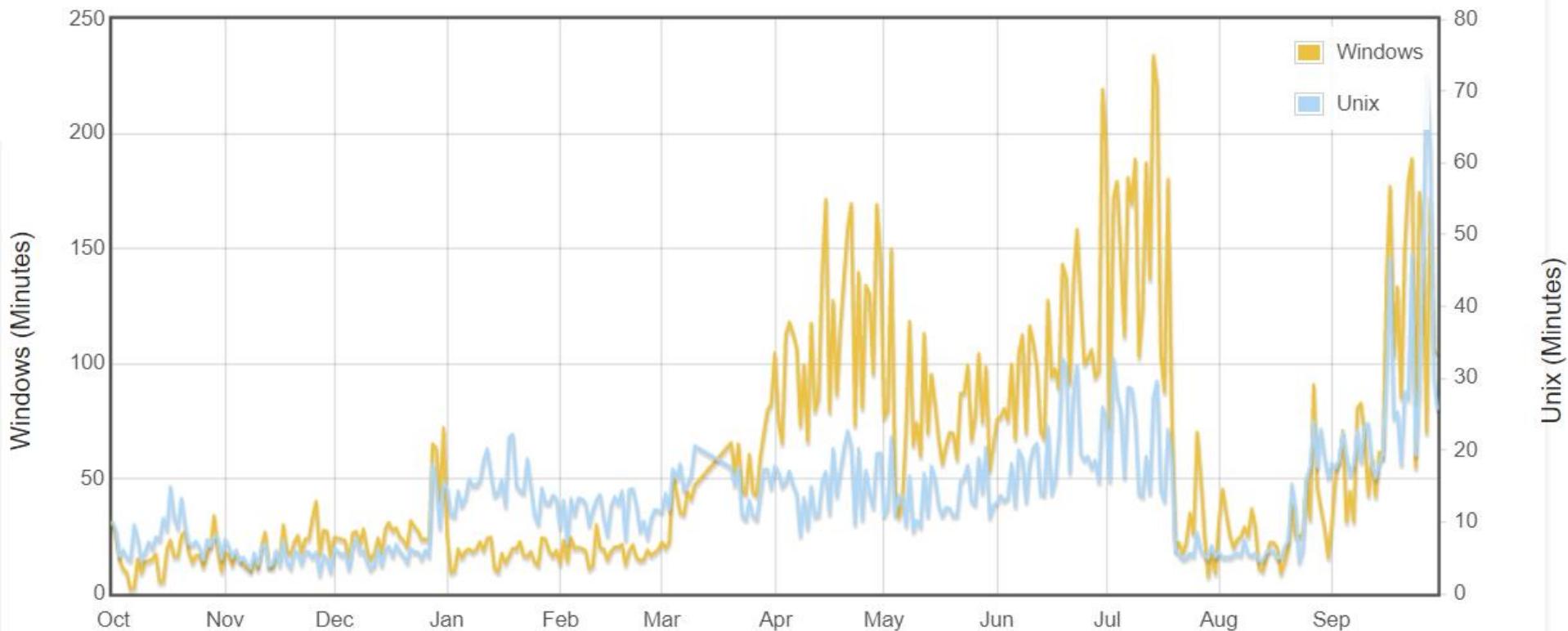
- E o mesmo acontece com as arquiteturas de hardware
- Porque é que o MS Windows é um alvo primordial?
 - E o MAC OS nem por isso? → Mais popular, mais alvos, mais profit
- Está a usar um telemóvel Android?
 - Qual é a probabilidade de estar na linha da frente das vítimas?
 - iOS pode ser pior, pois o ecossistema é ainda mais homogéneo

- Coordenação é um grande auxílio

Mean Survival Time

Oct 2020 – Oct 2021

(<http://isc.sans.org/survivaltime.html>)



- Um defensor tem de investir constantemente na segurança de um sistema
- Um atacante só necessita de ter sucesso uma vez em cada sistema
 - Atacantes podem tentar constantemente com ferramentas automáticas.

CERT: Computer Emergency Readiness Team

- Organização para garantir que as práticas de gestão de tecnologias e sistemas são usadas para:

- Resistir a ataques em sistemas distribuídos (em rede)
- Limitar o dano, garantir a continuidade de serviços críticos

- Mesmo considerando ataques realizados com sucesso, acidentes e falhas

*Sistemas separados fisicamente mas ligados
por rede, fornecendo mais uma linha de ataque*

- CERT/CC (Coordination Center) @ CMU

- Um componente do CERT Program
- Um hub para questões de segurança na Internet
 - Criado em Novembro 1988 depois do "Morris Worm"
 - Tem demonstrado a crescente exposição da Internet a ataques

CSIRT: Computer Security Incident Response Team

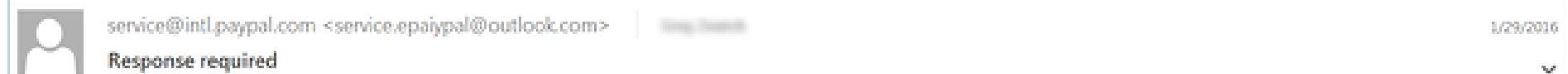
- **Organização responsável por receber, rever e responder a relatórios de incidentes e atividade**
 - Serviço 24/7 para usuários, companhia, agências governamentais e organizações
 - Ponto único de contato fiável e confiável para reportar incidentes de segurança à escala global
 - Meios para reportar incidentes e disseminar informação relativa a incidentes
- **CSIRTs Nacionais**
 - CERT.PT:
 - <https://www.facebook.com/CentroNacionalCibersegurancaPT>
 - National CSIRT Network
 - <https://www.redecsirt.pt>
 - CSIRT @ UA
 - <https://csirt.ua.pt>

Alertas de segurança & tendências de atividades

- **Vitais para a disseminação rápida de conhecimento sobre novas vulnerabilidades**
 - US-CERT Technical Cyber Security Alerts
 - US-CERT (non-technical) Cyber Security Alerts
 - SANS Internet Storm Center
 - Aka DShield (Defense Shield)
 - Microsoft Security Response Center
 - Cisco Security Center
- E muitos outros

Ataques Comuns: Phishing

- Criam réplicas de páginas/serviços
 - Imitam serviços fidedignos
 - URL tenta ser semelhante ao original
- Link enviado para vítimas através de email/SMS
 - Por vezes de computadores de colegas
 - Maior probabilidade da vítima confiar no serviço
- Objetivo
 - obter dados das vítimas
 - Senhas dos serviços
 - Números de cartões de crédito
 - obter dinheiro
 - levar vítima a instalar malware



 **Response required.**

Dear [REDACTED],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Ataques Comuns: Malware

- Infetam sistemas com código malicioso
 - Vírus: Necessitam de um hospedeiro (binário/documento)
 - Worm: Não necessita de um hospedeiro
 - Trojan: Disfarça-se de um programa benigno
- Operação
 - Vítima executa ficheiro infetado
 - Ou malware infeta sistema através de porto aberto
 - Vírus propaga-se para outros sistemas
 - Portos, documentos escritos, envio de emails
 - Malware pode tornar-se persistente
 - BIOS, Impressoras, outros suportes de armazenamento
 - Malware pode manter-se adormecido
 - Parte de uma infraestrutura de Comando e Controlo (C2)

Ataques comuns: Ransomware

- Têm como objetivo obter um pagamento por parte da vítima
- Operação
 - Executam código malicioso num computador
 - Código compromete CIA
 - C: Envia informação para um servidor remoto
 - I: Apaga/corrompe/cifra informação
 - A: Cifra informação
 - Atacante exige pagamento para:
 - Não divulgação de informação
 - Recuperação de informação (fornece chave de decifra)
 - Ou atacante utiliza diretamente informação
 - Cartões VISA, credenciais de páginas



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37



Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT+5 (Moscow, Paris, Berlin)

[About bitcoin](#)

[How to buy bitcoins?](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

[Copy](#)

[Contact Us](#)

[Check Payment](#)

[Decrypt](#)

Ataques comuns: keyloggers/spyware

- **Programa que regista eventos num sistema**
 - Teclas pressionadas
 - Capturas de ecrã
 - Imagens das webcam
- **Dados são enviados para sistema do atacante**
- **Objetivo:**
 - Extorsão (imagens capturadas)
 - Uso de informações obtidas
 - Passwords
 - Números de cartão de crédito

