Date :

| | | | Date: |
|---------------------------|--------------------|-------------------------------|-------------------------------|
| Androx gh Ost | Bothel | Sleals credentials prexploits | Regularly epolate software |
| | | volnorabilities | I web server |
| Lunna Stenler | Info Stealer | Steals credentials, | Use hardware vallets 1 |
| | | crypto currency mallety | avoid suspicious dominada |
| Clop Ronsomwore | Ransom were | Energpts data, demands | Use offlire backups |
| Argest August Sun A | w and the | vansom | apply patches |
| LOTE Cliving Of the Lord) | Fileles, Malvore | Vses built-in system | Resolved Powershell, disable |
| | | hols for attacles | wni |
| Naturalising. | Ad-borred Notwore | Insects systems via | Use ad-blockers, avoid |
| Larger of | Eukas The Lat | nulicious ads | pop-ups |
| BIG-Gome Ransonware | Pansomware | torgets large bryanization | Implement zero-trust security |
| | The second second | for runsom | policies |
| Enotet | Bonking Trajan | Steals banking credentials | Ereble At dor only booking |
| Jane 1 1 Sept Jak | a zanak | and here has | Do not open unknown affach. |
| Grootloader | Malvare Loader | Disdributes rensommare, | be cautions of search |
| | and the second | Trojans via date rebsites | engine results. |
| Dridex | Banking Trojan | Injects malicious ende | Enable MFA for online |
| | and and the second | into browsers | naw - se |
| A20 Rult | Info stealer | Stewl possmords | Regularly update subdence, |
| the warmen and the | 2,0,24 0,000 | emplo corrency walleds | ise antiviris |
| lad 10 | Banking Trojon | hjects malicious code | Do not stove passing. |
| | | into browsers | in brousers. |
| Redline Steuber | Indo shealer | Sheals credentials | Use two-factor |
| Hant turning | | crypto walled | cubhendiantion |
| Trick Bot | Nodular Trojan | Pourloady additional | Block known relicious |
| Comes made Silv. Lake | walted ass. | rature, steal evedentials | IPs, use security dools |
| Resphery Robin | Worm | Sprends via USB done | Pisable Autokun lor |
| 13/11/19 11/10 | The the | | USB Device. |
| | | | |

Date:

Joseph Huelende Virduero

BSIT III-B

INFOSEC

CHAPTER 2

MALWARE PPPLICATIONS

| the topic will be | | 1 1 = (40 00010) | 1919 St. 1917 C. |
|-----------------------|--|---------------------------------------|------------------------------------|
| No. 1 hi | Total de la companya | | |
| Name of Malmare | Dounloader, trojan | Type of Alfaile | Prévention & Protection |
| Fale Updates | Dounloader, Trojan | Installs majurare via | Avoid chicking pop-ups |
| " (Soc Gholish) | 13,750 11 11 11 11 11 11 11 11 | Sale update prompts | me antizvirus |
| Q bot (Qalebot) | Banking Trojan | Steals credentials, | A .) |
| and and and stu | The second of the second | logs, kendrokes | Avoid spam emails; |
| Form book | Indo stealer | Steals credentials, | 1 1 1 |
| A Company of the same | polisticand . | Scorend 1 1 1 | Use password manager, |
| Neno core | Permote Access | Screenshots, logs; keysholice | ovoid unknown darnload, |
| | Trojan | Enables remote control | Disable Office macros, |
| Async RAT | Pernote Access Trojan Pernote Access Trojan | melocan access | use firewalls |
| Joseph Control (4) | The process of the | Monitors Addivity | block melicious emails. |
| | , 24-800 (20-2) (6 upon) | downloads & executes | reep software updated |
| REN Cos | R I A | malvore | |
| | Renote Access Trojan | Gains high- here | Avoid enabling macros in |
| Phorpiex | College of the Colleg | priviliges via Offree Siles | Avoid enabling macros in documents |
| , rot | Botnet | Sends span enails, | 1/3 054 |
| p -1 | that the part are agreed | Spreads malvare | Scan USB Levicos, use email |
| Ramnif | Bonking Trojan | Steals banking credentials | second sitters. |
| N+o.1 | 120000 | l personal data | Use security banking looks, |
| MJPat | Renote Arcess Trajan | Captures key shokes | · Search . I I I I I |
| - 00 to 1000 | | accesse medicanis | Segment mediantes, black |
| Agort Tesla | Keylogger/Infostenter | Steals credardials | suspicious draffic. |
| Land on 191 | de la | 1 1 1 | Keep second softwore. |
| Vecro | Mobile Malvare | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | polared, use strong passmord, |
| | | Infects apps, displayis | Download apps from drusted |
| | | hidden ads | stores, enable Play Project |
| | | | |

| | Date. |
|--|-------|
| T. II II DI | |
| I Identil Nahrane Types | |
| *· · · · · · · · · · · · · · · · · · · | |
| 1. Mit Mo 6. Trojan Horse | |
| 2 Ransom Worl 7. Adware | |
| 3. Root kit 8. Bot | |
| 4 Spy work 9. Scareman | |
| 4. Spy work 9. Scaremani 5. Virus 10. Worm | |
| | |
| I. Idealy the Type of Address | |
| 1. DoS | |
| 2. PPoS | |
| 3. PDoS | |
| 4. DoS | |
| s. SEG Poisoning | |
| 6. Sto Possoring | |
| 7. PP05 | |
| 8. Dos, DPos | |
| 8. 1)62 / 34 | |
| I Identify Velneralility Terminology | |
| dentity () | |
| 1. Non- Validated Input - | |
| (i) n 1 | |
| h (1): | |
| | |
| | |
| 5. Access Confro Problems | |
| | |
| | |
| | |