## 2023-12-29 (FRIDAY): GOOTLOADER INFECTION

### CHAIN OF EVENTS:

- Fake forum post page --> link to zip download --> zip --> extracted .js file --> Gootloader C2

### EXAMPLE OF FAKE FORUM POST PAGE:

- hxxps[:]//www.repslagarna[.]se/2022/02/17/exhibit-vs-attachment-contract/

### LINK FOR ZIP DOWNLOAD FROM THE FAKE FORUM PAGE:

- hxxps[:]//v207[.]ru[.]is/blog.php

### ASSOCIATED MALWARE:

- SHA256 hash: 0ac828616de9d1bcedafe3dbdef9a82cd0fac24c8a3a79604ac42a9475d66ee3
- File size: 233,876 bytes
- File name: Exhibit_vs_attachment_contract_74334.zip
- File type: Zip archive data, at least v2.0 to extract, compression method=deflate
- File description: Malicious zip archive
- Timestamp for earliest contents modification: 2023-12-29 21:56 UTC
- Note 1: The above file was downloaded at 18:16 UTC, and modified timestamp is 3 hours ahead of the actual time.
- Note 2: Zip files downloaded from the blog.php URL are a different name and hash each time they are downloaded.

- SHA256 hash: b0b15f3b69612073e61442f0c93e14f98b01c16a64606bf2979997c77d8f83d5

- File size: 861,520 bytes
- File name: exhibit vs attachment contract 51002.js
- File type: Unicode text, UTF-8 text, with very long lines (414)
- File description: JavaScript file extracted from the above zip archive
- Any.Run analysis: https://app.any.run/tasks/3335dc86-981f-48ab-bf1f-26e465f83b97

- SHA256 hash: 718a5bd86508e1431f8921f2451ac3fc5c2c33897540f586676a639a9799fb12
- File size: 43,888,911 bytes
- File location: C:\Users\[username]\AppData\Roaming\[random existing directory]\Clinical Software.js
- File type: ASCII text, with very long lines (65536), with no line terminators
- File description: Persistent malware from this infection
- Persistence method: Scheduled task

POST-INFECTION TRAFFIC:

- hxxps[:]//diskodrugarputovanja[.]rs/xmlrpc.php
- hxxps[:]//elevencoffees[.]com/xmlrpc.php
- hxxps[:]//gambrick[.]com/xmlrpc.php
- hxxps[:]//instawp[.]io/xmlrpc.php
- hxxps[:]//lacomun[.]net/xmlrpc.php
- hxxps[:]//latesthentai[.]com/xmlrpc.php
- hxxps[:]//parubok-lesia[.]com/xmlrpc.php
- hxxps[:]//tattoo-mall[.]ru/xmlrpc.php
- hxxps[:]//wdtprs[.]com/xmlrpc.php
- hxxps[:]//yowieworld[.]com/xmlrpc.php