MintsLoader and a Glimpse Into the History of Scottish Protestantism

An Unusual Threat Hunting Opportunity

Simon Vernin (@Bongoknight)

orange Cyberdefense

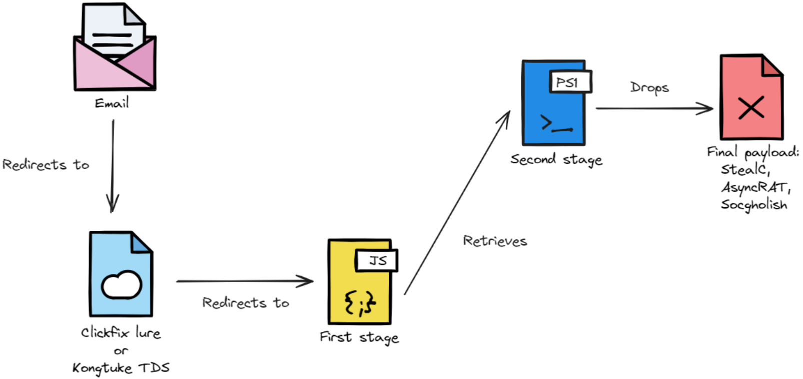
A Quick Overview: MintsLoader

- Two stages loader: JS then PowerShell, both obfuscated
- Documented by OCD, known to deliver BOINC, AsyncRAT, Vidar, SocGholish, StealC. . .
- After Kongtuke/ClickFix lures
- First samples seen in early 2023
- Use of a day-based DGA for C2 infrastructure

A Quick Overview: Infrastructure

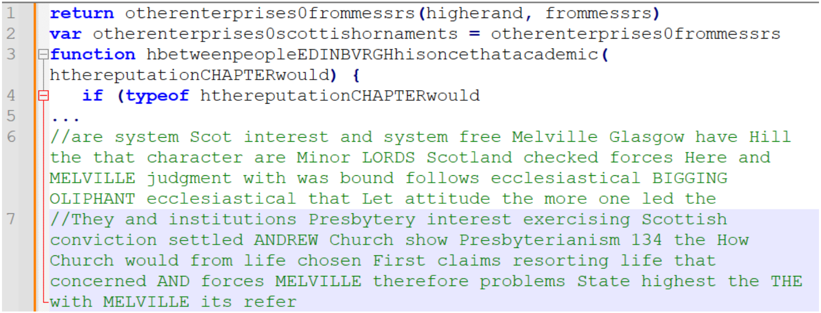
- URL pattern:
  - Initially detected by a campaign-specific pattern `?s=mints\d+`
  - Parameters seen include `boinc`,`flibabc\d+`,`5\d{2}` (around 15 campaigns ID)
- Domains resolution switched from **BL Networks** to **Stark Industry** since February 2025

A Quick Overview



Cyberdefense

JS Obfuscation: Example



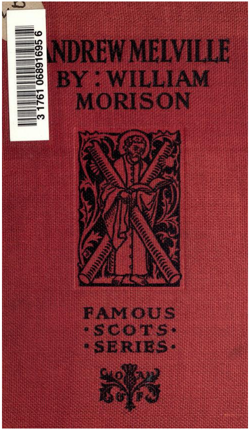
```
return otherenterprises0frommessrs(higherand, frommessrs)
var otherenterprises0scottishornaments = otherenterprises0frommessrs
function hbetweenpeopleEDINBVRGHhisoncethatacademic(hthereputationCHAPTERwould) {
   if (typeof hthereputationCHAPTERwould
...
//are system Scot interest and system free Melville Glasgow have Hill the that character are Minor LORDS Scotland checked forces Here and MELVILLE judgment with was bound follows ecclesiastical BIGGING OLIPHANT ecclesiastical that Let attitude the more one led the
//They and institutions Presbytery interest exercising Scottish conviction settled ANDREW Church show Presbyterianism 134 the How Church would from life chosen First claims resorting life that concerned AND forces MELVILLE therefore problems State highest the THE with MELVILLE its refer
```

Cyberdefense

JS Obfuscation: Some Questions?

- Why do so many words refer to church and Scotland?
- Why some words randomly capitalized?

JS Obfuscation: Some Answers



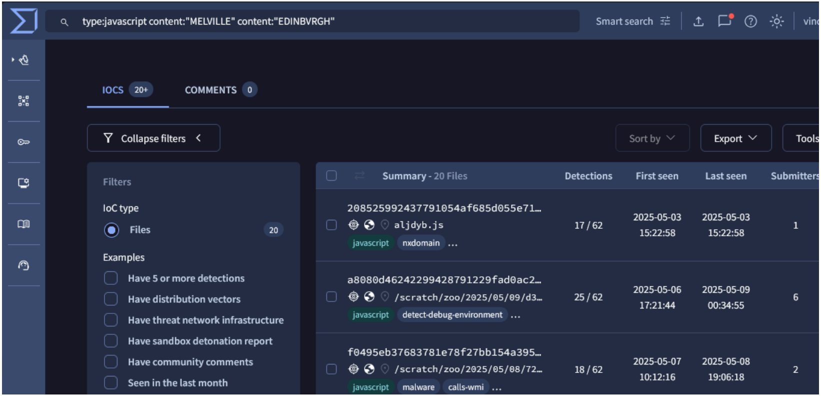
- All words in obfuscated code and attached comments appear in this book.
- UPPERCASE words are also UPPERCASE in this book.
- Chapter headings on each page make some UPPERCASE words more likely.

A bit of History

Quote : Wikipedia

Andrew Melville (1 August 1545 – 1622) was a Scottish scholar, theologian, poet and religious reformer. His fame encouraged scholars from the European continent to study at Glasgow and St. Andrews.

JS Obfuscation: VT as Ssual



type:javascript content:"MELVILLE" content:"EDINBVRGH"

Filters

IoC type

● Files 20

Examples

- □ Have 5 or more detections
- □ Have distribution vectors
- □ Have threat network infrastructure
- □ Have sandbox detonation report
- □ Have community comments
- □ Seen in the last month

Summary - 20 Files	Detections	First seen	Last seen	Submitters
208525992437791054af685d055e71… aljdyb.js javascript nxdomain …	17 / 62	2025-05-03 15:22:58	2025-05-03 15:22:58	1
a8080d46242299428791229fad0ac2… /scratch/zoo/2025/05/09/d3… javascript detect-debug-environment …	25 / 62	2025-05-06 17:21:44	2025-05-09 00:34:55	6
f0495eb37683781e78f27bb154a395… /scratch/zoo/2025/05/08/72… javascript malware calls-wmi …	18 / 62	2025-05-07 10:12:16	2025-05-08 19:06:18	2

A Recent Domain

- baredaseco.pro (Protected behind Cloudflare)
- Seen in the banner of 2.58.15.254
- When queried, this IP always redirects to a random unregistered domain of constant length

Similar IP?

```
user@user-virtualbox:~$ curl --verbose 2.58.15.254
< HTTP/1.1 302 Found
< Server: nginx/1.24.0 (Ubuntu)
< Date: Wed, 30 Apr 2025 21:03:32 GMT
< Content-Length: 0
< Connection: keep-alive
< Location: http://dymop1sgssxmcfi.org
<
* Connection #0 to host 2.58.15.254 left intact
```

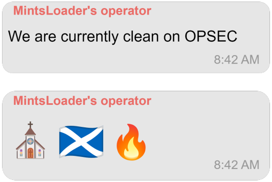
More IPs

IP	ASN	Country	AS Name
85.209.154.216	AS44477	GB	STARK-INDUSTRIES
94.131.120.29	AS44477	GB	STARK-INDUSTRIES
95.164.10.208	AS44477	GB	STARK-INDUSTRIES
95.164.16.184	AS44477	GB	STARK-INDUSTRIES
95.164.85.150	AS44477	GB	STARK-INDUSTRIES
213.159.64.103	AS44477	GB	STARK-INDUSTRIES
171.22.120.199	AS44477	GB	STARK-INDUSTRIES
104.194.222.166	AS22653	US	GLOBALCOMPASS
2.58.15.254	AS199959	AU	CROWNCLOUD
38.180.251.61	AS174	US	COGENT-174
38.244.163.166	AS174	US	COGENT-174
38.180.136.164	AS174	US	COGENT-174
38.180.136.192	AS174	US	COGENT-174
38.180.137.71	AS174	US	COGENT-174
38.180.242.197	AS174	US	COGENT-174
38.180.255.120	AS174	US	COGENT-174
38.180.255.122	AS174	US	COGENT-174

More Domains

- New IPs tend to be under AS174/COGENT (or AS58061/SCALAXY depending on AS source)
- These IPs resolve some recent MintsLoader domains:
  - `store` or `site` TLD
  - Contains hyphen
  - Some are tied to the known URL pattern `s=flibabc`

Key Takeaways



MintsLoader's operator

We are currently clean on OPSEC

8:42 AM

MintsLoader's operator

⛪ 🏴󠁧󠁢󠁳󠁣󠁴󠁿 🔥

8:42 AM

- MintsLoader JS payload is likely created with a custom obfuscator that takes Andrew Melville book text as input
- For now, infrastructure is a good way to track new MintsLoader payloads
- However, we have identified a fun hunting opportunity in case of infrastructure change