UnpacMe Weekly: New Version of IcedId Loader

blog.unpac.me/2023/05/03/unpacme-weekly-new-version-of-icedid-loader

Sean Wilson May 3, 2023

Sean Wilson

May 3, 2023

3 min read

Highlights

- Added support for newly observed version of IcedId Core Loader Fork and IcedId Loader Fork
- Nullmixer SEO search result poisoning delivering LegionLoader
- String search: Performance improvements and bug fixes

New Features

This week we continued work on improving our new string search feature. Based on your feedback and bug reports, we've made several improvements to the overall speed and stability of search. In addition to search we also pushed some changes to Yara Hunt to improve the overall scan performance of Yara scans.

Threat Spotlight: New IcedID Loader Fork

On April 30, 2023 we observed a new version of the previously forked *IcedID* loader and core loader. The initial fork of these components was detailed by Proofpoint in March 2023. This new fork contains some significant updates to both components.

Forked Loader Updates

- `b40076de066f06cfd29f43ae69d1e8c1627021a06bf2edff654626671acfb752`
- The loader configuration file is no longer encrypted using a simple XOR algorithm with a 64-byte key.
- The new load configuration file encryption algorithm is the same custom algorithm previously used by the *core loader* detailed in the mwcfg module icedid_peloader.py

Forked Core Loader Updates

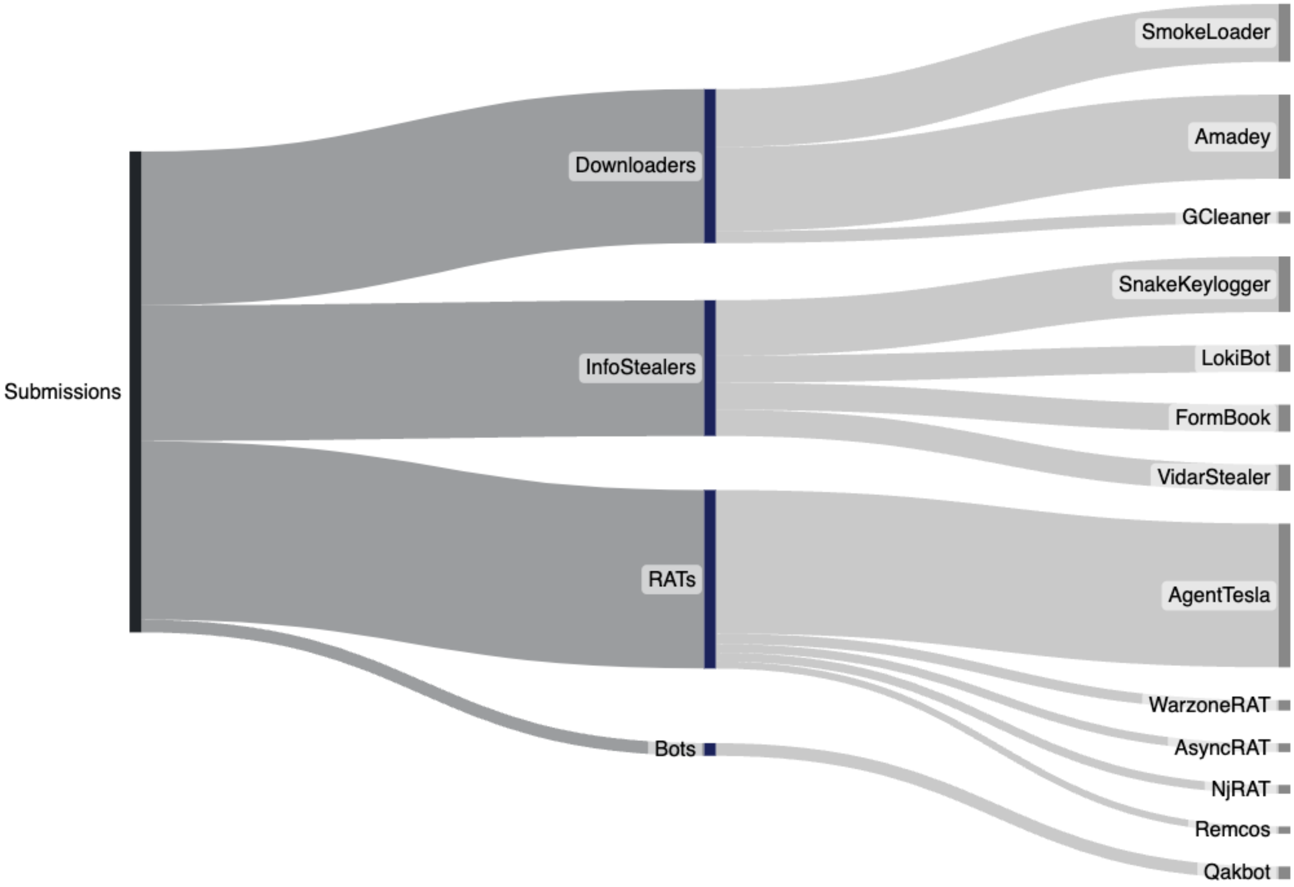
- `27483870f4df637c7532e41c61e2ee1b6734b28bf511855b68c61abad031c8c8`
- The *IcedID* bot is now embedded directly in the core loader instead of being delivered in a separate `.dat`file.
- With the bot embedded in the core loader the command line parameter `--tidu="license.dat"` is no longer required when launching loader.
- The embedded bot continues to use the same custom headerless “pe” format detailed by Malwarebytes in 2019.
- The bot "pe" sections are split between `.text` `.rdata` and `.data` sections in the core loader (one section in each).
- The core loader combines these disparate sections into a single blob of data which is then decrypted using XOR with a hard coded 32-byte ascii key `zzfersksximkogxswguwqvngtjkvvzjy`.
- The decrypted blob is then passed through the same custom decryption routine used by previous version of the core loader as detailed in the mwcfg module icedid_peloader.py
- Once decrypted the plaintext blob is then loaded into memory using the custom *IcedId* “pe” loader.
- The PDB path in the new core loader fork `E:\source\anubis\int-bot\x64\Release\int-bot.pdb` indicates that this new version is internally referred to as `int-bot`.

Weekly Threat Hunting

As in recent weeks, we continue to see an almost even distribution between *Downloaders*, *InfoStealers*, and *Remote Access Trojans (RATs)*. Analysis of the top user submitted files shows a near identical trend as last week with the top threats being *AgentTesla*, *Amadey*, SmokeLoader, and *SnakeKeylogger*. One notable change was an overall drop in submitted *FormBook* samples.

Continued analysis of .NET based malware families confirmed some of our suspicions last week regarding the use of XorStringsNET. We have been tracking samples from additional .NET malware families such as *RedLine Stealer* and *XWorm* leveraging the tool for an additional layer of obfuscation.

Over the past week, monitoring of the UnpacMe Threat Feed has corroborated our suspicions regarding the increase of AgentTesla samples. We are seeing that over 80% of submitted AgentTesla samples are using the XORStringsNET string encryption. We expect that over the next couple of weeks we will likely see an increase in several .NET malware families that leverage the tool, as it gains popularity among less-skilled threat actors.



Last Week's Top Submitted Threats

Threat Coverage

We've added and improved coverage for the following malware families.

- IcedId Fork(s) - A new fork of the previously forked *IcedId* first observed by ProofPoint in 2023. New versions of the forked loader and forked core loader were first observed by UnpacMe on April 30, 2023. This new fork contains significant changes from the previous version including a new custom decryption algorithm used by the core loader, and the inclusion of the bot in the core loader rather than deployed via separate `.dat` files. We have added a configuration extractors for both the forked loader and forked core loader.

- LegionLoader - LegionLoader (aka Satacom) a downloader and cryptocurrency stealer primarily distributed via the Nullmixer pay-per-install service. Nullmixer uses SEO to poison search results with high ranked links to their malware for common search terms such as "free pdfs" and "cracked software". We've added a new configuration extractor for LegionLoader to extract the command-and-control (C2) and encrypted strings.

As always, if you have any feedback or issues please let us know.

Happy Unpacking!