بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

شناسایی و تحلیل بدافزار Atomic macOS Stealer

گزارش بدافزار

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۴۰۲/۰۲/۱۹

طبقه‌بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ مقدمه

در سال‌های اخیر، macOS به طور فزاینده‌ای در بین کاربران محبوب شده‌است، که عمدتاً به دلیل رابط کاربرپسند آن است و اغلب به دلیل سادگی و سهولت استفاده مورد تحسین قرار می‌گیرد.

macOS همچنین ایمن‌تر از سایر سیستم عامل‌ها تلقی می‌شود. با وجود این، عوامل تهدید (TA) به هدف قرار دادن پلتفرم‌های macOS ادامه داده‌اند. پیش از این، موارد متعددی وجود داشته است که در آن عاملان تهدید کاربران macOS را با خانواده‌های مختلف بدافزار از جمله MacStealer، RustBucket، DazzleSpy و غیره هدف قرار داده‌اند.

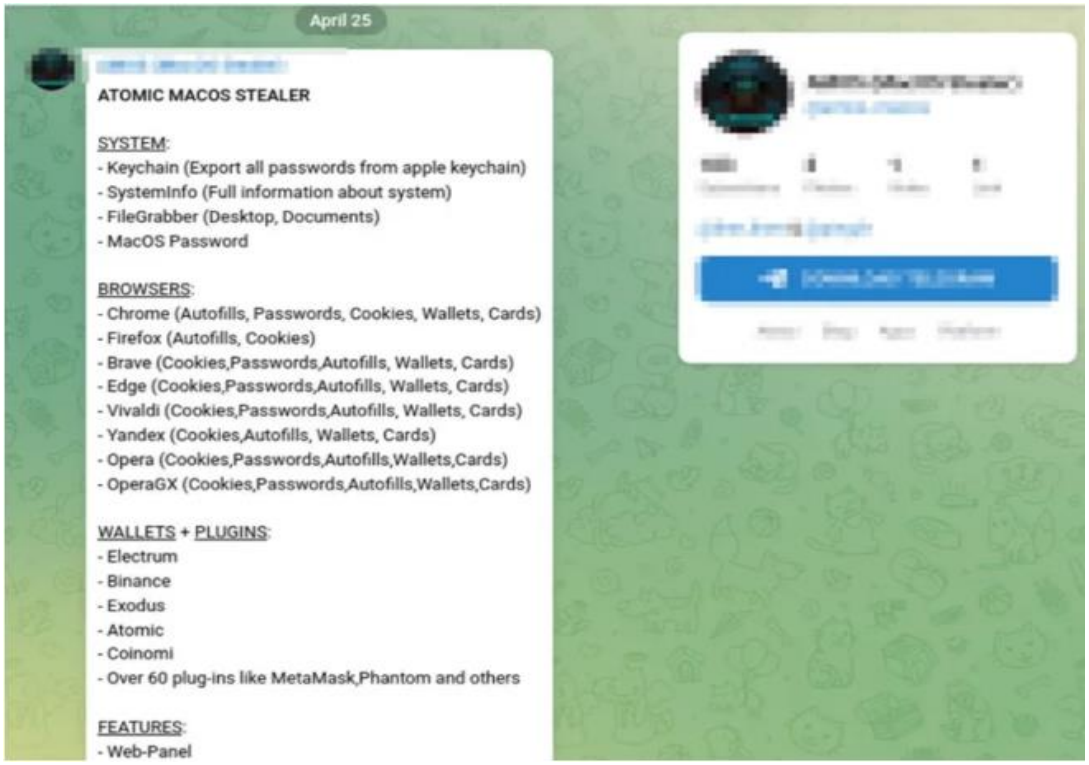
آزمایشگاه تحقیقات و اطلاعات Cyble (CRIL) اخیراً یک کانال تلگرامی را کشف کرده است که یک بدافزار جدید سرقت اطلاعات به نامAtomic macOS Stealer (AMOS) را تبلیغ می‌کند. این بدافزار به طور خاص برای هدف قرار دادن macOS طراحی شده و می‌تواند اطلاعات حساس را از دستگاه قربانی سرقت کند.

TA پشت این دزدی به طور مداوم در حال بهبود این بدافزار و اضافه کردن قابلیت‌های جدید برای موثرتر کردن آن است. آخرین به‌روزرسانی این بدافزار در پست تلگرامی در ۲۵ آوریل منتشر شد و آخرین ویژگی‌های آن را به نمایش گذاشت.

۲ جزئیات آسیب‌پذیری

Stealer می‌تواند انواع مختلفی از اطلاعات را از دستگاه قربانی سرقت کند، از جمله رمزهای عبور keychain، اطلاعات کامل سیستم، فایل‌های دسکتاپ و پوشه اسناد و حتی رمز عبور macOS. این بدافزار برای هدف قرار دادن چندین مرورگر طراحی شده و می‌تواند پر کردن خودکار (auto-fill)، رمز عبور، کوکی، کیف پول و اطلاعات کارت اعتباری را استخراج کند. به طور خاص، AMOS می‌تواند کیف پول‌های ارزدیجیتال مانند Electrum، Binance، Exodus، Atomic و Coinomi را هدف قرار دهد.

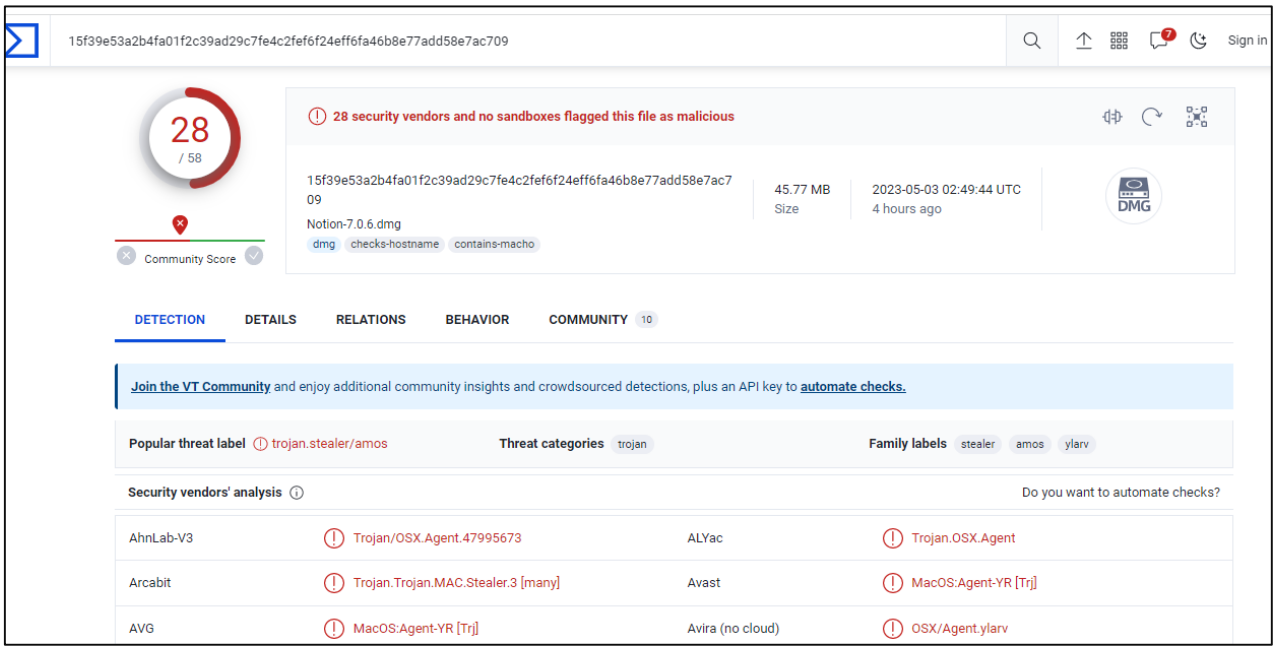
TA همچنین خدمات بیشتری مانند پنل وب برای مدیریت قربانیان، brute-forcing متاماسک برای سرقت seed و کلیدهای خصوصی، جستجوی رمزارز و نصب کننده dmg ارائه می‌دهد و پس از آن لاگ‌ها را از طریق تلگرام به اشتراک می‌گذارد. این خدمات با قیمت ۱۰۰۰ دلار در ماه ارائه می‌شود.



شکل ۱. پست تلگرام توسط توسعه دهنده بدافزار

برای تجزیه و تحلیل بدافزار، ابتدا نمونه هش (SHA256) «Setup.dmg» تحت عنوان *15f39e53a2b4fa01f2c39ad29c7fe4c2fef6f24eff6fa46b8e77add58e7ac709* رادر وبسایت Virustotal، بررسی کرده و نتایج آن به شرح زیر می‌باشند:

این بدافزار از نوع تروجان تشخیص داده‌شده و هدفش استخراج و سرقت اطلاعات بوده است. نام این بدافزار Notion-7.0.6.dmg می‌باشد.



شکل ۲. تشخیص بدافزار

خصوصیات اصلی این بدافزار که شامل درهم‌سازی با MD5، SHA-1، Vhash، SDEEP، TLSH، SHA-256 و نوع فایل از نوع Macintosh Disk Image می‌باشد. توسط ZLIB فشرده‌سازی شده و سایز فایل نیز به شرح زیر است:

Basic properties

MD5	5e0226adbe5d85852a6d0b1ce90b2308
SHA-1	0a87b12b2d12526c8ba287f0fb0b2f7b7e23ab4a
SHA-256	15f39e53a2b4fa01f2c39ad29c7fe4c2fef6f24eff6fa46b8e77add58e7ac709
Vhash	995b629b7e029614cd13ab0ae3aebb32
SSDEEP	786432:uX4XeQsZpv3x5Xvvz/yV9UOS5JBtkO+TaV+64JcQ9sZpv3x5Xvvz/yVB5JBtVO+/:uST2pv3xJvz/yV9UOS5JBmO+TgcN2pvY
TLSH	T1CEB733FDE9F35A16D5D54536EE14F9088F42445328970C29B2B7EBB7DA8AEB20170C8C
File type	Macintosh Disk Image
Magic	data
TrID	ZLIB compressed data (var. 4) (100%)
File size	45.77 MB (47995673 bytes)

شکل ۳. خصوصیات بدافزار

نام‌های شناسایی و ثبت‌شده برای این بدافزار به شرح زیر می‌باشند:

Names

Notion-7.0.6.dmg

Setup.dmg

شکل ۴. نام‌های بدافزار

فایل بررسی شده یک apple disk image می‌باشد که از فرمت جهانی dmg پیروی می‌کند. فایل اجرایی اصلی که با نصب dmg اجرا می‌شود، به شرح زیر می‌باشد:

Main Executable
/Setup.app/Contents/MacOS/My Go Application.app

شکل ۵. فایل اجرایی بدافزار

لیست مشخصات فایل سیستم به شرح زیر می‌باشد که شماره نسخه انتشاری ۱,۰ نسخه فعلی ساختار لیست اطلاعات ویژگی ۶,۰ آیکون موجود در فایلicon.icns می‌باشد.نام، نوع بسته نرم‌افزاری، شناسه منحصربه‌فرد بسته، نسخه و فایل اجرایی نیز به شرح زیر می‌باشند:

File System Property List	
CFBundleShortVersionString	1.0
CFBundleInfoDictionaryVersion	6.0
CFBundleIconFile	icon.icns
CFBundleGetInfoString	My Go Application by Appify by Machine Box
CFBundleIdentifier	Appify by Machine Box.My Go Application
CFBundleExecutable	MacOS/My Go Application.app
CFBundleName	My Go Application
CFBundlePackageType	APPL
CFBundleVersion	1.0

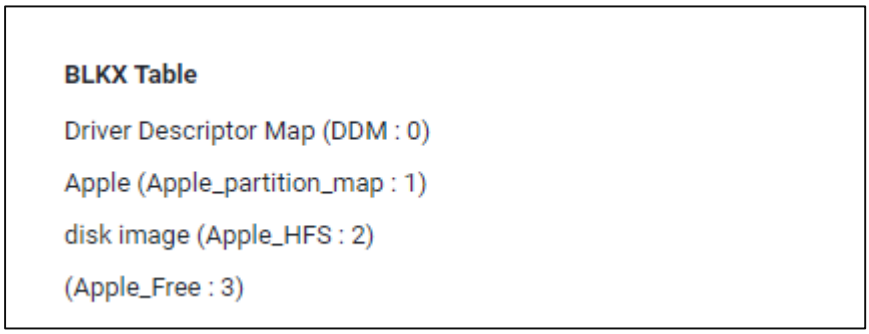
شکل ۶. لیست مشخصات بدافزار

ورودی‌های رمز نشده یافت‌شده در لیست خصوصیات dmg xml به شرح زیر است:

XML Property List Entries
ID:0

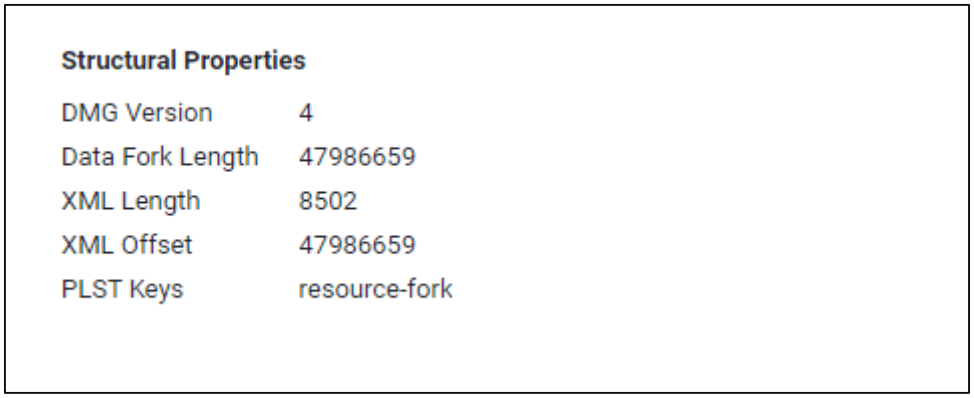
شکل ۷. ورودی‌های رمز نشده

جداول موجود در فایل dmg که توصیف‌کننده بلوک‌های داخلی آن هستند و اطلاعات بلوک‌ها به شرح زیر هستند:



شکل ۸. جداول موجود در dmg

خصوصیات بارز در خصوص ساختار ساخت بسته فایل dmg بررسی شده که شامل نسخه dmg، طول xml، آفست xml، Data Fork Length و plst keys هستند نیز به شرح زیر می‌باشد:



شکل ۹. خصوصیات ساختار بسته فایل dmg

این بدافزار با دامنه زیر ارتباط برقرار کرده و ip هایی که با این بدافزار contact شدند و مشخصاتشان به شرح زیر می‌باشند:

Domain	Detections	Created	Registrar
api.apple-cloudkit.com	0 / 87	2015-01-29	NOM-IQ Ltd dba Com Laude

Contacted IP addresses (15) ⓘ

IP	Detections	Autonomous System	Country
104.76.210.74	0 / 86	20940	US
17.248.186.139	0 / 86	714	US
17.248.186.142	0 / 86	714	US
17.248.186.165	0 / 86	714	US
17.248.186.166	0 / 86	714	US
17.248.186.167	0 / 86	714	US
17.248.186.200	0 / 88	714	US
17.248.186.203	0 / 86	714	US
17.248.186.9	0 / 87	714	US
23.203.100.224	0 / 86	16625	US

شکل۱۰. Ip های contact شده با بدافزار و خصوصیاتشان

۷ فایل در فایل بررسی‌شده ذخیره شده که نام، نوعشان و سایز فایل‌ها و درهم‌سازی آن‌ها به صورت زیر می‌باشد:

Scanned	Detections	File type	Name
2023-05-02	27 / 59	Mach-O	/Setup.app/Contents/MacOS/My Go Application.app
SHA-256	2c63ba2b1a5131b80e567b7a1a93997a2de07ea20d0a8f5149701c67b832c097		
File Size	51.55 MB		
?	?	file	/.fseventsd/0000000022042707
SHA-256	e4ffeb48f6adf39107669c2ff0c4d1ff32b2481537911f9f3d04f77045146e40		
File Size	69 B		
?	?	file	/.fseventsd/00000000220426bf
SHA-256	0ddf14d6eb7486c4cba300cd88482cc77478a91297158222045902d881b55c9f		
File Size	202 B		
?	?	file	/.fseventsd/0000000022042394
SHA-256	700f1da93cf25b4f2444758085308106620342 73bfdd5794178111e3363a8f5f		
File Size	72 B		
?	?	file	/.fseventsd/00000000220426c0
SHA-256	8b4ca9a20b52eecd2cbe855c5b2497d739ae938cfdd1e4ec8a1b713efe050946		
File Size	72 B		
?	?	file	/.fseventsd/0000000022042393
SHA-256	04ca20ab57fc8dd8b8a00976f7eafa9a0f7e84c993e65164f2c5e1d4c219cc87		
File Size	194 B		
?	?	file	/.fseventsd/0000000022042708
SHA-256	59a4096d73005555245ddba995a45c53233610ffe10f5cb924a5e2ffbaf5a62e		
File Size	71 B		

شکل۱۱. فایل‌های ذخیره شده در فایل بررسی

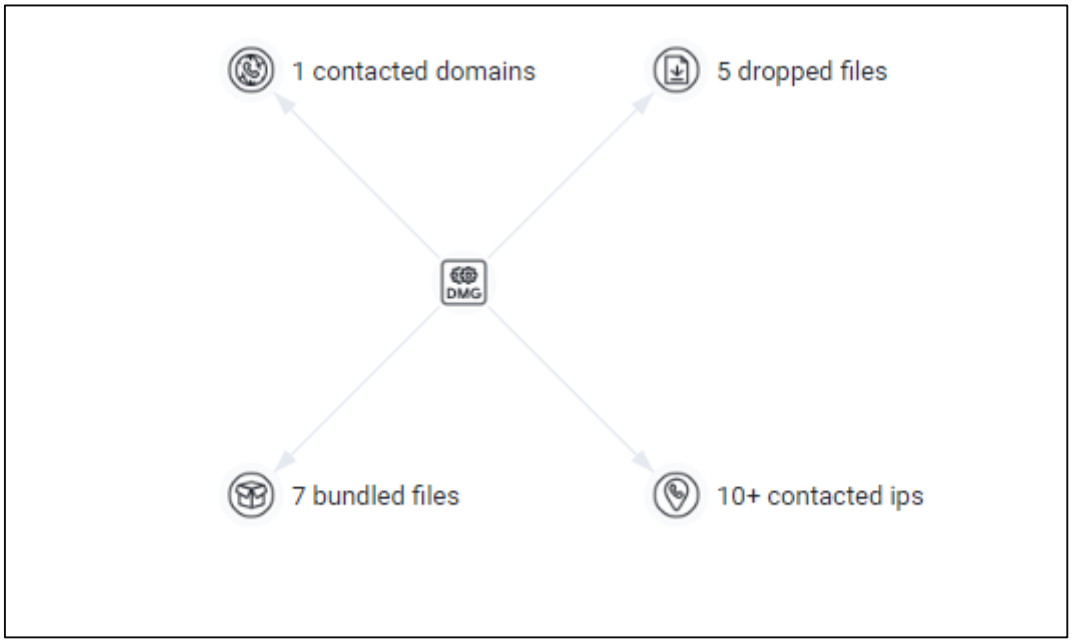
این بدافزار ۵ فایل را حذف کرده که اطلاعات مربوط به فایل‌ها نظیر نام، نوع، اندازه، درهم‌سازی‌شان به شرح زیر می‌باشد:

Dropped Files (5)

Scanned	Detections	File type	Name
2023-05-02	27 / 59	Mach-O	My Go Application.app
SHA-256	2c63ba2b1a5131b80e567b7a1a93997a2de07ea20d0a8f5149701c67b832c097		
File Size	51.55 MB		
2023-05-02	0 / 60	Mach-O	csparser
SHA-256	14d02f4336c0717cc33978bd9805f1fc0179c85c62f2ed9e5fa4c13ad5ca6438		
File Size	407.55 KB		
2023-05-02	0 / 59	Mach-O	CoreFP
SHA-256	4fa6ae34e068a7326fe5508054f9b1f5a0d59e1d8f2e51317d8294bb8ea7f1e9		
File Size	52.09 MB		
2023-05-02	0 / 60	Mach-O	support
SHA-256	68790f0203a061146216675283 21b49361c1cc6aa164ccae69e6429b564be5d6		
File Size	140.16 KB		
?	?	file	6a17c684bc209562e101f2935f4ea6f076f6a2168cc83b0ba1caaa1fbccb8899
SHA-256	6a17c684bc209562e101f2935f4ea6f076f6a2168cc83b0ba1caaa1fbccb8899		

شکل ۱۲. اطلاعات فایل‌های حذف شده توسط بدافزار

خلاصه گراف این بدافزار به صورت زیر می‌باشد که با یک دامنه ارتباط برقرار کرده و حاوی ۷ فایل همراه بوده ، همچنین با ۱۵ آدرس ip مرتبط شده و ۵ فایل را نیز حذف کرده‌است.



شکل ۱۳. گراف بدافزار

از پایگاه دانش جهانی MITRA ATT@CK استفاده‌شده در تحلیل رفتار بدافزار که تکنیک‌های مهاجم مبتنی بر مشاهدات دنیای واقعی هست. اجرای آن بدین‌صورت هست که AppleScript T1059.002 از اضافات

اسکریپت‌نویسی AppleScript حاوی قابلیت‌های اضافی برای اسکریپت‌های اپل استفاده می‌کند. از چارچوب، اجزاء AppleScript حاوی عملکردهای مرتبط با اسکریپت اپل استفاده می‌کند. اسکریپت‌های apple via سایر اسکریپت‌های زبان OSA را با دستور پوسته osascript اجرا می‌کند. ماندگاری بدین‌صورت می‌باشد که فایل-های لیست خصوصیات (plist.) را روی دیسک می‌نویسد. لیست خصوصیات plist روی دیسک نوشته می‌شود. سه گریز محافظتی دارد که شامل:

Masquerading: بسته برنامه حاوی فایل‌ها/دایرکتوری‌های مخفی فایل اجرایی فرآیند دارای پسوند فایلی است که غیرمعمول است (احتمالاً برای پنهان کردن فایل اجرایی)

مجازی‌سازی/Sandbox: حاوی نمادهایی با نام‌های مشکوک است که احتمالاً مربوط به ضد تحلیل است.

فایل‌ها و فهرست‌های مخفی: بسته برنامه حاوی فایل‌ها/دایرکتوری‌های پنهان است.

برای کشف اطلاعات سیستم، نام میزبان سیستم‌ها را می‌خواند. انتشار سیستم‌عامل سیستم‌ها و یا نوع آن را می‌خواند. مقادیر sysctl مربوط به سخت‌افزار را می‌خواند. مقدار راه‌اندازی امن sysctl را می‌خواند (احتمالا برای بررسی اینکه آیا سیستم در حالت راه‌اندازی امن است). فایل plist نسخه سیستم یا سرور را می‌خواند. در ادامه از مجازی‌سازی و sandbox نیز استفاده کردیم.

در بخش کنترل و فرمان، کانال رمزگذاری شده ذکر شده که کتابخانه امنیتی را وارد می‌کند که اغلب برای گواهی، کلید، زنجیره کلید یا حمل و نقل ایمن استفاده می‌شود.

هنگام اجرای فایل حاوی بدافزار ارتباطات شبکه domain name resolution و ترافیک شبکه و پروتکل استفاده شده آن به شکل زیر انجام شده:

شکل۱۴. ارتباط و ترافیک شبکه

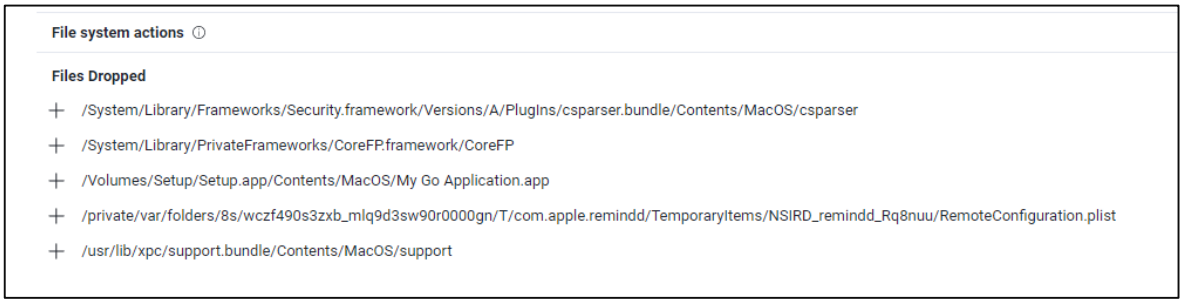
اطلاعات پروتکل لایه انتقال استفاده شده در ارتباطات شبکه این فایل به شرح زیر می‌باشد:

شکل۱۵. اطلاعات پروتکل

دو فایل با رفتار مشابه با بدافزار بررسی شده و درهم‌سازی آن‌ها به شرح زیر می‌باشند:

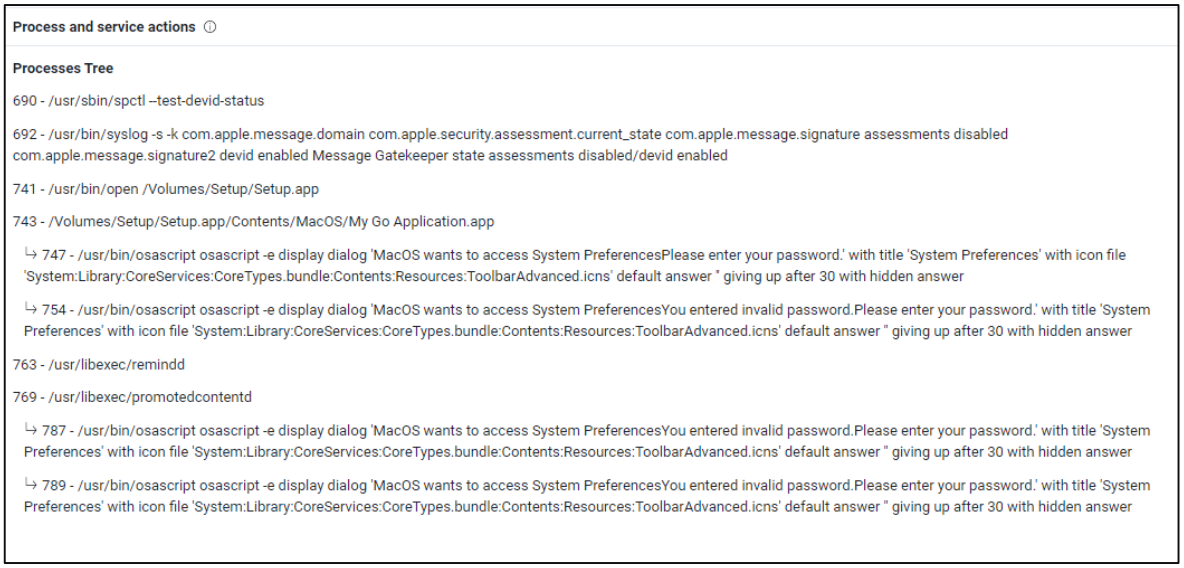
شکل۱۶. درهم سازی فایل های مشابه با بدافزار

هنگام اجرای فایل حاوی بدافزار، عملیات حذف فایل‌های زیر که یکی از نوع xml می‌باشد، در محیط sanfbox روی سیستم انجام شده است.



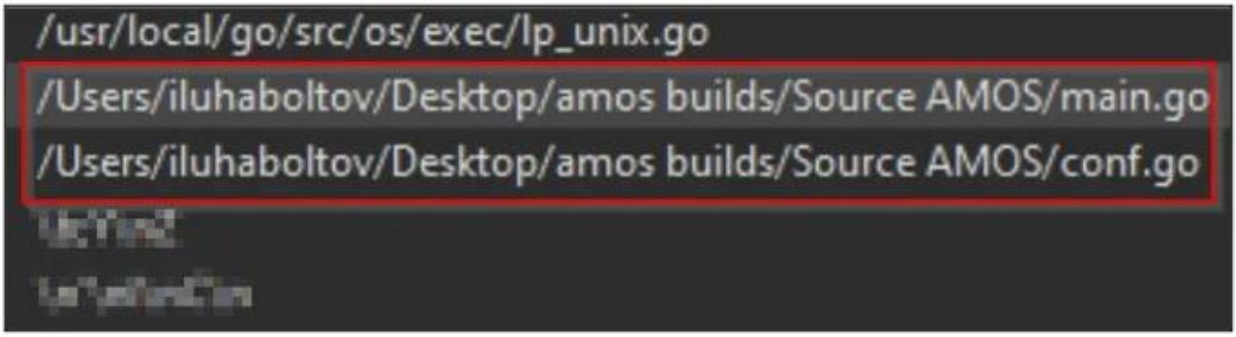
شکل۱۷. فایل‌های حذف شده هنگام اجرای بدافزار

هنگام اجرای فایل حاوی بدافزار، اقدامات زیر با توجه به فرآیندها و خدمات در محیط sandbox اجرا شدند که در ابتدا به دایرکتوری دسترسی پیدا می‌کند و راه نفوذ خود را باز می‌کند تا فایل بدافزار اجرا شود(ارزیابی های امضا هنگام دسترسی را غیر فعال می‌کند)، به تنظیمات سطح دسترسی روت دسترسی یافته و درخواست وارد کردن رمزعبور می‌کند و اطلاعات مورد نیاز خود که در ادامه توضیح داده شده را بدست آورد، بعد از مدتی که گفته شده ۳۰ ثانیه پاسخ پنهان شده و پیغام رمز ورود اشتباه وارد شده را نمایش داده و پس از آن فایل‌های ایجاد شده طی این فرآیند را از بین می‌برد. در واقع دسترسی سطح بالا می‌گیرد و اطلاعات مورد نظر را استخراج می‌کند و پیغام های نامتناسب نمایش می‌دهد و فایلهایی که به آن‌ها اشاره شد را حذف می‌کند.درخت فرآیند آن نیز مطابق تصویر زیر می‌باشد.



شکل۱۸. درخت فرایند

TAها از یک فایل «dmg.» "/Setup.app/Contents/macOS/My Go Application.app" برای انتشار این بدافزار استفاده می‌کنند که شامل یک فایل اجرایی Mac OS X، واقع در و یک فایل اجرایی Golang ۶۴ بیتی است.



شکل۱۹. رشته های مربوط به فایل‌های منبعGo

عملکرد اصلی Atomic macOS Stealer شامل تمام قابلیت‌های آن، از جمله استخراج زنجیره کلید (keychain)، سرقت کیف پول ارز دیجیتال، سرقت اطلاعات مرورگر، گرفتن فایل‌های کاربر، جمع‌آوری اطلاعات سیستم و ارسال تمام داده‌های دزدیده شده به سرور C&C راه دور است.

توابع اصلی بدافزار در شکل زیر نشان داده شده است.

```
void __cdecl main_main()
{
  __int64 v0; // r14
  void *retaddr; // [rsp+0h] [rbp+0h] BYREF

  while ( (unsigned __int64)&retaddr <= *(_QWORD *)(v0 + 16) )
    runtime_morestack_noctxt_abi0();
  main_keychain();
  main_GrabWallets();
  main_GrabChrome();
  main_GrabFirefox();
  main_FileGrabber();
  main_systeminfo();
  main_sendlog();
  main_doAlert();
}
```

شکل۲۰. تابع اصلی بدافزار

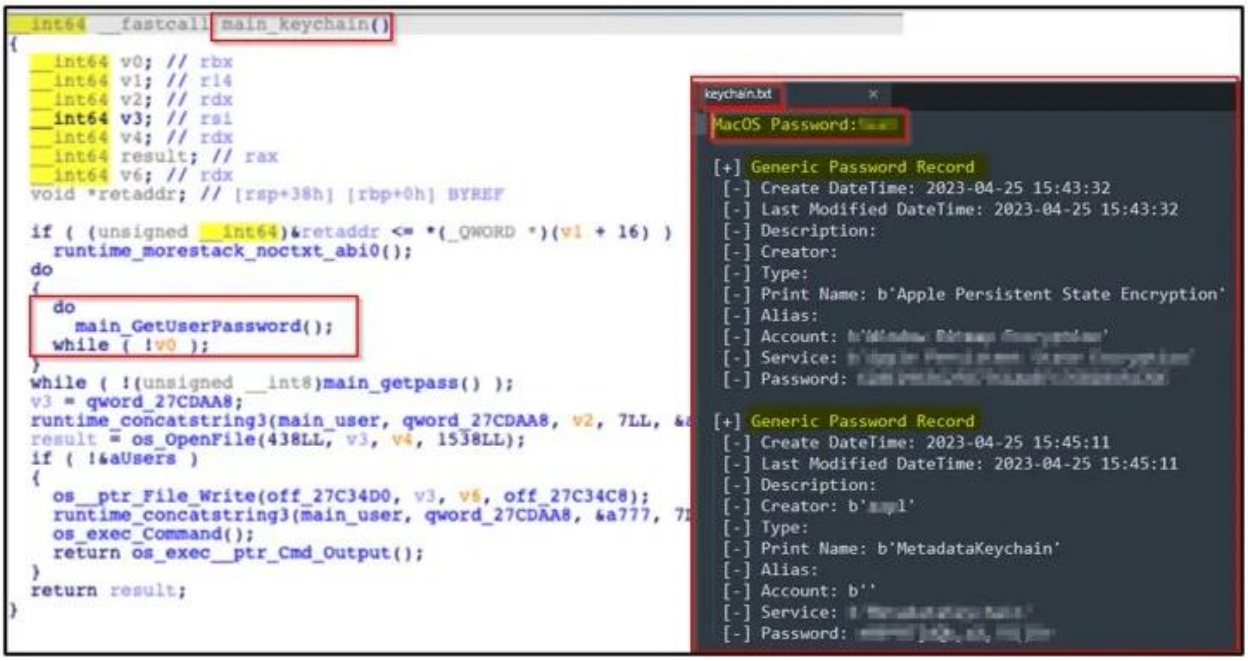
هنگامی که کاربر فایل را اجرا کند، یک پنجره جعلی مانند شکل زیر برای دریافت رمز عبور سیستم نمایش داده می‌شود.

شکل۲۱. پنجره جعلی دریافت پسورد

۲-۱ استخراج رمز عبور زنجیره کلید (keychain)

این بدافزار علاوه بر بدست آوردن رمز عبور سیستم، ابزار مدیریت رمز عبور را نیز با استفاده از تابع main_keychain() به منظور استخراج اطلاعات حساس از دستگاه قربانی، هدف قرار می‌دهد. Keychain یک سیستم مدیریت رمز عبور macOS است که کاربران را قادر می‌سازد تا داده‌های حساس مانند اطلاعات ورود به وب‌سایت، رمزهای عبور Wi-Fi، اطلاعات کارت اعتباری و غیره را با خیال راحت ذخیره کنند.

قطعه کد نشان داده شده در شکل زیر تابع main_keychain() را نشان می‌دهد که برای جمع‌آوری اطلاعات حساب کاربر پیاده‌سازی شده است.



شکل ۲۲. استخراج رمزعبور keychain

۲-۲ سرقت کیف پول‌های ارزدیجیتال

پس از آن، بدافزار با انجام پرس‌وجو (query) و خواندن فایل‌ها از دایرکتوری‌های خاص با استفاده از تابع main_GrabWallets() شروع به استخراج اطلاعات مربوط به کیف پول‌های ارزدیجیتال می‌کند. همانطور که در زیر نشان داده شده، بدافزار کیف پول هایی مانند Electrum، Binance، Exodus و Atomic را هدف قرار می‌دهد.

```
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_telegram);
else
  main_telegram = v43;
v45 = runtime_concatstring3(main_user, qword_27CDAA8, v44, 7LL, "/.electrum/wallets/", 19LL);
qword_27CEE48 = (__int64)"/Users/";
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&qword_27CEE40);
else
  qword_27CEE40 = v45;
v47 = main_library;
v48 = runtime_concatstring2("Coinomi/wallets/", 16LL, v46, qword_27CDA68);
qword_27CEE58 = v47;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&qword_27CEE50);
else
  qword_27CEE50 = v48;
v50 = main_library;
v51 = runtime_concatstring2("Exodus/", 7LL, v49, qword_27CDA68);
qword_27CEE68 = v50;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&qword_27CEE60);
else
  qword_27CEE60 = v51;
v53 = main_library;
result = runtime_concatstring2("atomic/Local Storage/leveldb/", 29LL, v52, qword_27CDA68);
qword_27CEE78 = v53;
if ( runtime_writeBarrier )
  return runtime_gcWriteBarrier(&qword_27CEE70);
qword_27CEE70 = result;
return result;
```

شکل ۲۳. کیف پول‌های ارز دیجیتال مورد هدف

۳-۲ افزونه کیف پول ارز دیجیتال

مخرب Atomic macOS همچنین می‌تواند از افزونه‌های کیف پول کریپتو مرورگر، اطلاعات را استخراج کند. این افزونه‌ها از طریق کدنویسی سخت (hard coding) در باینری مخرب ادغام می‌شوند و تاکنون بیش از ۵۰ افزونه مورد هدف قرار گرفته‌اند.

جدول زیر برخی از کیف پول‌های کریپتو با شناسه‌های افزونه مرورگر را که توسط این بدافزار هدف قرار گرفته‌اند، نشان می‌دهد.

جدول ۱. کیف پول‌های کریپتو مورد هدف بدافزار

acmacodkjbdgmoleebolmdjonilkdbch	Rabby Wallet
aeachknmefphepccionboohckonoeemg	Coin98 Wallet
afbcbjpbpfadlkmhmclhkeeodmamcflc	Math Wallet
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
aiifbnbfobpmeekipheeijimdpnlpgpp	Station Wallet
amkmjjmmflddogmhpjloimipbofnfjih	Wombat – Gaming Wallet for Ethereum & EOS
apnehcjmnengpnmccpaibjmhhoadaico	CWallet
bcopgchhojmggmffilplmbdicgaihlkp	Hycon Lite Client
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom
bocpokimicclpaiekenaeelehdjllofo	XDCPay
cgeeodpfagjceefieflmdfphplkenlfk	EVER Wallet
cihmoadaighcejopammfbmddcmdekcje	LeafWallet
cjelfplplebdjjenllpjcblmjkfcffne	Jaxx Liberty
cjmkndjhnagcfbpiemnkdpomccnjblmj	Finnie
cmndjbecilbocjfkibfbifhngkdmjgog	Swash

cnmamaachppnkjgnildpdmkaakejnhae	Auro
copjnifcecdedocejpaapepagaodgpbh	Freaks Axie
cphhlgmgameodnhkjdmkpanlelnlohao	NeoLine
dhgnlgphgchebgoemcjekedjjbifijid	Crypto Airdrops & Bounties
dkdedlpgdmmkkfjabffeganieamfklkm	Cyano
dmkamcknogkgcdfhhbddcghachkejeap	Keplr
efbglgofoippbgcjepnhiblaibcnclgk	Martian Wallet for Sui & Aptos
egjidjbpglichdcondbcbdnbeeppgdph	Trust Wallet
ffnbelfdoeiohenkjibnmadjiehjhajb	Yoroi
fhbohimaelbohpjbbldcngcnapndodjp	BinanceChain
fhilaheimglignddkjgofkcbgekhenbh	Oxygen
flpiciilemghbmfalicajoolhkkenfel	ICONex
fnjhmkhhmkbjkkabndcnnogagogbneec	Ronin
fnnegphlobjdpkhecapkijjdkgcjhkib	Harmony Wallet
hcflpincpppdclinealmandijcmnkbgn	KHC
hmeobnfnfcmdkdcmlblgagmfpfboieaf	XDEFI

hnfanknocfeofbddgcijnmhnfnkdnaad	Coinbase
hnhobjmcibchnmglfbldbfabcgaknlkj	Flint Wallet
hpglfhgfnhbgpjdenjgmdgoeiappafln	Guarda
ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
imloifkgjagghnncjkhggdhalmcnfklk	Trezor Password Manager
jojhfeoedkpkglbfimdfabpdfjaoolaf	Polymesh
klnaejjgbibmhlephnhpmaofohgkpgkd	ZilPay
kncchdigobghenbbaddojjnnaogfppfj	iWallet
kpfopkelmapcoipemfendmdcghnegimn	Liquality
lodccjjbdhfakaekdiahmedfbieldgik	DAppPlay
mfhbebgoclkghebffdldpobeajmbecfk	Starcoin
mnfifefkajgofkcjkemidiaecocnkjeh	TezBox
nhnkbkgjikgcigadomkphalanndcapjk	CLW
nkbihfbeogaeaoehlefnkodbefgpgknn	Metamask
nknhiehlklippafakaeklbeglecifhad	Nabox
nlbmnnijcnlegkjjpcfjclmcfggfefdm	MewCx
nlgbhdfgdhgbiamfdfmbikcdghidoadd	Byone
nphplpgoakhhjchkkhmiggakijnkhfnd	Ton
ookjlbkiijinhpmnjffcofjonbfbgaoc	Temple
pdadjkfkgcafgbceimcpbkalnfnepbnk	KardiaChain
pnndplcbkakcplkjnolgbkdgjikjednm	Tron Wallet & Explorer – Tronium
pocmplpaccanhmnllbbkpgfliimjljgo	Slope
ppdadbejkmjnefldpcdjhnkpbjkikoip	Oasis

۴-۲ استخراج اطلاعات مرورگر

پس از جمع‌آوری اطلاعات کیف پول، بدافزار دایرکتوری‌های مرورگرهای نصب شده روی دستگاه قربانی را جستجو می‌کند و فایل‌های مربوط به مرورگر خاص را برای استخراج داده‌های محرمانه جستجو می‌کند، مانند:

- تکمیل خودکار (autofill)
- رمزهای عبور
- کوکیها
- کارت‌های اعتباری

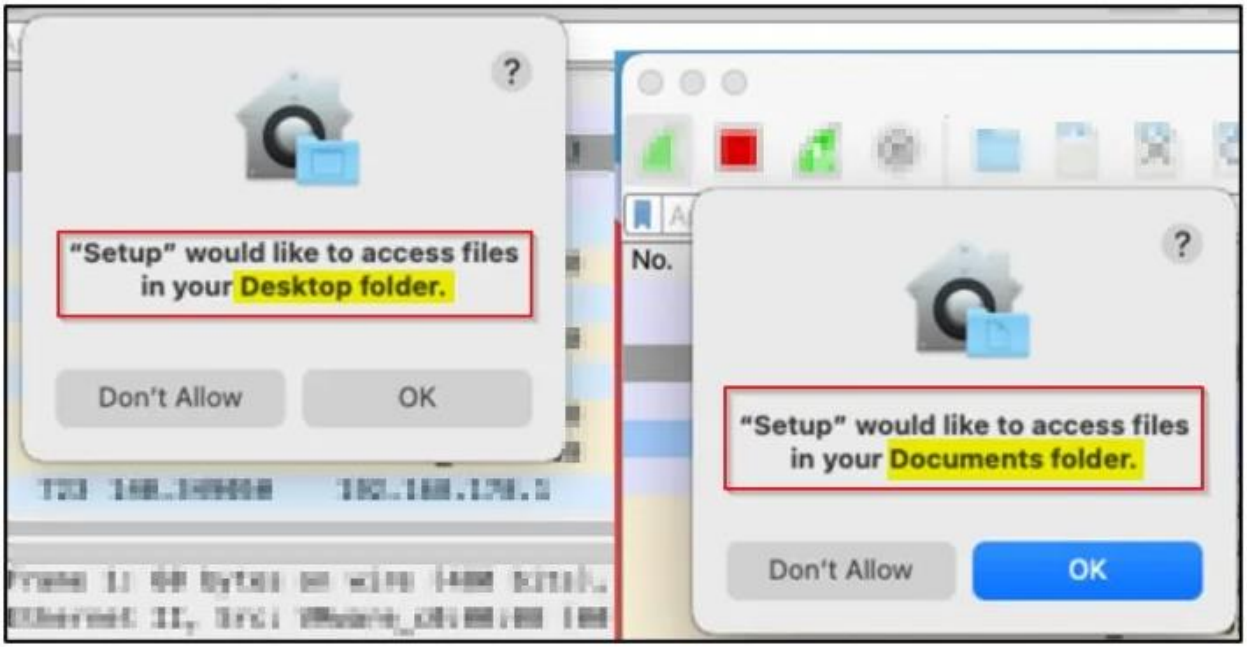
همانطور که در زیر نشان داده شده، این بدافزار می‌تواند فایل‌ها را از مرورگرهای مختلف از جمله Firefox، Google Chrome، Microsoft Edge، Yandex، Opera و Vivaldi بدزدد.

```
v20 = runtime_concatstring2("Firefox/Profiles/", 17LL, v18, qword_27CDA68);
qword_27CDA58 = v19;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_firefox);
else
  main_firefox = v20;
v22 = main_library;
v23 = runtime_concatstring2("Google/Chrome/", 14LL, v21, qword_27CDA68);
qword_27CDA18 = v22;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_chrome);
else
  main_chrome = v23;
v25 = main_library;
v26 = runtime_concatstring2("BraveSoftware/Brave-Browser/", 28LL, v24, qword_27CDA68);
qword_27CDA08 = v25;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_brave);
else
  main_brave = v26;
v28 = main_library;
v29 = runtime_concatstring2("Microsoft Edge/", 15LL, v27, qword_27CDA68);
qword_27CDA48 = v28;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_edge);
else
  main_edge = v29;
v31 = main_library;
v32 = runtime_concatstring2("Vivaldi/", 8LL, v30, qword_27CDA68);
qword_27CDAB8 = v31;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_vivaldi);
else
  main_vivaldi = v32;
v34 = main_library;
v35 = runtime_concatstring2("Yandex/YandexBrowser/", 21LL, v33, qword_27CDA68);
qword_27CDAC8 = v34;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_yandex);
else
  main_yandex = v35;
v37 = main_library;
v38 = runtime_concatstring2("com.operasoftware.Opera/", 24LL, v36, qword_27CDA68);
qword_27CDA78 = v37;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_opera);
else
  main_opera = v38;
v40 = main_library;
v41 = runtime_concatstring2("com.operasoftware.OperaGX/", 26LL, v39, qword_27CDA68);
qword_27CDA88 = v40;
```

شکل۲۴. مرورگرهای هدف

۵-۲ فایل گیر (file grabber)

مخرب در این مرحله فایل‌های قربانی را از دایرکتوری‌هایی مانند Desktop و Documents با استفاده از تابع main_FileGrabber() می دزدد. شکل زیر بدافزاری را نشان می‌دهد که درخواست مجوز برای دسترسی به فایل‌های درون دایرکتوری‌های مشخص دارد.



شکل۲۵. درخواست مجوز برای دسترسی به فایل‌ها توسط مخرب

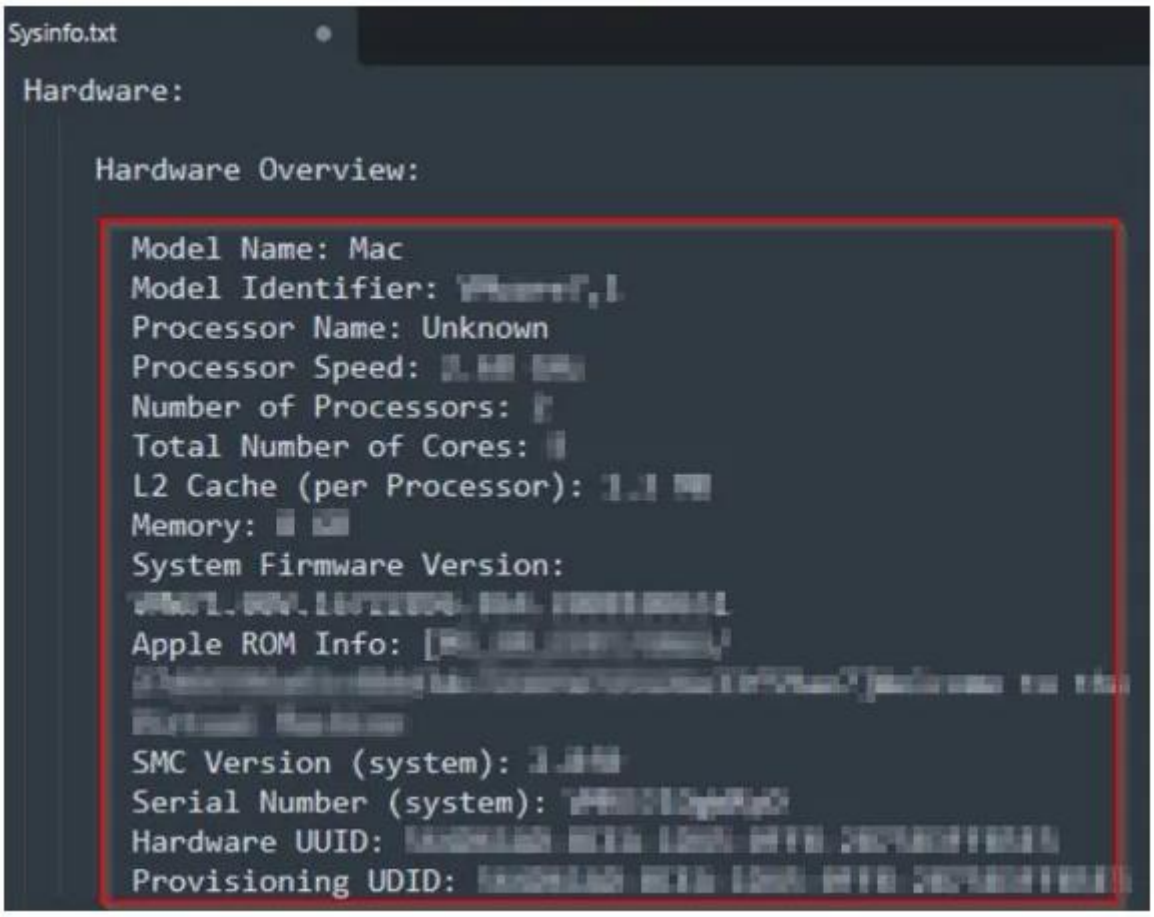
قطعه کد شکل زیر تابع main_FileGrabber() را نشان می‌دهد که برای برداشتن فایل‌ها از سیستم قربانی پیاده‌سازی شده است.

```
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_library);
else
  main_library = v13;
v15 = runtime_concatstring3(main_user, qword_27CDAA8, v14, 7LL, "/Desktop/", 9LL);
qword_27CDA28 = (__int64)"/Users/";
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_desktop);
else
  main_desktop = v15;
v17 = runtime_concatstring3(main_user, qword_27CDAA8, v16, 7LL, "/Documents/", 11LL);
qword_27CDA38 = (__int64)"/Users/";
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier(&main_documents);
```

شکل۲۶. فایل گیر

۶-۲ جمع‌آوری اطلاعات سیستم

متعاقباً، بدافزار فرآیند به دست آوردن اطلاعات بیشتر مربوط به سخت افزار سیستم، مانند نام مدل، UUID سخت افزار، اندازه RAM، تعداد هسته‌ها، و شماره سریال را از بین سایر اطلاعات آغاز می‌کند که در شکل زیر نشان داده شده است.



شکل ۲۷. اطلاعات جمع آوری شده سیستم

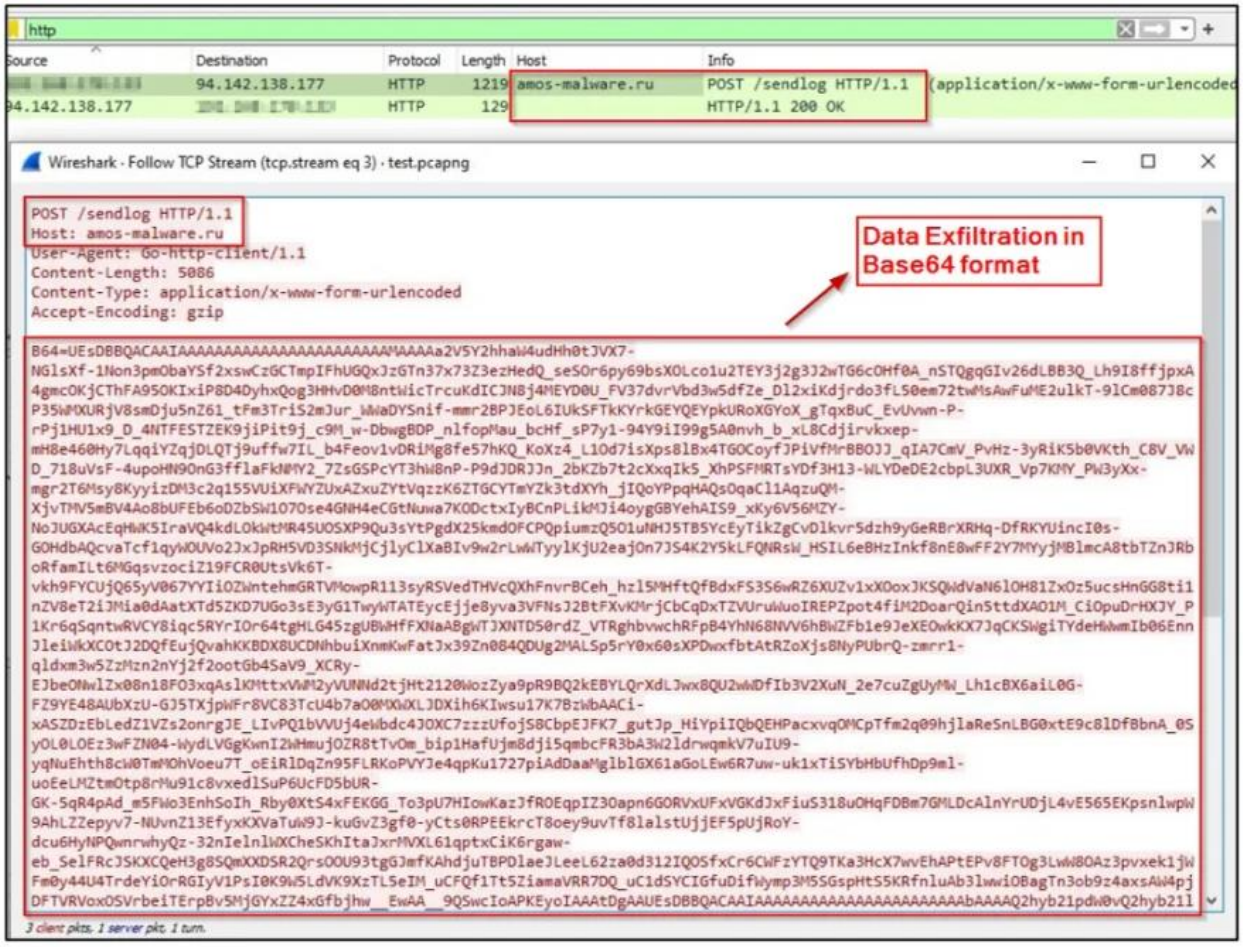
۷-۲ فرمان و کنترل (C&C)

در نهایت، مخرب Atomic macOS اطلاعات دزدیده شده را از طریق فشرده‌سازی در ZIP و رمزگذاری آن با استفاده از فرمت Base۶۴ برای نفوذ پردازش می‌کند.

مخرب با URL سرور C&C زیر ارتباط برقرار می‌کند و اطلاعات دزدیده شده را ارسال می‌کند.

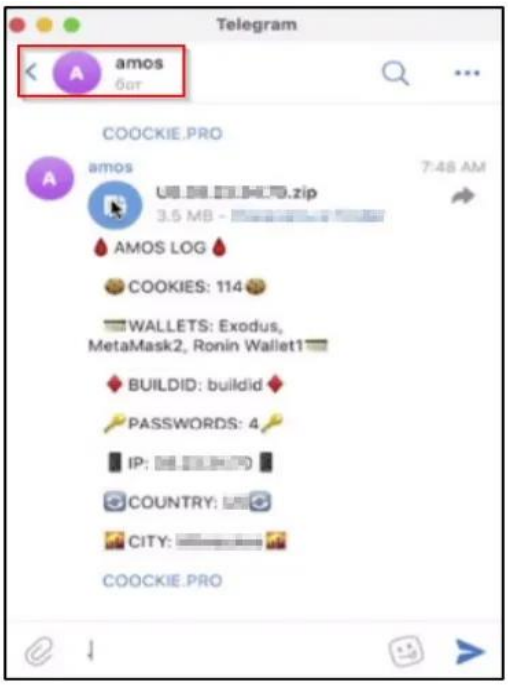
- *hxxp[:]//amos-malware[.]ru/sendlog*

شکل زیر ارتباط شبکه‌ای استخراج داده از دستگاه قربانی را نشان می‌دهد.



شکل۲۸. داده‌های مستخرج

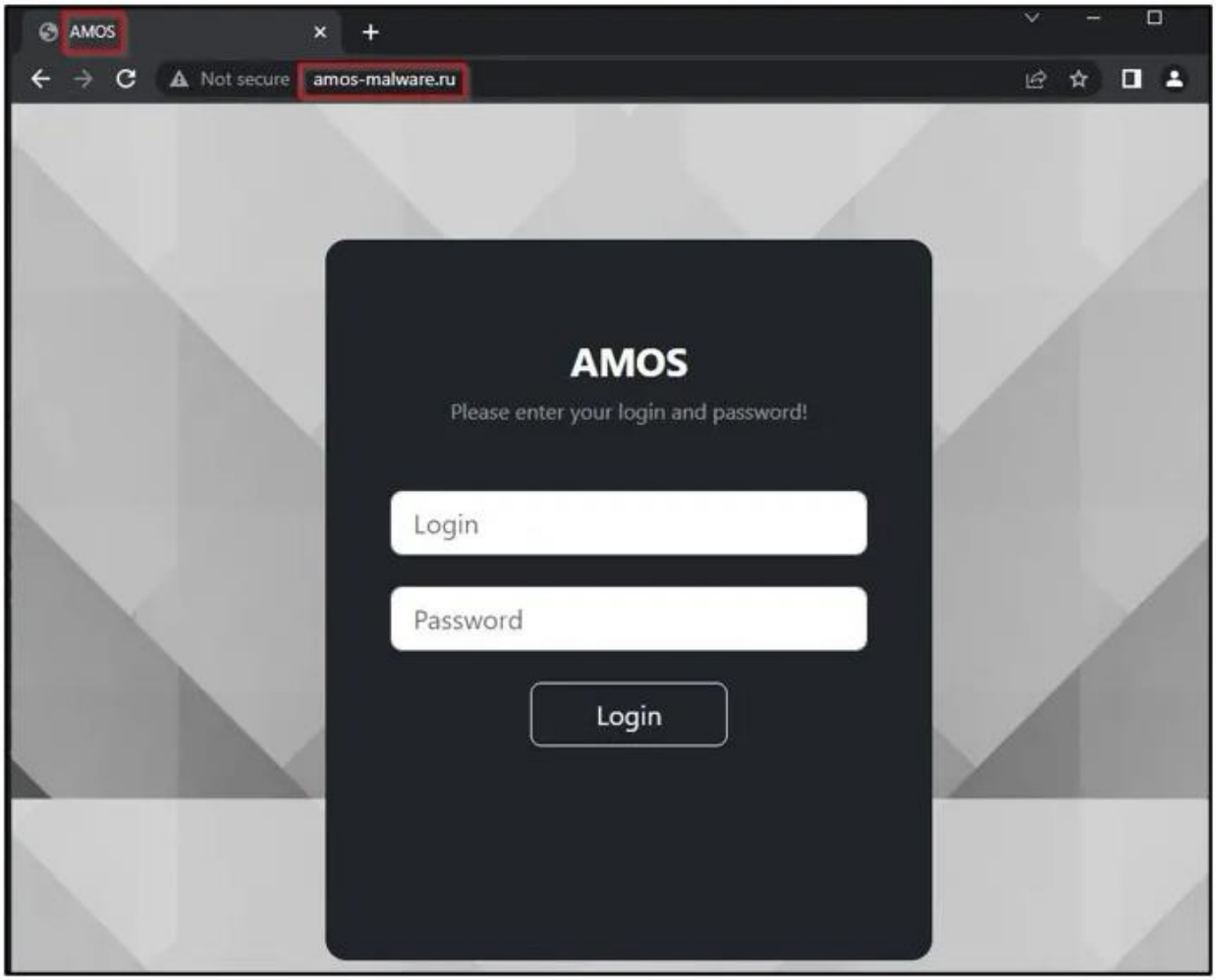
هم‌زمان، مخرب Atomic macOS اطلاعات منتخب را به همراه فایل ZIP کامپایل شده مطابق شکل زیر به کانال‌های تلگرام ارسال می‌کند.



شکل۲۹. ارسال فایل زیپ به کانال تلگرام

۸-۲ پنل C&C

شکل زیر پنل فعال C&C مخرب Atomic macOS را نشان می‌دهد.



شکل ۳۰. AMOS C&C panel

۳ محصولات تحت تأثیر

سیستم عامل macOS با توجه به ویژگی‌های امنیتی قوی، برای بسیاری از افراد مورد ترجیح است. هدف قرار دادن macOS روند جدیدی نیست و خانواده‌های بدافزار مختلفی وجود دارند که به طور خاص هدفشان نفوذ به این سیستم عامل است.

بدافزارهایی مانند Atomic macOS Stealer را می‌توان با بهره‌برداری از آسیب‌پذیری‌ها یا میزبانی وب‌سایت‌های فیشینگ نصب کرد. عاملان تهدید می‌توانند از داده‌های سرقت شده برای جاسوسی یا منافع مالی استفاده کنند. بدافزارهای macOS در حالی که معمول نیستند، می‌توانند اثرات مخربی بر قربانیان داشته باشند.

۴ توصیه‌های امنیتی

برخی از بهترین اقدامات ضروری امنیت سایبری را فهرست کرده‌ایم که اولین خط کنترل را در برابر مهاجمان ایجاد می‌کند. به خوانندگان توصیه می‌کنیم که راهکارهای زیر را دنبال کنند:

- نرم افزار را فقط از اپ استور رسمی اپل دانلود و نصب کنید.
- از یک پکیج نرم افزار آنتی ویروس و امنیت اینترنت معروف بر روی سیستم خود استفاده کنید.
- از رمزهای عبور قوی استفاده کنید و احراز هویت چند عاملی را تا جایی که ممکن است اعمال کنید.
- ویژگی‌های امنیتی بیومتریک مانند اثر انگشت یا تشخیص چهره را برای باز کردن قفل دستگاه در هر کجا که ممکن است فعال کنید.
- مراقب باز کردن پیوندهایی باشید که از طریق ایمیل به شما تحویل داده می‌شود.
- هنگام دادن هرگونه دسترسی مراقب باشید.
- دستگاه‌ها، سیستم عامل‌ها و برنامه‌های خود را به روز نگه دارید.

۵ منابع خبر

[1] https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/