گزارش فنی تحلیل بدافزار Caphaw

معرفی بدافزار

بدافزار Caphaw یکی از انواع مختلف بدافزارهای بانکی است که عملکردی مشابه تهدیدات Carberp ، Ranby، Tinba دارد. این بدافزار حدود ۱۰۰۰۰ کامپیوتردر انگلستان و حدود ۳۰۰۰۰ کامپیوتر در سرتاسر دنیا را آلوده کرده است.

بدافزار Caphaw با کلیک کاربر روی لینک مخرب و دانلود آن، وارد سیستم می شود. پس از ورود، به دنبال اطلاعات بانکی کاربر می گردد و آن ها را به سرور C&C ارسال می کند.

این بدافزار با تزریق خود به فرآیندهای قانونی مانند explorer.exe یا iexplore.exe مانع شناسایی خود می گردد، همچنین از الگوریتم تولید دامنه (DGA) برای مسیردهی ترافیک خود، از طریق تعدادی آدرس IP که با استفاده از گواهی های خود ساخته ی SSL ایجاد شده است، استفاده می‌کند.

الگوریتم تولید دامنه پیش از این نیز توسط برخی خانواده های بدافزاری به کار گرفته شده است تا از شناسایی توسط سرویس ها و نرم افزار ها در امان بمانند. این الگوریتم ها مداوماً دامنه های جدیدی را تولید و آزمایش می‌کنند و تعیین می نمایند که سرور کنترل و فرمان دهی به درخواست آن‌ها پاسخ می‌دهد یا خیر. به این ترتیب با استفاده از DGA دیگر نیاز نیست که مهاجمان زیرساختی از سرورهای کنترل و فرمان دهی را مدیریت کنند؛ چرا که این زیرساخت ممکن است توسط پژوهشگران و مقامات اجرایی کشورها شناسایی و تعطیل شود.

این بدافزار Caphaw چندین بار تغییر پیدا کرده و ویژگی‌های جدیدی به آن اضافه شده است که به فرار از شناسایی آن کمک می‌کند. از سایر ویژگی‌های اضافه شده به این بدافزار می‌توان به قابلیت تزریق وب اشاره کرد که

امکان نصب بدافزار در سامانه‌ی در معرض خطر را فراهم کرده است. همچنین افزونه‌ای به آن اضافه شده که به گسترش از طریق پیام‌های فوری اسکایپ کمک می‌کند.

محققان بر این باورند که یک بسته‌ی نفوذی در آخرین آلودگی‌های Caphaw به کار گرفته شده و این بدافزار با بهره‌گیری از آسیب‌پذیری‌های جاوا به سامانه‌ی شخص قربانی راه پیدا کرده‌اند. Caphaw پس از ورود به سامانه پرونده‌ی اجرایی را در آن رها می‌سازد که در موارد مختلف متفاوت بوده است.

این بدافزار قادر است تشخیص دهد که در یک ماشین مجازی به اجرا درآمده یا میزبانش در حالت برخط به سر می‌برد. در صورتی که یکی از این موارد وجود داشته باشد، اجرا نخواهد شد. همچنین این بدافزار برای پایداری بیشتر رجیستری خودکار و فرآیندهای سیستمی را ایجاد می‌کند تا مانع از حذف خود گردد.

زمانی که این بدافزار در سیستم اجرا می شود مجموعه ای از فایلها را تغییر می دهد و یک کلید رجیستری برای اجرا در هر بار راه اندازی ویندوز ایجاد می کند. در زمان حضور بدافزار Caphaw، برنامه های آنتی ویروس و دیگر نرم افزارهای امنیتی ممکن است غیر فعال شوند. این بدافزار به طور معمول به فرآیندهای در حال اجرا مربوط به آنتی ویروس، دیوار آتش، و دیگر برنامه های حفاظتی پایان می دهد.

Caphaw به یک سرور از راه دور با استفاده از پورت HTTP یا FTP برای آپلود اطلاعات جمع آوری شده از کامپیوتر متصل می‌شود. این بدافزار بسته های ICMP که می تواند در حمله انکار سرویس توزیع شده (DDoS) مورد استفاده قرار گیرد ارسال می کند.

زمانی که بدافزار برای اولین بار بر روی دستگاه اجرا شود یک گزارش دقیق در کامپیوتر قربانی تولید می باشد. این گزارش رمزگذاری می شود و با دستور ‘cmd=log&w=cmpinfo’ به سرور ارسال می شود.

این گزارش شامل جزئیات توسعه یافته از میزبان آلوده می باشد که در زیر به برخی از آنها اشاره می شود:

- نسخه، سریال و CDKey مربوط به سیستم عامل
- اطلاعات RAM و CPU
- ساختار سیستم فایل و فضای در دسترس
- نام کامپیوتر، نام کاربر و سطح دسترسی
- نسخه مرورگر
- لیستی از محصولات ضد بدافزار
- این که آیا در حال اجرا در یک ماشین مجازی است
- برخی از اطلاعات فایل اجرایی محلی ، از جمله: vsdrv.exe، cftmon.exe،userinit.exe
- لیستی ازسرویس های در حال اجرا
- لیستی از فرایندهای در حال اجرا
- لیستی از برنامه های نصب شده

از دیگر فعالیتهای مخرب این بدافزار می توان به موارد زیر اشاره کرد:

- دسترسی به فایل ها و پوشه از طریق یک سرور FTP داخلی
- سرقت اطلاعات حساس مانند کلمات عبور، کارت های اعتباری، اطلاعات حساب بانکی و غیره
- تغییر مسیر ترافیک اینترنت از طریق یک پروکسی سرور
- بروزرسانی خود
- خاموش و راه اندازی دوباره کامپیوتر
- حذف خود پس از اجرای روتین مخرب

به گفته‌ی محققان ۲۴ بانک زیر توسط این بدافزار هدف قرار داده شده‌اند:

- Bank of Scotland
- Barclays Bank
- First Direct
- Santander Direkt Bank AG
- First Citizens Bank
- Bank of America
- First Direct
- Santander Direkt Bank AG
- First Citizens Bank
- Bank Of the West
- Sovereign Bank
- Co-operative Bank
- Capital One Financial Corporation
- Chase Manhattan Corporation
- Citi Private Bank
- Comerica Bank
- E*Trade Financial
- Harris Bank
- Intesa Sanpaolo
- Regions Bank
- SunTrust
- Bank of Ireland Group Treasury
- U.S. Bancorp
- Banco Mercantil, S.A.
- Varazdinska Banka
- Wintrust Financial Corporation
- Wells Fargo Bank

نحوه شناسایی سیستم آلوده از طریق لاگ های شبکه

این بدافزار برای ارسال و دریافت اطلاعات به دامنه های زیر متصل می شود:

- jdqela.thepohzi.su
- il7b2m20rh1dzy81k3.tohk5ja.cc
- hsagn30bgkeoo.oogagh.su
- y71lp8ut45njq6xvn.thepohzi.su
- mrmotgritap7.thepohzi.su
- a0peo1v05xt80b.thepohzi.su
- lv255wwyu1rb3.www5.thepohzi.su
- xt7hr6x62bt74.tohk5ja.cc
- 3rltxhgfpfspap40.tohk5ja.cc
- gd4xenyf31fsl63d.www5.tohk5ja.cc
- t4wof941nn1x7.tohk5ja.cc
- 97x4p00hzatk1.oogagh.su
- hq5rrfz.oogagh.su
- abo2vkgxv6wes3lhw.www5.oogagh.su
- gg7ovhhv.oogagh.su
- yue3opjoo9ly32tduy.thepohzi.su
- ppnvknr6lzlwb.tohk5ja.cc
- bzb25e1t6mev4.oogagh.su
- lh12r2tju0.thepohzi.su
- oabyhm80.tohk5ja.cc
- tc5ftlkmud8whf0.oogagh.su
- 982nzzytjopk1.thepohzi.su
- 5ps5u9r5l.tohk5ja.cc

آدرس های IP که بدافزار Caphaw به آنها متصل می شود:

- 204.95.99.251
- 13.107.4.50

نحوه بررسی وجود آلودگی

۱- وجود یک کپی از بدافزار در یکی از مسیرهای زیر:

- % AppData % \adobe\linguistics\dictionaries\adobe custom dictionary\all\
- %AppData%\adobe\linguistics\dictionaries\adobe custom dictionary\eng\
- %AppData%\microsoft\cryptneturlcache\metadata\
- %AppData%\microsoft\drm\
- %AppData%\microsoft\excel\xlstart\
- %AppData%\microsoft\internet explorer\
- %AppData%\microsoft\office\
- %AppData%\microsoft\word\
- % AppData % \ Microsoft \ Media Player \

این بدافزار برای جلوگیری از شناسایی از نام های قانونی استفاده می کند. برای اینکار پوشه <system folder> را برای فایل های قانونی اسکن می کند و سپس خود را در پوشه %AppData% با استفاده از همین نام های قانونی کپی می کند.

نام هایی که بدافزار بکار می برد شامل موارد زیر می باشد:

- csrss.exe
- eventvwr.exe
- expand.exe
- ie4uinit.exe
- mem.exe
- mobsync.exe
- qappsrv.exe
- route.exe
- rundll32.exe
- winmine.exe

۲- وجود یکی از فایل های زیر در سیستم

- C:\AUTOEXEC.BAT
- % APPDATA% \Roaming\Adobe\Acrobat\9.0\Forms\NAPSTAT.EXE
- rdpclip.exe

۳- تغییر کلید رجیستری زیر برای ماندگاری و اجرای دوباره در هر بار راه اندازی ویندوز

- Software\Microsoft\Windows\CurrentVersion\Run
  value: "<random CLSID>"
  برای مثال {FAD5ADC3-DABB-6BFF-ED11-CB329C7D70E2}
  data: "<مسیر بدافزار>"
  برای مثال "%APPDATA%\Microsoft\Excel\xlstart\winmine.exe"

۴- وجود یکی از کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\dcc876357354acaf2b61ee3e839154ad_RASAPI32
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\[random numbers]
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\userinit
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\[random]
- HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\cookie=

۵- وجود دسترسی به نام های دامنه ذکر شده

نحوه پاکسازی سیستم

۱- حذف فایلهای مربوط به بدافزار با نام های ذکر شده در مسیرهای زیر در ویندوز:

- % AppData % \adobe\linguistics\dictionaries\adobe custom dictionary\all\
- %AppData%\adobe\linguistics\dictionaries\adobe custom dictionary\eng\
- %AppData%\microsoft\cryptneturlcache\metadata\
- %AppData%\microsoft\drm\
- %AppData%\microsoft\excel\xlstart\
- %AppData%\microsoft\internet explorer\
- %AppData%\microsoft\office\
- %AppData%\microsoft\word\
- % AppData % \ Microsoft \ Media Player \

۱- حذف فایل های زیر در سیستم:

- C:\AUTOEXEC.BAT
- % APPDATA% \Roaming\Adobe\Acrobat\9.0\Forms\NAPSTAT.EXE
- rdpclip.exe

۲- حذف کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\dcc876357354acaf2b61ee3e839154ad_RASAPI32
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\[random numbers]
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\userinit
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\[random]
- HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\cookie=

۲- مسدودسازی دسترسی به نام های دامنه ذکر شده

۳- راه اندازی مجدد سیستم

نحوه اطمینان یافتن از پاک بودن سیستم

۳- نبود فایلهای مربوط به بدافزار با نام های ذکر شده در مسیرهای زیر در ویندوز:

- % AppData % \adobe\linguistics\dictionaries\adobe custom dictionary\all\
- %AppData%\adobe\linguistics\dictionaries\adobe custom dictionary\eng\
- %AppData%\microsoft\cryptneturlcache\metadata\
- %AppData%\microsoft\drm\
- %AppData%\microsoft\excel\xlstart\
- %AppData%\microsoft\internet explorer\
- %AppData%\microsoft\office\
- %AppData%\microsoft\word\
- % AppData % \ Microsoft \ Media Player \

۲- نبود فایل های زیر در سیستم:

- C:\AUTOEXEC.BAT
- % APPDATA% \Roaming\Adobe\Acrobat\9.0\Forms\NAPSTAT.EXE
- rdpclip.exe

۳- نبود کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\dcc876357354acaf2b61ee3e839154ad_RASAPI32
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\[random numbers]
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\userinit
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\[random]
- HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\cookie=

۴- نبود دسترسی به نامهای دامنه ذکر شده

توصیه های امنیتی برای پیشگیری

۱. بروزرسانی نرم افزارهای ضد بدافزار

۲. روشن کردن فایروال

۳. دریافت آخرین به روز رسانی نرم افزار مرورگر

۴. خودداری از باز نمودن ایمیلهای ناشناس، هرزنامه ها و فایلهای الصاق شده به آنها

۵. عدم استفاده از کرکهای نامعتبر برای نرم افزارها

۶. محدودسازی سطح دسترسی کاربر

۷. مسدودسازی دسترسی به نام های دامنه ذکر شده

۸. اجتناب از باز کردن فایل هایی با دو پسوند مانند .txt.vb یا .jpg.exe

۹. عدم ذخیرسازی گذرواژه های حساس بر روی نرم افزارها

۱۰. اجتناب از مشاهده وب سایت های ناامن

۱۱. دانلود برنامه ها، فایل ها و بسته های به روز رسانی از منابع قابل اعتماد