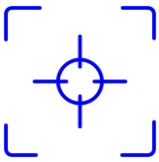
تحلیل بدافزار

MSIL/ClipBanker

شبکه گستر

امنیت شما | وظیفه ما



گروه تحقیق و توسعه
شرکت مهندسی شبکه گستر
مرداد ۱۴۰۲

چکیده مدیریتی

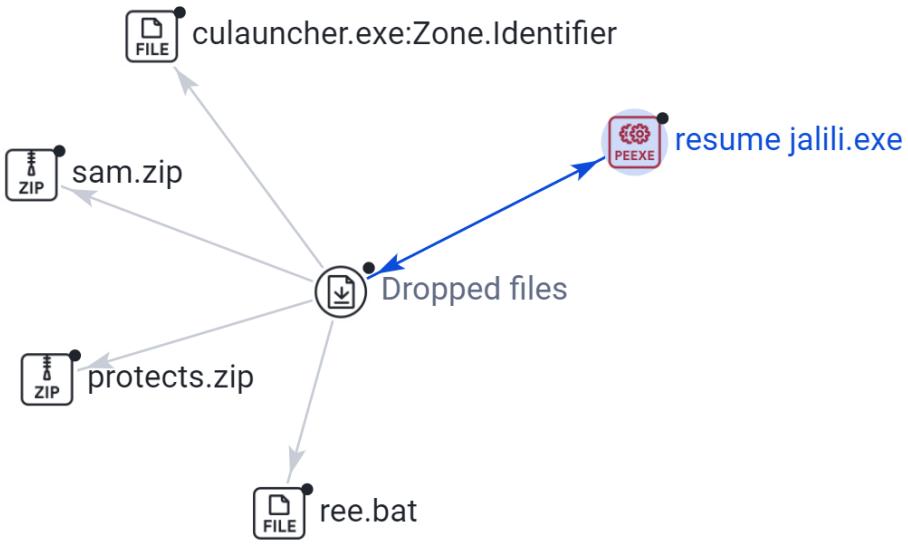
در این گزارش، به تحلیل عملکرد یکی از نمونه‌های اخیر بدافزار Trojan.MSIL/ClipBanker پرداخته شده است.

روش انتشار این بدافزار، ایمیل‌های حاوی لینک یا پیوست مخرب است. استفاده از اسامی ایرانی در نامگذاری فایل‌های مخرب، نشان‌دهنده آن است که کاربران ایرانی از اهداف اصلی این نمونه اخیر محسوب می‌شوند.

هدف این نمونه از بدافزار Trojan.MSIL/ClipBanker ، جمع‌آوری نام‌های کاربری و رمزهای عبور ذخیره‌شده در مرورگرهای Chrome و Opera است.

روش ارتباطی این بدافزار با گردانندگان آن، پودمان SMTP و سرویس ایمیل Gmail است.

استفاده از ضدویروس قدرتمند و اطمنیان از به‌روز بودن مستمر آن، بکارگیری محصولات ضدهرزنامه و همچنین آگاهی‌بخشی به کاربران در پرهیز از اجرای فایل‌های مشکوک، اصلی‌ترین راهکار در مقابله با این بدافزارها و تهدیدات مشابه محسوب می‌شود.

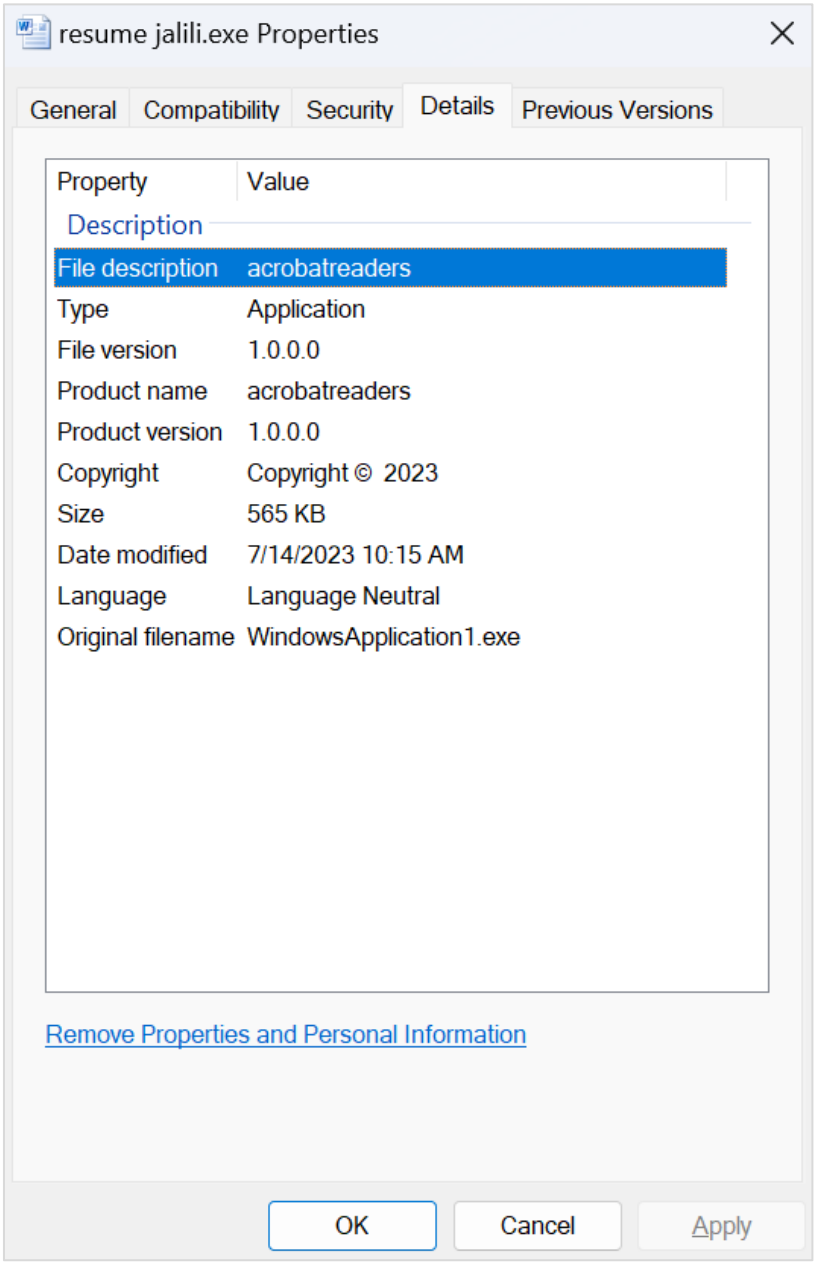


فهرست مطالب

مشخصات فایل

جدول زیر، مشخصات فایل مخرب این بدافزار را نمایش می‌دهد.

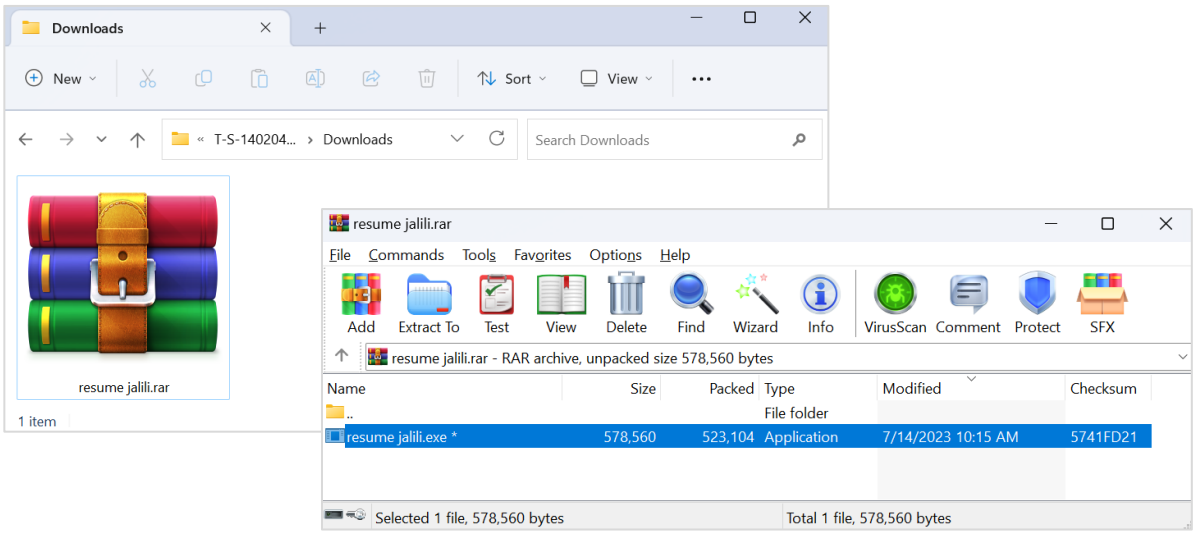
نام اصلی	WindowsApplication1.exe
نام در جریان حمله	resume jalili.exe
درهم‌ساز MD1	e32f9229d7d6ec11ba192f0ec1535752
درهم‌ساز SHA-1	28614906f5914ab21df0f22d7242ad97ed3836e4
درهم‌ساز SHA-256	2ccd01ec8b514294f7a90e491281bf0ba2c4deaea93e36c409fbcfbec10fef0b
نوع	Win32 EXE
اندازه	۵۶۵ کیلوبایت (۵۷۸۵۶۰ بایت)
زبان برنامه‌نویسی	Visual Basic .NET
تاریخ ایجاد	2023-06-08 17:47:46 UTC
نسخه	1.0.0.0
شرح در File Version	acrobatreaders
کپی‌رایت	Copyright © 2023
امضا	فاقد امضا


resume jalili.exe Properties
General
Compatibility
Security
Details
Previous Versions
Property
Value
Description
File description
acrobatreaders
Type
Application
File version
1.0.0.0
Product name
acrobatreaders
Product version
1.0.0.0
Copyright
Copyright © 2023
Size
565 KB
Date modified
7/14/2023 10:15 AM
Language
Language Neutral
Original filename
WindowsApplication1.exe
Remove Properties and Personal Information
OK
Cancel
Apply

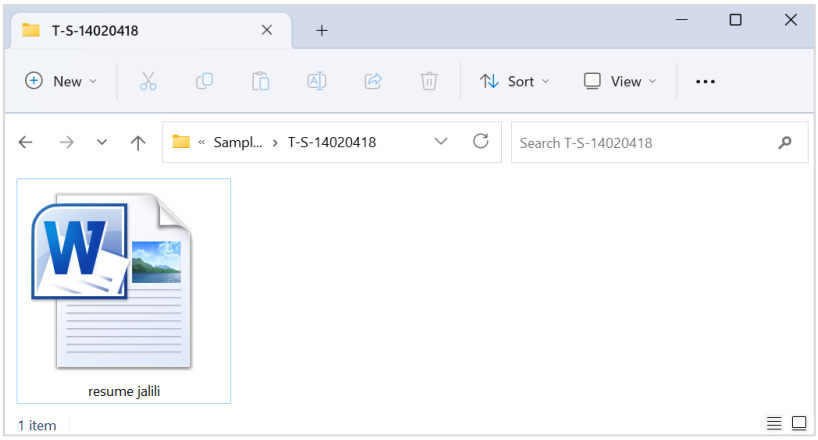
روش انتشار

اصلی‌ترین روش انتشار این بدافزار، ایمیل حاوی لینکی است که کلیک بر روی آن، کاربر را به دانلود یک فایل با پسوند RAR هدایت می‌کند.

برای باز کردن فایل RAR مذکور، کاربر باید رمزی را که در ایمیل به آن اشاره شده وارد کند.

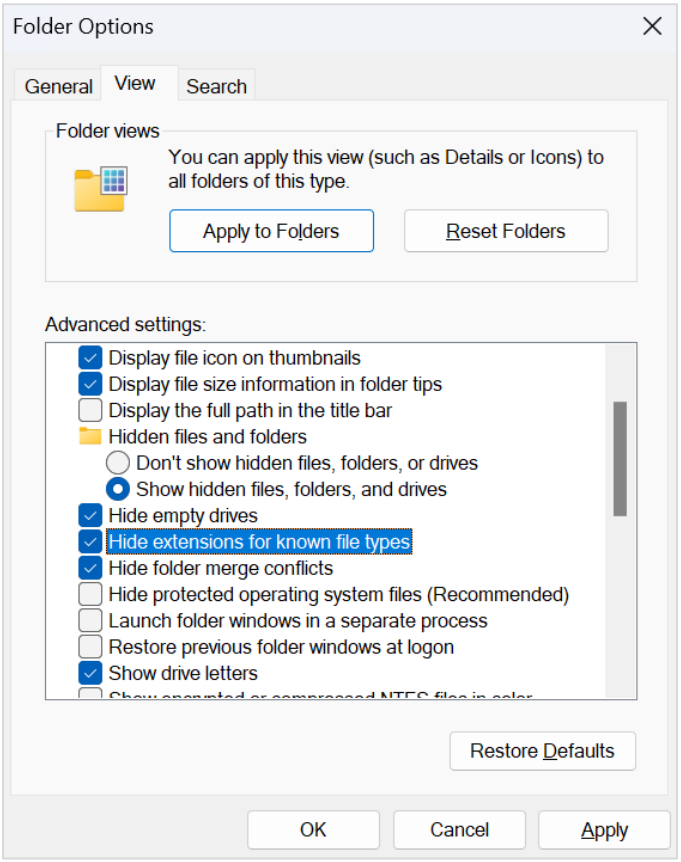


علاوه بر عنوان فریبنده فایل، فایل اجرایی درون فایل RAR دارای آیکونی مشابه با آیکون برنامه Word است. بنابراین آن چه که کاربر پس از باز کردن فایل RAR با آن مواجه می‌شود، در ظاهر، یک فایل Word است.



در صورت اجرای فایل توسط قربانی، دستگاه به بدافزار خواهد شد.

به‌صورت پیش‌فرض در سیستم عامل Windows، پسوند فایل‌های شناخته‌شده و متعارف از دید کاربر مخفی می‌مانند. غیرفعال کردن گزینه Hide extension for known file types در تنظیمات Folder Options، می‌تواند موجب نمایش پسوند تمامی فایل‌ها و در نتیجه کم اثر شدن تکنیک مخفی‌سازی فایل‌های اجرایی در پس آیکون برنامه‌های غیراجرایی می‌شود.



سازوکار ماندرگاری

بدافزار، جهت ماندگار کردن خود بر روی سیستم، رونوشتی از فایل مخرب را در پوشه Startup کپی می‌کند.

%Profile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\resume_jalili

بدین‌ترتیب، فایل مخرب، در هر بار راه‌اندازی سیستم به صورت خودکار و بدون نیاز به دخالت کابر اجرا می‌شود.

جاسوسی

این بدافزار به منظور دستیابی به اطلاعات حساس در مرورگرهای Chrome و Opera اقدام به استخراج کوکی‌های ذخیره‌شده در مسیرهای زیر می‌کند:

%Profile%\AppData\Local\Google\Chrome\User Data\Default
%Profile%\AppData\Roaming\Opera Software\Opera Stable

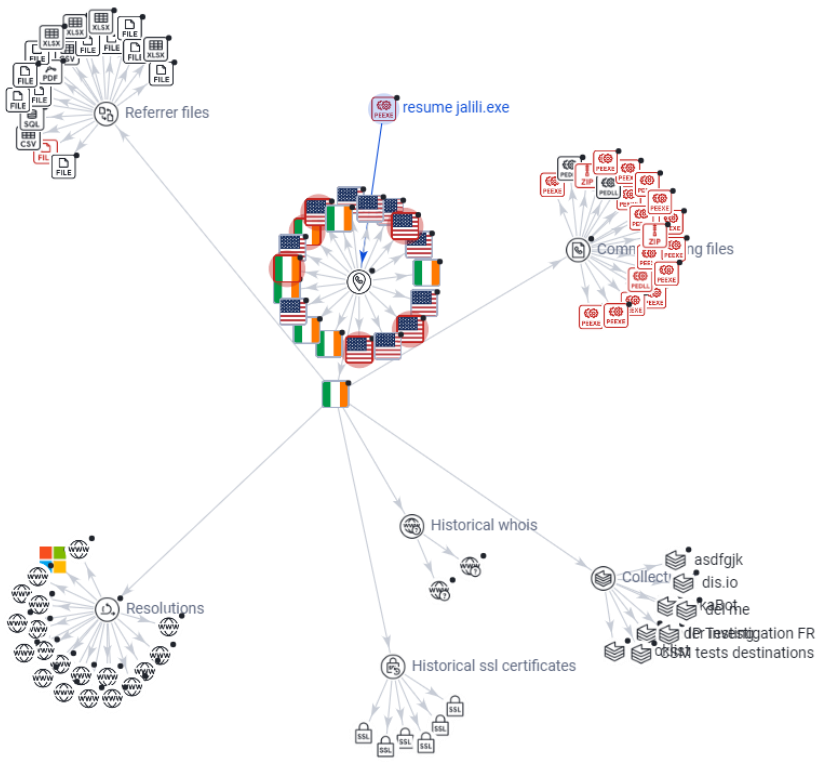
ارتباطات

روش ارتباطی این بدافزار با گردانندگان آن، پودمان SMTP و سرویس ایمیل Gmail (نشانی‌های زیر) است.

smtp.gmail.com:465
smtp.gmail.com:587

همچنین در جریان اجرا، با نشانی‌های IP زیر نیز ارتباط برقرار می‌شود:

20.99.133.109	142.250.145.108
20.99.184.37	142.250.145.109
20.99.186.246	172.253.117.108
23.216.147.64	172.253.63.108
23.223.246.81	192.229.211.108
40.126.31.69	20.190.159.2
40.126.31.71	20.190.159.23
40.126.31.73	20.190.159.68
74.125.135.109	20.190.159.71
74.125.20.109	20.190.159.73
8.8.8.8	20.69.140.28



فایل‌های ایجادشده

در حین اجرا، فایل‌های زیر بر روی دستگاه قربانی ایجاد می‌شود:

- C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\resume_jalili
- C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\resume_jalili:Zone.Identifier
- C:\Users\user\AppData\Roaming\Microsoft\protects.zip
- C:\file\ree.bat
- C:\file\sam.zip
- %USERPROFILE%\AppData\Local\acrobatreaders
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_fzixunshwohls4hn1ikw5bezk1lcmlpy
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_fzixunshwohls4hn1ikw5bezk1lcmlpy\1.0.0.0
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_fzixunshwohls4hn1ikw5bezk1lcmlpy\1.0.0.0\xpxotobl.newcfg
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_fzixunshwohls4hn1ikw5bezk1lcmlpy\1.0.0.0\xpxotobl.tmp
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_l5fdzk2usqtz1bsnwe3z2q0mmtmi1dk0
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_l5fdzk2usqtz1bsnwe3z2q0mmtmi1dk0\1.0.0.0
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_l5fdzk2usqtz1bsnwe3z2q0mmtmi1dk0\1.0.0.0\5gjqpe1g.newcfg
- %USERPROFILE%\AppData\Local\acrobatreaders\2ccd01ec8b514294f7a90e491_Url_l5fdzk2usqtz1bsnwe3z2q0mmtmi1dk0\1.0.0.0\5gjqpe1g.tmp
- %USERPROFILE%\AppData\Local\acrobatreaders\resume_jalili.exe_Url_poxth0ga35wf4cocpfrod3cvbwo54x5c
- %USERPROFILE%\AppData\Local\acrobatreaders\resume_jalili.exe_Url_poxth0ga35wf4cocpfrod3cvbwo54x5c\1.0.0.0
- %USERPROFILE%\AppData\Local\acrobatreaders\resume_jalili.exe_Url_poxth0ga35wf4cocpfrod3cvbwo54x5c\1.0.0.0\f14b5np5.newcfg
- %USERPROFILE%\AppData\Local\acrobatreaders\resume_jalili.exe_Url_poxth0ga35wf4cocpfrod3cvbwo54x5c\1.0.0.0\f14b5np5.tmp
- %USERPROFILE%\AppData\Roaming\Microsoft\protects.zip
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER10F3.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER10F3.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER11ED.tmp

- C:\ProgramData\Microsoft\Windows\WER\Temp\WER11ED.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER11FD.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER11FD.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER120D.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER120D.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER126C.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER126C.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER126D.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER126D.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DB4.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DB4.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F3B.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F3B.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7A.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7A.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER4001.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER4001.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER40DC.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER40DC.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER411C.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER411C.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER43F9.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER43F9.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER441A.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER441A.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER442B.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER442B.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER468A.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER468A.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER469B.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER469B.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER469C.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER469C.tmp.txt
- C:\Users\<USER>\AppData\Roaming\Microsoft\protects.zip
- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_cco0gvbemn4phdkvjgifanpii0j4bz3x\1.0.0.0\0v4wm3mw.newcfg
- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_cco0gvbemn4phdkvjgifanpii0j4bz3x\1.0.0.0\rtmnivkx.newcfg

- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_cco0gvbemn4phdkvjgifanpii0j4bz3x\1.0.0.0\user.config (copy)
- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_s3hpnk4px334jhazs53bnttee44d5x3j\1.0.0.0\ruvw2aof.newcfg
- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_s3hpnk4px334jhazs53bnttee44d5x3j\1.0.0.0\user.config (copy)
- C:\Users\user\AppData\Local\acrobatreaders\resume_jalili_Url_s3hpnk4px334jhazs53bnttee44d5x3j\1.0.0.0\yw4toloc.newcfg
- C:\Windows\System32\spp\store\2.0\cache\cache.dat
- C:\Windows\System32\spp\store\2.0\data.dat.tmp

تاکتیک‌ها و تکنیک‌ها

به طور کلی، این بدافزار از تاکتیک‌ها و تکنیک‌های زیر – بر طبق چارچوب MITRE – بهره می‌گیرد:

Execution

- T1059 Command and Scripting Interpreter
- T1064 Scripting

Persistence

- T1547.001 Registry Run Keys / Startup Folder
- T1542.003 Bootkit
- T1574.002 DLL Side-Loading

Privilege Escalation

- T1055 Process Injection
- T1547.001 Registry Run Keys / Startup Folder
- T1574.002 DLL Side-Loading

Defense Evasion

- T1036 Masquerading
- T1112 Modify Registry
- T1562.001 Disable or Modify Tools
- T1497 Virtualization/Sandbox Evasion
- T1055 Process Injection
- T1064 Scripting
- T1027 Obfuscated Files or Information
- T1542.003 Bootkit
- T1027.002 Software Packing
- T1574.002 DLL Side-Loading

Credential Access

- T1003 OS Credential Dumping
- T1056 Input Capture

Discovery

- T1518.001 Security Software Discovery
- T1057 Process Discovery
- T1497 Virtualization/Sandbox Evasion
- T1018 Remote System Discovery
- T1083 File and Directory Discovery
- T1082 System Information Discovery

Collection

- T1056 Input Capture
- T1005 Data from Local System
- T1115 Clipboard Data

Command and Control

- T1571 Non-Standard Port
- T1095 Non-Application Layer Protocol
- T1071 Application Layer Protocol

درباره شرکت مهندسی شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس شد. این شرکت یکی از باسابقه‌ترین شرکت‌های فعال در حوزه امنیت فناوری اطلاعات است. با بیش از سه‌دهه تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگ‌ترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیواره آتش در کشور بوده است.

شرکت مهندسی شبکه گستر، از ابتدای تأسیس، گواهینامه احراز صلاحیت و طبقه‌بندی از شـورای عالی انفورماتیک کشور را کسب کرده است. با حفظ استانداردهای مورد لزوم و افزایش سوابق و فعالیت‌ها، علاوه بر ارتقاء رتبه این شرکت در طبقه‌بندی شورایعالی انفورماتیک، تعداد بخش‌های تخصصی که شرکت مهندسی شبکه گستر مجاز به فعالیت در آن‌ها می‌باشد نیز افزایش یافته است.

همچنین شرکت مهندسی شبکه گستر دارای پروانه فعالیت از مرکز راهبردی افتای ریاست جمهوری و سازمان فناوری اطلاعات در حوزه ارائه خدمات فنی افتا می‌باشد.

این شرکت، همکاری نزدیکی با مرکز راهبردی افتای ریاست جمهوری در تهیه اخبار و هشدارهای امنیتی در حوزه فناوری اطلاعات دارد.

تهران، خیابان شهید دستگردی (ظفر)، بین خیابان آفریقا و خیابان ولیعصر شماره ۲۷۳، طبقه اول شرقی

تارنما	www.shabakeh.net
اتاق خبـر	newsroom.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net