Die erste Ransomware in JavaScript: Ransom32

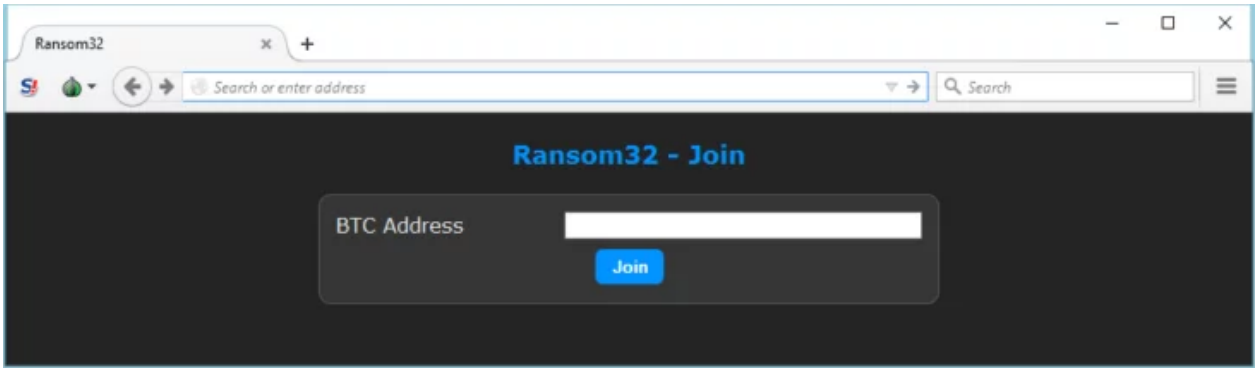
blog.emsisoft.com/de/21077/meet-ransom32-the-first-javascript-ransomware/

Sarah January 1, 2016

Software as a service (Software als Dienstleistung) – kurz SaaS – ist ein relativ neues Geschäftsmodell, dem sich viele Softwareanbieter heutzutage mit großem Erfolg bedienen. Daher dürfte es nicht überraschen, dass Malware-Programmierer und andere digitale Strauchdiebe das Modell auch für ihre gemeinen Zwecke einsetzen wollen. Im vergangenen Jahr erschienen mit Tox, Fakben oder Radamant bereits etliche dieser „Ransomware as a Service"-Kampagnen auf der Bildfläche. Heute möchten wir Sie über die neueste Aktion informieren.

Hier kommt Ransom32

Auf den ersten Blick ist Ransom32 eine Malware-Kampagne wie jede andere. Die Anmeldung erfolgt über einen im Tor-Netzwerk versteckten Server. Dazu muss lediglich eine Bitcoin-Adresse eingegeben werden, an die alle von der Ransomware erpressten Lösegelder gesendet werden sollen.



Für eine persönliche Ransomware wird nur eine Bitcoin-Adresse benötigt, an die die „Einnahmen“ gesendet werden sollen.

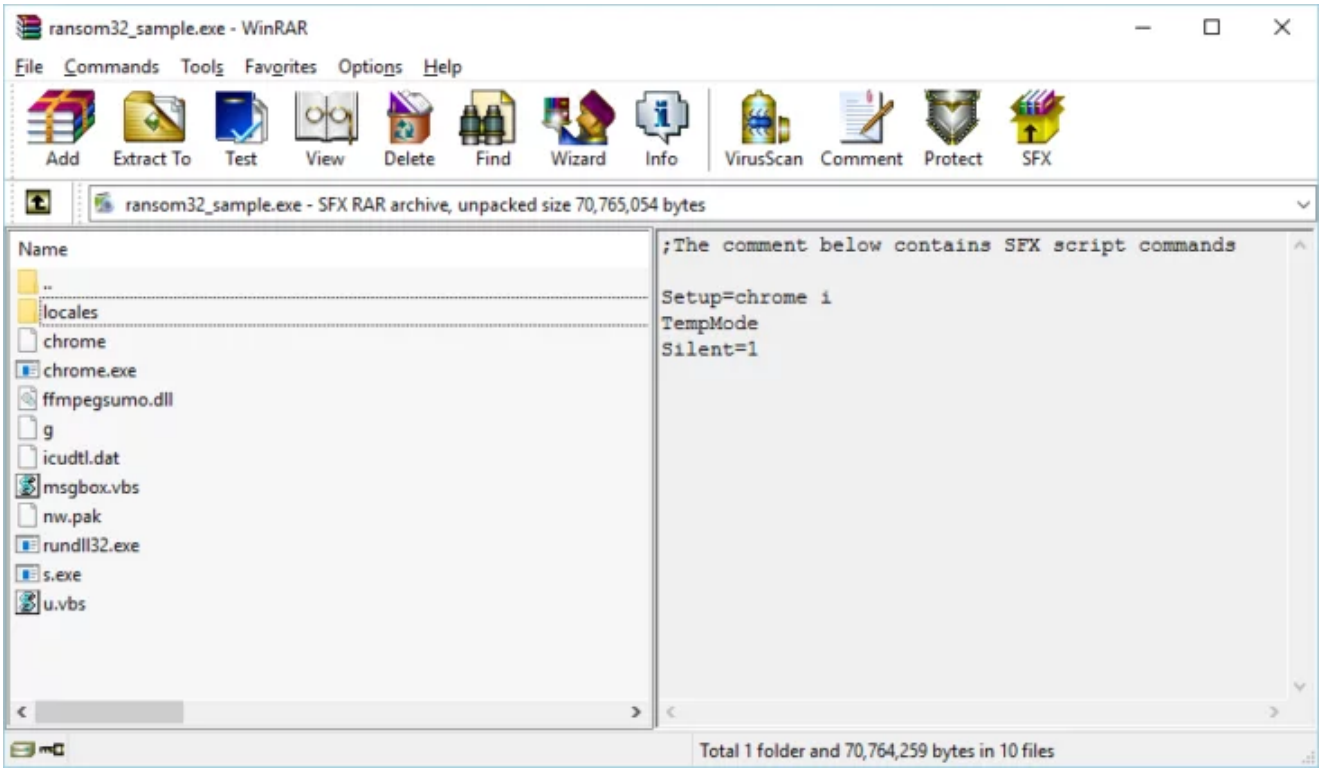
Nachdem die Bitcoin-Adresse abgeschickt wurde, erhalten die Benutzer Zugriff auf einen grundlegenden Verwaltungsbereich. Hier werden verschiedene Statistiken angezeigt, etwa wie viele Systeme infiziert sind und wie viele Personen bereits gezahlt haben. Außerdem kann der „Client“ – so wird die eigentliche Malware von den Kampagnengründern genannt – konfiguriert werden. Es lassen sich beispielsweise der Bitcoin-Betrag ändern, den die Malware fordert, und weitere Parameter konfigurieren, beispielsweise beim Installieren der Malware zur Täuschung angezeigte Meldungen.

Über eine Weboberfläche kann die Malware angepasst werden und der Benutzer erhält einen Überblick, wie viele Systeme infiziert und wie viele Bitcoins eingenommen wurden.

Mit dem Klick auf „Download client.scr“ wird die Malware entsprechend der vorgenommenen Einstellungen erzeugt und die 22 MB große Client-Datei heruntergeladen. Spätestens jetzt wird klar, dass Ransom32 keine typische Ransomware ist. Deren Dateien sind in der Regel selten größer als 1 MB. Einige Ransomware-Programmierer werben sogar mit den kleinen Dateigrößen ihrer tückischen Produkte, wenn sie ihre Kampagnen in den illegalen Hackerforen anpreisen. Ransom32 hatte unser Interesse geweckt.

Der Gigant im Detail

Nach näherer Untersuchung entpuppte sich die heruntergeladene Datei als ein selbstentpackendes WinRAR-Archiv.

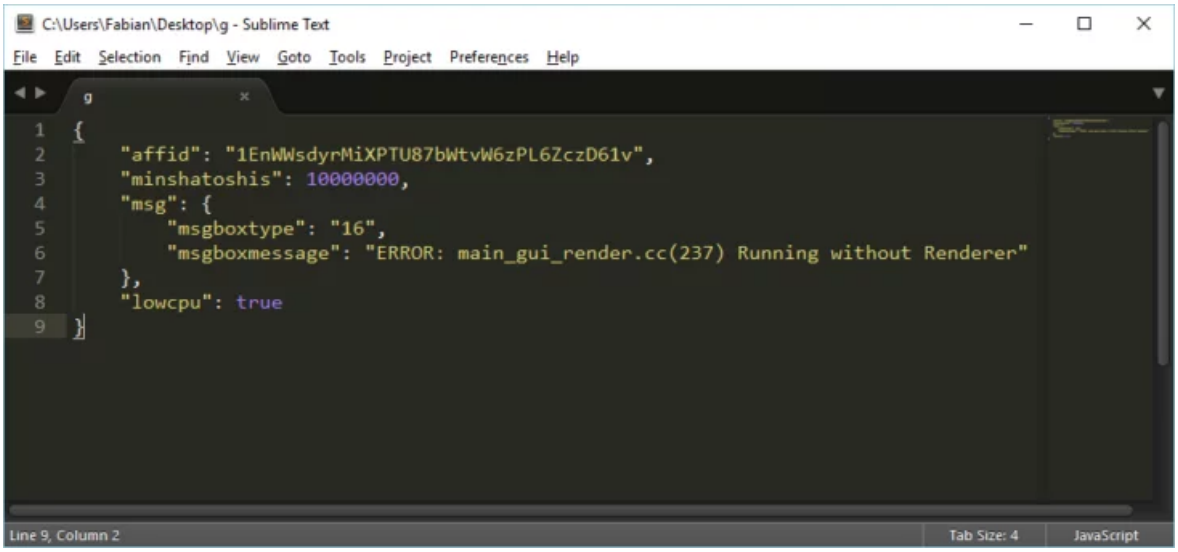


Der Inhalt des SFX-Archivs.

Die Malware nutzt die in WinRAR integrierte Scriptsprache, um ihren Inhalt automatisch in den temporären Ordner des Benutzers zu entpacken und die darin enthaltene Datei „chrome.exe“ auszuführen. Die Dateien in dem Archiv haben folgende Zwecke:

- „chrome“ enthält eine Kopie der Lizenzvereinbarung für freie Software (GNU GPL).
- „chrome.exe“ ist eine gepackte NW.js-Anwendung. Sie enthält den eigentlichen Malware-Code und bildet den sogenannten Framework (also das Gerüst) zum Ausführen der Malware.
- „ffmpegsumo.dll“, „nw.pak“, „icudtl.dat“ und „locales“ enthalten die für den NW.js-Framework erforderlichen Daten.
- „rundll32.exe“ ist eine umbenannte Kopie des Tor-Clients.
- „s.exe“ ist eine umbenannte Kopie von Optimum X Shortcut. Mit dem Programm lassen sich Verknüpfungen auf dem Desktop und im Startmenü erstellen und ändern.
- „g“ enthält die Malware-Einstellungen, die über die Weboberfläche konfiguriert wurden.
- „msgbox.vbs“ ist ein kleines Script, über das die zuvor individuell angepasste Meldung angezeigt wird.

- „u.vbs“ ist ein kleines Script, das alle Dateien und Ordner in einem vorgegebenen Verzeichnis durchnummeriert und löscht.



Die Datei „g“ enthält die als JSON (ein Datenaustauschformat) formatierte Konfiguration der Malware.

Die interessanteste Datei in dem ganzen Paket ist die „chrome.exe“. Auf den ersten Blick sieht sie verdächtig wie eine Kopie des bekannten Browsers „Chrome“ aus. Die Fälschung verrät sich lediglich dadurch, dass sie keine eigene digitale Signatur hat und Versionsinformationen fehlen. Weitere Analysen enttarnen sie als eine gepackte NW.js-Anwendung.

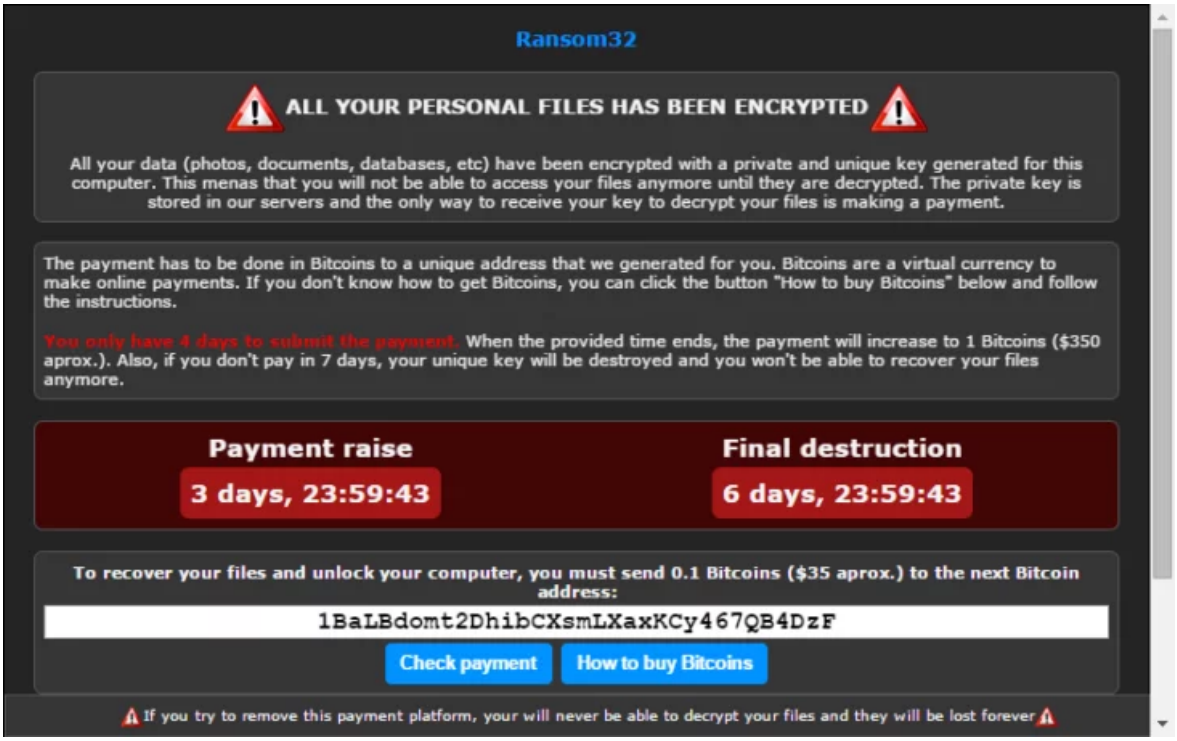
Moderne webbasierte Technologien und Ransomware

Was genau ist denn nun eine NW.js-Datei? Die NW.js ist im Wesentlichen das „Gerüst“, mit dem unter Verwendung von JavaScript normale Computeranwendungen für Windows, Linux und Mac OS X entwickelt werden. Als Basis dienen oftmals die Node.js– und Chromium-Projekte. JavaScript ist normalerweise auf den Browser beschränkt und hat keinen Zugriff auf das System, auf dem es ausgeführt wird. Die NW.js verfügt jedoch über wesentlich mehr Kontrolle und Berechtigungen in dem jeweiligen Betriebssystem. Dadurch wird JavaScript nahezu alles ermöglicht, was „normale“ Programmiersprachen wie C++ oder Delphi auch können. Für die Entwickler ist das natürlich ein großer Vorteil, weil sie aus ihren Anwendungen relativ leicht reguläre Computerprogramme machen können. Mit der NW.js lassen sich beispielsweise dieselben JavaScript-Codes auf unterschiedlichen Plattformen ausführen. Der Entwickler muss die Anwendung also nur einmal schreiben und kann sie dann unter Windows, Linux und Mac OS X einsetzen.

Das sollte bedeuten, dass sich Ransom32 auch leicht für Linux und Mac OS X packen lässt – zumindest in der Theorie. Bisher gibt es jedoch keine Hinweise auf derartige Pakete, sodass Ransom32 derzeit höchstwahrscheinlich allein unter Windows für Probleme sorgt. Ein großer Vorteil für die Malware-Programmierer ist die

Rechtmäßigkeit von NW.js-Frameworks und Anwendungen. Es ist also nicht verwunderlich, dass die Signatur-Erkennung noch immer unglaublich schlecht ist, obwohl die Malware bereits vor knapp 2 Wochen erstellt wurde.

Sobald Ransom32 auf ein System gelangt und ausgeführt wird, entpackt sie alle Dateien in den Ordner der temporären Dateien. Von hier kopiert sie sich in das Verzeichnis „%AppData%\Chrome Browser“. Mithilfe der enthaltenen „s.exe“ erstellt sie im Autostart/Startup-Ordner die Verknüpfung „ChromeService“, damit die Malware garantiert bei jedem Systemstart ausgeführt wird. Über den integrierten Tor-Client verbindet sie sich dann mit ihrem Befehls- und Steuerserver (C2-Server), der im Tor-Netzwerk versteckt auf Port 85 liegt. Von hier werden der zum Verschlüsseln verwendete Kryptografieschlüssel und die Bitcoin-Adresse abgerufen, an die das Lösegeld gehen soll. War die Verbindung zum C2-Server erfolgreich, wird von der Malware schließlich die Erpressermeldung angezeigt.



Die in der Malware angezeigte Erpressermeldung

Anschließend werden die Dateien des Benutzers verschlüsselt. Davon sind alle Dateien mit folgenden Endungen betroffen:

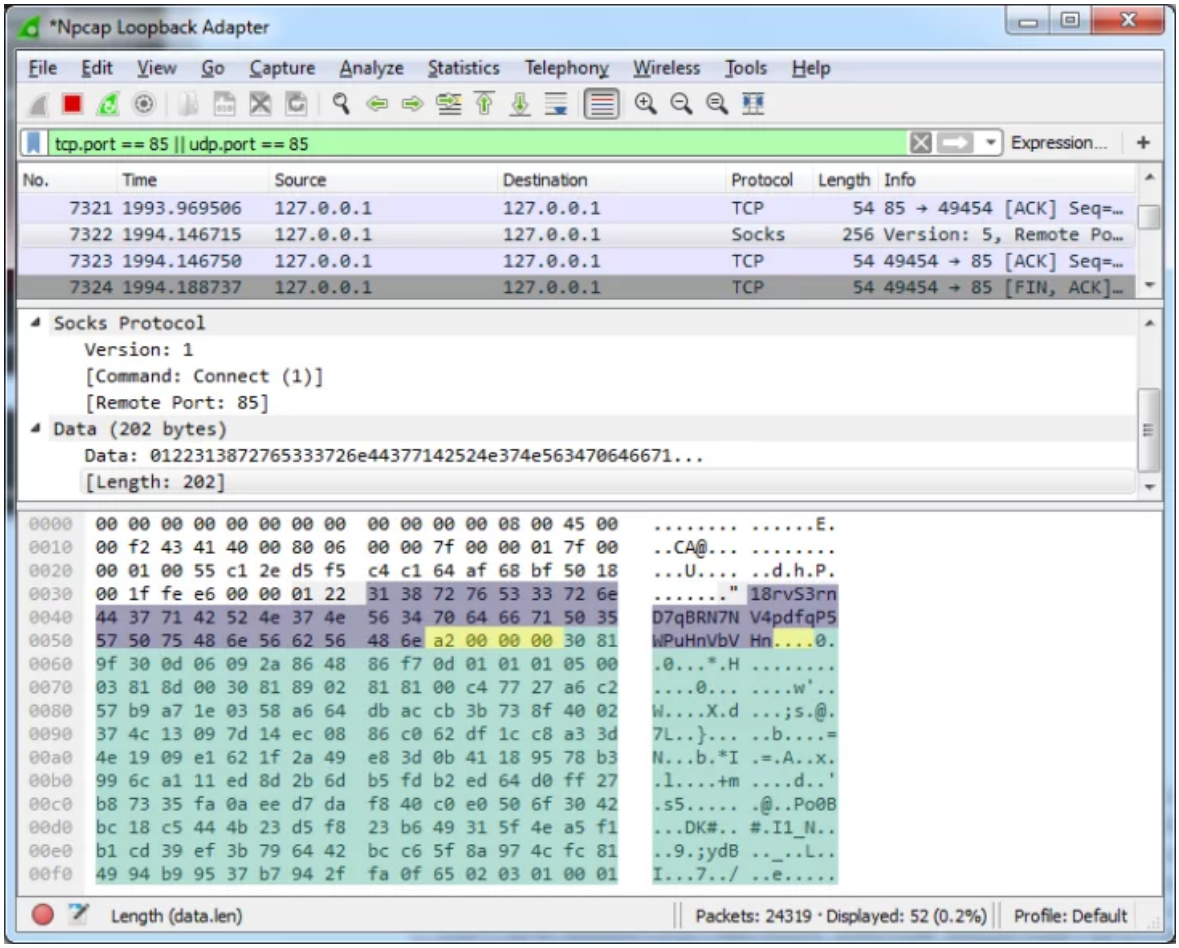
*.jpg, *.jpeg, *.raw, *.tif, *.gif, *.png, *.bmp, *.3dm, *.max, *.accdb, *.db, *.dbf, *.mdb, *.pdb, *.sql, *.*sav*, *.*spv*, *.*grle*, *.*mlx*, *.*sv5*, *.*game*, *.*slot*, *.dwg, *.dxf, *.c, *.cpp, *.cs, *.h, *.php, *.asp, *.rb, *.java, *.jar, *.class, *.aaf, *.aep, *.aepx, *.plb, *.prel, *.prproj, *.aet, *.ppj, *.psd, *.indd, *.indl, *.indt, *.indb, *.inx, *.idml, *.pmd, *.xqx, *.xqx, *.ai, *.eps, *.ps, *.svg, *.swf, *.fla, *.as3, *.as, *.txt, *.doc, *.dot, *.docx, *.docm, *.dotx, *.dotm, *.docb, *.rtf, *.wpd, *.wps, *.msg, *.pdf, *.xls, *.xlt, *.xlm, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xla, *.xlam, *.xll, *.xlw, *.ppt, *.pot, *.pps, *.pptx, *.pptm, *.potx, *.potm,

*.ppam, *.ppsx, *.ppsm, *.sldx, *.sldm, *.wav, *.mp3, *.aif, *.iff, *.m3u, *.m4u, *.mid, *.mpa, *.wma, *.ra, *.avi, *.mov, *.mp4, *.3gp, *.mpeg, *.3g2, *.asf, *.asx, *.flv, *.mpg, *.wmv, *.vob, *.m3u8, *.csv, *.efx, *.sdf, *.vcf, *.xml, *.ses, *.dat

Die Malware verschlüsselt jedoch keine Dateien in Verzeichnissen, die eine der folgenden Zeichenfolgen enthalten:

- :\windows\
- :\winnt\
- programdata\
- boot\
- temp\
- tmp\
- $recycle.bin\

Die Verschlüsselung erfolgt unter dem AES (Advanced Encryption Standard) als 128-Bit-Schlüssel mit der Betriebsart CTR. Für jede Datei wird ein neuer Schlüssel erstellt. Dieser wird wiederum mit dem RSA-Algorithmus und einem öffentlichen Schlüssel verschlüsselt, der bei der ersten Kommunikation mit dem C2-Server abgerufen wurde.



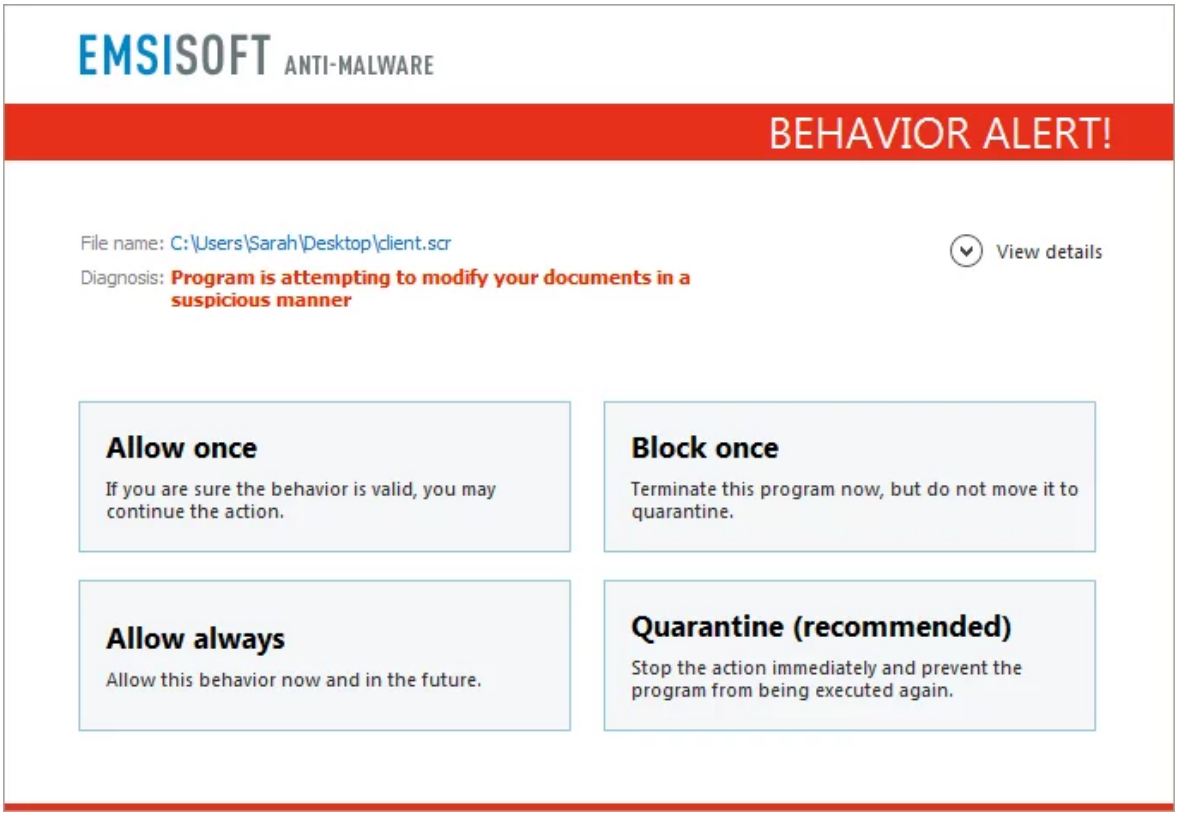
Auszug aus dem individuellen Protokollaustausch zwischen Ransom32 und dem C2-Server, um Bitcoin-Adresse (violett) und öffentlichen Schlüssel (Länge in Gelb, Schlüssel in Grün) abzurufen.

Der verschlüsselte AES-Schlüssel wird zusammen mit den AES-verschlüsselten Daten in der – jetzt ebenfalls verschlüsselten – Datei gespeichert.

Die Malware bietet auch an, eine einzelne Datei wieder zu entschlüsseln, um dem Opfer zu beweisen, dass der Malware-Entwickler die Verschlüsselung auch tatsächlich wieder aufheben kann. Dazu schickt sie den verschlüsselten AES-Schlüssel der gewählten Datei an den C2-Server, der dann den entschlüsselten AES-Schlüssel für die Datei zurücksendet.

Wie können Sie sich vor Ransom32 schützen?

Wie bereits in unserem letzten Artikel zu Ransomware erläutert, ist der beste Schutz eine gut organisierte Sicherungsstrategie. Als ein weiterer guter Schutz haben sich erneut die in Emsisoft Anti-Malware und Emsisoft Internet Security eingesetzten Technologien zur Verhaltensanalyse erwiesen. Damit sind alle unsere Benutzer vor dieser und Hunderten anderen Arten von Ransomware geschützt – unabhängig von Signaturen.



Users of Emsisoft Anti-Malware and Emsisoft Internet Security are protected from Ransom32 and other ransomware families by the behavior blocker

Benutzer von Emsisoft Anti-Malware und Emsisoft Internet Security sind durch die Verhaltensanalyse vor Ransom32 und anderen Ransomware-Familien geschützt.

Ransomware ist eine der größten Bedrohungen des vergangenen Jahres und wir werden auch 2016 unser Möglichstes tun, um unsere Benutzer wie bisher optimal zu schützen.

In diesem Sinne: Die Malware-Experten von Emsisoft wünschen Ihnen ein großartiges und malwarefreies neues Jahr.

Zu guter Letzt noch ein Wort des Dankes an unsere Freunde von BleepingComputer, die uns als Erste auf diese Bedrohung hingewiesen haben. Insbesondere xXToffeeXx von BleepingComputer sei in diesem Zusammenhang erwähnt. Sie hat uns mit ihren Beiträgen beim Analysieren und Rückentwickeln (Reverse Engineering) dieser Ransomware wertvolle Unterstützung geleistet.