NEWS ALERT

Panda Security analysiert neue Ransomware CryptoBit

Duisburg, den 22. April 2016 - PandaLabs, das Anti-Malware Labor von Panda Security in Spanien, hat eine neue Ransomware-Variante analysiert. Ihr Name: CryptoBit. Diese Cryptolocker-Variante kursiert seit einigen Tagen im World Wide Web und unterscheidet sich von anderer bisher bekannter Ransomware in einigen wichtigen Details, die wir im Folgenden erläutern.

ANALYSIERTES MUSTER

Dieser Bericht konzentriert sich auf die Analyse des folgenden Musters:

a67855dbd18652e99f13d29045b09391382bb8c817cda1e498cd01eb4a7bdf2c (sha256)

Dieses Muster ist durch einen „Packer" geschützt, der verhindert, dass eine Antivirensoftware es als einen Trojaner erkennt. Nach dem Entpacken konnten wir feststellen, dass es außer dem Datum der kürzlich erfolgten Kompilierung (5. April 2016 um 12:20:55 Uhr) keinerlei Strings gibt. Dies weist darauf hin, dass der Autor von CryptoBit mit allen Mitteln die Analyse des individuellen Schadcodes verhindern will.

VERBREITUNG

Nach der Analyse der Daten, die von Panda Securitys Collective Intelligence bereitgestellt wurden, ist es möglich, den Vektor zu bestimmen, der zur Verbreitung benutzt wurde: CryptoBit nutzt „Exploit Kits", die verschiedene Webbrowser betreffen.

VERHALTEN

Nach dem Entpacken des Musters und der Analyse seines Verhaltens konnten wir genauer bestimmen, wie CryptoBit grundlegend funktioniert:

```
void __noreturn start()
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  GetCommandLineW();
  GetModuleHandleA(0);
  // If the keyboard is whitelisted this block won't be executed
  // else, generate the AES key, decrypt some strings, set some
  // environment variables and launch some threads...
  if ( CHECK_KEYBOARD_GEN_AESKEY() )
  {
    INFECT_DRIVES_SHARES_AND_REMOVABLES();
    DESTROY_MEMORY_KEYS();
    v0 = DECRYPT_STRING(&byte_403577, 1);
    v1 = DECRYPT_STRING(dword_403EE4, 1);
    v2 = DECRYPT_STRING(&byte_401D0B, 1);
    INET_READFILE(v0, v1, v2);
    FREEHEAP(v2);
    FREEHEAP(v1);
    FREEHEAP(v0);
    v3 = GetModuleHandleW(0);
    SHOW_NAGSCREEN(v3, 0, 0, 1);
  }
  if ( dword_40601C )
    CloseHandle(dword_40601C);
  WaitForSingleObject(dword_406014, -1);
  CloseHandle(dword_406014);
  ExitProcess(0);
```

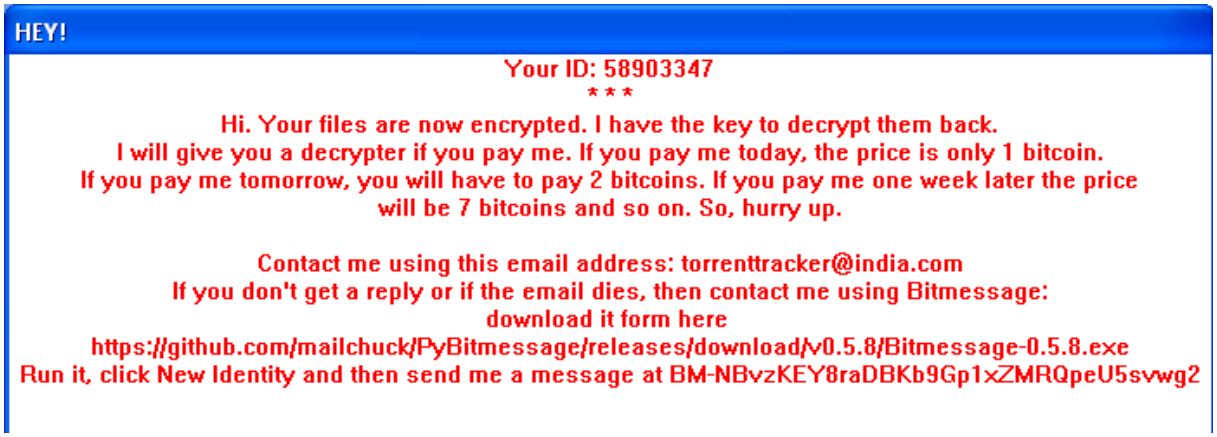
Zuerst überprüft CryptoBit die Sprach-Konfiguration der Tastatur. Wenn die Tastatur mit einem der folgenden Codes konfiguriert wurde: 0x1a7, 0x419 (Russisch) oder 0x43f (Kasachisch), verschlüsselt das Programm keine Dateien.

Nachdem sich CryptoBit versichert hat, dass die Tastatur nicht auf seiner Blacklist steht, überprüft es alle lokalen Laufwerke, Netzwerkordner und USB-Laufwerke und sucht nach Dateien, die die gewünschten Endungen enthalten. Was ist das Ziel von CryptoBit? Den gesamten Inhalt der Dateien zu verschlüsseln, um später deren Rettung bzw. Entschlüsselung kostenpflichtig anzubieten.

CryptoBit ist speziell an den folgenden Dateiendungen interessiert:

ods crp arj tar raw xlsm prproj der 7zip bpw dxf ppj tib nbf dot pps dbf qif nsf ifx cdr pdb kdbx tbl docx qbw accdb eml pptx kdb p12 tax xls pgp rar xml sql 4dd iso max ofx sdf dwg idx rtf dotx saj gdb wdb pfx docm dwk qba mpp 4db myo doc xlsx ppt gpg gho sdc odp psw psd cer mpd qbb dwfx dbx mdb crt sko nba jpg nv2 mdf ksd qbo key pdf aes 3ds qfx ppsx sxc gxk aep odt odb dotm accdt fdb csv txt zip

Wenn der Verschlüsselungsprozess begonnen hat, wird dem Anwender ein Fenster angezeigt, das dem hier abgebildeten ähnlich ist:



In dieser Nachricht sehen wir einige Details, die genutzt werden können, um diesen neuen Typ von Ransomware zu klassifizieren:

ID wird angezeigt als „58903347“

Diese ID ist immer dieselbe. Es spielt keine Rolle, ob man diese Malware wiederholt ausführt oder auf verschiedenen Geräten. Dies deutet darauf hin, dass es sich hier nicht um eine Art Kundennummer oder Rechner-ID, sondern eher um eine Versionsnummer der Ransomware handelt.

Die Anzahl der Bitcoins, die Sie zahlen müssen

Häufig stehen die geforderten Bitcoin-Beträge fest oder haben ein Limit. In diesem neuen Fall haben wir es mit einer sich stetig erhöhenden Summe zu tun, je nachdem, wieviel Zeit das Opfer bis zur Zahlung verstreichen lässt.

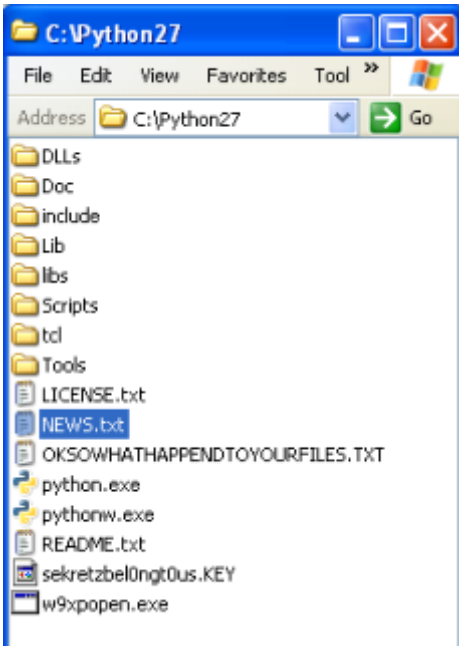
Wie Sie Kontakt zu den Hackern aufnehmen

Der Anwender kann den Hacker nicht über einen Webserver, auf den man über eine URL zugreifen kann, kontaktieren. Stattdessen wird der User aufgefordert, sich unter Verwendung einer bestimmten E-Mail-Adresse zu melden (hier: torrenttracker@india.com). Sollte das Opfer keine Antwort erhalten, so bietet der Autor die Möglichkeit, über eine Applikation namens „Bitmessage“ Kontakt aufzunehmen, ein Ableger einer anderen Anwendung, die in „GitHub“ zu finden ist.

Falls diese Nachricht nicht ausreicht, um die Opfer davon zu überzeugen, dass ihre Dateien verschlüsselt wurden, werden sie zudem jedes Mal, wenn sie auf einen Ordner zugreifen, der eine der verschlüsselten Dateien enthält, eine Reihe von zusätzlichen erstellten Dateien entdecken, zum Beispiel:

OKSOWATHAPPENDTOYOURFILES.TXT

Wenn wir uns diese Datei näher ansehen, finden wir hier dieselbe Nachricht (diesmal im Textformat), die dem Anwender nach der Verschlüsselung seiner Dateien angezeigt wird.



sekretzbel0ngt0us.KEY

In dieser zweiten Beispiel-Datei sehen wir eine hexadezimale Sequenz mit einer Länge von 1024 Zeichen, die nach dem Entschlüsseln einer Binärsequenz von 512 Bytes (oder 4096 Bits) entspricht.

Im verschlüsselten Bereich wird uns die Bedeutung der Datei mit dem Namen „**sekretzbel0ngt0us.KEY**“ gezeigt, wo die Verschlüsselung benutzt wurde, um andere Dateien zu verschlüsseln.

Eine weitere Aktion von CryptoBit, die für den Anwender sichtbar ist, ist eine HTTP-Anfrage, die wie folgt aussieht:

http://videodrome69.net/knock.php?id=58903347

Hinweis: Das angeforderte Skript „knock.php“ existiert nicht. Was es tut, ist, die Absichten der letzten Aktion zu ignorieren.

VERSCHLÜSSELUNG VON DATEIEN

Den Schlüssel verschlüsseln, der die Daten verschlüsselt – bei jedem Durchlauf nutzt CryptoBit den Algorithmus AES, oder „Advanced Encryption Standard“ (ein zufälliger Schlüssel mit einer Länge von 32 Bytes oder 256 Bits), der es praktisch unmöglich macht, Dateien zu entschlüsseln.

Damit der Schlüssel nicht verloren geht, der es uns im Fall der Lösegeldzahlung ermöglicht diese Dateien wieder zu entschlüsseln, speichert der Autor dieser Ransomware den generierten AES-Schlüssel mit einer Verschlüsselung, die den RSA-Algorithmus verwendet.

In dem von uns analysierten Exemplar hat ein öffentlicher Schlüssel, der gewählt wurde, eine Länge von hartkodierten 4096 Bits. Nach der Verschlüsselung mit einem RSA AES Key wird er in den Dateien namens “*sekretzbel0ngt0us.KEY*“ gespeichert und ist nur mit entsprechenden RSA „Private Keys“zu dechiffrieren (die theoretisch nur im Besitz des Malware-Autors sein können).

In diesem Bereich stellen wir ein besonderes Detail fest: das Fehlen von Aufrufen der systemeigenen Bibliotheken, die Dateien mittels RSA-Algorithmus verschlüsseln. CryptoBit nutzt eine Reihe von statisch kompilierten Routinen, die es ihm ermöglichen, mit großen Zahlen („big numbers“) zu arbeiten. Dies wiederum ermöglicht es, den RSA-Verschlüsselungsalgorithmus zu reproduzieren.

CryptoBit wurde analysiert von: Alberto Mor, Abel Valero und Daniel Garcia

Pressekontakt:

Kristin Petersen
Presse & PR
PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de