DigiTask

Spezielle Kommunikationssysteme

DigiTask GmbH · Postfach 11 19 · D-35701 Haiger

Ihr Zeichen:
Ihre Nachricht vom:
Unser Zeichen: ap-bm
Telefon: 02773-747880
Name: Achim Pulverich
Datum: 11.10.2011

Analyse einer Regierungs-Malware

Sehr geehrte Damen und Herren,

hiermit bezieht die Firma DigiTask Stellung zu dem veröffentlichten Dokument des Chaos Computer Clubs „ Analyse einer Regierungs-Malware" vom 08.10.2011.

Die Firma DigiTask stellt den Behörden eine Software für die Realisierung einer Quellen-TKÜ zur Verfügung. Die Software wird nach den Vorgaben der Behörden kompiliert und enthält nur die Funktionalitäten die von der entsprechenden Behörde vorgegeben wurden. Weitere Funktionen können mit dieser Version nicht realisiert werden. Anpassungen und Updates können durch DigiTask nach Aufforderung bereitgestellt werden und von der Behörde installiert werden. Dies wird in der Recording Unit protokolliert und mit einer MD5 Prüfsumme versehen.

Updates können erforderlich sein bei Erweiterungen der Maßnahme (z.B. weitere Messenger) oder bei Updates des Betriebssystems und der eingesetzten Sicherheitssoftware.

Die vom Chaos Computer Club (im folgenden CCC genannt) veröffentlichte Software hat nach den momentanen Erkenntnissen einen Stand der bis November 2008 entwickelt wurde. Auf Kundenanlagen wurde dieser Stand bis April 2009 gepflegt.

DigiTask GmbH
Hüttenstr. 48
D-35708 Haiger

Telefon:
+49 (0) 2773-74788 0

Fax:
+49 (0) 2773-74788-60

E-Mail:
info@DigiTask.de

Geschäftsführer:
Achim Pulverich

AG Wetzlar:
HRB3177

USt/DNr.
DE812926032

Konto:
Sparkasse Dillenburg
BLZ: 516 500 45
Kto-Nr: 186700

Beim Inhalt des Dokumentes handelt es sich um vertrauliche Informationen. Jede unbefugte Vervielfältigung, Benutzung oder Bekanntmachung dieses Dokumentes, oder Teilen davon, ist strengstens untersagt. Dieses Dokument ist nur zur Nutzung für Mitarbeiter der Firma DigiTask und deren ermächtigten Kunden freigegeben. Änderungen, auch im Sinne des technischen Fortschritts, vorbehalten. © DigiTask GmbH

Aufbau

Ein symmetrischer AES Schlüssel wurde verwendet, um eine Datendekodierung in einer TKÜ-Anlage zu ermöglichen.
Seit der Version 1.4.4 vom 02.07.2010 kann ein AES Schlüssel global für eine Recording Unit vergeben werden. Die neuste aber noch nicht veröffentlichte Version ermöglicht es auch einen AES Schlüssel pro Maßnahme zu vergeben.
Wie der CCC bestätigte war der Trojaner nicht durch Antiviren-Software erkennbar.

Der CCC bestätigt des Weiteren dass nur das Anfertigen von Screenshots und das Abhören von VoIP Gesprächen inkl. Skype zum Umfang der Software gehörten.

Infektion

Die beiden aufgelisteten Dateinamen mfc42ul.dll und winsys32.sys werden im Moment noch genutzt. Dies könnte von Antiviren-Software erkannt werden und den Trojaner enttarnen. Hier wird für die Zukunft eine maßnahmen-spezifische Konfiguration möglich sein.

Der AppInit-DLLs Registry-Key wird in 32-Bit-Versionen seit August 2009 in der Regel nicht mehr verwendet. Dies ist eine fallspezifische Entscheidung die in Abstimmung mit den Behörden, nach Analyse des Zielsystems getroffen wird. Für 64-Bit-Versionen existiert eine Alternative dazu bei signierten Treibern.

Kommunikation mit Kommandozentrale

Es wird hier nicht nur der Explorer Prozess genutzt. Je nach Einstellung einer ggf. beim ZÜA vorhandener Personal-Firewall können auch andere Prozesse eingesetzt werden.

Die IP-Adresse des Hart-Codierten Control-Servers kann durch die Behörden jederzeit durch ein vorliegendes Tool geändert werden.

Verschlüsselung

Wie bereits erläutert sind die AES-Keys in den aktuellen Versionen jederzeit änderbar.

Die Daten vom ZÜA[1] zur RecUnit waren schon immer verschlüsselt. Der Rückkanal ist seit der RecUnit Version 1.3x und der Capture Unit Version 3.5x vom 08.01.2009 ebenfalls verschlüsselt.

Der Abgebildete String „C3PO-r2d2-POE" dient zur Authentifizierung des ZÜA gegenüber der Recording Unit. Dieser String hat nur die Bedeutung ZÜAs von zufälligen Zugriffen (Portscans auf Port443) zu unterscheiden.

DigiTask GmbH
Hüttenstr. 48
D-35708 Haiger

Telefon:
+49 (0) 2773-74788 0

Fax:
+49 (0) 2773-74788-60

E-Mail:
info@DigiTask.de

Geschäftsführer:
Achim Pulverich

AG Wetzlar:
HRB3177

USt/DNr.
DE812926032

Konto:
Sparkasse Dillenburg
BLZ: 516 500 45
Kto-Nr: 186700

[1] ZÜA = zu Überwachender Anschluss

Beim Inhalt des Dokumentes handelt es sich um vertrauliche Informationen. Jede unbefugte Vervielfältigung, Benutzung oder Bekanntmachung dieses Dokumentes, oder Teilen davon, ist strengstens untersagt. Dieses Dokument ist nur zur Nutzung für Mitarbeiter der Firma DigiTask und deren ermächtigten Kunden freigegeben. Änderungen, auch im Sinne des technischen Fortschritts, vorbehalten. © DigiTask GmbH

Zu den aufgeführten Angriffsszenarien:

Punkt 1: Ein Dritter müsste wissen dass dieser PC überwacht wird um eine solche Attacke zu fahren. Um dieses Wissen zu erlangen, braucht ein Angreifer zumindest Zugriff auf den Netzwerkverkehr des ZÜA. Das Unterschieben von falschen Beweisen kann z.B. über eine vorhandene DSL-Überwachung erkannt werden.

Punkt 2: Wenn individuelle AES-Keys verwendet werden und dadurch der Rückkanal verschlüsselt ist, ist dieses Szenario nicht mehr denkbar.

Punkt3: Hier würde ein Dritter darauf hoffen dass eine Quellen-TKÜ-Software auf dem anzugreifenden PC vorhanden ist um die Quellen-TKÜ Software für die Verbreitung seiner Installation zu nutzen. Wir halten dieses Beispiel für sehr weit her gegriffen, da die Quellen-TKÜ Software bekanntlich sehr selten eingesetzt wird.

Bewertung

Zur Bewertung des CCC geben wir keinen Kommentar ab.

Verbindungsaufbau und Datenstrukturen

Auf Seite 8 ist ersichtlich dass den Behörden nur die geforderten Funktionalitäten zur Verfügung gestanden haben.

Hintertür in der Hintertür

Es ist so, dass die Programme für die Behörden individuell fertiggestellt werden.
Jede Funktionalität ist wie beschrieben von den Behörden vorgegeben. Wie schon beschrieben, wird der Dateiname zurzeit noch nicht geändert, die Schlüssel können aber schon seit einiger Zeit geändert werden.

Natürlich muss eine Quellen-TKÜ Software die Möglichkeit besitzen, Updates durchführen zu können. Dies wurde in der Einleitung bereits erwähnt.

Die in der Technischen Analyse und Bewertung aufgeführte Verschleierung der CreateProcessA-Funktion dient wie auch festgestellt wurde, der Umgehung von Antiviren-Programmen.

In der Exploitation hat der CCC ein eigenes Programm geschrieben und hochgeladen.

Dies würde im Umkehrschluss bedeuten, dass die Behörden eigene nicht richterlich zugelassene Funktionen selbst schreiben und auf das ZÜA System laden. Dieser Vorwurf der Manipulation durch eine Sicherheitsbehörde ist technisch möglich, würde aber geloggt werden und mit einem MD5 Hash Wert versehen.

DigiTask GmbH
Hüttenstr. 48
D-35708 Haiger

Telefon:
+49 (0) 2773-74788 0

Fax:
+49 (0) 2773-74788-60

E-Mail:
info@DigiTask.de

Geschäftsführer:
Achim Pulverich

AG Wetzlar:
HRB3177

USt/DNr.
DE812926032

Konto:
Sparkasse Dillenburg
BLZ: 516 500 45
Kto-Nr: 186700

Beim Inhalt des Dokumentes handelt es sich um vertrauliche Informationen. Jede unbefugte Vervielfältigung, Benutzung oder Bekanntmachung dieses Dokumentes, oder Teilen davon, ist strengstens untersagt. Dieses Dokument ist nur zur Nutzung für Mitarbeiter der Firma DigiTask und deren ermächtigten Kunden freigegeben. Änderungen, auch im Sinne des technischen Fortschritts, vorbehalten. © DigiTask GmbH

Audio-Aufzeichnung

Der Code zum Abgreifen des Mikrophones dient nur der Quellen-TKÜ. Auch vom CCC wurde keine Möglichkeit gefunden Ihn anderweitig zu aktivieren.

Windows Kernel Treiber

Die Analyse des Kernel Treibers ist weitgehend korrekt. Der CCC bestätigt auch hier, dass nichtzugelassene Funktionen (Keylogger) nicht aktiviert werden können.

Fazit

Die Quellen-TKÜ Software der Firma DigiTask ist ein ständig gepflegtes Produkt das in einer fast drei Jahre alten Version untersucht wurde. Die Firma DigiTask ist ständig dabei die Software auf die aktuellen Anforderungen und Sicherheitsstandards anzupassen. Ein Großteil der bemängelten Sicherheitslücken ist in den aktuellen Versionen wie beschrieben schon behoben. Individuelle Versionen können auf Wunsch schon länger durch Code-Obfuszierung erstellt werden. Für die gegenseitige Authentifizierung arbeitet die Firma DigiTask derzeitig an einem Konzept.

Mit freundlichen Grüßen

Achim Pulverich

DigiTask GmbH

DigiTask GmbH
Hüttenstr. 48
D-35708 Haiger

Telefon:
+49 (0) 2773-74788 0

Fax:
+49 (0) 2773-74788-60

E-Mail:
info@DigiTask.de

Geschäftsführer:
Achim Pulverich

AG Wetzlar:
HRB3177

USt/DNr.
DE812926032

Konto:
Sparkasse Dillenburg
BLZ: 516 500 45
Kto-Nr: 186700

Beim Inhalt des Dokumentes handelt es sich um vertrauliche Informationen. Jede unbefugte Vervielfältigung, Benutzung oder Bekanntmachung dieses Dokumentes, oder Teilen davon, ist strengstens untersagt. Dieses Dokument ist nur zur Nutzung für Mitarbeiter der Firma DigiTask und deren ermächtigten Kunden freigegeben. Änderungen, auch im Sinne des technischen Fortschritts, vorbehalten. © DigiTask GmbH