## Beta Bot attackiert Antivirenprogramme

*G Data Kunden sind vor dem gefährlichen Schädling geschützt*

(ddp direct) Bots gehören zum Standardrepertoire von Cyberkriminellen, wenn es darum geht DoS-Attacken zu starten, millionenfache Spam-Kampagnen durchzuführen oder Daten zu stehlen. Die G Data SecurityLabs haben in einem speziellen eCrime-Untergrund Markt jetzt einen speziellen Bot entdeckt, der Antivirenprogramme attackiert um diese auszuschalten. Dabei unterbindet der ?Beta Bot? u.a. die Auto-Update-Funktion der auf dem infizierten Computer installierten Security Software und versucht die Firewall mit manipulierten Programmen zu umgehen. Das Schadprogramm ist so in der Lage, die Schutzmechanismen außer Kraft zu setzen um beliebige Schädlinge auf dem infizierten PC einzuschleusen um beispielsweise Kreditkartendaten zu stehlen. G Data Kunden sind vor dem gefährlichen Schädling geschützt, die Security-Lösungen des deutschen IT-Security-Herstellers lassen sich nicht deaktivieren.

Wie wird der Bot auf dem infizierten PC aktiv?
Gelangt der Beta Bot auf den Computer, versucht das Schadprogramm an erweiterte Windows-Benutzerrechte zu gelangen um die Schadfunktionen auszuführen und das installierte Antivirenprogramm auszuschalten. Dem Nutzer wird hierzu ein angeblich kritischer Festplattenfehler oder einen Meldung über beschädigte Dateien im Ordner ?Eigene Dokumente? und gleichzeitig auch ein Lösungsweg zur Fehlerbeseitigung angezeigt. Möchte der Anwender das Problem lösen, wird er per sogenannten User Account Control-Dialog aufgefordert, Windows erweiterte Berechtigungen zu gewähren. Dann kann der Bot aktiv werden und die installierte Virenschutzlösung deaktivieren.

Um nicht nur deutschsprachige Nutzer anzugreifen, liefert der Beta Bot die Fehlermeldung und den UAC-Dialog u.a. auch auf Englisch, Spanisch, Französisch und Niederländisch aus.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/s5kh7i

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/wirtschaft/beta-bot-attackiert-antivirenprogramme-28261

=== Gefälschte Fehlermeldung durch den Beta Bot (Bild) ===

Bots gehören zum Standardrepertoire von Cyberkriminellen, wenn es darum geht DoS-Attacken zu starten, millionenfache Spam-Kampagnen durchzuführen oder Daten zu stehlen. Die G Data SecurityLabs haben in einem speziellen eCrime-Untergrund Markt jetzt einen speziellen Bot entdeckt, der Antivirenprogramme attackiert um diese auszuschalten. Dabei unterbindet der Beta Bot u.a. die Auto-Update-Funktion der auf dem infizierten Computer installierten Security Software und versucht die Firewall mit manipulierten Programmen zu umgehen. Das Schadprogramm ist so in der Lage, die Schutzmechanismen außer Kraft zu setzen um beliebige Schädlinge auf dem infizierten PC einzuschleusen um beispielsweise Kreditkartendaten zu stehlen. G Data Kunden sind vor dem gefährlichen Schädling geschützt, die Security-Lösungen des deutschen IT-Security-Herstellers lassen sich nicht deaktivieren.

Shortlink:
http://shortpr.com/tznnuh

Permanentlink:
http://www.themenportal.de/bilder/gefaelschte-fehlermeldung-durch-den-beta-bot

=== Beta Bot - Screenshot mit Anfrage auf Erweiterung der Berechtigungen (Bild) ===

Wie wird der Bot auf dem infizierten PC aktiv?
Gelangt der Beta Bot auf den Computer, versucht das Schadprogramm an erweiterte Windows-Benutzerrechte zu gelangen um die Schadfunktionen auszuführen und das installierte Antivirenprogramm auszuschalten. Dem Nutzer wird hierzu ein angeblich kritischer Festplattenfehler oder einen Meldung über beschädigte Dateien im Ordner Eigene Dokumente und gleichzeitig auch ein Lösungsweg zur Fehlerbeseitigung angezeigt. Möchte der Anwender das Problem lösen, wird er per sogenannten User Account Control-Dialog aufgefordert, Windows erweiterte Berechtigungen zu gewähren. Dann kann der Bot aktiv werden und die installierte Virenschutzlösung deaktivieren.

Um nicht nur deutschsprachige Nutzer anzugreifen, liefert der Beta Bot die Fehlermeldung und den UAC-Dialog u.a. auch auf Englisch, Spanisch, Französisch und Niederländisch aus.

Shortlink:
http://shortpr.com/bqoswt

Permanentlink:
http://www.themenportal.de/bilder/beta-bot-screenshot-mit-anfrage-auf-erweiterung-der-berechtigungen

### Pressekontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

presse@gdata.de

**Firmenkontakt**

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

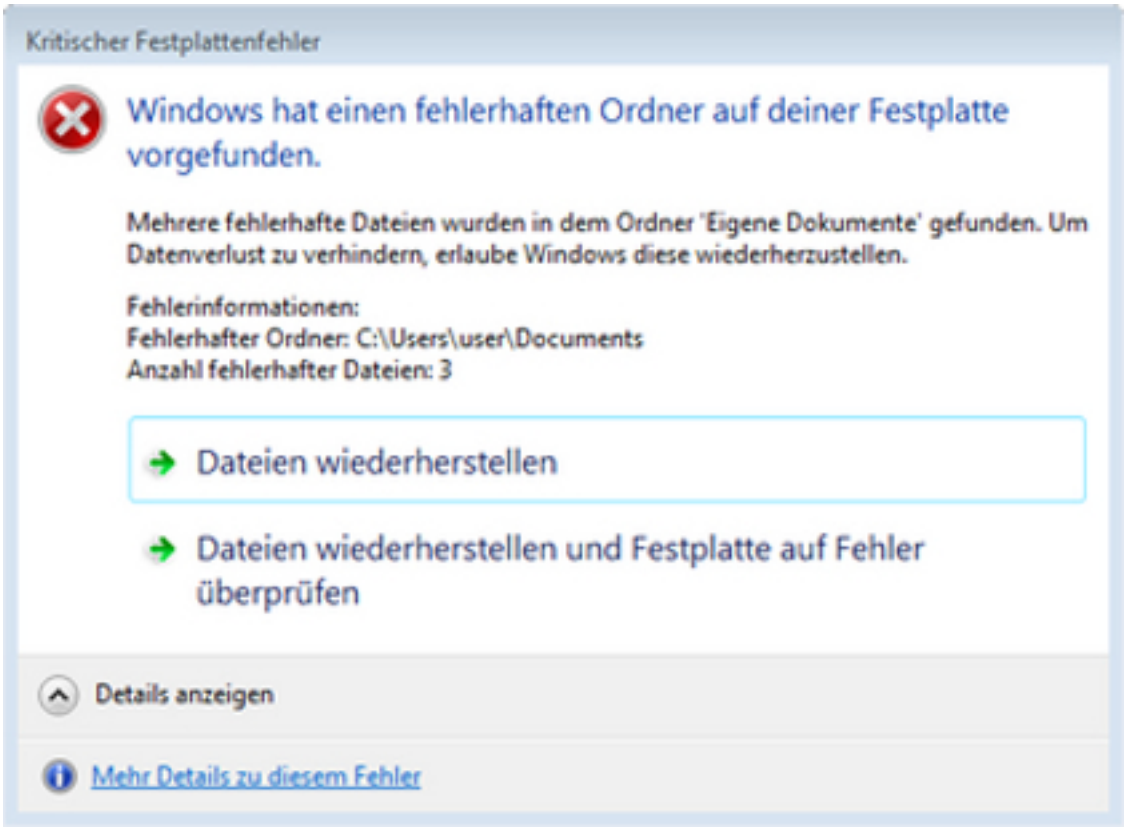
gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

**Anlage:** Bild


Kritischer Festplattenfehler
Windows hat einen fehlerhaften Ordner auf deiner Festplatte vorgefunden.
Mehrere fehlerhafte Dateien wurden in dem Ordner 'Eigene Dokumente' gefunden. Um Datenverlust zu verhindern, erlaube Windows diese wiederherzustellen.
Fehlerinformationen:
Fehlerhafter Ordner: C:\Users\user\Documents
Anzahl fehlerhafter Dateien: 3
Dateien wiederherstellen
Dateien wiederherstellen und Festplatte auf Fehler überprüfen
Details anzeigen
Mehr Details zu diesem Fehler