



Baden-Württemberg

LANDESKRIMINALAMT

Medieninfo



PRESSESTELLE LKA BW

TELEFON 0711 5401-2020 ODER -2021, FAX 0711 5401-2025

E-MAIL PRESSESTELLE@LKA.BWL.DE, INTERNET WWW.LKA-BW.DE

Stuttgart/Offenburg 4. März 2009

Gemeinsame Pressemitteilung von Staatsanwaltschaft Offenburg und Landeskriminalamt Baden-Württemberg:

Schlag gegen Internethacker: Internetermittler des Landeskriminalamts Baden-Württemberg (LKA) nehmen Hackerforum vom Netz

Das bekannte und große deutschsprachige Hackerforum - **www.codesoft.cc** - wurde auf Initiative der Internetermittler des LKA vom Netz genommen. Auf dieser Internetplattform wurde unter anderem Schadsoftware beworben und auch verkauft. In den Foren konnte man nahezu alles über Hacking, das Ausspähen von Daten und das Fälschen von Kreditkarten erfahren. Ausgespähte Kreditkartendaten sollen auf dem Forum ebenfalls angeboten worden sein.

Als Administrator und Betreiber des Hackerforums fungierte ein 22-jähriger Schweizer aus dem Kanton Luzern/Schweiz. Der Informatiker entwickelte die Schadsoftware – Codesoft PW Stealer 0.5 – die er unter dem Nicknamen „tr1p0d“ auf dem Forum angeboten haben soll. Auf seine Spur waren die Spezialisten des LKA durch langwierige und umfangreiche Ermittlungen und Internetrecherchen gestoßen.

Auf Grund eines Rechtshilfeersuchens der Staatsanwaltschaft Offenburg wurde die Wohnung des 22-Jährigen am 25. Februar 2009 von Schweizer Kriminalbeamten durchsucht.



Baden-Württemberg

LANDESKRIMINALAMT

Hierbei wurden zwei PC Anlagen mit Speicherkapazitäten von mehreren Terabyte sowie umfangreiche Aufzeichnungen aufgefunden und sichergestellt. Auch die Benutzerdatenbank des Hackerforums mit allen Erreichbarkeiten und IP Adressen von Usern wurden gesichert und werden nun ausgewertet.

Ausgangspunkt waren Ermittlungen gegen Tatverdächtige wegen der Ausspähung von Daten mit der Schadsoftware PW Stealer. Hierbei waren die Internetspezialisten des LKA auf einen Server bei einem deutschen Internet Service Provider gestoßen. Darauf waren illegal ausgespähte Daten, die von infizierten PCs dorthin gesandt wurden und in einer so genannten „Dropzone“ zwischengelagert waren. Die Internetfahnder des LKA werteten die Zugriffe auf diesen Server aus und konnten so zwei mutmaßliche Haupttäter, einen 25-Jährigen aus dem Ortenaukreis und einen 28-Jährigen aus Niedersachsen identifizieren. Sie stehen im Verdacht, seit September 2008 über 80.000 PC weltweit mit der Schadsoftware „Codesoft PW Stealer“ infiziert zu haben.

Die Verbreitung des Computertrojaners erfolgte vor allem über Tauschbörsen (so genannte „Peer to Peer“-Netze). Vor dem Trojaner war praktisch nichts sicher: Von jedem infizierten PC wurden sämtliche sensiblen Daten wie Benutzernamen, Kennwörter, E-Mail-Accounts, auf gängigen Browsern auch gespeicherte Zugangsdaten zu Webseiten sowie alle im Betriebssystem gespeicherten Benutzerdaten ausgelesen. Auch Zugangsdaten zu Online-Banking-Konten, Accounts zu Auktionsplattformen, Konten zu Online Zahlungssystemen oder Zugangsdaten zu Netzwerken und Servern waren ebenfalls betroffen.

Diese illegal beschafften Informationen sollen dann anschließend in einschlägigen Internetforen gewinnbringend verkauft worden sein.

Neben privaten Rechnern wurden auch Zugangsdaten zu ausländischen Behörden und internationalen Firmen ausgespäht.

Die weiteren Ermittlungen zielen nun auf eine bisher noch nicht bestimmbare Anzahl von Tatverdächtigen, die mit den ausgespähten Daten betrügerische Warenkäufe im Internet begangen haben sollen.



Baden-Württemberg

LANDESKRIMINALAMT

Durch das schnelle Eingreifen der beteiligten Ermittlungsbehörden konnte jedoch größerer Schaden verhindert werden, so dass nur ein geringer Anteil der ausgespähten Daten in unbefugte Hände gelangte. Der tatsächliche Schadensumfang kann bisher noch nicht abgeschätzt werden.

Damit Sie mit Ihrem PC möglichst sicher online gehen, rät das Landeskriminalamt:

- Verwenden Sie sichere **Passwörter** und speichern Sie diese nicht auf Ihrem PC. Ändern sie diese regelmäßig
- Nutzen Sie **Firewall** und **Virens Scanner**. Halten Sie den Virens Scanner durch regelmäßige Updates auf dem aktuellen Stand
- Aktualisieren Sie regelmäßig ihr Betriebssystem und die verwendete Software
- dies gilt insbesondere auch für **E-Mail-Programme** und **Browser**, die Sie für das Surfen im Internet verwenden
- Seien Sie vorsichtig beim Öffnen von **E-Mails** und Dateianhängen. Fragen Sie im Zweifelsfall beim Absender nach, um was für eine Anlage es sich handelt
- Sichern Sie Ihre **drahtlose (Funk-) Netzwerkverbindung (WLAN)**
- Überlegen Sie sich genau, wo Sie **persönlichen Daten** eingeben. Informieren Sie sich über die Seriosität von Anbietern
- Überprüfen Sie regelmäßig Ihre Bankkonten, insbesondere wenn Sie **Schadsoftware** auf Ihrem Rechner festgestellt haben. Sperren Sie ggf. sofort Ihre Konten bzw. Karten



Einen Sicherheitskompass und weitere Tipps finden Sie im Internet auf www.polizei-beratung.de oder www.bsi.de