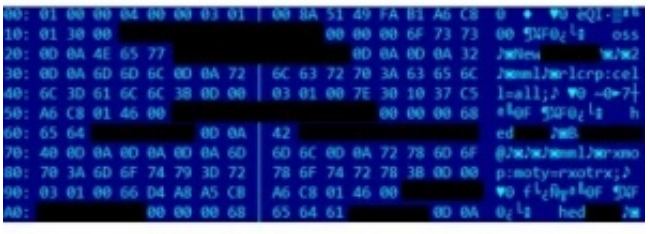
Kaspersky Lab: Cyberwaffe Regin griff Mobilfunk-Basisstationen an

Regin kann Admin-Passwörter für Mobilfunk-Netzwerke auslesen und so Basisstationen angreifen. Zudem kann es wohl Geheimdienstschnittstellen nutzen. Die Cyberwaffe kam auch in Deutschland zum Einsatz.



Regin GSM Activity Log (Bild: Kaspersky)

Ein Hauptmodul von Regin kann GSM-Basisstationen überwachen und Daten über GSM-Zellen und die Netzwerkinfrastruktur weiterleiten. Es kam nach Angaben von Kaspersky Lab auch in Deutschland zum Einsatz.

Über die Cyberangriffsplattform Regin hatte zuerst das Sicherheitsunternehmen Symantec berichtet. Laut den Untersuchungen von Kaspersky wurden neben bisher bekannten Cyberspionage-Aktivitäten erstmalig GSM-Netzwerke infiltriert und ausgespäht. Netzwerke und Computer in mindestens 14 Ländern wurden infiziert. Der Schwerpunkt der Angriffe richtete sich gegen Telekommunikationsunternehmen, Regierungseinrichtungen, Finanzinstitute, Forschungsorganisationen, multinationale politische Organisationen und Einzelpersonen, die im Bereich Mathematik oder Kryptographie forschen.

Opfer seien neben Deutschland in Afghanistan, Algerien, Belgien, Brasilien, Indien, Indonesien, Iran, dem Inselstaat Kiribati, Malaysia, Pakistan, Fidschi, Russland und Syrien identifiziert worden.

Komplexe Plattform aus zahlreichen Modulen

Die Regin-Plattform besteht aus verschiedenen Tools, mit denen die Angreifer Zugriff auf das gesamte kompromittierte Netzwerk einer Organisation erhalten können. Eine komplexe Kommunikation zwischen den infizierten Netzwerken und den Command-and-Control-Servern (C&C) ermöglichte verdeckte Fernsteuerung und Datenübertragung.

Im April 2008 seien Administrations-Zugangsdaten gestohlen worden, mit denen GSM-Netzwerke im Nahen Osten manipulierbar wurden.

"*Die Fähigkeit, in GSM-Netze einzudringen und sie zu überwachen, ist vermutlich der ungewöhnlichste und interessanteste Aspekt dieser Operation*", erklärte Costin Raiu, Director Global Research und Analysis Team bei Kaspersky Lab. Diese arbeiten aber auf Basis von veralteten Kommunikationsprotokollen. "*Für Strafverfolgungsbehörden sind Mechanismen in GSM-Netze eingebaut, um verdächtige Personen zu überwachen und zu verfolgen*", dies könne genutzt werden, um Angriffe verschiedenster Art auf Mobilfunkkunden ausführen, sagte Raiu.

Die Analyse ergab, dass es sich bei Regin nicht nur um ein einzelnes Schadprogramm, sondern um eine komplexe Plattform handelt, die aus zahlreichen Modulen besteht. "*Kaspersky Lab ist im Frühjahr 2012 auf Regin aufmerksam geworden*", erklärte das Unternehmen. Die Frage ist, warum die Öffentlichkeit erst jetzt informiert wurde. ■

1
54
59
86
Kommentarübersicht

Re: SecureSafe und Co.

axolot 25. Nov 2014

GSM an sich ist nicht geknackt. Es sind einige der genutzten Algorithmen in einigen...

Re: Unsere Regierung wendet die effektivste...

Wallbreaker 25. Nov 2014

Effektiv? Nein, sowas schürt nur ein gewaltiges Misstrauen, was irreparable Schäden...

Re: Genau DESHALB sind Steuergelder für 0-Days...

Malocchio 24. Nov 2014

Nee, das ist unerheblich. Auch in dem Fall bleibt es falsch. Wenn nicht sogar doppelt falsch.

Kommentieren

Regin verwendet, hat das BSI dem... mehr

SPIONAGESOFTWARE: KASPERSKY ENTTARNT REGIN ALS NSA-...
Code des Trojaners Regin findet sich auch in den Dokumenten von Edward Snowden. Damit dürfte der Urheber der Cyberwaffe eindeutig feststehen. mehr

GCHQ-DROHUNG GEGEN AUSSCHUSS: SCHWEIGEN IM AUFTRAG...
Eine Drohung des britischen GCHQ belastet die Arbeit des NSA-Ausschusses. Die Aufklärung der Geheimdienstaktivitäten soll nach dem Willen... mehr

Artikel
Datum: 24.11.2014, 19:05
Autor: Achim Sawall
Startseite **Themen:** Malware, Cyberwar, Hacker, Passwort, Regin, Trojaner, Virus, Symantec, Applikationen, Internet
Teilen:
1
54
59
26

Tools: Drucken

Weitere Angebote

Folgen Sie uns

Videos


Apple Health-App - Trailer

Verwandte Artikel
The Intercept
NSA und GCHQ sollen Cyberwaffe Regin eingesetzt haben
Stuxnet lässt grüßen
Trojaner hat Unternehmen in großem Stil ausgespäht
Dailymotion
Infiltration für Angriffe auf Flash-, Java- und IE-Nutzer
Trojaner
Duqu-Code erweist sich als "Oldschool"
Ransomware
Europol lässt Entwickler von BKA-Trojaner auffliegen

Meistgelesen
New Nintendo 3DS & XL im Test
Dagegen sehen die Alten blass aus
Intelligente Stromzähler
Regierung erspart Normalverbrauchern teure Geräte
Spielwarenmesse 2015
Sicherheitsnetze, First-Person-Loks und App-Steine
Workshop
Amazons Fire TV wird zur Multimedia-Zentrale
Kundenkonto
Urteil verbietet Mail zu Anmeldebestätigung für Onlineshop

Meistkommentiert
Arbeitsstättenverordnung: Droht der Telearbeit das Aus?
Kommentare: 266 | letzter Beitrag 14:22 Uhr
Intelligente Stromzähler: Regierung erspart Normalverbrauchern teure Geräte
Kommentare: 260 | letzter Beitrag 16:42 Uhr
Kundenkonto: Urteil verbietet Mail zu Anmeldebestätigung für Onlineshop
Kommentare: 182 | letzter Beitrag 16:18 Uhr
Today Calendar: Mit Piratencontent gegen Softwarepiraterie
Kommentare: 152 | letzter Beitrag 12:03 Uhr
Bundesnetzagentur: Telekom zeigt kein Interesse an ländlichem Ausbau
Kommentare: 115 | letzter Beitrag 16:37 Uhr
Mehr

Haben wir etwas übersehen?
E-Mail an news@golem.de

Vorabtest
DirectX-12 macht, was es soll
Bereits ein gutes halbes Jahr vor der Veröffentlichung von Windows 10 und DirectX-12 liefert die Schnittstelle die erwartet hohe Leistung in CPU-limitierten Spielen. Noch hat AMDs Mantle-API aber Vorteile.
IMHO Juhu, DirectX 12 gibt's auch für Windows-7-Besitzer
Benchmark-Beta DirectX 12 und Mantle gleich schnell in 3DMark
Grafikschnittstelle AMD zieht Aussage zu DirectX 12 zurück

Facebook

Seiten melden
Facebook hält sich nicht an seine Richtlinien
Hassbotschaften, Sex, Gewalt: Wenn Facebook-Nutzer Seiten melden, werden sie eingehend geprüft. Entscheidend bei der Sperrung sind aber offenbar weniger die Richtlinien des Netzwerks als seine Moral.
Place Tips Facebook wird zum Stadtführer
Facebook-AGB Akzeptieren oder austreten
Quartalsbericht Facebook gibt 2,7 Milliarden US-Dollar aus

IMHO

IMHO
Motorola hofft auf das verflixte siebte Jahr
Alle sieben Jahre verschwindet der Marktführer bei Mobiltelefonen, glaubt Motorola-Mobility-Präsident Osterloh - und dann kommt die Chance für Motorola. Nach Nokia und Blackberry müsste demnach Samsung bald abtreten.
IMHO Zertifizierungen sind der falsche Weg

IMHO Sichert Firmware endlich nachprüfbar ab!
IMHO Video-Netzwerke sind die Plattenfirmen des 21. Jahrhunderts

---

Forumsbeiträge »
eDP 1.4a Displayport-Standard für 8K-Bildschirme ist fertig
schon fast zu fein
FaLLoC | 16:59
Intelligente Stromzähler Regierung erspart Normalverbrauchern teure Geräte
Re: 6000kWh bei modernen Gebäuden normal
Peter Brülls | 16:58
eDP 1.4a Displayport-Standard für 8K-Bildschirme ist fertig
Re: Hört der Wahn auch irgend wann mal wieder auf?
FaLLoC | 16:57
Spielwarenmesse 2015 Sicherheitsnetze, First-Person-Loks und App-Steine
Re: Schade das mit den Lego Raumschiffen
Little_Green_Bot | 16:57
Schließung Sharehoster Rapidshare wird alle Nutzerdaten löschen
Re: 1-Click Hoster leben meist nur für/von...
plutoniumsulfat | 16:56

Ticker »
NSA-Überwachung Obama bittet Deutsche um Vertrauensvorschuss
16:23
TLS-Zertifikate Schweizer OCSP-Server ist offline
16:10
Astronomie Dunkle Begleitgalaxie der Milchstraße entdeckt
15:55
Pentax K-S2 Spiegelreflexkamera mit Schwenkdisplay trotzt Regenschauern
15:42
Privater Filehoster Owncloud Server 8 vereinfacht Datentausch
15:35
Xperia E4 Sony bringt neues Smartphone mit langer Akkulaufzeit
15:21
The Witness Ex-Indie-Millionär nimmt Kredit für nächstes Projekt auf
15:10
Schließung Sharehoster Rapidshare wird alle Nutzerdaten löschen
14:48
