Subject: Fwd: Abuse Hinweis zu v22016114014940435 - RS 1000 SAS G7 SE 12M
From: Samuel Philipp <samuel.philipp@t-online.de>
Date: 05.04.2017 10:59
To: "Johns, Martin" <martin.johns@sap.com>
CC: team@securitysquad.de

Hallo Martin,

ich hab gerade die angehängte Abuse-Mail von netcup bekommen und wollte dich jetzt mal nach deiner Meinung fragen. Ich hab unsere Blacklists mal geprüft und wir haben die aufgeführte Domain in unseren Blacklists, also ist es sehr wahrscheinlich, dass wir diese tatsächlich aufgerufen haben.

Soll ich dem Support einfach eine Antwort schreiben, in der ich unsere Studienarbeit und das Projekt erkläre, oder was würdest du tun?

Viele Grüße,
Samuel

-------- Weitergeleitete Nachricht --------
Betreff: Abuse Hinweis zu v22016114014940435 - RS 1000 SAS G7 SE 12M
Datum: Wed, 05 Apr 2017 10:42:01 +0200
Von: abuse@netcup.de
An: samuel.philipp@t-online.de

Guten Tag Samuel Philipp,

wir haben heute eine Abusemeldung betreffend Ihres Produkt v22016114014940435 - RS 1000 SAS G7 SE 12M erhalten. Einzelheiten dazu finden Sie am Ende dieser E-Mail.

Bitte prüfen Sie den geschilderten Sachverhalt und teilen Sie uns innerhalb von 14 Tagen mit, was die Ursache der Meldung ist. Sollten Sie uns nicht antworten oder weitere Abusemeldungen eintreffen, werden wir Ihr Produkt deaktivieren, um weiteren Schaden zu vermeiden.

Bitte beachten Sie, dass wir zur Sicherheit jeder Abusemeldung nachgehen müssen. Sollte der Grund für die Meldung nicht nachvollziehbar oder Sie nicht der Verursacher sein, benötigen wir dennoch eine Rückmeldung von Ihnen.

Abusemeldung:

[English version below]

Sehr geehrte Damen und Herren,

mit dieser E-Mail informieren wir Sie über Schadprogramm-Infektionen in Ihrem Netzbereich.

Strafverfolgungsbehörden haben international koordinierte Maßnahmen zur Deaktivierung der Botnetz-Infrastruktur 'Avalanche' durchgeführt. Die Infrastruktur wurde von Cyberkriminellen für die Steuerung zahlreicher Botnetze verwendet. Weitere Informationen hierzu finden Sie unter:
<https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/

Botnetz_Avalanche_01122016.html>

Im Zuge der durchgeführten Maßnahmen wurden Domainnamen, welche von Schadprogrammen in Bezug auf diese Botnetze zur Kontaktaufnahme mit einem Kontrollserver der Täter verwendet werden, auf so genannte 'Sinkholes' umgeleitet. Weitere Informationen zum Sinkhole-Verfahren finden Sie unter:
<https://reports.cert-bund.de/schadprogramme>

Ein Zugriff auf diese Sinkholes ist ein gutes Indiz, dass sich unter der Quell-IP-Adresse mit hoher Wahrscheinlichkeit ein System befindet, welches mit einem entsprechenden Schadprogramm infiziert ist.
CERT-Bund erhält Protokolldaten dieser Sinkholes, um die zuständigen Netzbetreiber entsprechend informieren zu können.

Nachfolgend senden wir Ihnen eine Liste protokollierter Zugriffe auf die Sinkholes aus Ihrem Netzbereich. Neben IP-Adresse, Zeitstempel und Bezeichnung der Schadprogramm-Familie sind jeweils (soweit uns diese Daten vorliegen) Quell-Port, Ziel-IP-Adresse, Ziel-Port und Ziel-Hostname zu den einzelnen Verbindungen angegeben.

Eine Angabe der Schadprogramm-Familie "generic" bedeutet:
a) Das betroffene System hat sich zu einem Domainnamen verbunden, welcher zur Avalanche-Botnetzinfrastruktur gehört, aber noch nicht eindeutig einer Schadprogramm-Familie zugeordnet werden konnte.
oder
b) Der HTTP-Request des betroffenen Systems enthielt keine Angabe eines Domainnamens. Daher kann auf der Sinkhole nicht ermittelt werden, welchen Domainnamen das System vorher aufgelöst hat, um sich zu der entsprechenden IP-Adresse zu verbinden.

Die meisten der hier gemeldeten Schadprogramme verfügen über Funktionen zum Identitätsdiebstahl (Ausspähen von Benutzernamen und Passwörtern) und/oder zur Manipulation der Kommunikation beim Online-Banking.
Informationen zu den einzelnen Schadprogrammen sowie weitere Hilfe finden Betroffene unter:
<https://www.bsi-fuer-buerger.de/avalanche>

Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen zur Bereinigung der Systeme einzuleiten bzw. Ihre Kunden zu informieren.

Diese E-Mail ist mittels PGP digital signiert.
Informationen zu dem verwendeten Schlüssel finden Sie unter:
<https://reports.cert-bund.de>

Bitte beachten Sie:
Dies ist eine automatisch generierte Nachricht. Antworten an die Absenderadresse <reports@reports.cert-bund.de> werden NICHT gelesen und automatisch verworfen. Bei Rückfragen wenden Sie sich bitte unter Beibehaltung der Ticketnummer [CB-Report#...] in der Betreffzeile an <certbund@bsi.bund.de>.

==========

Dear Sir or Madam,

this is a notification on systems on your network most likely infected with malware.

With an internationally coordinated operation, law enforcement agencies took down the 'Avalanche' botnet infrastructure.
The infrastructure was used by cybercriminals for controlling various botnets. Additional information is available at:

<https://www.europol.europa.eu/newsroom>

In the course of this operation, domain names used by malware
related to those botnets for contacting command-and-control
servers operated by the criminals have been redirected to
so called 'sinkholes'. Additional information on this technique
is available at:
<https://reports.cert-bund.de/en/malware>

Any connection to a sinkhole is usually a good indicator for the
host sending the request being infected with an associated malware.
CERT-Bund receives log data from the sinkholes for notification
of the responsible network operators.

Please find below a list of logged requests to the sinkholes from
your networks. Each record includes the IP address, a timestamp
and the name of the corresponding malware family. If available,
the record also includes the source port, target IP, target port
and target hostname for each connection.

A value of 'generic' for the malware family means:
a) The affected system connected to a domain name related to the
   Avalanche botnet infrastructure which could not be mapped to
   a particular malware family yet.
or
b) The HTTP request sent by the affected system did not include
   a domain name. Thus, on the sinkhole it could not be decided
   which domain name the affected system resolved to connect to
   the respective IP address.

Most of the malware families reported here include functions for
identity theft (harvesting of usernames and passwords) and/or
online-banking fraud. Further information on the different
malware families as well as additional help is available at:
<https://www.bsi-fuer-buerger.de/EN/avalanche>

We would like to ask you to check the issues reported and to take
appropriate action to get the infected hosts cleaned up or notify
your customers accordingly.

This message is digitally signed using PGP. Information on the
signature key is available at:
<https://reports.cert-bund.de/en/>

Please note:
This is an automatically generated message. Replies to the
sender address <reports@reports.cert-bund.de> will NOT be read
but silently be discarded. In case of questions, please contact
<certbund@bsi.bund.de> and keep the ticket number [CB-Report#...]
of this message in the subject line.

==========

Betroffene Systeme in Ihrem Netzbereich:
Affected systems on your network:

Format: ASN,IP,Last seen (UTC),Malware,Source Port,Destination
IP,Destination
Port,Destination Hostname

"197540","188.68.39.59","2017-04-04
23:42:06","ranbyus","55351","216.218.185.162","80","vrfkllxhaimrhrqpo.tw"

Mit freundlichen Grüßen / Kind regards
Team CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat CK22 - CERT-Bund
Godesberger Allee 185-189
D-53175 Bonn

Mit freundlichen Grüßen / best regards

Ihr netcup Team

---

netcup GmbH
Daimlerstr. 25
D-76185 Karlsruhe

Telefon: +49 721 / 7540755 - 0
Telefax: +49 721 / 7540755 - 9

Kunden- und Interessenten-Hotline: 08000 netcup
(Kostenlos aus dem Festnetz der Deutschen Telekom)

Web: www.netcup.de
E-Mail: mail@netcup.de

Handelsregister: HRB 705547, Amtsgericht Mannheim

Geschäftsführer (Executive directors):
- Dipl.-Ing. (BA) Felix Preuß
- Dipl.-Ing. (BA) Oliver Werner

USt.-IdNr. (VAT Reg. No.): DE262851304
